universität
wien

DISSERTATION

Titel der Dissertation

„A PRIVACY CONSERVING APPROACH FOR THE DEVELOPMENT OF SIP SECURITY SERVICES TO PREVENT CERTAIN TYPES OF MITM AND TOLL FRAUD ATTACKS IN VOIP SYSTEMS”

verfasst von

Dipl.-Ing.(FH) Stefan Hofbauer, MSc

angestrebter akademischer Grad

Doktor der technischen Wissenschaften (Dr. techn.)

Wien, 2014

Studienkennzahl lt. Studienblatt:	A 786 881
Dissertationsgebiet lt. Studienblatt:	Dr.-Studium der technischen Wissenschaften Informatik
Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Abstract

In the last years the need for VoIP security has risen. This work intends to give some ideas on how to protect this quickly evolving technology. A holistic security approach, including technical as well as organizational means is used to overcome the threats. Many companies have already switched to VoIP or are considering doing so. This new technology, however, must be secured. It is using the SIP (Session Initiation Protocol) protocol, which has been developed as the main signaling protocol for VoIP and the RTP (Real-time Transport Protocol) protocol, whose function is the transmission of audio and video data. Nevertheless, SIP is insecure and many attackers are trying to obtain information from the transmission. The described framework, called CDRAS (Call Detail Records Analysis System) is an analytical system to enable the monitoring of calls and to enable appropriate action to be taken in a VoIP environment. The model is based on white-, grey- and black-listing of conversations, performed through an analysis of call detail records (CDRs) passing through a telephone system. The problem specification serves as a basis to compare state of the art technology with this model. Attacks on Voice-over-IP calls happen frequently. A specific type of these attacks is toll fraud attacks. The prevention of these attacks depends on understanding the attack patterns. These can be derived from communication records. However, these records contain privacy relevant information of the call participants. This thesis proposes a method for changing communication records in such a way that the forensic analysis for VoIP attacks is possible and the privacy of the call participants is preserved. Privacy requirements for communication records are derived from laws, regulations and concerns of call participants. Selected patterns of communication records are based on real world examples, which are presented to demonstrate the viability of the approach. Further a framework for privacy attack identification and privacy data minimization for a structured analysis of communication records is introduced. Moreover, an analysis pattern for toll fraud attacks is introduced, which decides which data communication relations in the communication records have to survive the data minimization.

Zusammenfassung

In den letzten Jahren ist das Bedürfnis nach VoIP Sicherheit gestiegen. Diese Arbeit möchte ein paar Hinweise geben, wie es möglich ist diese neue, aufkommende Technologie zu schützen. Ein holistischer Sicherheitsansatz, der nicht nur Technik beinhaltet, wird verwendet um gegen die Bedrohungen heranzutreten. Viele Unternehmen haben bereits auf VoIP umgestellt oder überlegen es zu tun. Diese neue Technologie muss aber auch geschützt werden. Sie verwendet das SIP (Session Initiation Protocol) Protokoll, welches als Signalisierungsprotokoll für VoIP entwickelt wurde und das RTP (Real-time Transport Protocol) Protokoll, dessen Funktion die Übertragung der Audio und Video Daten sind. Nichtsdestotrotz ist SIP unsicher und viele Angreifer versuchen Informationen während der Übertragung zu erspähen. Das vorgestellte Framework, CDRAS (Call Detail Records Analysis System) ist ein analytisches System, das es ermöglicht Anrufe zu überwachen und gezielte Maßnahmen in einer VoIP Umgebung zu treffen. Das Modell basiert auf einem White-, Grey- und Blacklist Ansatz von Konversationen mittels der Analyse von Call Detail Records (CDRs) in Telefonanlagen. Die Spezifizierung des Problems dient als Basis um aktuelle Forschungsergebnisse mit diesem Modell zu vergleichen. Die Attacken gegen das Voice-over-IP Protokoll erfolgen häufig. Eine besondere Form dieser Attacken sind Toll fraud Attacken. Um diese Attacken verhindern zu können, müssen die Muster der Attacke verstanden werden. Diese können von den Communication Records abgeleitet werden. Diese Records beinhalten aber Datenschutz relevante Informationen der Teilnehmer. Es wird eine Methode vorgeschlagen, bei der die Communication Records so verarbeitet werden, dass die forensische Analyse der VoIP Attacken möglich ist und die Privatsphäre der Teilnehmer gewahrt bleibt. Die Anforderungen an den Datenschutz der Communication Records kommen von Gesetzen, Regulierungen und Bedenken der Teilnehmer. Es werden auch Muster von Communciation Records präsentiert, welche auf realen Beispielen basieren. Es wird weiterhin ein Framework gezeigt zur Identifizierung von Attacken gegen den Datenschutz und Minimierung der Datenschutz relevanten Informationen für eine strukturierte Analyse der Communication Records. Darüber hinaus wird ein Analysemuster für Toll fraud Attacken eingeführt, das aufzeigt welche Datenkommunikation Beziehungen in den Communication Records durch die Datenreduktion bestehen bleiben müssen.

Acknowledgement

I would like to thank my academic supervisor, Prof. DDr. Gerald Quirchmayr, my second supervisor, Priv.-Doz. Dr. Edgar Weippl, Kristian Beckers, co-author of my scientific papers, Johann Ehm, chief executive officer of Danube IT and Amadeus Data Processing, who supported me within my research work. Special thanks go to Duncan Jones from Amadeus Data Processing for proof reading. Most importantly, I would like to thank my wife Katerina, my parents, brother and relatives for their great support and everyone who has supported me during the last few years.

The thesis contains work already published in:

- Hofbauer, S., Quirchmayr, G. and Wills, C. C., An approach to dealing with Man-in-the-Middle attacks in the context of Voice over IP, ARES 2011 Proceedings, pp. 249–255, 2011 (August 2011), 2011.
- Beckers, K., Hofbauer, S., Quirchmayr, G., Sorge, C.: A Lightweight Privacy Preserving Approach for Analyzing Communication Records to Prevent VoIP Attacks using Toll Fraud as an Example, In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012. TRUSTCOM ’12. International Conference on (June 2012), 2012.
- Beckers, K., Hofbauer, S., Quirchmayr, G., Sorge, C.: A process for the automatic generation of white-, grey-, and black-lists from Call Detail Records to prevent VoIP attacks while preserving privacy, In: Availability, Reliability and Security, 2012. ARES ’12. International Conference on (August 2012), 2012.
- Beckers, K., Hofbauer, S., Quirchmayr, G.: Conducting a Privacy Impact Analysis for the Analysis of Communication Records, In: 11th International Conference on Persepectives in Business Informatics Research, 2012. BIR ’12. International Conference on (September 2012), 2012.
- Beckers, K., Côté, I., Hofbauer, S.: A pattern-based Method for Establishing a cloud-specific Information Security Management System, 2013. Springer ’13. Requirements Engineering Journal (January 2013), 2013.
- Beckers, K., Hofbauer, S., Quirchmayr, G., Wills, C.C.: A Method for Re-Using existing ITIL processes for creating an ISO 27001 ISMS process applied to a high availability video conferencing cloud scenario, 2013. CD-ARES 2013 (April 2013), 2013.

The purpose of this early publication of results was to get feedback from the scientific community in the form of review comments and discussions, which actually helped to tremendously improve the quality of the arguments used to substantiate the approach taken in this thesis.

Contents

1 Introduction & Motivation

In this chapter the topic herein is introduced and the author's motivation to write about this topic and work in this field.

The number of worldwide Voice-over-IP (VoIP) customers is well over 38 million and thanks to the popularity of inexpensive, high quality services, such as Skype, that number is projected to increase to nearly 300 million by the end of the year 2013 according to a study carried out in 2010 [BW10]. The future of voice transport has officially arrived. As this promising technology's popularity increases, new demands for improved quality, reduced cost, and seamless operation will only increase.

Telecommunications companies have already adopted VoIP technology or are considering doing so. This technology however still suffers from several security vulnerabilities. Vulnerabilities, exploited by VoIP attacks, are addressed. One way to identify these vulnerabilities is the analysis of existing communication records, e.g., from telecommunications companies. These analyzes have to be carried out in large numbers by forensic experts in order to keep up with the attackers. Telecommunications companies cannot carry this burden alone. Third parties, e.g. security analysts or academic researchers can support these analyzes. The transfer and storage of VoIP communication records, however, is restricted by privacy regulations and laws.

A way to modify communication records is derived, so that privacy is preserved and vulnerabilities can be analyzed. The approach is illustrated on real world CDRs and Cisco CDRs are chosen as an example.

The toll fraud attack is an old problem, which can be seen in various examples. The problem has not yet been solved, let alone generally. Within the SIP context it is especially dangerous, because there are attack points between the network borders from one technology to another and according to systems theory, it is probable that variances may be generated at such sub-system boundaries, so that it is possible to launch a toll fraud attack [BD06]. Often, SIP messages are transmitted over the Internet in plain text with standard ASCII characters. A toll fraud attack can occur when a private branch exchange (PBX) is installed for the first time. The toll fraud attack on an Internet scale has reached a new level of complexity. The ever increasing sophistication of the technology is of course, accompanied by increasing complexity. With physical lines, the medium of conversation and its transmission was clear. Now, the conversation takes place through unknown transmission routes and thus needs a new approach. With the toll fraud attack it is possible for an intruder to abuse a PBX and route calls through it.

With this kind of attack, hackers can be able to fraudulently use the hacked gateway. The approach is illustrated via a real life example, where a voice router (gateway) has been hacked and toll fraud has occurred. It is shown, how this kind of attack could have been avoided and the privacy of the callers preserved.

Communication records contain information about telephone calls, e.g., which person called who and the duration of the call. This information can be used for different kinds of security analyzes, for instance, to prevent toll fraud attacks [BHQS12]. However, communication records also contain personal information. Hence, the privacy of the callers and callees in these records has to be preserved. A structured approach is presented to elicit privacy requirements for communication record analysis. In addition, privacy measures are presented that fulfill these measures.

1.1 Motivation

There are a lot of unsolved problems within the SIP protocol, like Distributed Denial of Service (DDOS) attacks, Man-in-the-middle (MITM) attacks or Spam over Internet Telephony (SPIT). These threat scenarios are motivating to find a solution against them. The successful countermeasure against the MITM attack will be the contribution of this scientific method.

The research questions are derived from the requirements. A methodological approach must be taken to control it whereas the requirements are built from the model of the threats to be defended against.

1.2 Research questions

- How can a MITM attack be dealt with when authenticating against a SIP server?
- How can a design development framework be built for VoIP to manage certain types of attacks?
- How can a methodological approach be developed against the MITM attack, which is not fully prevented with current resources?

- How can a methodologically new approach be developed that covers these attacks?

Literature analysis and state of the art analysis:

Different points of views have been considered when writing this thesis. There is the opinion of a scientific community, as well as privacy considerations and practical contributions by the prototype implementation.

The topic is interesting, because there are unsolved conceptual issues. Therefore, there is still much work to do.

Threats exist on the physical layer, application layer and on the network layer. The MITM attack is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can be used for conducting other sub attacks such as eavesdropping or DDOS.

Different types of MITM attack types in VoIP:

There are two main groups of attacks, called passive attacks (read, trace & evaluate data) and active attacks (manipulate data, creation of new faked information). Information about some common attacks is given:

- Injection attack

A false Diffie-Hellman (DH) Part1 message is injected to weaken the final DH result.

– Voice forgery attack

An attacker is able to imitate the voice of the callee. Sub attacks of voice forgery attacks are the “Bill Clinton” attack (I know Bill, Bill does not know me), the “6 month” attack (false shared secrets, people do not talk with one another for a long time), the “court reporter” attack (the caller and the recipient do not know each other) and the hybrid “Clinton- Court reporter” attack (an attacker can forge Alice’s voice and Alice does not know Bob’s voice, but Bob knows Alice’s voice).

– REFER attack

The “REFER attack”, similar to a MITM attack, involves an eavesdropper manipulating the referred-by header to cause denial of service (DOS).

REFER attacks can be mitigated by deploying S/MIME to detect possible manipulation of the referred-by header data [ONYS08]. S/MIME is offering a punctual solution but no master plan.

– Piggybacking attack

Additional data is inserted into the voice data. The attacker can become active in a moment or later. If a customer is executing a bank transaction, the attacker can change the recipient bank account without the client becoming aware of the change.

– Manipulation

Registration records can be manipulated. Also the content of a voice conversation can be manipulated. Manipulation can also be used to execute phishing attacks to steal money from bank accounts. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls have come from a trusted organization.

– 3xx response codes attacks

3xx response codes are used for redirection of data. The 3xx response codes class of SIP based attacks relies upon forged responses.

The attack outline is as followings: First, the victim issues a SIP request (e.g. INVITE). Then, the attacker sends a 3xx code response to the initiator. The attacker usurps the identity of either the recipient user agent or one of the SIP components (proxy, registrar server, etc.). After that, the victim's SIP client receives the forged 3xx response and redirects its communication through the attacker's system for the rest of its request. The attack is complete.

– Hijacking attacks

There are some types of hijacking attacks, such as "call hijacking", "registration hijacking" or "media session hijacking" within the RTP stream.

– Biddown attack

A lower encryption level is forced in the INVITE message. Often, a combination of these attacks takes place, which makes it more difficult to secure the transmission.

Existing approaches that cover part of the issue:

A solution can be the usage of Transport Layer Security (TLS) or Internet Protocol Security (IPSec) within SIP. TLS provides mutual authentication through a TLS handshake. IPSec can be secured in an environment, together with firewalling, SSL and SSH to withstand attacks on the application layer. A solution against the MITM attack is the introduction of 802.1X / EAP (Extensible Authentication Protocol) for the authentication process. 802.1X (an IEEE Standard for port based Network Access Control) is widely used with WLAN, where it is offering a secure line to the dial-in node. But there is no end-to-end security, as the traffic, after passing the dial-in node is insecure. The different authentication mechanisms within SIP are either proxy to proxy or proxy to client or client to proxy.

Against network authentication sniffers it is better to use the MD5 or SHA-1 hash algorithm, so the attacker can only read a hash digest instead of the plaintext password. But it is still possible to MITM attack if the attacker does not get the plaintext. He just intercepts the hash and resends it to the proxy with his own IP address. For registering a MITM for conversation it is easier to MITM attack the DH key.

S/MIME is used to encrypt and sign the Source Description Protocol (SDP) portion of SIP packets, while the header is still transmitted in plain text. S/MIME guarantees end-to-end security. As this security mechanism is designed for end-to-end communication, there is no need to adapt the network infrastructure to secure communication. Only the callees get the transmitted information as the traffic is transparent for the network. SIP defines some security mechanisms such as Digest and S/MIME. With HTTP authentication, you can choose between Basic Authentication and Digest Access Authentication.

S/MIME offers the following security services for SIP messages:

There is the authentication of the sender, as well as integrity of information within the SDP portion of the SIP packet. Another security service is confidentiality for data in SDP. This is essential because within the SDP part, keys will be exchanged for media data security.

Though it is possible with S/MIME to MITM attack during the first exchange of keys, using pre-shared keys can help prevent this.

There are several security mechanisms in SIP version 2.0 (RFC 3261):

It is comprised of the encryption and signature of the SDP body and SIP tunneling with encrypted and signed body. There is the chance to only encrypt the body or encrypting the signature and the body [DR07].

There are some protocols for the media key exchange within the Secure Real-time Transport Protocol (SRTP) to establish encrypted telephone calls. One of them is ZRTP, developed by Phil Zimmermann.

ZRTP has two working modes:

- Pre-shared mode (authentication relies only on previously shared secrets)
- DH mode (authentication relies on a DH exchange and on previously shared secrets)

ZRTP is generating SRTP master keys and salt using a Hashing Message Authentication (HMAC) function. The overall key and security negotiation is purely peer-to-peer realized by ZRTP. CFB, an algorithm, is an encrypted transmission of the Short Authentication String (SAS) verified flag. If a fake trusted server is used with SAS, the user will recognize it. ZRTP provides means like strong secrecy (having a pool of possible valid keys) or SAS for the key exchange to detect a MITM attack. It is important to carry out a SAS authentication when contacting somebody for the first time and checking the SAS verified flag, for connection with which the SAS has already been carried out. The theoretical Achilles heel of the ZRTP protocol is the SAS endpoint authentication. SAS, which requires a trusted server, also makes the server resistant against DDOS attacks and can blacklist IP addresses.

ZRTP is designed to provide authentication between parties, secrecy, and end-to-end Perfect Forward Secrecy (PFS) between sessions.

AES is used for payload encryption and the SRTP packet including headers is authenticated using SHA-1. ZRTP is vulnerable to adversaries with strong capabilities.

Some experts advise for modifying the protocol to include a randomized start time for the conversation [RS06]. This method is called pseudonymization.

An example in practices is the Zfone software installation of a SIP phone that has encryption already implemented. Hardware SIP phones are not so vulnerable than software phones. Where software phones are attackable on the guest operating system, hardware phones run on proprietary operating systems with limited network services.

MD5 is commonly used for 802.1X, certificates for authentication, IPSec, TLS and Secure SIP (SIPS) for the signaling security, SRTP for media security and MIKEY-RSA for the media key exchange. Security relevant parameters between the clients are exchanged by parameters and a secret key is generated with the Key Management Protocol (KMP).

Internet Key Exchange (IKE) is used in IP networks and Multimedia Internet Keyring (MIKEY) for VoIP connections. The secret key, which must be known for both sides but must not be sent across the network, is supplied by the DH process. For encrypting the user data, session keys are applied, which are derived from the DH-process created master key. The authentication check is done with HMAC.

Testing of hard-phones, Wi-Fi phones and terminal adapters show that many still have weak security. The typically identified problems can be grouped as follows:

- open ports, default passwords, weak provisioning, weak cryptography
- defective software
- low tolerance for fuzzing and flooding

Currently, secure SIP services offer signaling links secured by TLS and media data security transport realized by SRTP. As there are many VoIP protocols, like SIP, RTP/RTCP, SRTP, ZRTP and many more, chaos exists [SRT04].

A problem associated to the DH key is its vulnerability to the MITM attack, because of the absence of user authentication in DH key exchange. Therefore the use of ZRTP is advised. Commonly, the key exchange is not secured against MITM attacks.

Profiling the normal traffic behaviors, the goal is to seek a threshold of measured distances that could differentiate among different kinds of traffic anomalies and normal behavior.

1.3 Organization

The thesis is organized as follows. First, background on CDRs, privacy and telecommunications laws are presented. Then a structured method for eliciting privacy requirements for communication records is shown. Later, an analysis for VoIP attack patterns is provided and it is described how privacy is preserved during the analysis. A usage example of the method is added, based upon a toll fraud attack and related work is presented. In the end, a conclusion and directions for future research are given.

1.4 Goal of the Thesis and expected contributions

Based on the research question, this thesis aims to keep pace with existing phone attack problems and close these gaps. The approach can not only be used in the domain of VoIP, but also be implemented in other domains, such as video. The same problems exist within this domain, namely MITM and toll fraud attacks. This approach can be used for instance to refrain from having an open, not authenticated SIP registration open on the bridge, at the boundaries to the WAN.

It can be seen in examples that often unencrypted data is sent over the LAN, which can be easily tapped. It is therefore always a good idea to use secure protocols, such as LDAPS instead of LDAP or HTTPS instead of HTTP. Also the use of certificates on devices and proper DNS resolution from the LAN and from the WAN is recommended. Further, ruling out old technology, such as ISDN gateways is recommended for security and cost reasons. It is recommended to constantly upgrade to new firmware versions, because of bug fixing and security reasons. Often, there are vulnerabilities with older firmware, which make it easy for attackers to get access to a company network. Devices should also not have a public IP address, but an internal address and reside behind a firewall. If a connection to a central device, such as the Call manger is not possible, the use of virtual private network (VPN) technology is favored.

It is expected that with the use of this approach the number of attacks can be reduced to a minimum and further forensic evidence is in place, too. This makes it easier for attacked companies to proof their liability towards law and insurance companies. The logging of network devices with use of Syslog and sending of status messages across the network to a central correlation station for analysis and alerting by the use of SNMP helps too. It is the obligation and especially the CEO of a company to care for security and have up to date mechanisms in place. This awareness must be raised for all employees and involved parties. Of course, external help and consulting can be ordered to comply with laws and regulations.

This approach can be easily extended and enlarged with the protection against other novel attacks, because the underlying communication data records for the analysis remain.

Hopefully, this work will also attract other researchers and thus will contribute to the open source community. The following chapter gives further background information and introduces related work and state-of-the-art technology.

2 Background & Related Work

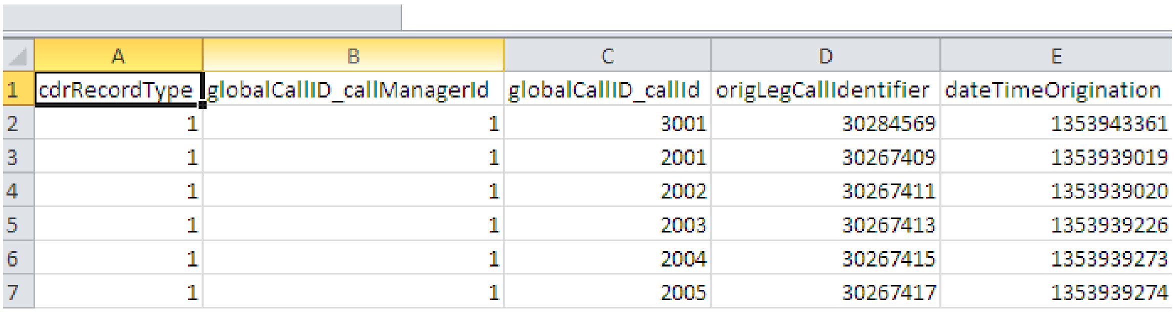
In this section a very short overview of the most relevant existing work, which this thesis is building on, is presented. The literature citations are intended to give the reader an idea of the current situation and to show the major outcomes of existing research used in further chapters of this thesis. For more detailed information, the reader is referred to the references section of the end of this thesis and the literature section of the papers already published by the author.

As of Gartner's Magic Quadrant for Unified Communications 2010 [GAR10], Cisco is again positioned in the leader's quadrant. This is the reason why this thesis is based on Cisco Unified Communication Manager and its CDRs.

Customers have requirements to log CDRs from VoIP systems for accounting or billing purposes. This thesis goes a little bit further and issues the CDRs for further analysis. When troubleshooting issues in a PBX system, it is found very helpful to refer to some sort of historical record of what was going on in the system at the time the reported issue occurred. Many customers are using H.323 as a trunk to their PBX. As H.323 and the SIP protocol can coexist on a phone system, it is also referred to H.323 besides SIP in this thesis. SIP is only text based and looks like HTML. In contrast to the monolithically H.323, SIP is structured modular and therefore far more flexible for extensions. This chapter also gives an overview of existing technologies and concepts that serve as a basis for developing and testing the envisaged approach.

2.1 The Structure of Call Detail Records

"CDRs contain the following information that has a relation to the privacy of call participants. CDRs are stored in tabular format on a PBX. From there they can be copied via Secure Copy (SCP) file transfer.



	A	B	C	D	E
1	cdrRecordType	globalCallID_callManagerId	globalCallID_callId	origLegCallIdentifier	dateTimeOrigination
2	1	1	3001	30284569	1353943361
3	1	1	2001	30267409	1353939019
4	1	1	2002	30267411	1353939020
5	1	1	2003	30267413	1353939226
6	1	1	2004	30267415	1353939273
7	1	1	2005	30267417	1353939274

Figure 2.1: Example Call Detail Records from Cisco Unified Communications Manager

-dateTimeOrigination

This field identifies the date and time when the user goes off hook or the date and time that the H.323 Setup message is received for an incoming call. The time gets stored as Coordinated Universal Time (UTC).

-origIpAddr

This field identifies the IP address of the device that originated the call signaling. For Cisco Unified IP Phones, this field specifies the address of the phone. For public switched telephone network (PSTN) calls, this field specifies the address of the H.323 gateway. For inter cluster calls, this field specifies the address of the remote Cisco Unified Communications Manager.

-callingPartyNumber

This field specifies numeric strings of up to 25 characters. For calls that originate at a Cisco Unified IP Phone, this field shows the extension number of the line that is used. For incoming H.323 calls, this field specifies the value that is received in the Calling Party Number field in the Setup message. This field reflects any translations that are applied to the Calling Party Number before it arrives at the Cisco Unified Communications Manager (such as translations at the gateway). For server calls, where Cisco Unified Communications Manager originates a half call without a calling party, this field may remain empty. CallingPartyNumber could contain a SIP Uniform Resource Identifier (URI).

-callingPartyUnicodeLoginUserID

This field specifies the calling party login user ID. The format of this field specifies UTF 8. Default – Empty string ” ”. If the user ID does not exist, this field stays empty.7

-origMediaTransportAddress IP

This field identifies the IP address of the device that originates the media for the call. For Cisco Unified IP Phones, this field specifies the address of the phone.

For PSTN calls, this field specifies the address of the H.323 gateway. For inter-cluster calls, this field specifies the address of the remote phone.

-origMediaTransportAddress IP

This field identifies the IP port number that is associated with the OrigMediaTransportAddress IP field.

-destIpAddr

This field identifies the IP address of the device that terminates the call signaling. For Cisco Unified IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. For inter cluster calls, this field specifies the address of the remote Cisco Unified Communications Manager.

-originalCalledPartyNumber

This field specifies the number to which the original call was presented, prior to any call forwarding. If translation rules are configured, this number reflects the called number after the translations have been applied. This field represents a numeric string of up to 48 characters that can be either digits or a SIP URL.

-finalCalledPartyNumber

This field specifies the number to which the call finally gets presented, until it is answered or rings out. If no forwarding occurs, this number shows the same number as the originalCalledPartyNumber.

For calls to a conference bridge, this field contains the actual identifier of the conference bridge, which is an alphanumeric string (for example, b0019901001). This field represents a numeric string of up to 48 characters that can be either digits or a SIP URL.

-destMediaTransportAddress IP

This field identifies the IP address of the device that terminates the media for the call. For Cisco Unified IP Phones, this field designates the address of the phone.

For PSTN calls, this field designates the address of the H.323 gateway. For inter cluster calls, this field shows the address of the remote phone.

-destMediaTransportAddress Port

This field identifies the IP port number that is associated with the DestMediaTransportAddress IP field.

-dateTimeConnect

This field identifies the date and time that the call connects. The time gets stored as UTC. If the call is never answered, this value shows zero.

-dateTimeDisconnect

This field identifies the date and time when the call is cleared. This field gets set even if the call never connects. The time gets stored as UTC.

-duration

This field identifies the difference between the Connect Time and Disconnect Time. This field specifies the time that the call remains connected, in seconds. This field remains zero if the call never connects or if it connects for less than 1 second [CDR10].”

CDRs contain information seen in Figure 2.1 that has a relation to the privacy of call participants.

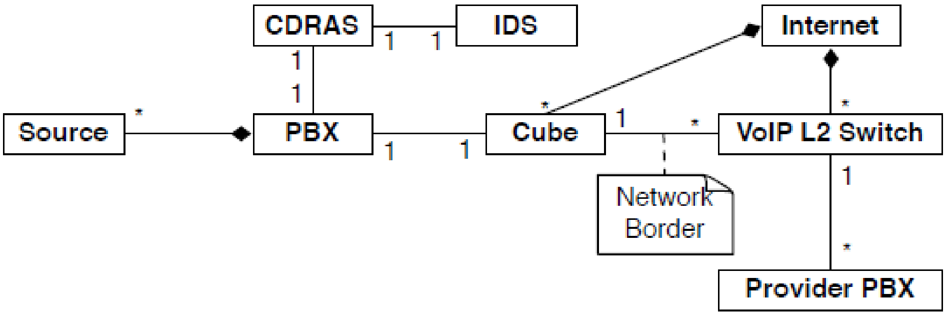


Figure 2.2: UML class diagram::SIP

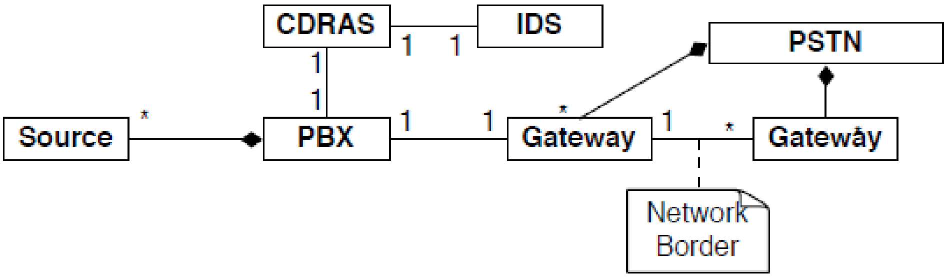


Figure 2.3: UML class diagram::ISDN

2.2 Privacy Issues and Regulations

Pfleeger and Pfleeger [PP07, p. 607] define privacy as “the right to control who knows certain aspects about you, your communication and your activities”. A number of guidelines for privacy are available, the Fair Information Practice Principles – (or short FIPs) [OEC80] are widely accepted, which state that a persons informed consent is required for the data that is collected, collection should be limited for the task it is required for and erased as soon as this is not the case anymore. The collector of the data shall keep the data secure and shall be held accountable for any violation of these principles.

In the European Union the EU Data Protection Directive, Directive 95/46/EC” doesn’t permit processing personal data at all, except when a specific legal basis explicitly allows it or when the individuals concerned consented prior to the data processing [EUD95].”

Germany implements the European Privacy Directive in the Federal Data Protection Act (BDSG). According to the appendix of Section 9 Sentence 1 BDSG all organizations and companies that automatically process, store, and use personal data have to comply with the BDSG.

The US has no central data protection law, but separate privacy laws for e.g. the Gramm-Leach-Bliley Act financial information, the Health Insurance Portability and Accountability Act (HIPAA) for medical information, and the Children's Online Privacy Protection Act (COPPA) for data related to children [HSC08].

Pfitzmann and Hansen [PH11] introduced a terminology for privacy via data minimization. The authors define central terms of privacy using items of interest (IOIs), e.g., subjects, messages and actions. Anonymity means a subject is not identifiable within a set of subjects, the anonymity set. Unlinkability of two or more IOIs means that within a system the attacker cannot sufficiently distinguish whatever these IOIs are related or not. Undetectability of an IOI means that the attacker cannot sufficiently distinguish whether it exists or not.

Unobservability of an IOI means undetectability of the IOI against all subjects uninvolved in it and anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI. A pseudonym is an identifier of a subject other than one of the subject's real names. Using pseudonyms means Pseudonimity.

Identity Management means managing various partial identities (usually denoted by pseudonyms) of an individual, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.

The ISO 15408 [ISO09] - Common Criteria for Information Technology Security Evaluation - (or short CC) standard contains the privacy requirements anonymity, pseudonimity, unlinkability, and unobservability. The definitions of these terms in the CC are similar to the ones from Pfitzmann and Hansen.

Deng et al. [DWSPJ11] generate a threat tree for privacy based upon the threat categories: linkability, identifiablitiy, non-repudiation, detectability, information disclosure, content unawareness, and policy/consent noncompliance. These threats are modeled for the elements of an information flow model, which has data flow, data store, processes and entities as components. Privacy threats are described for each of these components.

Nissenbaum [NIS04] develops a model of informational privacy in terms of contextual privacy. The model considers the context of a given situation, the kind of information, the relation of the information to the context, the role of agents receiving the information, their relationship to information subjects; on what terms the information is shared by the subject and the terms of further distribution. For example a patient sharing information about her physical condition with a physician is appropriate, but not vice versa. Nissenbaum further describes that contextual privacy norms have three different sources. These are laws, culture, and the history of a stakeholder.

Sorge et al. [SNS10] investigate the legal issues involved with call filtering solutions to prevent SPIT.

This thesis describes the legal situation for the US and the German legal system. Deng et al. [DWSPJ11] present a comprehensive framework to model privacy threats in software-based systems. They also provide a systematic methodology to model privacy-specific threats. Hofbauer et al. [HQW11] present an approach to dealing with MITM attacks in the context of VoIP. Legal aspects are also covered in this paper as well as a suggested approach to risk management. Tartarelli et al. [TDN10] describe how information is stored in different types of CDRs and how to check the sanity of telecommunications data stored in these.

Fernandez et al. [FPL07] design several UML models of some aspects of VoIP infrastructure, including architectures and basic use cases. The authors also present security patterns that describe countermeasures to VoIP attacks.

Telecommunications companies have already widely adopted VoIP technology or are at least considering doing so. This technology, however, suffers from several security vulnerabilities [VOI05]. Cryptographic solutions have been proposed to secure VoIP communications, e.g., the ZRTP protocol, but vendors use different implementations in their systems [ZRT10]. In addition, these solutions require a certificate authority and significant knowledge in the configuration of VoIP phones and VoIP servers.

Hence, compatibility issue and significant financial and financial efforts prevent specifically small and medium businesses from adapting cryptography as a solution.

In order to create a solution that requires minimal changes in existing VoIP systems, it is proposed to include the analysis of communication records. These records exist in numerous VoIP systems. This solution analyzes these records and identifies malicious VoIP participants. The approach also integrates with existing Intrusion Detection Systems (IDS). A general model of timings, derived from communication records, is used in order to scan the data for possible attacks. Timing patterns of call participants, e.g., the frequency of call attempts from a specific caller to a callee, are analyzed. Furthermore, patterns are created that include the systems used by call participants. For example, the call attempts made from a VoIP system to an ISDN phone via a VoIP gateway. Call patterns are derived and analyzed. The previously mentioned pattern of a high frequency of call attempts indicates a DOS attack.

It is a lightweight approach that can be used by any VoIP vendor. Moreover, the plan is to use a socio-technical approach to address VoIP security. Hence, the configuration of VoIP hard and software and the participation of a human administrator to supervise decisions of the system are part of this solution.

Communication records contain personal information of the call participants. These are for example the telephone numbers, user names, call durations, etc. The deletion of the personal information and, hence, anonymizing the records is not a viable option, because in this case the information of possible malicious users would be erased in the process. A structured analysis of the laws and regulations in the EU and the US is presented in order to derive privacy requirements. The callers and callees rights are investigated and this solution provides guidance for implementing VoIP security based on communication record analysis compliance.

Several approaches use white-, black-, grey lists to classify VoIP participants. In this approach, whitelists contain valid call participants, blacklists contain malicious participants and grey lists contain hosts that are under observation and human interaction is required to classify these. The observations of IDS regarding incoming and outgoing VoIP calls serve as input for the (semi-) automatic generation of whitelists within CDRAS. Existing approaches use these in isolation. It is proposed to combine all three lists in this solution, running together with a system architecture presented in [CIS10].

In this thesis toll fraud is used as example of an attack vector for this approach. In this context toll fraud is the abuse of a hacked PBX, where outgoing calls, placed over one's voice gateway connected to this PBX are causing high telephone bills.

This is usually achieved by the fraudster through calling overseas destination or expensive satellite phones via a hacked VoIP system.

2.3 Related Work this thesis can build on

Shin et al. [SAS06] present a flexible grey listing approach for SPIT detection. In this approach the system decides, if the call will be connected or blocked. The system uses a Bayesian network to make filter decisions.

This approach can complement this thesis. However, only the results would be used, as suggestions for human operators. In addition, this approach is using white-, grey-, and blacklists for the CDRAS system. Quittek et al. [QNTS07] analyze human communication patterns in VoIP calls and derive Turing tests in order to prevent SPIT. This approach is not based on human communication records, but on the analysis of CDRs and it is not intended to carry out Turing tests. d'Heureuse et al. [DSNE08] present a framework to protect SIP based infrastructures. The framework is protecting against SPIT using only black-, and whitelists. This thesis is also using grey lists and wants to protect against other VoIP attacks. Their heavyweight approach is placed at three different locations in the operator's network, the Session Border Controller (SBC), Application Server (AS) and IP phone. This solution is a lightweight approach, placed only between the voice router and the PBX.

Tartarelli et al. [TDN10] describe how information is stored in different types of CDRs and how to check the sanity of telecommunications data stored in these. The authors also propose methods to aggregate the data to reduce the amount of data. This work can complement our own. Fernandez et al. [FPL07] design several UML models of some aspects of VoIP infrastructure, including architectures and basic use cases. The authors also present security patterns that describe countermeasures to VoIP attacks. The presented security patterns can complement this work. Nevertheless, Fernandez et al. do not propose to build a system.

None of the aforementioned approaches consider privacy requirements. That is why the used approach is based on a privacy impact analysis.

Sorge et al. [SNS10] investigate the legal issues involved with call filtering solutions to prevent SPIT. The authors describe the legal situation for the US and the German legal system. Sorge et al. investigate the problem in general, but not in the scope of a specific system. Hung et al. provide a survey of VoIP threats and solutions [HM06]. Butcher et al. [BLG07] also provide an overview of VoIP security challenges. The authors present VoIP specific attacks and countermeasures. Both works include attacks for toll fraud. Ehlert et al. [EWMS08] present a framework for detecting deviations in SIP networks. The framework can protect SIP infrastructures from several attacks, including DOS attacks. However, the approach has no protection against toll fraud attacks, but it is listed as future work.

Fernandez et al. [FPL07] design several UML models of some aspects of VoIP infrastructure, including architectures and basic use cases. The authors also present security patterns that describe countermeasures to VoIP attacks. These could be used to design secure VoIP systems.

Sorge et al. [SNS10] investigate the legal issues involved with call filtering solutions to prevent SPIT. The authors describe the legal situation for the US and the German legal system.

Hofbauer et al. [HQW11] present an approach to dealing with MITM attacks in the context of VoIP. Legal aspects are also covered in this paper as well as a suggested approach to risk management. Kalajdzic et al. [KP11] present active detection and prevention of sophisticated ARP-poisoning MITM attacks on switched Ethernet LANs. They are achieving this with two methods, one is reverse ARP poisoning with active IP probing and the other one is IP probing with CAM table poisoning. Carnut et al. [CG03] describe a feasibility study on ARP spoofing detection on switched Ethernet networks. They are talking about detection of ARP spoofing on hub networks as well as on switched networks and on switches via SNMP.

First of all, this thesis is developing a software solution and not providing a survey of VoIP threats and solutions, like Hung et al. This approach is different from Butcher et al., as the attack scenario is based on a MITM attack. In contrast to Ehlert et al., there are already means presented to protect against toll fraud. Compared to Fernandez et al., this thesis does not only build UML models, but presents a solid architectural approach. Contrary to Sorge et al. this is not concentrating on SPIT but on the SIP protocol. Unlike Hofbauer et al, this work is more concentrating on the privacy remediation in VoIP networks in offering privacy preserving methods.

As opposed to Patel et al. this work is not based on switched Ethernet LANs, neither a mechanism for ARP spoofing detection is presented. Finally, unlike Carnut et al., this thesis is not working in the field of hub networks, switched networks or switches. All of them are precious contributions so far; however this thesis tries to close some of the existing gaps.

There is still a lot of work missing and as the technology is evolving, there are even new gaps, which need to be closed. It can be seen as a basis for future scientific research in this direction. The next chapter shows how to protect against certain types of attacks and the use of attack patterns for analysis.

3 Problem Specification

This chapter gives some ideas, how to protect against well-known attacks and shows proposals for the solution in place.

So far, the mitigation of vulnerabilities in VoIP has been difficult to ensure the integrity and authenticity of the SIP messages and RTP traffic between the appropriate VoIP servers and the SIP phone. Combinations of various technologies that are compatible with each other are required.

However, hop-by-hop encryption (e.g. SSL or TLS), or authentication is intended to be solved, but still can be vulnerable to the MITM attack, unless both communicating parties can reliably authenticate each other. While Public Key Infrastructure (PKI) is able to provide strong mutual authentication, it is not clear if it is feasible to require every VoIP phone and server to support PKI [WZYJW08]. Because of the high complexity with having millions of subscribers, the solution of a PKI is not scalable. The problem is also associated with the trust chain. Who trusts whom? Have all the nodes in the network implemented a PKI solution? If not, it will not be possible to have a global authentication scheme.

The real-time communication in VoIP makes it even more difficult to secure. Often, calls are redirected, modified or terminated. In the case of a MITM attack, the attacker sits between two endpoints and is trying to intercept and alter the data stream direction between the subscribers. The MITM attack is used for information gathering, manipulating packets and getting further network access by taking over the client’s role against the server and obtaining his privileges. By filtering traffic and patching network components, one can defend against VoIP attacks. Intelligent routing switches are preferred for VoIP installations. The VoIP traffic can be tunneled through a VPN from host to host by a firewall. Three different MITM attack types amongst others are eavesdropping, packet spoofing and replay attacks. Today, the most used MITM method is called ARP poisoning. This type of attack is based on systems, receiving and saving ARP entries in their ARP cache. Nevertheless, an ARP request would already have been sent, or not. Now an attacker can outwit one or both parties, so they think that the attacker’s MAC address is the address of the other party or SIP server. From this point in time, the attacker becomes a mediator between the subscribers and may eavesdrop or modify any communication between them [VR10].

3.1 Protection against the Man-in-the-Middle attack in VoIP systems

Protection can be achieved by using MAC address based authorization on every switch port in the local network. Further by segmenting the LAN into VLAN subnets. The idea here is that the “users” VLAN won’t be able to ARP poison the “VoIP” VLAN. Encryption on different layers guarantees a good protection. SIP uses TLS encryption. Another idea is using applications for ARP poisoning detection (Arpwatch [LBL10] for Linux and Xarp [M10] for Windows).

Intruders eavesdropping on the network might also be able to alter CDRs, modifying call setup information or corrupting billing data. An attacker might spoof SIP responses and redirect the caller to a rouge SIP address that intercepts the call. Not only is the SIP protocol vulnerable for the MITM attack, but also the transport of the voice data with the SRTP protocol.

Adopt the SRTP using AES counter mode to provide security measures:

There is confidentiality for RTP by encrypting the respective payloads and integrity for all RTP packets, together with replay protection. The possibility to refresh the session keys periodically limits the amount of cipher text produced by a fixed key. An extensible framework permits upgrading new cryptographic algorithms and cope with state of the art technology. A secure session key deviation helps with a pseudo-random function at both ends. There is also the usage of salting keys to protect against pre-computation attacks and security for unicast and multicast RTP applications.

3.2 Protection against toll fraud attacks

One effective means to protect against the toll fraud attack is to change the registration of the devices. Strong credentials are favored to be in place and there should also be a policy in place, which denies auto registration of new devices from unauthenticated sources on the PBX. For authentication, client certificates as well as server certificates of the PBX have to be valid. The logging of CDRs should as well be enabled on the PBX and the duration of the logging set to 3 months at least.

For this reason, there must be enough disk space or external storage space to log the CDRs data. It is a good idea to store and keep this data for a longer period, as there might be billing questions with a service provider. It is the duty of every company to look after this. Also the firewall rules should be checked on a regular basis to harden the PBX and make it more difficult for attackers to reach the registrar.

The behavior of an attacker is that they trace registrar servers, which are reachable over the Internet and which have an open authentication. Under such circumstances it is very easy for them to register a softphone and make expensive calls over the hacked gateway. Standardization like ISO27001 and IT Infrastructure Library (ITIL) can help in ensuring an attack free environment. But not only externals can launch attacks. It is seen that the majority of attacks are coming from malicious insiders, who want to take revenge against the company or not needed are bribed by another pressure group. This makes it even more difficult to distinguish between good and bad traffic. It can also be the case that a valid account has been hijacked, because of a poor password policy or lost password and an external is hiding behind an internal account. Regular security audits help in being secure against diverse kinds of attacks.

The risks have to be defined and corrective actions and controls put in place. A company security policy makes it more clearly for personal to understand the need for security in this context. This is not only the case within the domain of VoIP, it is applicable generally.

3.3 Analysis of attack patterns

As there is a lack of a formal way to describe VoIP vulnerabilities, the development of tools that could be utilized for identifying such vulnerabilities or for testing the security level of the offered services are missing. With the knowledge of the attack patterns, certain types of attacks can be avoided. Such a formal way would be a VoIP specific ontology for attacks. A meta-model of the proposed IDS can be seen in Figure 3.1.

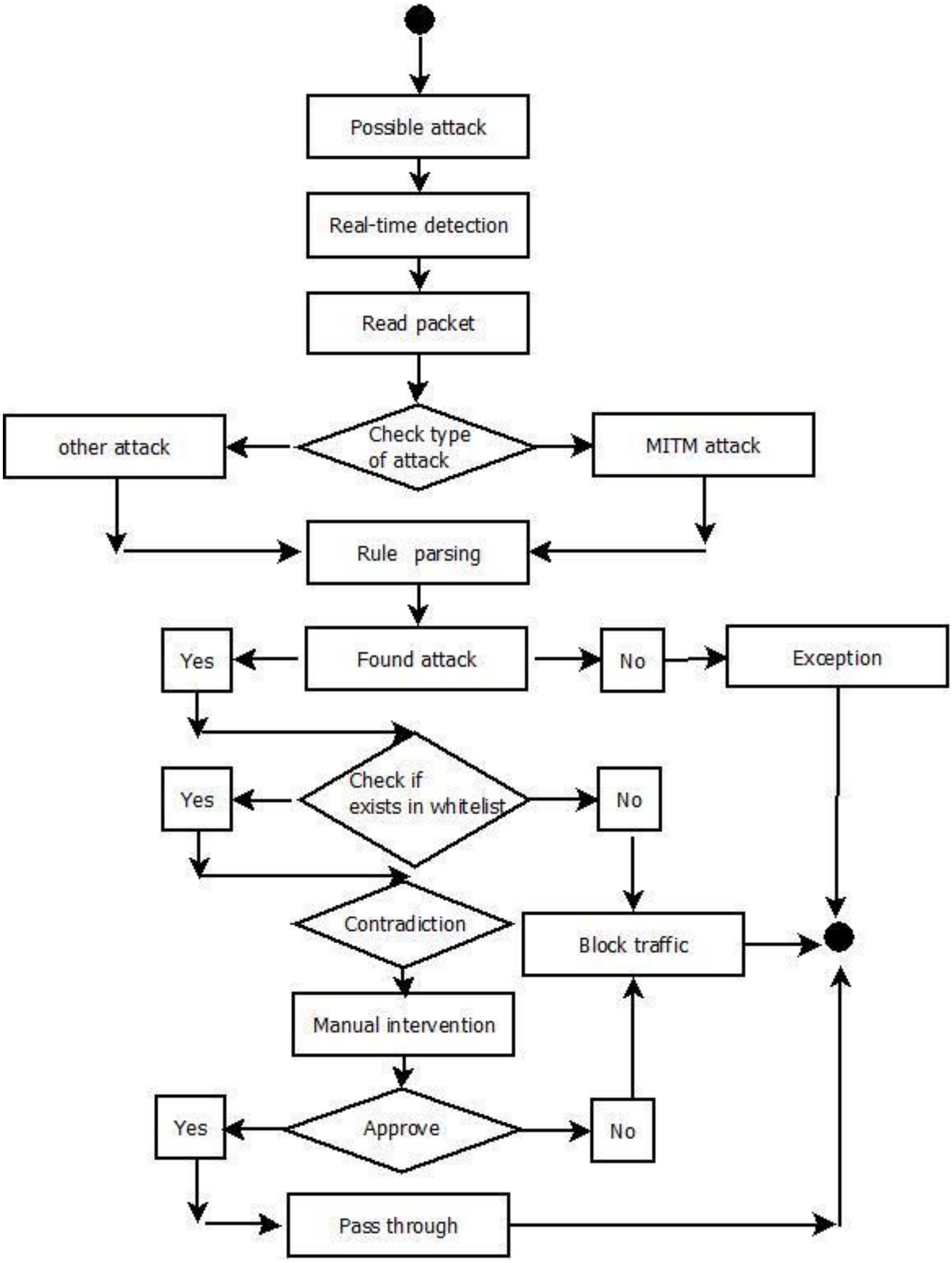

Possible attack
Real-time detection
Read packet
Check type of attack
other attack
MITM attack
Rule parsing
Yes
Found attack
No
Exception
Yes
Check if exists in whitelist
No
Contradiction
Block traffic
Manual intervention
Yes
Approve
No
Pass through

Figure 3.1: Meta-model of the IDS

Semi-Automatic generation of white-, grey-, and black-lists:

Once the CDRs file is retrieved, the analysis system can use this information for pattern (detecting suspicious call), trends (early warnings) and building call relationships (who is connected with whom for calling). CDRAS processes telephone call information (date, time, calling/called numbers or extensions, duration, etc.) stored within the telephone system in conjunction with other software and hardware to perform management reporting, cost allocation, and fraud prevention procedures. CDRs help detect unusual calling patterns that characteristically represent hacked systems. The analysis module analyzes the information stored in the file and gives outputs of information like top clients, killer numbers, statistics of routes, operator's performance, destination analysis, prefix analysis and many more. CDRAS identifies CDRs generated by incoming and outgoing calls of unauthorized network users, creating from the identified CDRs, a disallowed list of digits dialed by the unauthorized users as well as phone numbers which have dialed unauthorized users, filtering this list in a sequential manner to remove from the list any dialed digits or phone numbers which are considered unacceptable as a determining factor for call completion blocking, then providing this disallowed list to a mechanism for blocking call completion based on dialed digits or originating phone number. It is believed that by analyzing large amounts of data, from multiple sources around the world, it will be possible to ascertain the fingerprint of a telecom bound attack - being able to alert the respective users of the service and maybe in a future version, also provide a means to block the attack as it advances across the world. The source file that is being analyzed is in text format and taken from the PBX to which the customer's phone is registered [US08].

This file is imported through a text import wizard within Microsoft Excel. The comma is used as delimiter between the records. The converted file has 94 columns, but only a few, shown in Table 6.2 and Table 6.3 are important for the analysis of the CDRs.

The ”dateTimeOrigination” column within the file has to be casted to UTC using the following process:

- In cell A1 type the number that is found in the last record for dateTimeOrigination
- In cell A2, paste the formula =A1/86400+DATE(1970;1;1)
- Right-click on cell A2 and select format cells
- Under the Number tab select Time where the format is 3/14/98 130 PM

Use one column for the date and another column with the same procedure applied for the time. The result will be a human readable time format using UTC time. The new inserted columns are called ”dateOrigination” and ”timeOrigination”.

The columns are imported to the Microsoft SQL database of CDRAS into the table ”unfilteredprimary” and ”unfilteredsecondary”. The tables ”modifiedprimary” and ”modifiedsecondary” contain the columns ”dateOrigination” and ”timeOrigination. Now, several attack patterns can be applied to the table ”unfilteredprimary” and ”unfilteredsecondary” to filter for possible attacks. A threshold value can easily be used for the data herein. If the threshold value is not hit, the records are moved to the table ”whitelistprimary” and ”whitelistsecondary”. If the threshold value is met the records are moved to the tables ”greylistprimary” and ”greylistsecondary”. And if the threshold value is surpassed, the records are moved to the table ”blacklistprimary” and ”blacklissecondary”.

The whitelist is the summary of all records within the tables ”whitelisprimary” and ”whitelistsecondary” (SELECT * FROM whitelistprimary, whitelistsecondary), whereas the blacklist contains all records within the tables ”blacklistprimary” and ”blacklistsecondary” (SELECT * FROM blacklistprimary, blacklistsecondary) and the greylist is built of all records that are member of the tables ”greylistprimary” and ”greylistsecondary” (SELECT * FROM greylistprimary, greylistsecondary). The corresponding database model can be seen in Figure 6.1. The records with primary personal data are pseudonymized and for all tables, access control mechanisms built on user roles are applied.

On basis of the current status, a gap analysis is done in the next chapter. Identifying the gaps is important when conducting a thesis about a known, but not yet solved problem.

4 GAP Analysis

In this chapter an analysis of the different existing gaps is done. These gaps are the main reason for building the approach described in this thesis.

4.1 Methodological Gap that leads to practically relevant problems / issues

The methodological gap is further distinguished into the practical gap and the scientific gap. The gaps always lead to practically relevant issues.

4.1.1 Practical Relevance

“The lack of a formal way to describe VoIP vulnerabilities hinders the development of tools that could be utilized for identifying such vulnerabilities or for testing the security level of the offered services [GL07].”

Quality of service (QOS) for real-time communication is a gap in many enterprises. Providers must also care for roaming between different networks and technologies by further QOS techniques (First In First Out, Priority Queuing, Custom Queuing, Class Based Queuing, Fair Queuing, Weighted Fair Queuing, Class-based weighted fair queuing, Round Robin).

A problem associated to the DH key is its vulnerability to the MITM attack, because of the absence of user authentication in the DH key exchange. Therefore the use of ZRTP is advised. Common said the key exchange is not secured against MITM attacks. Very easily the MITM attack can occur during the time, the first key exchange takes place.

4.1.2 Methodological Gap

Current scientific research has shown that new approaches and solutions are needed to address the open security questions. There are a number of open issues and unsolved problems. A combination of different technical and organizational aspects has led to a methodological new approach. The combination of whitelists, greylists and blacklists makes it possible to defend by doing further data analysis. There are a number of fields within the CDRs, which are relevant and needed for this analysis. Furthermore, these fields and the use of them for the analysis must be protected and limited to authorized personnel. Certain attack patterns can be identified by doing traffic analysis. A new kind of VoIP attack, which needs attention, is Dial through fraud (DTF) attacks. Also for this specific attack is it possible to generate an attack pattern and successfully counterfeit it. It is obvious that with current means, these different, unique attacks cannot be mastered; let alone the problem in general. A mapping between the fields to distinguish good traffic from bad traffic has to be carried out, as well as a mapping between the different attack patterns. The amount of traffic to be analyzed is also important for the false positive rate and the accuracy of the decision making system. For the decision process there is logic with AND, OR, NOR and logical conjunctions in place. The logic is further part of the algorithm developed for this system.

4.2 Gaps identified in the literature

“A meta-model that could be used for the identification of non-legal behavior and for security testing could result from a formal representation of the protocol, performed on the basis of its operational characteristics and specifically in terms of: (a) the way it processes messages and (b) the behavior of a legitimate user (message flow). However, such formalization does not exist in traditional IDS nor it is utilized for security testing. More specifically existing IDSs can identify and consequently protect only against potential intrusions that are represented in accordance to a particular classification and signature language. Traditionally IDSs identify several attacks but there is not a common way to describe such security flaws in the systems. The formalization of VoIP protocols would provide a valuable tool for the identification of security flaws in VoIP architectures. Ontologies could be considered as a model capable of providing the required formalization and the powerful constructs that include machine interpretable definitions of the concepts within a specific domain and the relation between them.

The introduction of ontologies in VoIP architectures could contribute towards more robust infrastructures, as it can provide a common shared description for any type of attack, independently from the specifics of the system implementation. To the best of our knowledge there is only limited literature on the utilization of ontologies for attack description or for their use in existing IDSs, while there is no literature at all addressing the issue of engaging a security ontology in VoIP environments [GL07]."

"While VoIP threat mitigation systems are not currently available, they will become a key part of the VoIP security infrastructure in the next two to three years (2008, 2009), and should be planned for, as stated in 2006 [M06]."

4.3 Perceived threats and real gaps

People generally assume that they are secure, because they have the latest Antivirus software and firewall installed. This however does not cover the attacks mentioned in this thesis at all. A firewall alone is not enough as security mechanism. Security is a process and needs more protection. The gap is that people do not know that they are endangered by threats. After the identification of the gaps the thesis concentrates on future work and what must be done to reach the goals.

Existing applications have raised technical gaps. Furthermore, a technical and organizational approach is used to handle the privacy issues. More details can be found in the literature of the cited papers. The following chapter shows how the different attacks can be blocked effectively.

This thesis is addressing technical, as well as organizational problems and introduces some solutions. The aim of the thesis is to present a model and best practices to prevent certain types of attacks in VoIP systems, like the MITM attack or toll fraud attack. These attacks have not been solved yet, let alone generally. There are a lot of threats for people that are using VoIP systems today. Often, they are not aware of that their call could be recorded or being spied on sensitive information. And even, if they are aware, they do not care much about privacy and security.

People also tend to exchange sensitive information via phone, which attracts attackers to attack this communication medium. The circumstances presented pose real problems for users, when using this technology.

5 Towards an approach for solving the Man-in-the-Middle and toll fraud problems in VoIP

In this chapter the author’s solution, CDRAS is presented and it is shown how it can help in defending against the problems in VoIP.

So what are the requirements for such a conceptual model? The MITM attack is an old problem, which can for example be seen in online banking. The problem has not yet been solved. Within the SIP context it is dangerous, because there are attack points between the network borders from one technology to another and as it is known from systems theory, it is probable that variances may be generated at such sub-system boundaries. It is possible to launch an MITM attack and read and/or modify the content of SIP messages. Often, SIP messages are transmitted over the Internet in plain text with standard ASCII characters. MITM can occur when the first exchange of keys takes place. Now it is a matter of encryption, which is part of the problem. If no encryption is used, the whole message can be read, while with encryption a decision has to be made concerning securing the key. The MITM attack has reached a new level of complexity. The ever increasing sophistication of the technology is of course, accompanied by increasing complexity. With physical lines, the medium of conversation and its transmission was clear. Now, the conversation takes place through unknown transmission routes and thus needs a new approach. With the MITM attack it is possible for an intruder to steal and forward gained information. With this kind of attack, hackers can be able to listen to calls or even manipulate them. What has to be secured is the RTP audio stream. As RTP is User Datagram Protocol (UDP) based, it is vulnerable against all well-known UDP weaknesses (easy to forge etc.). Moreover, RTP uses a lot of UDP ports, which makes it again vulnerable to attack. Encryption with SRTP, currently in proposed status at the IETF, can be used to authenticate the participating VoIP endpoints.

This chapter is focused on an implementation of a CDRs analysis system to defend against the MITM threat. The proposed solution is an architectural development framework. A new model, such as a filter, is needed as part of the framework. A filter interprets the filtered information and triggers appropriate action. Underneath the filter is a support tool. This tool includes a central authentication service used to give protection from unauthorized access, combined with a firewall to control limited access. The proposed network consists of an authentication server, a registration server and a database, all of which will provide a secure authentication mechanism. But it is not a central server, because then it would be very likely to be attacked by an insider attack. The same single point of failure is seen with a PKI infrastructure. The key for success is pseudonymization. A procedure model will be taken from the SIP registration procedure. So far, there is no defense against the MITM attack.

5.1 Technical requirements

There are different technical requirements. Starting with an acceptable performance of the devised solution and continuing with the acceptance of the concerned users. The user friendliness of the solution also plays an important role, when a company thinks about the enrolment of this tool. A technical requirement of the analysis tool is that all the CDRs data is pulled out of the PBX and that all data acquired matches the original data. Also an accurate logging is needed to see, who has had access to the data and when. Only authorized personal are allowed to pull data and do further editing.

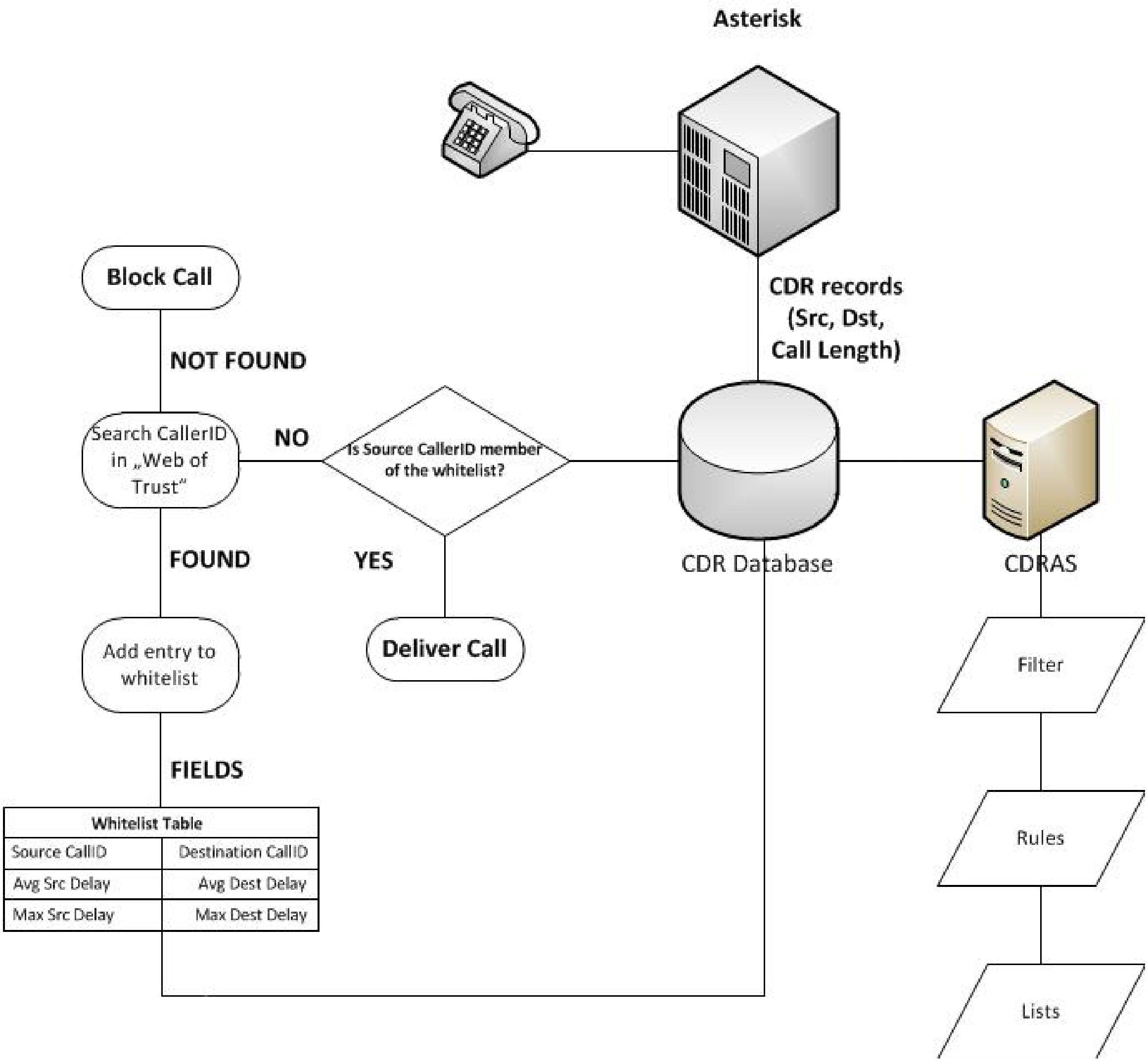
It is obvious that the administrator of such a tool needs access to all infrastructure equipment in place and have full administrative rights. Without this, it is not possible to carry out such analysis and successfully defend against attackers.

It is recommended to have at least two technical engineers, so it might be less probable to misuse such rights and use this tool for the wrong purpose. Also the quality of the data must be guaranteed and regularly checked. Only active, real users shall be filtered and not any other party. The selected data of the big amount of raw data must be carefully selected by the engineers.

5.2 The CDRAS Approach

Every calling or called party has a list of subscribers, whom they trust. Those, who are not on the list, cannot initiate a call. There is a problem, when parties not on the list are regular callers and a caller would like to call them. It helps to allow such calls, when accessing a web of trust. Each subscriber grants his trust to several other subscribers. In the whitelist, the legal traffic of registered hosts is defined. Other traffic is not allowed. More particularly, this tool relates to a method for the automated creation of a list of network points known to be connected to only be authorized endpoints, and use of that list to prevent unauthorized access to the network. For an average network user, a specific list of destinations can be established which account for the majority of the network time used during connections established by that user. The violation of thresholds is essentially the final determining factor in deciding whether fraudulent usage is occurring or not.

These thresholds are expressed as follows: N=number of sessions from certain IP address, Nt=threshold of acceptable number of session from certain IP address, T=time interval over which sessions with a certain IP address have taken place, Tt=time interval threshold triggering suspicion. From this, the following algorithm can be derived: If N>Nt and T>Tt then suspect MITM attack, otherwise it is legitimate traffic. This whitelist will be provided to external systems for use in further analysis. These features and advantages are obtained in an automated CDRs analysis system which interprets the dialed digits and originating phone numbers of CDRs as destination connection points (DCPs). With the whitelist function you can explicitly indicate, which sources are allowed to establish a phone conversation with you. The CDRs analysis system identifies CDRs generated by incoming and outgoing calls, creating from the identified CDRs a whitelist.


Asterisk
Block Call
CDR records (Src, Dst, Call Length)
NOT FOUND
Search CallerID in „Web of Trust"
NO
Is Source CallerID member of the whitelist?
YES
FOUND
CDR Database
CDRAS
Add entry to whitelist
Deliver Call
Filter
FIELDS
Rules
Lists

Whitelist Table	
Source CallID	Destination CallID
Avg Src Delay	Avg Dest Delay
Max Src Delay	Max Dest Delay

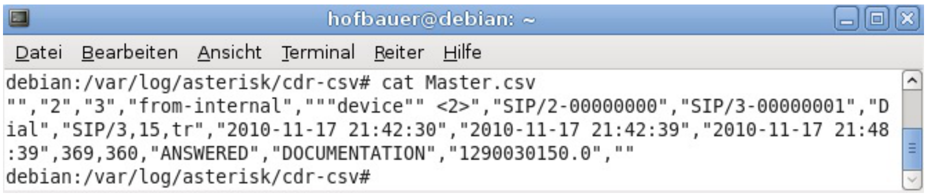
Figure 5.1: CDRAS architecture diagram

For creating a whitelist, enabling the provision of security for a telephone system, the required data includes a set of CDRs comprising call activity from valid subscribers not known to have been compromised.

Once the required data is acquired, the processes of filtering, archiving, restoral and transfer of the whitelist entries to a real-time mechanism are applied to the data. Further, each entry in this whitelist contains statistical fields for tracking the quantity of CDRs which are contained in these dialed digits or phone numbers. This whitelist is used in CDRAS to more efficiently accomplish two tasks. First, the whitelist is used to calculate the maximum and average time delay between attempts to connect to destinations for entries which have more than one attempt made to or by them. These figures can be used to automatically establish a quantity of time which, if no attempts to connect to a destination occur for this quantity of time, the destination or phone number can be removed from the whitelist. Second, the whitelist is used during statistically based filtering. A check is performed for the existence of attempts to connect in conjunction with the requested destination or originating phone number, or network address on active the whitelist.

This is done prior to allowing the connection attempt to succeed, with the network connection setup process blocking the attempt, if the destination of the connection attempt or the originating phone number or network address is not contained in the whitelist. The CDRs analysis system contains the additional components of a globally valid connection points list, commercial connection points list, pattern rules and statistical rules. Globally valid connection points contain a list of DCPs, which are considered by the network operator to be unacceptable for blocking (i.e. in the case of emergency numbers, the carrier’s main office telephone number, etc.). Commercial connection points contain a list of DCPs which are owned or operated by commercial interests (i.e. businesses, business services, public services, etc.). Pattern rules contain a set of rules which, when applied to a group of CDRs, filter out DCPs based on pattern analysis of certain aspects of the connection attempt activities (i.e. quantity of events, quantity of connections, quantity of connection time, etc.). For the detection process to find suspicious traffic, a combination of a signature based IDS and an anomaly detection IDS that can decrease false positives, is used. The IDS in use is an enlargement of the well-known IDS SNORT, which is used as packet sniffer, packet logger and network IDS. The problem with SNORT is that it is still a misuse detection system and it only catches known attacks or unusual behavior. In general, with IDS there exist much redundancy and high false alarm rates while relevant information may be missing or incomplete. As the calls are always made through the Asterisk server, which makes it possible to gather information / data at the time of calls, all data that is needed can be monitored.

The information provided by the CDRs file is as follows:



```
debian:/var/log/asterisk/cdr-csv# cat Master.csv
"","2","3","from-internal","""device"" <2>","SIP/2-00000000","SIP/3-00000001","D
ial","SIP/3,15,tr","2010-11-17 21:42:30","2010-11-17 21:42:39","2010-11-17 21:48
:39",369,360,"ANSWERED","DOCUMENTATION","1290030150.0",""
debian:/var/log/asterisk/cdr-csv#
```

Figure 5.2: Sample output from the CDRs file stored on the Asterisk PBX

CDRs fields are for instance the call date, duration, source and destination. The information is stored in a CSV file on the Asterisk PBX under the folder /var/log/asterisk/cdr-csv/. Once the CDRs file is retrieved, the analysis system can use this information for pattern (detecting suspicious call), trends (early warnings) and building call relationships (who is connected with whom for calling).

CDRs process telephone call information (date, time, calling/called numbers or extensions, duration, etc.) stored within the telephone system in conjunction with other software and hardware to perform management reporting, cost allocation, and fraud prevention procedures. CDRs help detect unusual calling patterns that characteristically represent hacked systems.

5.3 Suggested solution

The CDRAS approach [HQW11] relies on timings of IDS analysis in the Internet to generate host lists: white-, grey-, and blacklists for VoIP participants. Patterns are derived from different combinations of timings that occur in CDRs, e.g., processing time for a call request, the call duration, and the time to destination. In addition, these timing-patterns are related to call participants in the CDRs. A timing pattern that can lead to an attack is, e.g., call requests in relatively short time intervals. The timings can also relate to the number of available, busy and idle voice channels. The whitelist in our approach is the summary of all hosts known as valid, whereas the blacklist presents all hosts, which are known to be malicious. A host that is member of the grey list is sent to quarantine, where an administrator has to check whether the host is allowed or disallowed. It is expected that the detection of malicious users that are sent to quarantine will never be perfect. Hence, a semi-automated approach is proposed, in which a human operator can correct the mistake of a false positive. This correction can be a recall a short time later.

The alarming of a human operator or even the call destination is part of this solution. The difference to fully automated approaches is that in these false positive are more difficult to reconcile, because the machine makes the final decisions. In case of a host being added to the blacklist, the call will not be passed through and, thus, blocked. Of course, hosts need not always reside on the same list. If a host becomes malicious, he will be moved to the blacklist. The host can as well be changed from the blacklist to the whitelist. With this approach in use, it is planned to be aware also of other VoIP attacks. The approach complements existing IDS approaches via detecting timing based attacks and gives a recommendation to existing IDS.

The solution CDRAS determines the occurrence of fraudulent usage based upon thresholds. The number of acceptable VoIP sessions from an IP address depends on the available bandwidth, but it should of course also be limited to maintain an acceptable quality of service. Traditional network traffic detection techniques used by IDS are not sufficient to analyze VoIP specific communication records.

A basic installation of IDS like SNORT without VOIP rules does not protect against VoIP attacks, but CDRAS is used complementary to the IDS SNORT and extended with the detection of VoIP attacks through extended rules. The difference to SNORT is that this approach uses behavior based learning, based on Bayesian networks to also protect against novel attacks. This work is based on a hybrid IDS. A hybrid detection system is a signature based IDS combined with an anomaly detection system. Signature-based IDS compare the state of a system against a number of attack signatures, while anomaly based detection systems capture the normal behavior of a system in a profile and detect when the system diverges significantly from the profile [PP07]. The thesis author and Zhang et al. [ZZH08] believe that a hybrid detection system is better compared to a signature based IDS or anomaly detection system alone, in terms of false positive rates and the detection of unknown attacks. The proposed solution also aims at increasing the detection rate and protect against novel attacks. The signatures for the IDS are taken from the open source community and are one decision tree for this hybrid system.

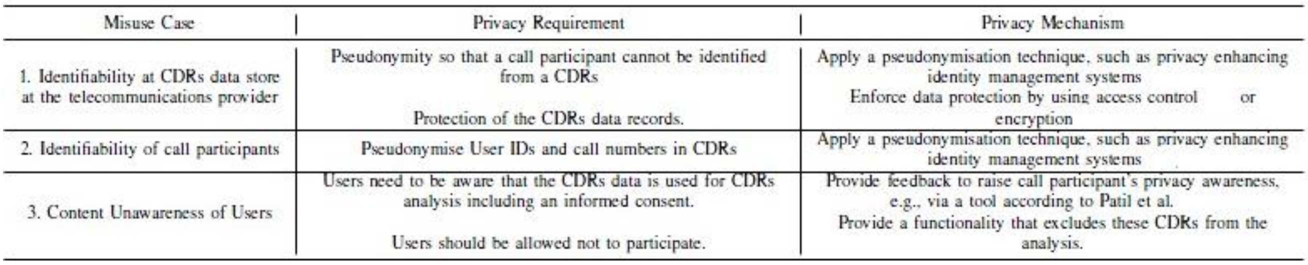
5.4 A Defense Algorithm dealing with typical Attack Vectors

Toll fraud attack vectors occur when calls are routed from the VoIP domain to other telephone networks, e.g., PSTN. Either there is a high frequency of calls to expensive destinations, e.g., international calls, or there are few calls with large duration to expensive destinations, e.g., satellite phones. The learning in the detection phase of CDRAS helps the threshold value to reflect the legitimate changes in the call pattern and thus reduce false positives.

As mentioned by [ZZH08] and [HCCQ07] a false positive rate between 2% and 3% is an acceptable value for a test environment. This percentage needs to be further reduced in a production environment and this solution of course. In addition, even if the calls are grey listed, a fast response from a human operator on the system can reduce the severity of this rate and callbacks can be initiated. In addition, it is planned to implement a learning algorithm into CDRAS that will reduce the false positive rates even further.

The following variables are introduced:

- N := number of sessions from an IP address
- Nt := threshold of acceptable number of sessions from an IP address
- T := time interval over which sessions with an IP address have taken place
- Tt := time interval threshold triggering suspicion



Misuse Case	Privacy Requirement	Privacy Mechanism
1. Identifiability at CDRs data store at the telecommunications provider	Pseudonymity so that a call participant cannot be identified from a CDRs Protection of the CDRs data records.	Apply a pseudonymisation technique, such as privacy enhancing identity management systems Enforce data protection by using access control or encryption
2. Identifiability of call participants	Pseudonymise User IDs and call numbers in CDRs	Apply a pseudonymisation technique, such as privacy enhancing identity management systems
3. Content Unawareness of Users	Users need to be aware that the CDRs data is used for CDRs analysis including an informed consent. Users should be allowed not to participate.	Provide feedback to raise call participant's privacy awareness, e.g., via a tool according to Patil et al. Provide a functionality that excludes these CDRs from the analysis.

Table 5.1: Initial idea: From Misuse Cases to Privacy Requirements and Mechanisms

CDRAS defines a possible attack as follows: N > Nt ^ T > Tt. Hence, the violation of thresholds is essentially the final determining factor in deciding whether fraudulent usage is occurring or not. An alert ”Warning”, is raised when a threshold of 80% of the acceptable value defined is met and an alert ”Error”, when a threshold of 90% of the acceptable value is met.

CDRAS has two system states, letting the traffic pass through or blocking the call. If there is a contradiction, for example a calling source that is member of the whitelist of the CDRs system, but the IDS has found an attack, a manual intervention is raised and a human administrator must manually decide whether the call is approved or not.

Figure 5.3 is a UML sequence diagram of a call flow between a caller (source) and a callee (destination) [UML10]. The source connects to the PBX via the Internet. The PBX routes the call from the source to the destination. The destination can either be a VoIP client or a PSTN client. Hence, the PBX is a connecting gateway between VoIP-to-VoIP and VoIP-to-PSTN calls. The CDRAS system and IDS are connected with the PBX.

In Figure 5.3 there are two results within this data flow, which is always initiated from the source (initiateCall()). The PBX compiles a pattern from several CDRs fields and sends it to CDRAS (matchPattern()).

The pattern consists of: callingPartyNumber, callingPartyUnicodeLoginUserID, originalCalled-PartyNumber, dateTimeConnect and dateTimeDisconnect. The callingPartyNumber is the call initiator and phone extension in our scenario. The callingPartyUnicodeLoginUserID is the user name associated with the IP phone. As originalCalledPartyNumber the up to 16 digits length called destination is meant. CDRAS then goes through the existing host lists and might see that the caller has been an attacker before or is considered as an attacker as he surpasses the thresholds defined in our algorithm. The host lists of the PBX are updated in the next step. If a call fails, the source will get a busy tone or number not available or unknown number reply.

5.5 The filtering mechanism driving the defense algorithm

CDRAS calculates the duration of the calls from the dateTimeConnect and dateTimeDisconnect and uses this information for the call timings method to find deviation from normal behavior and thus attacks. When a client is having 12 concurrent sessions and a session lasting longer than 120 minutes, then an attack is possibly conducted. Mobile phone provider also cut a voice session for security reasons, if it is longer than 2 hours [DRO05]. In this formula it can be seen that $12 > 11 \wedge 121 > 120$. The CDRs fields are input for the CDRAS system, which will analyze the given information. The information is initially stored on the PBX and is used in an anonymized way at CDRAS, where the records are also encrypted. The two states of the CDRAS system are described in the diagram with areas. The first diagram states that a call is an intrusion. The CDRAS system sends the host-list-classification of the source to the IDS (issueHostLists()). The IDS checks for hosts on white- and grey-lists if they are known to the IDS as malicious hosts. In this case the IDS modifies the lists and moves the host to grey- or black-list.

If the CDRAS system listed a host to the black-, or grey-list, the IDS system does not change the host list. When a host is listed in the grey or black-list the IDS warns the CDRAS system that a possible intrusion occurred (intrusionDected()) and the CDRAS system forwards the new host lists to the PBX (updateHostLists()). The PBX denies the call and sends a message to the source (denyCall()). For example, this could be a caller not available message. The PBX sends a message to the destination that a malicious call attempt happened (forbidCall()). The else case in the area, calcifies the source as not malicious. In this case the host remains on the whitelist and the IDS informs CDRAS that the source is not malicious (noIntrusionDetected()).

The CDRAS system forwards this information to the PBX (update-HostLists()), which sends a message to the destination that a call is initiated (allowCall()). The destination replies with a call connection (connectCall()). For simplicities sake, the possibility that the destination refuses the call for whatever reason is not investigated. The PBX connects the call to the source (connectCall()).

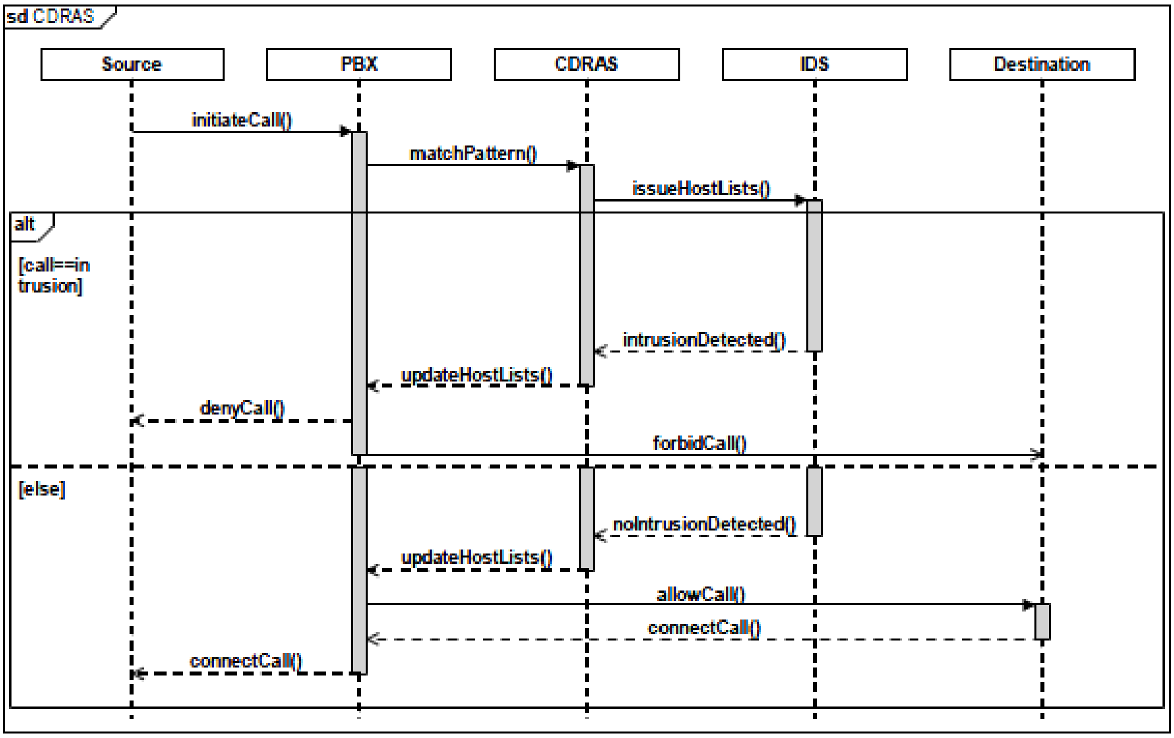


Figure 5.3: Sequence diagram of the call flow

This sequence diagram, together with an attack classification is later tested on the prototype. The relation of timings between attacks plays a dominant part. Also two example attack vectors are discussed in the prototype testing chapter. This timings pattern is based on the CDRs underneath and the understanding of timings is further explained.

The patterns of valid and malicious calling patterns are collected from the PBX in use. Patterns for the following VoIP attacks will be considered. These include DDOS attack, MITM attack, eavesdropping, toll fraud and timing attacks. Pattern of valid calls and malicious VoIP attacks are taken from the PBX in use. These include DDOS attack, MITM attack, eavesdropping, toll fraud and timing attacks. This is a basic set of assumptions and further refinements are the next logical steps.

The description only covers an exemplary set of typical patterns to demonstrate the general idea. It is obvious that in a realistic scenario, further details are elaborated. With a high number of calls within a short time frame, a DDOS attack might be carried out. The characteristics for a MITM attack are additional network packets from a sniffer on a shared medium that can be seen in the IDS traffic capture. This can be seen in chapter 8, testing of the prototype, using the network analyzer software Wireshark. Eavesdropping can be found by looking for spoofed packets and toll fraud is presented by a high number of active and long lasting calls on a voice gateway (router). A high CPU load often is an indication of an attack or anomaly. The use of Bayesian networks is added for prediction (classification) of attacks. New kind of attacks demand for new patterns, meaning the presented system must be updated regularly.

”*Our goal in Bayesian modeling is, at least largely, to find the most accurate representation of a real system about which we may be receiving inconsistent expert advice, rather than finding ways of modeling the inconsistency itself. A Bayesian network is a graphical structure that allows us to represent and reason about an uncertain domain. In general, modeling with Bayesian networks requires the assumption of the Markov property. So Bayesian networks can be used for calculating new beliefs when new information is available. Bayes’ theorem allows us to update the probabilities of variables whose state has not been observed given some set of new observations. Bayesian networks automate this process, allowing reasoning to proceed in any direction across the network of variables. They do this by combining qualitative information about direct dependencies (perhaps causal relations) in arcs and quantitative information about the strengths of those dependencies in conditional probability distributions. Validating a Bayesian network* *means to confirm that it is an accurate representation of the domain or process being modeled. First there is a general consideration. The Bayesian networks are (usually) built or learned under an explicitly causal interpretation. But much validation work in the literature concerns testing the probability distribution represented by the network against some reference distribution.*

By a reference distribution (or, reference model, etc.) we mean a known distribution which is being used as the source for sample data; typically, this is a Bayesian network which is being used to artificially generate sample data by simulation. Sample data can then be used to see how well the learned network predicts the values of the query nodes when the evidence nodes take the values observed in the sample. This can be done whether the query nodes are answers to diagnostic queries (i.e., causes of the evidence nodes) or are causally downstream from the evidence nodes. But if we are interested in testing or validating a model for a real process, then we presumably do not know in advance what the true model is. If we did, we would already be done. So, the practical validation problem is to test some models, constructed by hand or learned, against real data reporting the history of the process to be modeled [KN11].”

The different types of attacks are stored in patterns and queried for during the pattern matching phase. The system is able to identify thus the type of attack by analyzing real data.

In a first step, the occurrence of different sources and destinations is queried:

```
SELECT callingpartynumber, count (*) from unfilteredprimary
Group by callingpartynumber
Order by count(*) desc
```

```
SELECT calledpartynumber, count (*) from unfilteredprimary
Group by calledpartynumber
Order by count(*) desc
```

With these hot numbers, the attack pattern can be mapped and may result in positive identification of attackers.

The SQL database is prepared and built using the following SQL script:

```
##########################################################################
#######

-- Declaration of variables
--
##########################################################################
#######



DECLARE @DatabaseName sysname
DECLARE @DatabaseUserName sysname
DECLARE @DatabaseServer sysname
DECLARE @ReadUserName sysname
DECLARE @TmsReadUserPassword NVARCHAR(100)
DECLARE @EtlStartTime NVARCHAR(8)
DECLARE @EtlResolveSystemsOnInitialLoad BIT



--
##########################################################################
#######

-- Make sure the following values have the correct values for your installation
--
##########################################################################
#######
```

```
SET @DatabaseServer = '< SERVER_FQDN>'

SET @ReadUserName = '<USERNAME>'

SET @ReadUserPassword = '<PASSWORD>'

SET @EtlStartTime = '05:00:00' -- HH:MM:SS

SET @EtlResolveSystemsOnInitialLoad = 1


-- You can safely leave this at its default

SET @DatabaseName = 'cdras'


-- Specify the login that will be assigned the db_owner role for the

-- database. This user will be used to connect to the reporting database


SET @DatabaseUserName = '<DOMAIN_ACCOUNT>'


--
#########################################################################
#######

-- END of customization section

--
#########################################################################
#######



--
=================================================================
===============

-- Editing below this point is normally not needed.

=================================================================
===============
-- The script performs the following main tasks:
--
--   1. Creates the data database
--
--   2. Adds the specified @DatabaseUserName as a login to the
--      server (if it's not already in), and adds this login as a
--      db_owner user in the database.
--
--   3. Creates a linked server connection to the database.
--
--   4. Sets some configuration information on the created database

-- ----------------------------------------------------------------------------
-- 1. Create the database
-- ----------------------------------------------------------------------------
SET XACT_ABORT ON
SET IMPLICIT_TRANSACTIONS OFF

-- Declaration of variables

DECLARE @errorMessage NVARCHAR(4000)
DECLARE @errorSeverity INT;
DECLARE @errorCode INT;

DECLARE @errorState INT;
DECLARE @errorProcedure sysname;
DECLARE @errorLine INT;


DECLARE @rollbackDb BIT
DECLARE @rollbackLogin BIT
DECLARE @rollbackLinkedServer BIT;


BEGIN TRY


-- The database collation must be Latin1 General CI (case insensitive) and AI (accent
-- insensitive). (Latin1_General_CI_AI)


EXEC('CREATE DATABASE [' + @DatabaseName + '] COLLATE
Latin1_General_CI_AI')
SET @rollbackDb = 1
-- Snapshot isolation greatly reduces concurrency related problems
EXEC('ALTER DATABASE [' + @DatabaseName + '] SET
ALLOW_SNAPSHOT_ISOLATION ON')
EXEC('ALTER DATABASE [' + @DatabaseName + '] SET
READ_COMMITTED_SNAPSHOT ON')



-- Simple recovery, to avoid excessive log file growth.


EXEC('ALTER DATABASE [' + @DatabaseName + '] SET RECOVERY SIMPLE WITH
NO_WAIT')


-- ---------------------------------------------------------------------------
-- 2. Create the db_owner login and db user
-- ---------------------------------------------------------------------------
-- Only create the login if it doesn't already exist


IF(NOT EXISTS(SELECT * FROM sys.server_principals WHERE name = @DatabaseUserName)) BEGIN

   EXEC('CREATE LOGIN [' + @DatabaseUserName + '] FROM WINDOWS')

   SET @rollbackLogin = 1


END


-- The user must be added as a user in the database


-- If the user running the script is the same as the specified

-- DatabaseUserName, then he will already be in the DB as dbo

-- (because he created the DB), and we don't need to add him.


DECLARE @CreateUserSql NVARCHAR(2000)

SET @CreateUserSql = '

SET IMPLICIT_TRANSACTIONS OFF;

SET XACT_ABORT ON;

USE [' + @DatabaseName + '];




IF(NOT EXISTS(SELECT * FROM sys.database_principals dp INNER JOIN sys.server_principals sp ON sp.sid = dp.sid AND sp.name = ''' + @DatabaseUserName + ''')) BEGIN

   CREATE USER [' + @DatabaseUserName + '] FOR LOGIN [' + @DatabaseUserName + '];

   EXEC sp_addrolemember N''db_owner'', ''' + @DatabaseUserName + '''' + '

END'
```

```
EXEC(@CreateUserSql)


-- -----------------------------------------------------------------------------

-- 3. Create the linked servers

-- -----------------------------------------------------------------------------


DECLARE @sourceLinkName NVARCHAR(250)

SET @sourceLinkName = 'REPORTING_SRC_' + @DatabaseServer + '_' + @DatabaseName


-- Linked server connected to the data source


EXEC master.dbo.sp_addlinkedserver



    @server=@sourceLinkName

    ,@provider='SQLNCLI'

    ,@datasrc=@DatabaseServer

    ,@catalog=@DatabaseName

    ,@srvproduct=@sourceLinkName


SET @rollbackLinkedServer = 1;




EXEC master.dbo.sp_addlinkedsrvlogin

    @rmtsrvname=@sourceLinkName

    ,@useself='False'

    ,@rmtuser=@ReadUserName
    ,@rmtpassword=@ReadUserPassword


-- ---------------------------------------------------------------------------
-- 4. Pass some configuration variables to the DB
-- ---------------------------------------------------------------------------


DECLARE @ignored DATETIME
BEGIN TRY
   SET @ignored = CONVERT(DATETIME, @EtlStartTime, 108)
END TRY
BEGIN CATCH
   RAISERROR('The value specified for @EtlStartTime is invalid, please use the format
HH:MM:SS', 18, 1)
END CATCH


DECLARE @ssasDatabaseName NVARCHAR(200)


SET @ssasDatabaseName = @DatabaseName + 'AsDb'


-- Metadata needed by the rest of the script


EXEC('USE [' + @DatabaseName + ']; EXEC sp_addextendedproperty @name =
"LinkName", @value = ''' + @sourceLinkName + '''')
EXEC('USE [' + @DatabaseName + ']; EXEC sp_addextendedproperty @name =
"ServerName", @value = ''' + @DatabaseServer + '''')


EXEC('USE [' + @DatabaseName + ']; EXEC sp_addextendedproperty @name =
"DatabaseName", @value = ''' + @DatabaseName + '''')
```

```
EXEC('USE [' + @DatabaseName + ']; EXEC sp_addextendedproperty @name = "ETLResolveSystemsOnInitialLoad", @value = ''' + @EtlResolveSystemsOnInitialLoad + '''')

EXEC('USE [' + @DatabaseName + ']; EXEC sp_addextendedproperty @name = "ETLStartTime", @value = ''' + @EtlStartTime + '''')


EXEC('USE [' + @DatabaseName + ']; EXEC sp_addextendedproperty @name = "SSASDatabaseName", @value = ''' + @ssasDatabaseName + '''')


END TRY
BEGIN CATCH


  if(@@TRANCOUNT > 0) begin
    rollback tran
  end


  SELECT @errorMessage = ERROR_MESSAGE()
      ,@errorSeverity = ERROR_SEVERITY()
      ,@errorCode = ERROR_NUMBER()
      ,@errorProcedure = ERROR_PROCEDURE()
      ,@errorLine = ERROR_LINE()
      ,@errorState = ERROR_STATE()


  -- Roll back operations that were able to complete


  IF(@rollbackDb = 1) BEGIN
    EXEC('DROP DATABASE [' + @DatabaseName + ']')
  END
```

```
   IF(@rollbackLogin = 1) BEGIN
      EXEC('DROP LOGIN [' + @DatabaseUserName + ']')
   END



   IF(@rollbackLinkedServer = 1) BEGIN
      EXEC master.dbo.sp_dropserver @server=@sourceLinkName,
@droplogins='droplogins'
   END

   DECLARE @customErrorMessage VARCHAR(2000)
   SET @customErrorMessage = 'An unexpected error occurred. All changes have been
rolled back. The underlying error was: "' + @errorMessage + '", code ' +
CAST(@errorCode AS VARCHAR(10)) + ' at line ' + CAST(@errorLine AS
VARCHAR(10)) + ' with errorProcedure = ' + COALESCE(@errorProcedure, 'NULL');
   RAISERROR(@customErrorMessage, 18, @errorState)
   RETURN

END CATCH

PRINT 'All server level objects have been successfully created.'

--
======================================================================
================
-- END OF SCRIPT



--
======================================================================
================
```

Chapter 6 will start with a privacy impact analysis as basis for this solution. Based on the privacy and legal requirements it is easy to conduct a privacy threat analysis in a compliant way. Compliance is very important for companies, as they are being assessed by auditors on a regular basis. Important standards are for example the ISO 27001, Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Sarbanes-Oxley Act (SOX) or Basel 3. Many companies need external help, because they do not have the knowledge or the time to handle it.

6 Satisfying privacy requirements

This chapter describes the analysis in more detail, while being privacy compliant. It will make more clear, which mechanisms are adequate to master the privacy requirements.

6.1 A Privacy Impact Analysis approach building on the Australian PIA guide

According to widely accepted privacy impact analysis guides, the core steps in a privacy oriented analysis of IT projects are the mapping of the information flows and privacy framework, the privacy impact analysis and privacy management. One of the leading examples is the Australian Privacy Impact Analysis Guide (PIA) [AUS10], where the different steps are described on pages 11 ff. The recommendations derived from these analysis steps are documented in Table 6.6 for the given case. In the first column, misuse cases as introduced by Sindre and Opdahl [OS09] are used. These are textual representations of attacker's actions for threat identification. They are used to identify privacy threats. In the next column, resulting privacy requirements are presented that prevent the misuse cases from happening. In the last column, mechanisms that fulfill the privacy requirement are listed. This structure is derived from [DWSPJ11].

In essence, the following core privacy requirements for CDRs are identified:

- Data in CDRs has to be kept confidential
- Storing CDRs data requires a reason compliant with the law
- Analyzing CDRs requires an informed consent of the call participants
- CDRs have to be erased when the previous requirements are not fulfilled

It is shown in chapter 6.3.3 how the elicited legal privacy requirements for CDRs are fulfilled in the CDRAS solution. However, first the description of the VoIP security functionality of the approach is presented in the following sections.

6.2 Suggested Approach to Risk Management

With new challenges and types of attacks, VoIP clearly requires a more sophisticated approach to security than those currently used to secure data networks. Solutions based on network-based devices and signature-based applications are not going to address the real-time nature and complexity of VoIP networks. A system based approach that combines network and host-based security devices and applications with sophisticated, systems level threat mitigation systems will be required efficiently to protect the entire VoIP infrastructure. In building a systems-level approach to VoIP security, a unified VoIP specific security infrastructure architecture consists of three functional components: prevention, protection and mitigation.

Prevention:

Once VoIP is deployed, periodic or, where required, continuous vulnerability assessments should become a cornerstone of an overall proactive VoIP security strategy. Once security vulnerabilities are identified they should be addressed by appropriate actions such as patching, re-configuration and network tuning. These actions should be clearly defined as part of the company’s overall security policy to provide a framework for dealing with possible threats to VoIP security.

Protection:

The deployment of a multi-layer security infrastructure that provides both perimeter as well as internal network protection is recommended. In most cases, it will consist of a number of security devices and host based applications to protect VoIP networks, such as SBCs, VoIP Network Intrusion Prevention Systems (NIPS), VoIP DOS defenses, VoIP Network IDS, Host IPSs, Authentication, Authorization and Accounting (AAA) servers, encryption engines and VoIP anti-virus software. All the devices and applications have to be coordinated via a high level application providing unified view of the end-to-end VoIP infrastructure.

Mitigation:

Threat mitigation systems should be able to respond autonomously to the detected security threats and keep their impact at the level where VoIP services can still function albeit at lower QOS [M06].

6.3 Legal requirements

The analysis of the CDRs data has to be done in such a way that the privacy of the call participants is preserved. There are a number of laws, which protect the storage, analysis and further usage of personal and confidential data. Not only service provider, but also individuals have to obey these rules. There are slight changes, depending on the residence of the company. It is distinguished between EU law and US law. EU law takes precedence over national law, for example German law.

For the usage of this solution, the agreement of every person has to be considered, before starting with the collection and analysis of data. The users have to be informed beforehand, so that they have the chance to withdraw their consent. An informed consent is obligatory for the usage of this solution. For large companies, the solution must also be agreed on by the works council. Another rule to obey is the duration this data can and should be kept.

There are audits for certified companies, where the implementation of these rules is looked for and all documentation analyzed. So it is a good idea to have compliant procedures in place and be prepared for these unannounced controls. In case, the obligations are not considered, fines as well as the loss of certification might harm the company. Often, big companies have their own legal department for these questions and small and medium-sized businesses consult their own lawyer.

It is further recommended that legal department and technical departments work together to bridge the gap between legal and technical wording towards the employee and other companies. Once the requirements are known and the involved assets are identified, a company policy can be set up and enabled after introduction and signature of the employee and partners. Regular revisions of these policies are needed and extensions or modifications documented and sent to all affected parties in written format, for their approval. The structure of the policy is such that different topics and controls are categorized and needed actions are defined.

During the whole process, the privacy of all involved parties must be assured. A violation of the privacy might result in a court case, fines or even imprisonment.

6.4 Deriving Privacy Requirements for Communication Records

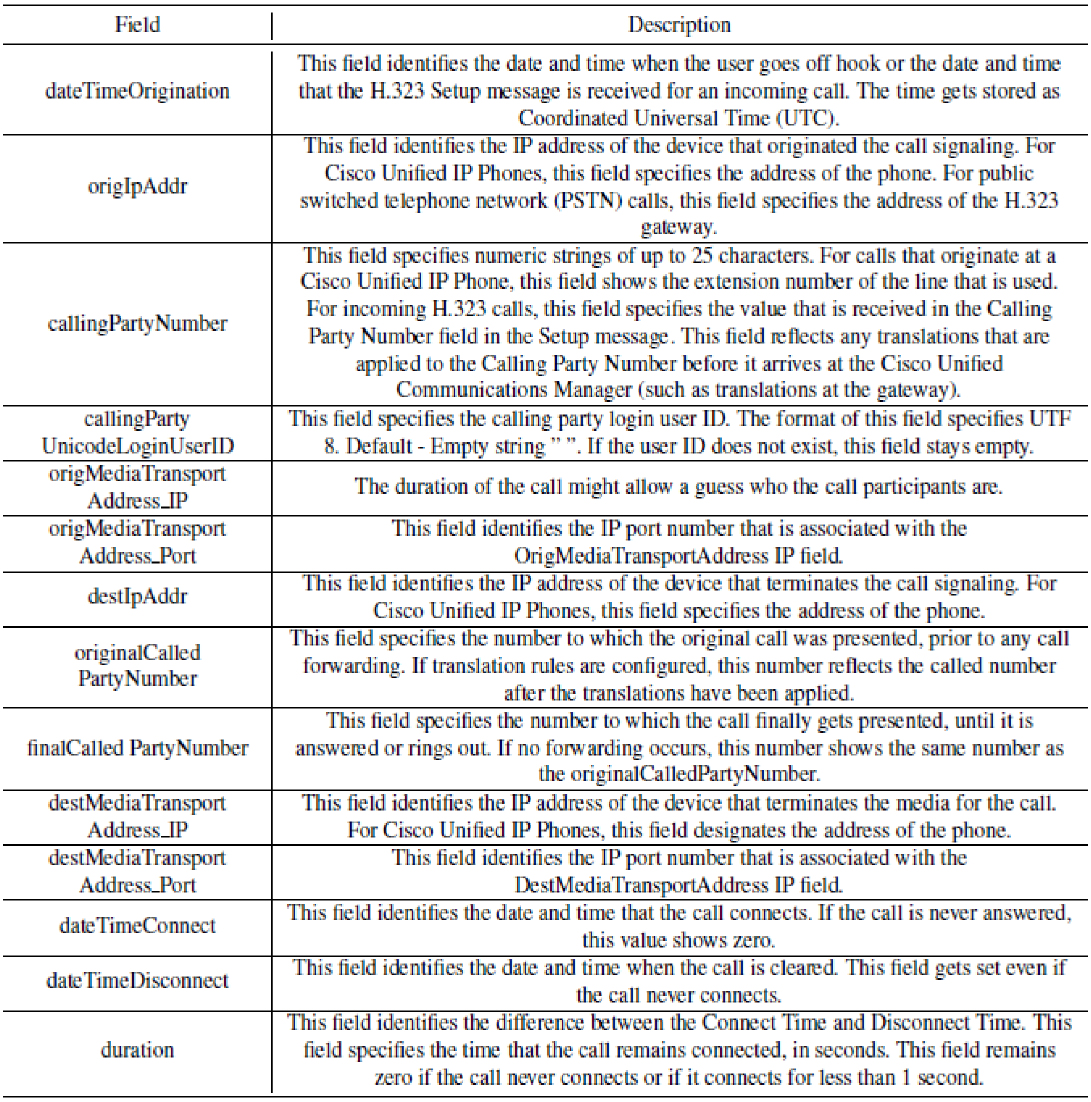
A method for ensuring privacy in a CDRs analysis is presented. Each step of the method is written in a sub chapter and the execution of the step is written in the following.

6.4.1 Describing the context and stakeholders

VoIP calls are conducted between caller and one or more callees. Both are customers of a telecommunications provider and they use the infrastructure of this provider. The VoIP technology uses VoIP hard phones, physical devices and soft phones, software running on a personal computer. In some cases, the call participants might use PSTN phones and the call is just transferred to VoIP via a PSTN gateway. The telecommunication provider has also relations to security analysts that can provide protection from VoIP attacks. These experts, however, are not employees of the telecommunication company. The data of the call, occurred, is stored in CDRs. These are stored at a data center owned by the telecommunication provider. The telecommunication provider forwards these calls to the security analysts to analyze possible VoIP attacks. The telecommunication provider uses the results of the analysis to generate automatic white lists for their clients.

The class diagram presented in Figure 2.2 is an example architecture for a standard IP connection to the VoIP provider. The VoIP Layer 2 Switch on the provider side provides connectivity and multi-client capability for the customers. The Internet consists of routers and firewalls, which partly belong to the provider itself, but also to Internet service provider along the data traffic from the customer to the provider. The Cisco Unified Border Element (CUBE) is acting as VoIP aware firewall restricting the SIP traffic between the customers’ PBX and the provider PBX.

If there is no CUBE placed between, security can also be accomplished by setting access control lists (ACL) on the customer’s PBX external interface itself. Additional security can be assured by adding the provider IP address to the trusted list.



Field	Description
dateTimeOrigination	This field identifies the date and time when the user goes off hook or the date and time that the H.323 Setup message is received for an incoming call. The time gets stored as Coordinated Universal Time (UTC).
origIpAddr	This field identifies the IP address of the device that originated the call signaling. For Cisco Unified IP Phones, this field specifies the address of the phone. For public switched telephone network (PSTN) calls, this field specifies the address of the H.323 gateway.
callingPartyNumber	This field specifies numeric strings of up to 25 characters. For calls that originate at a Cisco Unified IP Phone, this field shows the extension number of the line that is used. For incoming H.323 calls, this field specifies the value that is received in the Calling Party Number field in the Setup message. This field reflects any translations that are applied to the Calling Party Number before it arrives at the Cisco Unified Communications Manager (such as translations at the gateway).
callingParty UnicodeLoginUserID	This field specifies the calling party login user ID. The format of this field specifies UTF 8. Default - Empty string ” ”. If the user ID does not exist, this field stays empty.
origMediaTransport Address_IP	The duration of the call might allow a guess who the call participants are.
origMediaTransport Address_Port	This field identifies the IP port number that is associated with the OrigMediaTransportAddress IP field.
destIpAddr	This field identifies the IP address of the device that terminates the call signaling. For Cisco Unified IP Phones, this field specifies the address of the phone.
originalCalled PartyNumber	This field specifies the number to which the original call was presented, prior to any call forwarding. If translation rules are configured, this number reflects the called number after the translations have been applied.
finalCalled PartyNumber	This field specifies the number to which the call finally gets presented, until it is answered or rings out. If no forwarding occurs, this number shows the same number as the originalCalledPartyNumber.
destMediaTransport Address_IP	This field identifies the IP address of the device that terminates the media for the call. For Cisco Unified IP Phones, this field designates the address of the phone.
destMediaTransport Address_Port	This field identifies the IP port number that is associated with the DestMediaTransportAddress IP field.
dateTimeConnect	This field identifies the date and time that the call connects. If the call is never answered, this value shows zero.
dateTimeDisconnect	This field identifies the date and time when the call is cleared. This field gets set even if the call never connects.
duration	This field identifies the difference between the Connect Time and Disconnect Time. This field specifies the time that the call remains connected, in seconds. This field remains zero if the call never connects or if it connects for less than 1 second.

Table 6.1: Call Detail Records Field Descriptions

This toll fraud prevention feature is available on Cisco voice gateways from firmware release IOS 15.1(2)T. In this scenario, also QOS and Class of Service (COS) features can be implemented in an all IP network. Often companies with a large IP network use Multi-Protocol Label Switching (MPLS) technology for their data and voice network.

The class diagram presented in Figure 2.3 describes how a classical telephony system integrates with the PSTN network. The PSTN network always connects the customer's gateway with the provider's gateway.

Many of the aforementioned techniques cannot be implemented within PSTN. Not relying on an IP network makes the ISDN not so vulnerable against attacks. A wiretap attack on the line itself or an attack on voice switches can however be carried out. The next difference to the IP network is that there are always one-to-one connections between the customer site and provider site.

In an IP network, there can be many SIP trunks configured on the customer site that connect to one or many provider. As can be seen in Figure 2.2 and in Figure 2.3, the solution, consisting of CDRAS and an IDS, can be placed into both scenarios using different technology. The basis for CDRAS is always the CDRs generated on the PBX for every session occurred. The mission of the IDS is to detect anomalies and thus give recommendations to effectively block connections. In ISDN world, the calls and call flows cannot be modified using QOS and COS techniques.

6.4.2 Identifying personal information in data

The data in CDRs can be classified in primary and secondary personal information. Analysis of primary personal information can help identifying a stakeholder, while secondary information can derive actions of a stakeholder. Table 6.2 lists the fields with primary personal information. Table 6.3 describes CDRs fields containing secondary personal information.

Field	**Relation to Privacy**
origIPAddr	Might lead to identifying the caller with reasonable efforts in time and money.
callingPartyNumber	
callingPartyUnicode	
origMediaTransport Adress IP and Port	
destIpAddr	Might lead to identifying the callee with reasonable efforts in time and money.
originalCalled PartyNumber	
FinallyCalledParty Number	

destMediaTransport Address IP and Port	

Table 6.2: CDRs fields with primary personal information

Field	**Relation to Privacy**
dateTimeOrigination	This might lead to identify the callers habits or even to identify possible callees. For instance, most callers would not call their doctors at 8 p.m. on Christmas eve.
dateTimeConnect	This might lead to identify the callers habits or even to identify possible callees.
dateTimeDisconnect	The duration of the call might allow a guess to what subjects were discussed. For example, agreeing on a meeting point should be quick, while discussing a research matter might take longer.
duration	The duration of the call might allow a guess if the call participants are malicious.

Table 6.3: CDRs fields with secondary personal information

6.4.3 Eliciting privacy requirements from legal and cultural aspects

Nissenbaum [NIS04] stated that the sources of privacy norms are law, history, and culture. This thesis is focusing on norms from law and culture. Law will be further distinguished into US and German law.

First, culture as a source for privacy norms is researched, from which privacy requirements are derived. The definition of privacy by Pfleeger and Pfleeger [PP07] is used as a source for a cultural privacy norm.

The definition states that everyone can control the distribution of their personal information. The first part of this method already describes the context of the situation and the information in Table 6.2 and Table 6.3 states that the data in the CDRs are personal information.

The call participants have to decide if this information can be used by the telecommunications companies or not. In any case, should the call participants give their informed consent, it is clear that this data can be used for VoIP analysis and protecting against attacks. In addition, a privacy mechanism has to be used during the analysis [PH11].

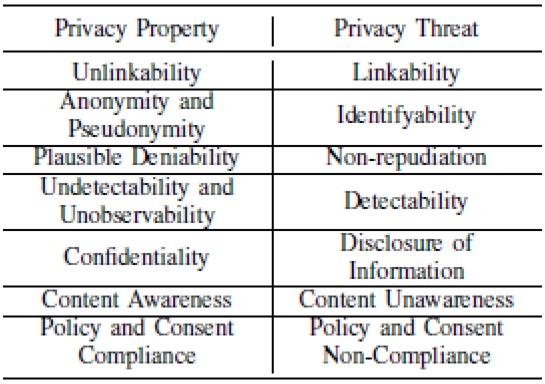
Pfitzmann further introduces a terminology for privacy via data minimization. The authors define central terms of privacy using IOIs, e.g., subjects, messages and actions. Anonymity means a subject is not identifiable within a set of subjects, the anonymity set. Unlinkability of two or more IOIs means that within a system the attacker cannot sufficiently distinguish whatever these IOIs are related or not. Undetectability of an IOI means that the attacker cannot sufficiently distinguish whether it exist or not. Unobservability of an IOI means undetectability of the IOI against all subjects uninvolved in it and anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI. A pseudonym is an identifier of a subject other than one of the subject’s real names. Using pseudonyms means pseudonimity. Identity Management means managing various partial identities (usually denoted by pseudonyms) of an individual, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.

Possible mechanisms are discussed during the threat analysis part of this method. The laws in the EU, Germany and the US also demand an informed consent for CDRs analysis, e.g., in FIPs, EU Data Protection Directive, BDSG and SCA. Moreover, telephone calls have to be kept confidential according to the telecommunications laws in the US and Germany. In general, confidentiality is seen as a mechanism to enforce privacy [DG11]. The SCA in the US, the EUDRD and the German laws TKG and TKÜV demand CDRs data retention.

This is in conflict with the cultural privacy requirements, where all persons should be allowed to deny the storage of their personal information. As this conflict cannot be solved, only the laws are considered.

However, this does not reflect the opinion of the thesis author. It is proposed to use stored CDRs data for security analysis and use the results to protect telecommunications users. When applying satisfying privacy mechanisms and getting the informed consent of the call participants this should be within reason.

The SCA in the US, the EUDRD and the German laws TKG and TKUEV demand CDRs data retention. This is in conflict with the cultural privacy requirements, where all persons should be allowed to deny the storage of their personal information.



Privacy Property	Privacy Threat
Unlinkability	Linkability
Anonymity and Pseudonymity	Identifyability
Plausible Deniability	Non-repudiation
Undetectability and Unobservability	Detectability
Confidentiality	Disclosure of Information
Content Awareness	Content Unawareness
Policy and Consent Compliance	Policy and Consent Non-Compliance

Table 6.4: Privacy Properties – Privacy Threats

The following privacy requirements for CDRs data from legal norms and laws are elicited:

- Communication records have to be kept confidential
- Communication records can only be stored as long as there is a valid reason, e.g., 6 months for the EU data retention directive or for billing purposes of the telecommunication provider
- Customers have to provide their informed consent if their communication data is used in an VoIP attack analysis

– Communication records have to be deleted if none of the cases above apply

6.4.4 Conducting a Privacy Threat Analysis

The combination of two privacy threat analysis approaches is used in this method. Deng et al. [DWSPJ11] introduce a privacy threat model that shows a threat for each privacy property presented in Table 6.4.

Spiekermann et al. [SC09] develop a framework for considering privacy in software systems. The authors identify two general approaches for preserving privacy in software systems. Privacy-by-policy is based upon the FIPs from the OECD, which is the so-called notice and choice approach. The user gets either informed why and how his/her information is used and additionally can choose not to provide data. Privacy-by-architecture is a design approach that does not store privacy relevant data on companies' IT-systems. The data could be stored e.g. on the users notebook or not needed in the first place. The authors further provide a framework that categorizes systems in four privacy stages 0-3. The stages 0 and 1 use privacy-by-policy and 2 and 3 use privacy-by-architecture. Systems can be categorized into this framework via their system characteristics e.g. transaction information is stored in a company database. The authors conclude with advices for implementing privacy-by-policy systems, when privacy-by-architecture approaches are not feasible, due to the systems characteristics.

The information in Table 6.2 and Table 6.3 can be classified as privacy stage 1 in the framework of Spiekermann et al. [SC09]. The reason is that the information in the CDRs, e.g., origIPAddr can be classified as a pseudonym. In stage 1 the pseudonym is linkable with reasonable and automatable effort.

The threat analysis approach by Deng et al. [DWSPJ11] is used in this method. The stakeholder shall reveal only the minimum amount of data that is necessary for performing a specific task. The policy and consent compliance property states the requirement for a privacy policy. Stakeholders, who control personal information of other stakeholders, have to inform these other stakeholders about their privacy policy. They also have to specify consents in compliance with legislation for the stakeholders that shall enter personal information into a system. Stakeholders that enter personal information into the system have to constant to these policies, before their personal information enters the system. The privacy threats for CDRs are listed in Table 6.5. A "+" in Table 6.5 marks a privacy threat to a CDRs field or a stakeholder. However, the free cells of the table do not imply that a

CDRs field or stakeholder is not subject to a privacy threat. The threat levels are classified as following: Serious (S), Normal (N) and Merely (M).

The misuse cases in Table 6.6 are derived from the subjects (Linkability, Identifyability, Non-repudiation, Detectability, Disclosure of information, Content unawareness, Policy and Consent Non-Compliance), while the privacy requirements are proposals. The privacy requirements state that users shall be informed, if their personal information in CDRs is used for a purpose that differs from the purpose these were collected for. In this case users should be allowed not to participate. The source and the destination are user telephones. Hence, users are located at these locations in our scenario. The destination is assumed to be users inside a company.

These can be informed in a meeting before using the telephone system for the first time and their informed consent can be collected or they deny their consent and the system is not used for these destinations.

Collecting an informed consent from the source, however, is difficult. For practical reasons, not every source can be queried. However, there are alternative options: the PBX can repeat an automated recorded message for first time callers, informing the caller of the usage of CDRAS and asks for her/his agreement or disagreement. Alternatively, the callers could be asked by their respective providers, and a PBX could include a list of providers who ask for that consent. If a source does not allow processing of his personal data for purposes of the system, the destination might use a policy to block calls from this source. Similarly, even nowadays, it is possible to block all calls whose caller ID is suppressed.

This is not illegal if the destination decides about the policy. In German law, for example, suppression of mailings is a criminal act, but this is not true for suppression of phone calls [SNS10].

Privacy Threat Target	**L**	**I**	**N**	**D**	**D**	**U**	**N**	**T**
origIPAddr	+	+	+	+	+		+	N
callingPartyNumber	+	+	+	+	+		+	S
origMediaTransport Addr. IP+Port	+	+	+	+	+		+	N
destIpAddr	+	+	+	+	+		+	M
originalCalledPartyNumber	+	+	+	+	+		+	N
finalCalledParty Number	+	+	+	+	+		+	S
destMediaTransport Addr. IP+Port	+	+	+	+	+		+	M
dateTimeOrigination	+	+	+	+	+		+	N
dateTimeConnect	+	+	+	+	+		+	N
dateTimeDisconnect	+	+	+	+	+		+	N
Duration	+	+	+	+	+		+	S
stakeholder caller	+	+				+		N
stakeholder callee	+	+				+		M

From the left-hand side to the right-hand side: Linkability(L), Identifyability(I), Non-repudiation(N), Detectability(D), Disclosure of information(D), Content unawareness(U), Policy and Consent Non-Compliance(N), Threat Level (T)

Table 6.5: Privacy Threats to CDRs fields and stakeholders

Misuse Case	Privacy Requirements	Privacy Mechanism
1. Linkability of the CDRs in data storage	Unlinkabilty of CDRs in the telecommunication providers database Protection of the stored CDRs data	Apply a pseudonymization technnique, such as privacy enhancing identity management systems [CKK05] Enforce data protection by using access control or even context-based access control
2. Identifiability at CDRs data store at the telecom-munications provider	Pseudonymity so that a call participant cannot be identified from a CDRs Protection of the CDRs data records.	Apply an pseudonymization technique, such as privacy enhancing identity management systems [CKK05]
3. Identifiability of call participants	Pseudonymize User IDs and call numbers in CDRs (see Table 5.1)	Apply an pseudonymization technique, e.g. privacy enhancing identity management systems [CKK05]
4. Detectability of CDRs data	Prevent an attacker to determine how many data sets exist in the CDRs storage	Allocate the maximum storage for CDRs in the database and fill it with randomly created CDRs, replace the randomly created CDRs with real ones

5. Information disclosure of the data in storage CDRs	Release of CDRs data store should be controlled according to the call participants’ privacy preference Keep CDRs records confidential	Enforce data protection by using access control [ANS04] and confidentiality in the form of encryption
6. Content Unawareness of Users	Users need to be aware that the CDRs data is used for VoIP attack prevention including an informed consent. Users should be allowed not to participate	Provide feedback to raise call participant’s privacy awareness, e.g., via a tool according to Patil et al. [PS11]

7. Policy and consent non-compliance of the VoIP system	Monitor the compliance of the VoIP system with law and guidelines Call participants are aware of the privacy policy and can recognize and react to a violation Employees of the telecommunications companies have specified privacy rules and they obey these rules Security analysts have a specific set of privacy rules and they obey these. They are only allowed to work with pseudonymized CDR data	Hire a legal expert to supervise the creation and operations of the VoIP system Install logging and monitoring software that documents the lifecycles of all personal information. This lifecycles include the creation, usage, access from persons, and deletion of the personal information Inform call participants of possible signs of a violation and provide a help desk to who these violations can be reported to Policy communication can be realized via P3P [P3P02] and policy enforcement via XACML [OAS05] Ensure that employees and security analysts are trained for privacy-enhancing operations of the VoIP system. If any of these persons disclose personal information they are penalized, e.g. pay a fine

Table 6.6: Revised idea: From misuse cases to privacy requirements and mechanisms

6.4.5 Deriving privacy requirements from the threat analysis and choose privacy enhancement technologies (PETs)

Several solution strategies exist for fulfilling privacy requirements [DWSPJ11]:

- A solution for low risk threats is to warn users
- Turning the risk to zero can only be achieved via removing or turning off the feature that causes the privacy threat
- Using countermeasures for privacy threats in the form of preventive or reactive PETs

The callers and callees shall be warned that their CDRs are analyzed for the purpose of preventing VoIP attacks. The feature can be adopted in such a way that users can object to it and is turned off for these users. However, our priority is to apply countermeasures to the privacy threats and enable a privacy preserving analysis feature. In order to identify suitable PETs, a number of misuse cases for privacy are presented in the given scenario. These are derived from the information collected in the method up to this point and the privacy threat tree from Deng et al. [DWSPJ11]. The selection of PETs is based upon [DWSPJ11, WSDJ09, KKG08, and SC09].

In comparison, the approach from Spiekermann et al. [SC09] describes that privacy-by-policy implementations have to consider four different areas. The privacy of the call participants shall be preserved in the CDRs information stored in the database. The authors Clauß et al. [CKK05] propose a method for privacy enhancing identity management. In order to achieve privacy for the call participants, it is the unlinkability between persons and their actions. One way of achieving this is to replace the information leading to the identity of a person with a pseudonym. The method also demands to specify if the data is stored in a database or if the information is also transported over a network. Only the information stored in the database is considered. The network transfer of information will be used in the future.

Short misuse cases are presented, privacy requirements derived and resulting privacy mechanisms shown in Table 6.6. A detailed pattern for misuse cases is not provided. In comparison, the approach from Spiekermann [SC09] describes that privacy-by-policy implementations have to consider four different areas. The relations between the Spiekermann et al. approach and Table 6.6 are then described. The first area Spiekermann et al. consider is to give users notice and choice. This area is covered by the 6th case. The second area concerns access control. This mechanism is suggested as a result of the 2nd case. The third is about the responsibility to inform users about data sharing. This is also part of the mechanisms of case 6. The last area concerns technical mechanisms to audit and enforce privacy. This is covered in the 7th case. Thus, all areas named in the work of Spiekermann et al. are covered in Table 6.6.

It is proposed to integrate CDRAS in this scenario to fulfill the privacy requirements listed in Table 6.6. In this example it is assumed that all the destinations, the telephone users of the providers or in the company, gave their informed consent to the call filtering. In addition, it is also assumed that a menace exists to inform the source that CDRAS is used and the source also gave an informed consent. In this system, the CDRs are substituted with pseudonyms. CDRAS will provide a database that is protected with access control that links the pseudonyms to the real values. In addition, the CDRs have a time stamp that states their creation. The database automatically erases the database records that link the pseudonyms to the values of real users after a reasonable time, in this example three days.

6.4.6 Reconciliation of legal, cultural and threat driven privacy requirements

The requirements derived from legal and cultural aspects have to be free of conflicts with the requirements derived from privacy threats. Relations between the legal and cultural requirements and the privacy requirement are shown in Table 6.6. The first legal and cultural requirement is that records have to be kept confidential. Confidentiality is part of the requirements of case 5. Further, the confidentiality requirements for CDRs are addressed.

This requires the configuration of access control measures in VoIP hard- and soft phones, as well as the PBX, IDS and CDRAS. The configuration has to reflect that only administrators are allowed to investigate CDRs and that the access to the CDRs is recorded in, e.g., log files. These files have to reflect the names of the persons that accessed the CDRs. Hence, non-repudiation of access to CDRs is guaranteed. Otherwise it is not possible to prove that the privacy requirement, confidentiality, is fulfilled.

The legal and cultural requirements that CDRs can only be stored for a limited amount of time are in accordance with the requirements from the 7th case. The informed consent legal-cultural requirement is in accordance with the privacy requirements of case 6. The last legal-and-cultural requirement is that CDRs have to be deleted if no legal regulation applies. This is part of the requirements of case 7.

6.5 Conserving Privacy while analyzing CDRs

For the analysis of the CDRs data, the privacy of individuals must be retained. The non-conformance to privacy rules, laws and regulations are a sharp intrusion into the individual's rights and freedom.

Analysis of CDRs records:

A different approach, based on a CDRs analysis system is introduced, consisting of white-, grey- and black-lists. With this lists it can be checked on legal or illegal network traffic. This model is capable of identifying current VoIP attacks as well as novel VoIP attacks. If the value surpasses the predefined threshold, the item set is assigned to the group of suspicious hot patterns. Given features selected for item sets and the known labels for training the data set, further inputs these suspicious items sets as false alarms or attacks into a decision-tree classifier for training. This decision-tree classifier works as a misuse detector in the testing phase. The final decision-tree classifier consists of rules that classify item sets into three groups: known attacks, false alarms, and unknown attacks.

By selecting a threshold empirically, attacks can be distinguished from normal data. The packets with anomaly scores above a threshold will be sent to a correlation engine. Traditional scan detection methods use rule-based thresholds. These techniques normally result in a low detection rate and an unacceptable False Acceptance Rate (FAR), the same problem as occurs in most of the anomaly detection systems. The use of Bayesian networks has been added for prediction (classification) of attacks.

”A decision network is an extension of Bayesian networks that is able to represent the main considerations involved in decision making: the state of the world, the decisions or actions under consideration, states that may result from an action and the utility of those resultant states. Bayesian and decision networks model relationships between variables at a particular point in time or during a specific time interval. Validating a Bayesian network means to confirm that it is an accurate representation of the domain or process being modeled. We will reserve the term for more statistically oriented evaluation methods and specifically for methods suited to testing the correctness of a Bayesian network when a reasonably large amount of data describing the modeled process is available. First there is a general consideration. The Bayesian networks are (usually) built or learned under an explicitly causal interpretation. But much validation work in the literature concerns testing the probability distribution represented by the network against some reference distribution. By a reference distribution (or, reference model, etc.) we mean a known distribution which is being used as the source for sample data; typically, this is a Bayesian network which is being used to artificially generate sample data by simulation. Now, since Bayesian networks within a single Markov equivalence class can be parameterized so as to yield identical probability distributions, testing their probability distributions against a reference distribution fails to show that you have the right causal model. One way of dealing with this problem is to collect experimental data, rather than simply take joint observations across the variables.

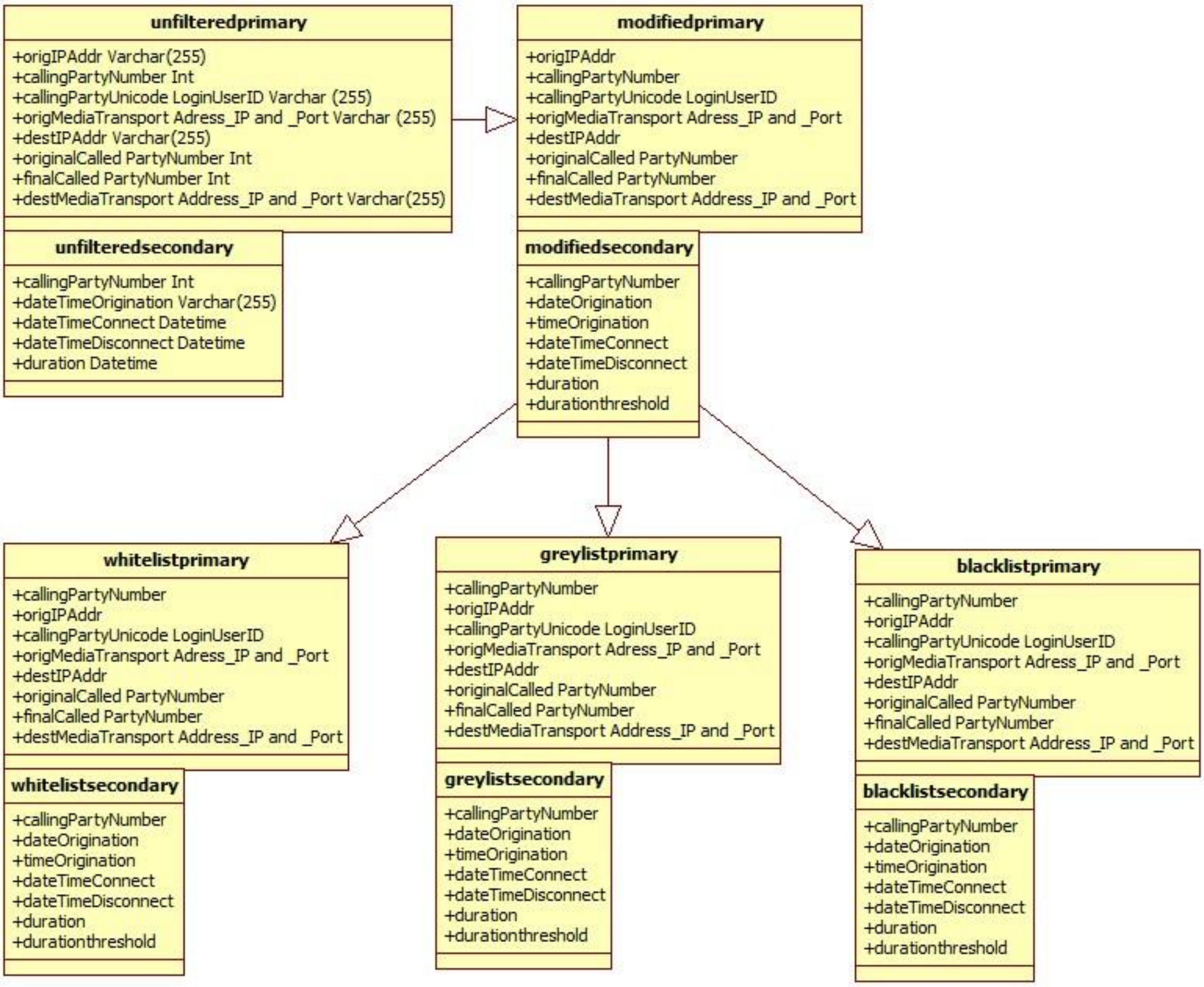


Figure 6.1: CDRAS database model

In that case, we can represent the causal interventions explicitly and distinguish between causal models. There are many reasons why this option may be unavailable, the main one being that collecting such experimental data may be prohibitively expensive or time consuming. A more readily available option is to analyze the problem and identify a subset of nodes which are characteristically going to be the query nodes in application and another subset which are going to be evidence nodes. Sample data can then be used to see how well the learned network predicts the values of the query nodes when the evidence nodes take the values observed in the sample. This can be done whether the query nodes are answers to diagnostic queries (i.e., causes of the evidence nodes) or are causally downstream from the evidence nodes. As described so far, this evaluation also does not take into account the causal structure being learned.

It will often turn out that the restricted sub network being examined has few Markov equivalent sub networks even when the full network does. But if we are interested in testing or validating a model for a real process, then we presumably do not know in advance what the true model is. If we did, we would already be done. So, the practical validation problem is to test some models, constructed by hand or learned, against real data reporting the history of the process to be modeled [KN11].”

This whitelist will be provided to external systems for use in further analysis. These features and advantages are obtained in an automated CDRs analysis system which interprets the dialed digits and originating phone numbers of CDRs as DCPs. With the whitelist function it can be explicitly indicated which sources are allowed to establish a phone conversation. The CDRs analysis system identifies CDRs generated by incoming and outgoing calls, creating a whitelist from the identified CDRs. This data can also be used for billing purposes and to identify top callers and top destinations. Based on this, special calling deals can be arranged with the phone provider or destinations even blocked. Normally, phone provider also monitor customers’ phone bills, looking for spikes and automatically generate a warning email to the customer in case a certain threshold in amount of calling time or generated costs is exceeded. This also helps the customer to counteract possible attacks. But the customer shall not rely on these mechanisms alone, but have an own dedicated monitoring system. It is a good idea that the same companies are used for extracting the CDRs, doing the analysis and make possible corrective actions. Such sensitive information shall not be outsourced to different companies, who can be competitors themselves. In the last years there has been recognized a trend for insourcing again after a long period of outsourcing boom. But this, of course, depends on the economic situation and budget possibilities of a company. Small and medium-sized businesses do not have the choice and no other chance to do outsourcing, because of economic reasons. This has also to be considered when defending against attackers. The security officer must be sure about the own company, other companies within the same industry and attackers’ habits. To know about the latest technology trends and security concerns are a must for a Chief Information Security Officer (CISO). It is expected that this position becomes even more important in the next years. Every company should have their own CISCO or an external responsible person.

As soon as all requirements have been identified and documented, the implementation of a prototype is the next logical step to prove the hypothesis and do validation. With the prototype in place, it is possible to conduct tests and even implement it in real world infrastructures. Tapering of information is an actual threat as can often be seen in daily news. Tapering is mostly done, because of economic or political reasons. The attacker wants to gain sensitive knowledge to be one step ahead, know about the competitor’s plans or just to steal important information. The next chapter explains in a descriptive way how an implementation can help for the different possible scenarios.

7 Implementation of a prototype

With the implementation of a prototype the feasibility of the approach in use, is shown. The prototype has been implemented during the doctoral studies.

7.1 Man-in-the-Middle attack using Ettercap

A MITM attack is exactly what it sounds like. The idea is to implement some attack by putting your computer directly into the flow of traffic. This can be done in several ways, but the thesis is focused on ARP poisoning. To accomplish a MITM and capture all the VoIP traffic, two hosts are ARP poisoned." [JC07] These are a VoIP soft phone on a notebook (192.168.247.1) and another one in a virtual machine (192.168.247.137) on this notebook. The two phones are registered to an Asterisk PBX [AST10]. The poisoning will be done from another virtual machine (192.168.247.150) on this notebook, running Ettercap [ETT10] on BackTrack4 [BAC10]. Ettercap's primarily functions are network sniffing (eavesdropping) and MITM attacking.

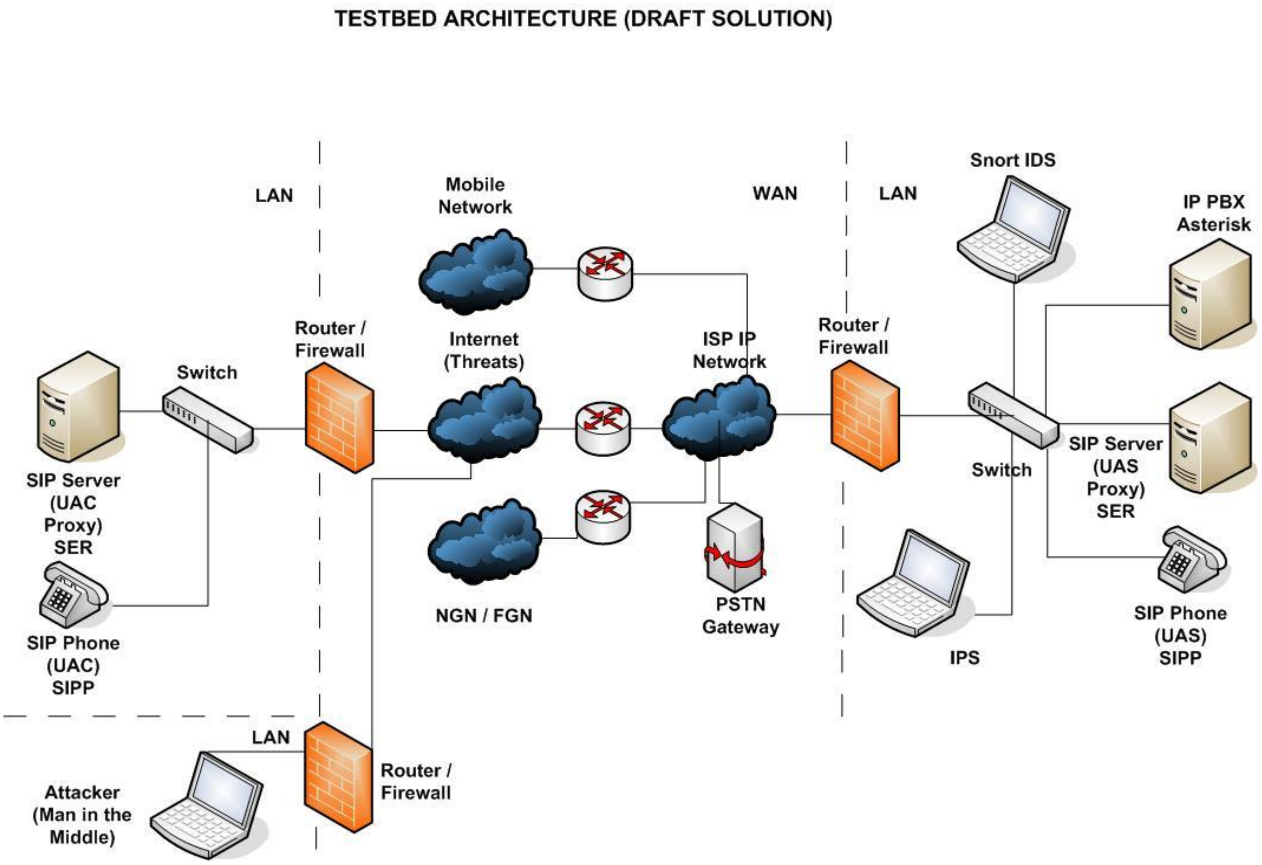


Figure 7.1: Test bed Architecture for the prototype

With the prototype it is possible to search for new defense algorithms. The experiments have been used as proof of concept. Further, the feasibility of different attacking methods is evaluated and effective countermeasure solutions are found. Last, but not least, different solutions have been evaluated in the test bed to finally come up with this approach. All the needed network environments, like the User Agent Client (UAC) or the User Agent Server (UAS) have been installed on virtualized machines on a laptop.

The framework consists of the following developments:

- Extending an existing solution framework with domain specific business logic
- Connecting information from different resources
- Designing context-rich user display and interaction services

The basis for the framework is a stable model. And the prototype helps in ensuring that everything is on the right way. The advantage of this framework is that it can be used for any system that is using communication records. So it is applicable also in other domains than VoIP. Ideas of dynamic ARP inspection (DARPI) and data mining have also influenced this work.

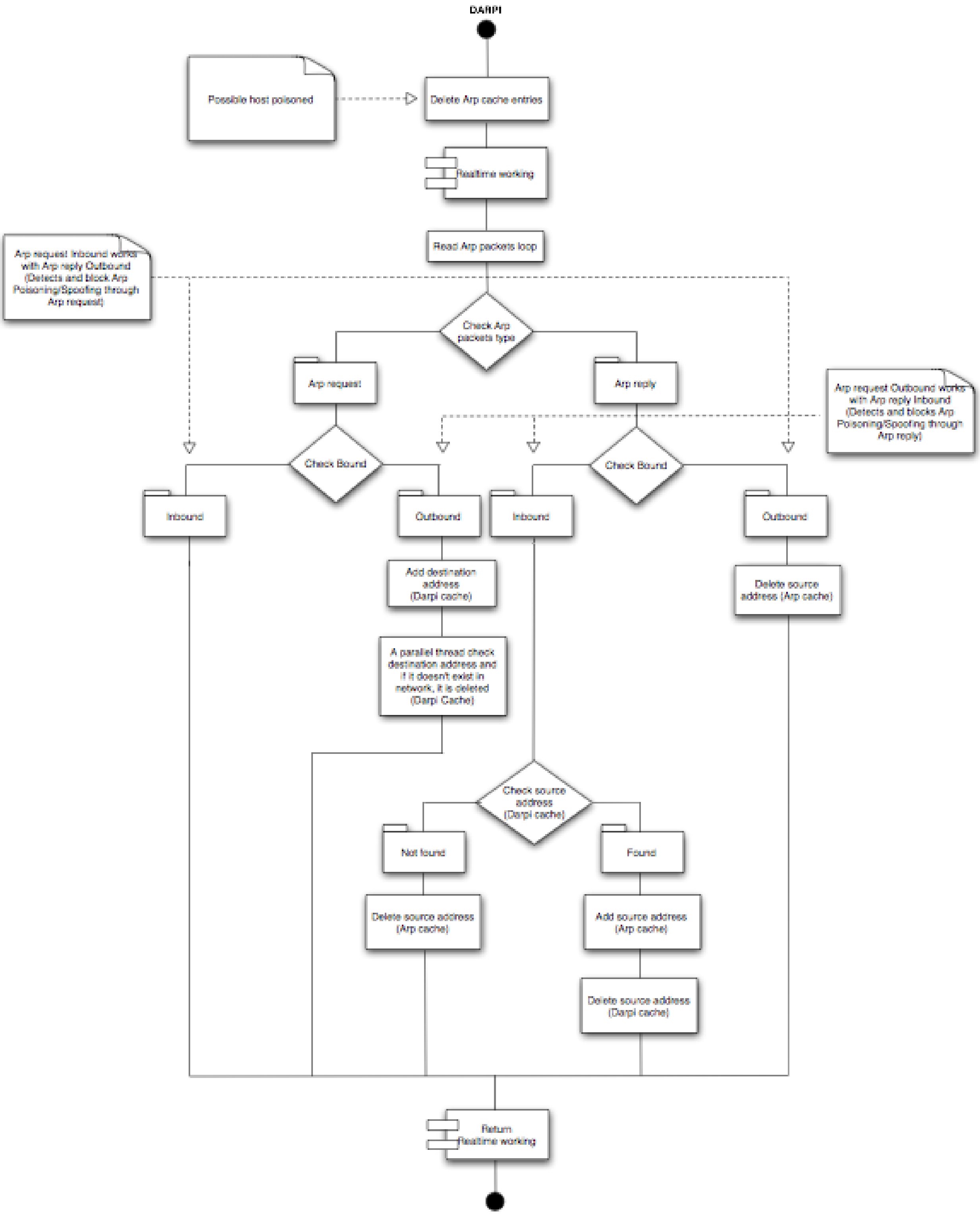
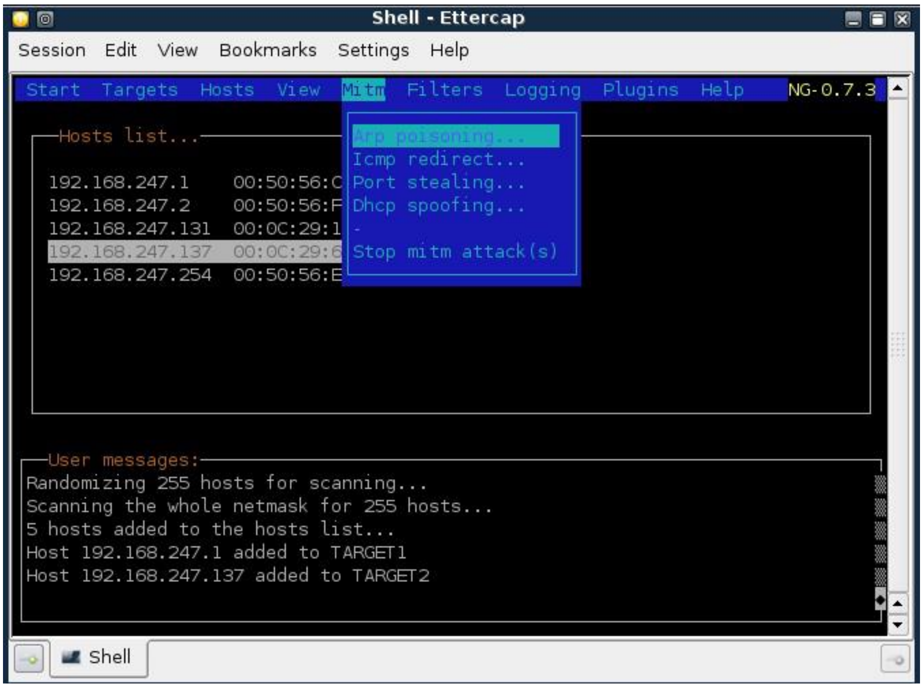

DARPI
Possible host poisoned
Delete Arp cache entries
Realtime working
Read Arp packets loop
Arp request Inbound works with Arp reply Outbound (Detects and block Arp Poisoning/Spoofing through Arp request)
Check Arp packets type
Arp request
Arp reply
Arp request Outbound works with Arp reply Inbound (Detects and blocks Arp Poisoning/Spoofing through Arp reply)
Check Bound
Check Bound
Inbound
Outbound
Inbound
Outbound
Add destination address (Darpi cache)
Delete source address (Arp cache)
A parallel thread check destination address and if it doesn't exist in network, it is deleted (Darpi Cache)
Check source address (Darpi cache)
Not found
Found
Delete source address (Arp cache)
Add source address (Arp cache)
Delete source address (Darpi cache)
Return Realtime working

Figure 7.2: ARPon Dynamic ARP inspection algorithm, taken from http://arpon.sourceforge.net/index.html

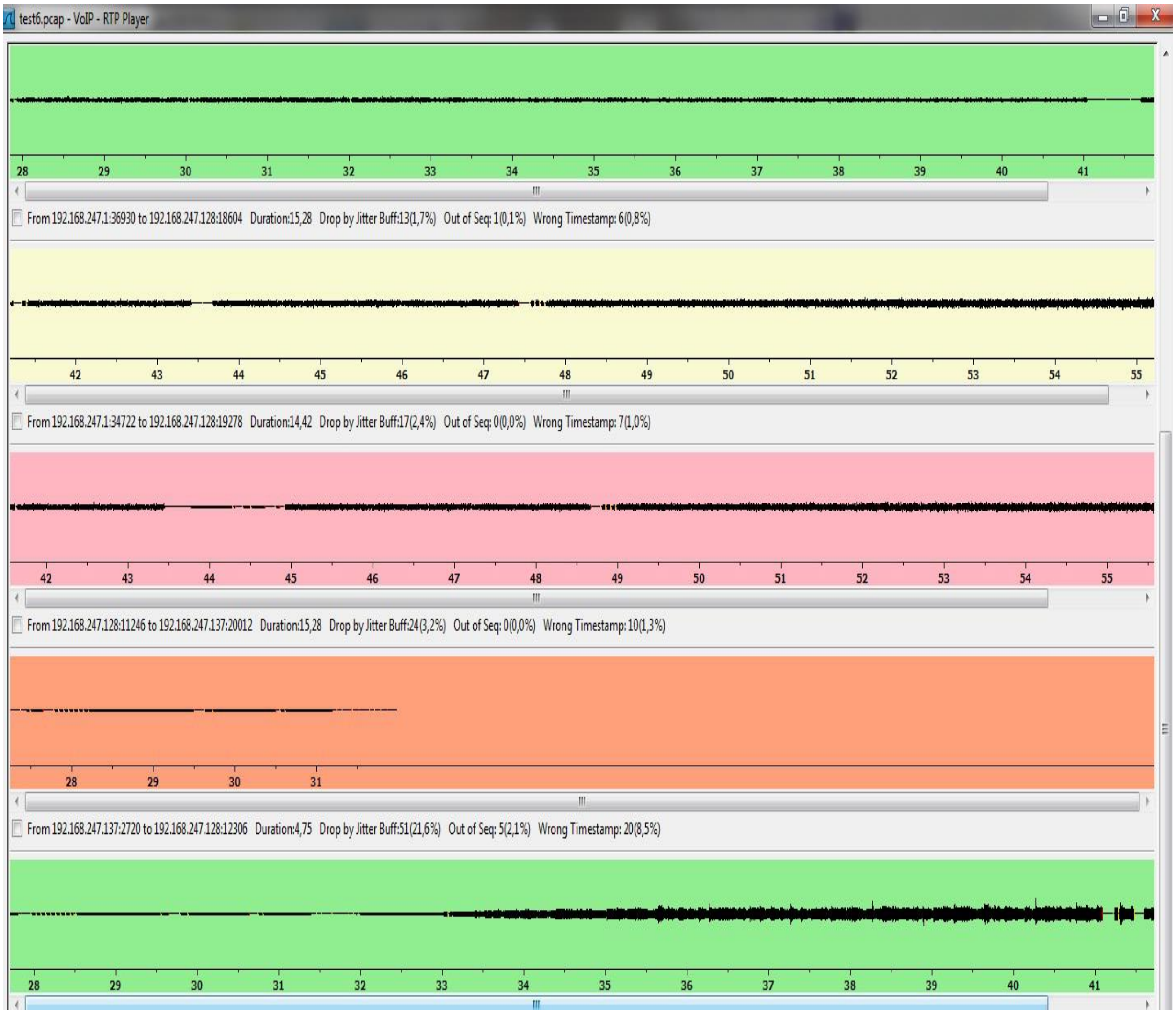

Shell - Ettercap
Session Edit View Bookmarks Settings Help
Start Targets Hosts View Mitm Filters Logging Plugins Help NG-0.7.3
Arp poisoning...
Icmp redirect...
Port stealing...
Dhcp spoofing...
-
Stop mitm attack(s)
Shell

```
Hosts list...

192.168.247.1     00:50:56:C
192.168.247.2     00:50:56:F
192.168.247.131   00:0C:29:1
192.168.247.137   00:0C:29:6
192.168.247.254   00:50:56:E

User messages:
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 192.168.247.1 added to TARGET1
Host 192.168.247.137 added to TARGET2
```

Figure 7.3: MITM Attack in BackTrack4 using Ettercap

Ettercap is scanning for hosts in a network by sending out ARP requests to all hosts. Then, Ettercap stores all these responses in a host list. From this list, the targets are selected and the MITM attack can begin. The results are then stored in a PCAP file, which can be analyzed in Wireshark [WIR10]. The complete call conversation can be reconstructed from the captured file. Besides audio, other data can also be extracted.

For example, authentication information used between devices during the call build up, or the Dual Tone Multi Frequency (DTMF) used to authenticate with other devices, such as voice mail.



□ From 192.168.247.1:36930 to 192.168.247.128:18604 Duration:15,28 Drop by Jitter Buff:13(1,7%) Out of Seq: 1(0,1%) Wrong Timestamp: 6(0,8%)

□ From 192.168.247.1:34722 to 192.168.247.128:19278 Duration:14,42 Drop by Jitter Buff:17(2,4%) Out of Seq: 0(0,0%) Wrong Timestamp: 7(1,0%)

□ From 192.168.247.128:11246 to 192.168.247.137:20012 Duration:15,28 Drop by Jitter Buff:24(3,2%) Out of Seq: 0(0,0%) Wrong Timestamp: 10(1,3%)

□ From 192.168.247.137:2720 to 192.168.247.128:12306 Duration:4,75 Drop by Jitter Buff:51(21,6%) Out of Seq: 5(2,1%) Wrong Timestamp: 20(8,5%)

Figure 7.4: Decoded RTP audio streams from the captured VoIP traffic

7.2 SIP Man-in-the-Middle attack based hijacking attack

Being in the middle, between two valid communication nodes, allows an attacker to see every single SIP packet. Of course they have to be transmitted in clear for the hacker to be able to understand them, but once intercepted and analyzed, every single packet can be modified.

Many implementations use authentication methods by each action performed by a user. While it helps to eliminate some dangers, the mechanisms have their vulnerabilities as well. Most often used authentication method is HTTP Digest, which sends the most part of the packet header in clear text and only some SIP parameters are encrypted for the sake of authentication. This method does not provide full message integrity protection, even if it detects replay attacks. Because of that, a MITM attacker can modify some packet parameters before forwarding it to a valid recipient. MITM based SIP session hijackings attacks are dangerous, as they may be carried out even in case of default authentication methods working correctly. As a consequence of such an attack, a hacker may compromise almost every single security requirement and realize most of the threats. All MITM issues mentioned above regard SIP signaling traffic. However, RTP media stream is also intercepted, which endangers also the content of the call. Even if an attacker decides not to modify signaling traffic in any way, he/she might still modify voice content. It is difficult to say to what extent such an attack is dangerous, since voice processing software is not so developed today. Due to this, no sophisticated attacks against media are possible yet, but this problem may occur in the future. Last but not least, an attacker could use regular update mechanisms to install some malicious software on devices where User Agents are running normally. Upon detection of an update request a MITM attacker could transmit his/her own software to the device. This regards both software and hardware VoIP phones [LAW07].

According to widely accepted privacy impact analysis guides, the core steps in a privacy oriented analysis of IT projects are the mapping of the information flows and privacy framework, the privacy impact analysis and privacy management. One of the leading examples is the PIA guide for government agencies [AUS10]. This assessment tool analyzes the flow of personal information and the possible privacy impacts of these flows on individuals of a given project.

A PIA has five key stages according to [AUS10]. It is extended by a sixth step: 1. Project description**:** Describe the scope of the project including the aims and if there is personal information involved. 2. Mapping the information flows and privacy framework: Describe the personal information flows in the project and document relevant laws and regulations, as well as organizational rules. 3. Privacy impact analysis: Identify and analyze the privacy impact of the project. 4. Privacy management: Choose mechanisms that manage the privacy impact and still achieve the goals of the project. 5. Recommendations: Generate a PIA report that contains recommendations based upon the previous stages. 6. Model scenario: Instantiate a model of the scenario described. The PIA for the scenario is conducted here.

7.3 Prototype description:

The project is focused on a business environment running a PBX. There, local, national and international VoIP calls are conducted. The calls can be carried out between subsidiaries of the company residing in different countries or externals, partners and customers, who are not part of the company's telephone network. Often, companies have contracts with low cost VoIP providers, who can offer cheap dial-outs. Again, CDRs are processed for these calls and stored at the customer site and/or the telecommunication provider. Cisco CDRs are investigated, because the vendor is of reasonable practical significance [GAR10]. For instance, the knowledge of the filled date time might lead to identify the caller's habits or even to identify possible callees.

7.3.1 Mapping the information flows and privacy framework:

The information flow in this scenario starts from a callee to the telecommunication provider and results at the callee. The laws in the EU, Germany and the US also demand that telecommunications data is only stored for a specific purpose and deleted after the purpose is no longer valid. The usage of the data beyond this purpose requires an informed consent of the owner of the personal information. Careful attention must be taken on the PBX side, where the duration these data is stored, can be set to an even longer time frame and thus conflicts with the law. The company must be sure about the location, where the data is stored and have full access to it anytime. This is important, when the data is outsourced to a cloud provider.

The following privacy requirements for CDRs data are elicited from legal norms and laws:

- Communication records have to be kept confidential
- Communication records can only be stored as long as there is a valid reason, e.g., for billing purposes of the telecommunication provider
- Customers have to provide their informed consent if their communication data is used in an VoIP attack analysis
- Communication records have to be deleted if none of the cases above apply

The review of the legal aspects and further privacy impact assessment is focused on a business perspective and does not consider any of the special exceptions for law enforcement. Nissenbaum [NIS04] states that the sources of privacy norms are law, history, and culture. According to Article 6 ePrivacy Directive 2002/46/EC, traffic data must be erased or made anonymous when it is no longer needed. Users of subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. The directive of the European parliament and the council regarding data retention states that this Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers’ or the network providers’ own services. ’Telephone service’ means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services) [HQW11]. After addressing law, norms originating from culture are investigated briefly, which are not focused on history. These definitions state that persons shall be able to control which personal information is released, to whom it is released to and in what context. It is believed that these needs can be addressed with an informed consent. However, the person shall also be able not to share personal information.

7.3.2 Privacy impact analysis:

The privacy impact is the amount of people involved and the severity of a possible leakage of personal information [CDR10]. The amount of people in this case is the amount of people using VoIP services of a telecommunications provider. The personal information contains data from which the person can be identified with reasonable amount of time and money. Thus, this leads to a high privacy impact of this project.

7.3.3 Privacy management:

In order to identify suitable PETs, a number of misuse cases are presented for privacy in the given scenario. The selection of PETs is based on [DWSPJ11, WSDJ09, KKG08, and SC09]. A detailed pattern for misuse cases is not provided.

Moreover, PETs for secondary personal information are not addressed, because it is proposed to use pseudonymization with primary personal information. Hence, secondary personal information is of no use to a privacy attacker, as long as he/she does not have a way to identify the person this information belongs to.

7.3.4 Recommendations:

The fifth step of the guide is excluded and thus extended with a sixth step, the model scenario.

7.4 Different scenarios:

In the following scenario, two possible call flows are described that have been identified from industrial experience. It describes that whether SIP or ISDN as telephone technology is used, the CDRs are stored on the PBX. A CUBE is placed between the PBX and the Internet and therefore knows about every session. For registering the phones to the PBX, either SIP or the Cisco proprietary Skinny Client Control Protocol (SCCP) is used. In the SIP scenario, a SIP trunk connects the source to the VoIP provider. Our contribution is based on the use of CDRAS and an IDS within the call flow. The H.323 protocol is mainly used to connect the network elements (CDRAS, IDS, voice router) to the PBX in use.

The CDRAS approach determines the occurrence of fraudulent usage based upon thresholds. The number of acceptable VoIP sessions from an IP address depends on the available bandwidth, but it should of course also be limited to maintain an acceptable QOS.

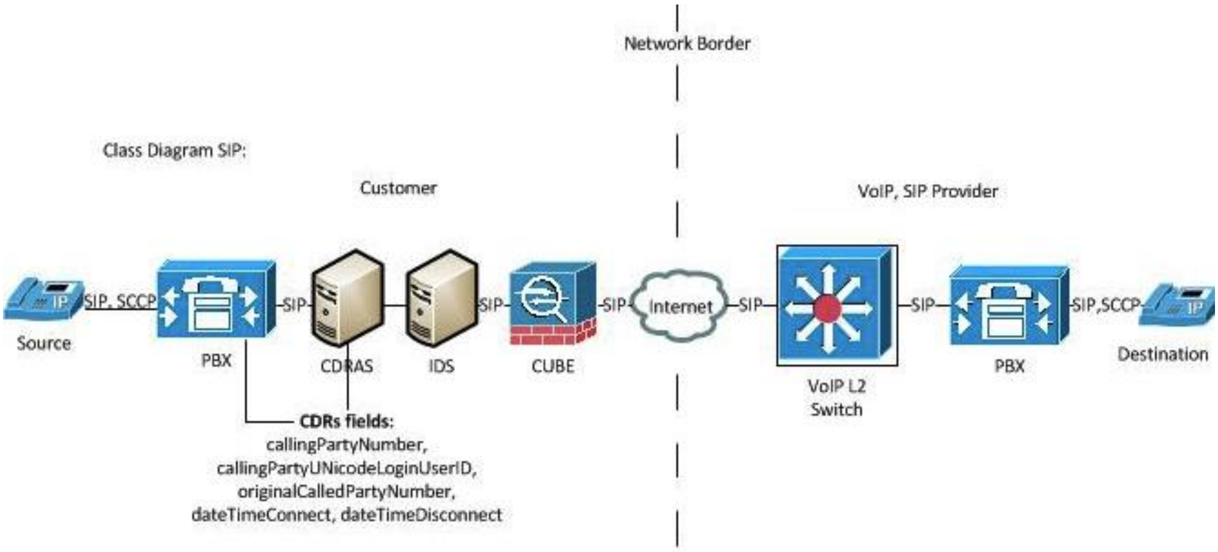


Figure 7.5: Class Diagram for a SIP scenario

This model can be instantiated and further used for other scenarios and domains. The prerequisite is the use of communication records within the call flow.

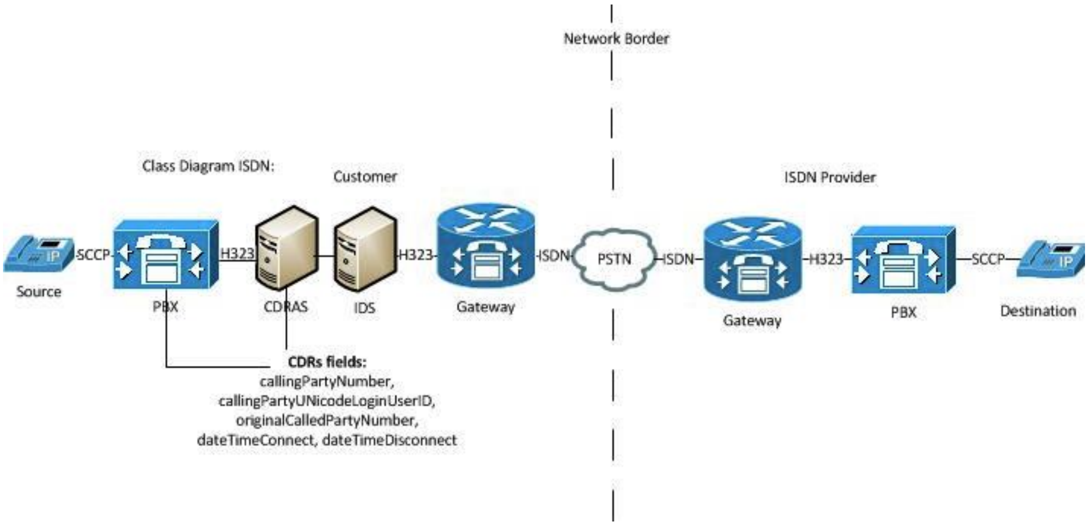


Figure 7.6: Class Diagram for an ISDN scenario

In essence, the following privacy requirements for CDRs have been identified:

- Confidentiality of data in CDRs
- Storing CDRs data requires a reason compliant with the law
- Analyzing CDRs requires an informed consent of the call participants
- CDRs have to be erased when the previous requirements are not fulfilled

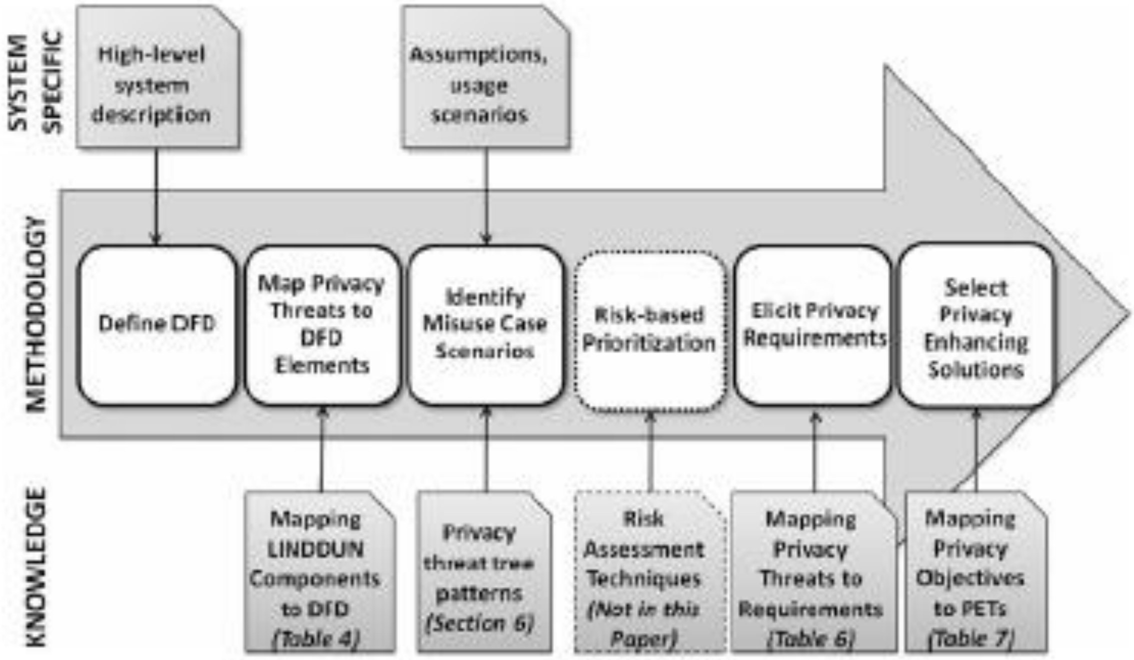

SYSTEM SPECIFIC
High-level system description
Assumptions, usage scenarios
METHODOLOGY
Define DFD
Map Privacy Threats to DFD Elements
Identify Misuse Case Scenarios
Risk-based Prioritization
Elicit Privacy Requirements
Select Privacy Enhancing Solutions
KNOWLEDGE
Mapping LINDDUN Components to DFD (Table 4)
Privacy threat tree patterns (Section 6)
Risk Assessment Techniques (Not in this Paper)
Mapping Privacy Threats to Requirements (Table 6)
Mapping Privacy Objectives to PETs (Table 7)

Figure 7.7: Data Flow Diagram Example and the LINDDUN methodology (taken from [DWSPJ11])

The authors Deng et al. [DWSPJ11] generate a threat tree for privacy based upon the threat categories: linkability, identifiablitiy, non-repudiation, detectability, information disclosure, content unawareness, and policy/consent noncompliance. The acronym of these threats forms the name of the method which is LINDDUN.

The method uses data flow diagrams (DFD) to describe the usage scenarios (see Figure 7.7), which has the following elements:

- External Entity: is an endpoint of the system, e.g., users or external services
- Process: is a computational unit, e.g., programs
- Data store: represents data at rest, e.g., databases, files etc.
- Data flow: represents data on the move, e.g. communication data
- Trust boundary: represent the border between untrustworthy and trustworthy elements

Privacy threats are described for each of these components. Thus, the authors create a mapping of specific privacy threats to software-based system components. The threats are the input for misuse cases that are in turn used to elect privacy requirements. The last step of the method is to select privacy enhancing solutions that fulfill the privacy requirements.

7.4.1 Data Flow Diagram

The DFD presented in Figure 7.8 combines SIP and ISDN networks in one diagram. Three different zones, named Client zone, Server zone and Internet zone exist. The CDRs are collected at one single point, which is secured by access lists and encryption. It is the PBX that will provide the CDRAS system with relevant data. The call flow for the SIP network is as following: Phone -> PBX -> CDRAS -> IDS -> CUBE -> L2 Switch -> Provider PBX. Whereas the call flow for the ISDN network is described herein: Phone -> PBX -> CDRAS -> IDS -> Gateway -> PSTN. The messages between Phone and PBX, CDRAS and PBX, CDRAS and IDS and PBX to PBX connections are bidirectional. The other exchanged messages in the data flow diagram are unidirectional. And there are attack points between the network borders (zones) from one technology to another. The physical caller and callee are also defined as single entities. Between the client and the server zone there is a many to one connection, while the connections between the server zone and Internet zone are one to many, by default. But there can also be one to one connections between the server zone and the Internet zone, when the customer has got a direct line between the customer site and the provider. This dedicated line can be restricted for voice traffic only, putting a Service Level Agreement (SLA) on it, in which the provider assures a certain QOS and a maximum downtime per year.

For a reliable voice connection and call-center, service desk and hotlines facing customers, it is essential to have such a dedicated, monitored line. In case of an outage and the connection being down, there can also be several defined backup destinations (mobile, fixed line).

Also the PBX and the Contact Center used for call center functionality (calling queue, night service, Interactive Voice Response (IVR) menus, and holidays) can be configured for high availability as hot standby. High availability is only a matter of licenses, hardware and additional costs. This question can be clarified when being sure about how long a voice outage can last for a company and how much the financial losses are for not being available. In case of emergency, let it be on the customer side or on the provider side, an availability through telephony systems is mandatory.

Techniques like pseudonymization and HMAC encryption can be applied on the CDRs fields itself to be aware of information disclosure and data breaches. Such sensitive data of a telephone system, which can be fraudulently used, must of course be secured.

7.4.2 Determining Privacy Threats

Deng et al. [DWSPJ11] introduced a privacy threat model that shows a threat for each privacy property presented in Table 6.4.

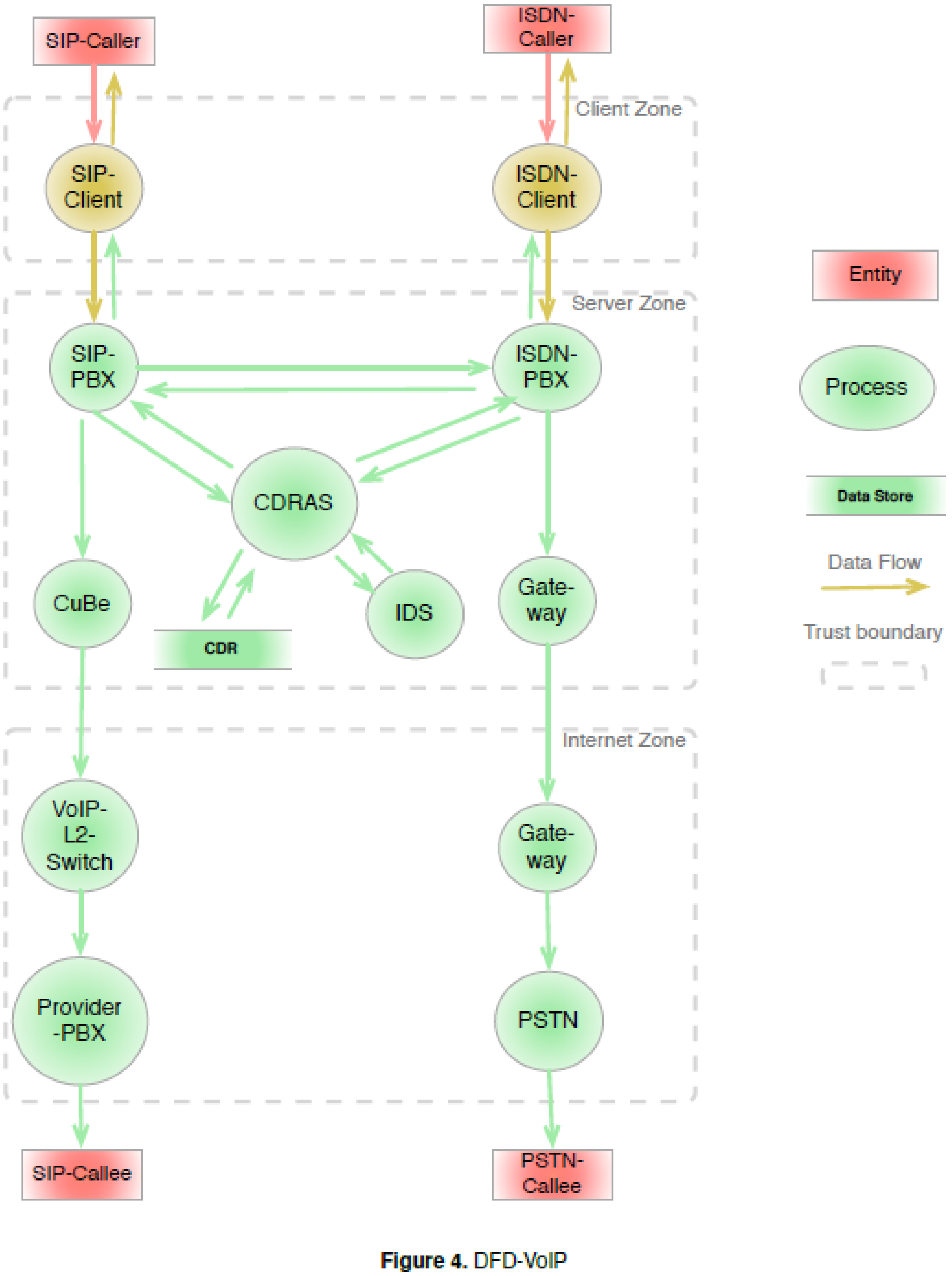


Figure 7.8: DFD-VoIP

It is claimed that the privacy properties unlinkability, anonymity and pseudonymity, plausible deniability, undetectability and unobservability, and confidentiality are classified as hard privacy. The goal of hard privacy is data minimization. This goal includes the assumption that personal data is not disclosed to a third party. The terms plausible deniability and confidentiality are not introduced by the Pfitzmann terminology.

Plausible deniability is the ability to deny that a certain action was performed. An attacker cannot prove that a user has done something, or said something. Confidentiality is hiding or controlled release of information. The remaining privacy properties are classified as soft privacy. Soft privacy is based upon the assumption that stakeholders have already lost the control of personal data. Hence, stakeholders have to trust another stakeholder to control the use of their personal data. The goal of soft privacy is to provide data security and process data only for a specific purpose and with an informed consent. The content awareness property makes sure that stakeholders are aware of their personal information.

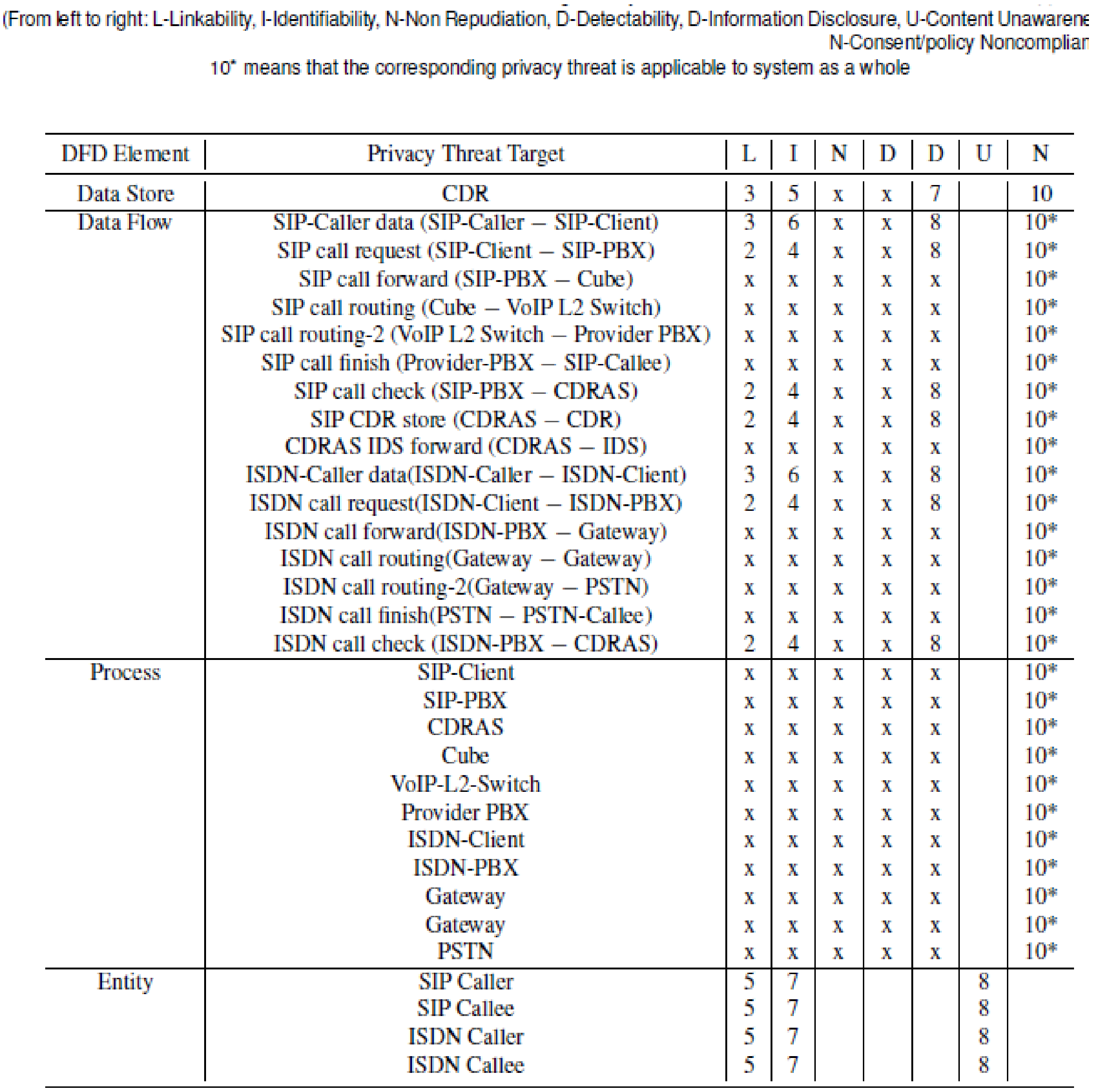
They also have to specify consent in compliance with legislation for the stakeholders that shall enter personal information into a system. Stakeholders that enter personal information into the system have to constant to these policies, before their personal information is entered into the system. The privacy threats for CDRs are listed in Table 6.5. A “+” in Table 6.5 marks a privacy threat to a CDRs field or a stakeholder.

However, the free cells of the table do not imply that a CDRs field or stakeholder is not subject to a privacy threat. Figure 7.8 states the relations between privacy threat categories and DFD elements. These relations are used as a foundation for Table 7.1. A scale from 1 to 10 is used to estimate the privacy risk of a DFD element. A “+”states that there exists a privacy risk that cannot be quantified. An empty field states that this type of DFD element is not subject to a privacy risk according to Table 7.2.

7.4.3 Misuse Cases

Several solution strategies exist for fulfilling privacy requirements [DWSPJ11]:

- A solution for low risk threats is to warn users
- Turning the risk to zero can only be achieved via removing or turning off the feature that causes the privacy threat
- Using countermeasures for privacy threats in the form of preventive or reactive PETs



(From left to right: L-Linkability, I-Identifiability, N-Non Repudiation, D̄-Detectability, D-Information Disclosure, U-Content Unawarene
N-Consent/policy Noncomplian
10* means that the corresponding privacy threat is applicable to system as a whole

DFD Element	Privacy Threat Target	L	I	N	D	D	U	N
Data Store	CDR	3	5	x	x	7		10
Data Flow	SIP-Caller data (SIP-Caller – SIP-Client)	3	6	x	x	8		10*
	SIP call request (SIP-Client – SIP-PBX)	2	4	x	x	8		10*
	SIP call forward (SIP-PBX – Cube)	x	x	x	x	x		10*
	SIP call routing (Cube – VoIP L2 Switch)	x	x	x	x	x		10*
	SIP call routing-2 (VoIP L2 Switch – Provider PBX)	x	x	x	x	x		10*
	SIP call finish (Provider-PBX – SIP-Callee)	x	x	x	x	x		10*
	SIP call check (SIP-PBX – CDRAS)	2	4	x	x	8		10*
	SIP CDR store (CDRAS – CDR)	2	4	x	x	8		10*
	CDRAS IDS forward (CDRAS – IDS)	x	x	x	x	x		10*
	ISDN-Caller data(ISDN-Caller – ISDN-Client)	3	6	x	x	8		10*
	ISDN call request(ISDN-Client – ISDN-PBX)	2	4	x	x	8		10*
	ISDN call forward(ISDN-PBX – Gateway)	x	x	x	x	x		10*
	ISDN call routing(Gateway – Gateway)	x	x	x	x	x		10*
	ISDN call routing-2(Gateway – PSTN)	x	x	x	x	x		10*
	ISDN call finish(PSTN – PSTN-Callee)	x	x	x	x	x		10*
	ISDN call check (ISDN-PBX – CDRAS)	2	4	x	x	8		10*
Process	SIP-Client	x	x	x	x	x		10*
	SIP-PBX	x	x	x	x	x		10*
	CDRAS	x	x	x	x	x		10*
	Cube	x	x	x	x	x		10*
	VoIP-L2-Switch	x	x	x	x	x		10*
	Provider PBX	x	x	x	x	x		10*
	ISDN-Client	x	x	x	x	x		10*
	ISDN-PBX	x	x	x	x	x		10*
	Gateway	x	x	x	x	x		10*
	Gateway	x	x	x	x	x		10*
	PSTN	x	x	x	x	x		10*
Entity	SIP Caller	5	7				8	
	SIP Callee	5	7				8	
	ISDN Caller	5	7				8	
	ISDN Callee	5	7				8	

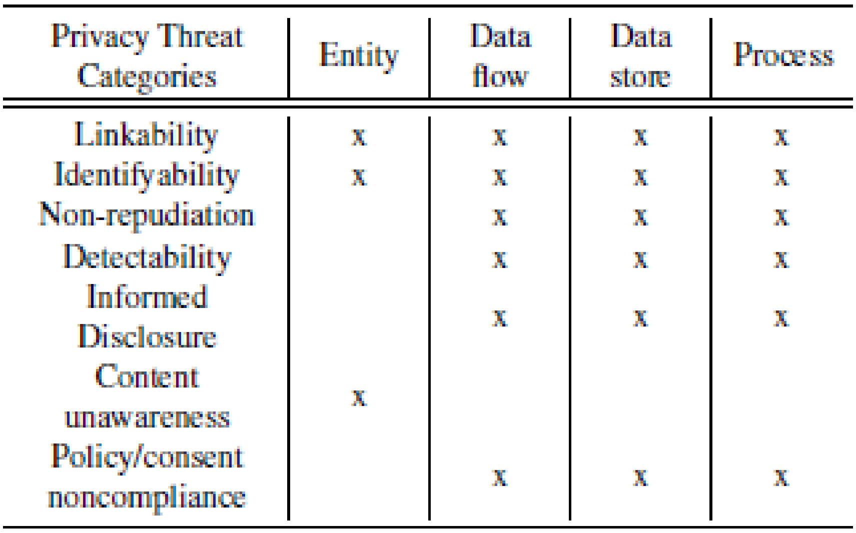
Table 7.1: Determining Privacy Threats for DFD Elements within the CDRAS application

The callers and callees shall be warned that their CDRs are analyzed for the purpose of preventing attacks. The feature can be adopted in such a way that users can object to it and it is turned off for these users. However, the priority is to apply countermeasures to the privacy threats and enable a privacy preserving analysis feature. The use cases are based on the threats identified in Table 7.1. In order to identify suitable PETs, a number of misuse cases for privacy are presented in the given scenario. These are derived from the information collected in the method up to this point and the privacy threat tree from Deng et al. [DWSPJ11].

The selection of PETs is based upon [DWSPJ11, WSDJ09, KKG08, and JOURNAL7]. The author presents short misuse cases, derives privacy requirements and resulting privacy mechanisms in Table 6.6., but does not provide a detailed pattern for misuse cases.

7.4.4 Usage Example

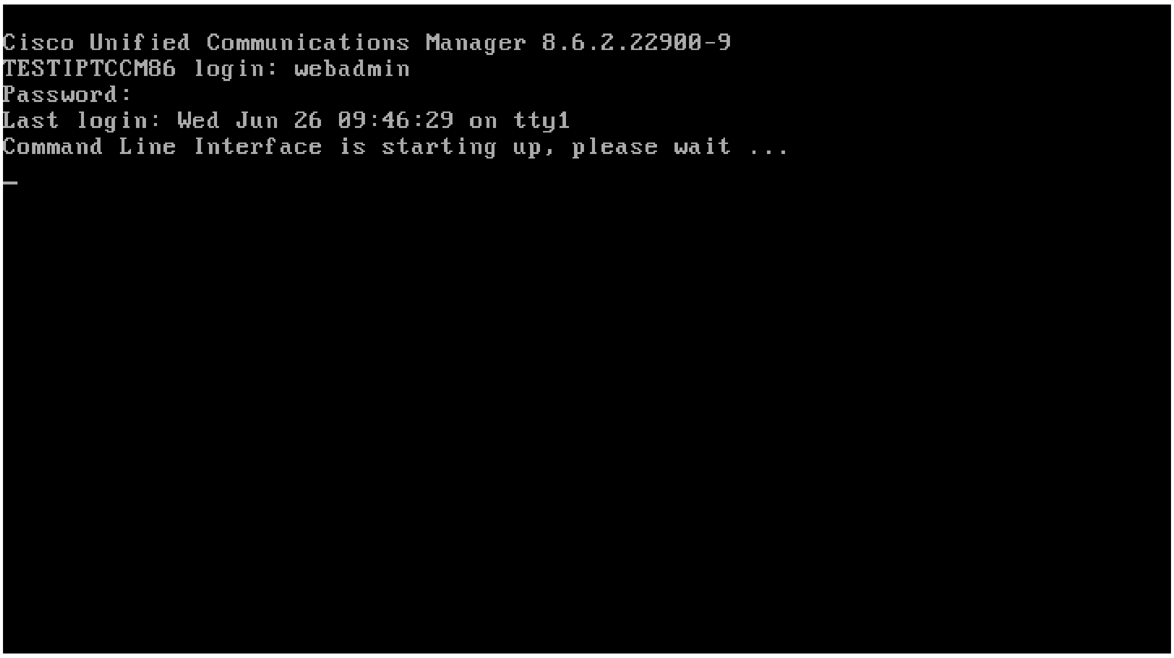
To access the CDRs data store, the user has to be member of the administrators group. This privilege is given by the PBX administrator. For all logins to the CDRs data store, the access log is written. The access log is the summary of all access and change attempts within the CDRs data store. The change record includes the user name, date, time, window from which the change was made, and the success or failure status of the update. Different groups and roles can be selected for users to grant or deny access to certain resources.



Privacy Threat Categories	Entity	Data flow	Data store	Process
Linkability	x	x	x	x
Identifyability	x	x	x	x
Non-repudiation		x	x	x
Detectability		x	x	x
Informed Disclosure		x	x	x
Content unawareness	x			
Policy/consent noncompliance		x	x	x

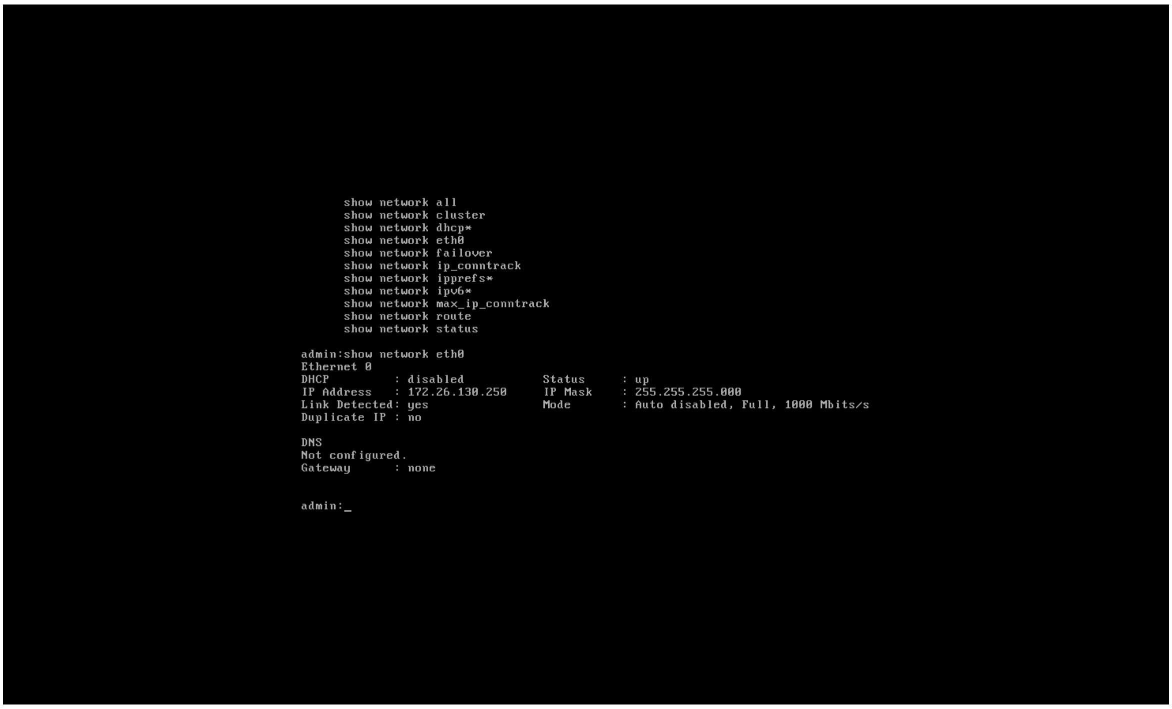
Table 7.2: Mapping LINDDUN components (privacy threats) to DFD element types (taken from [DWSPJ11])

The following screenshots give an idea of the prototype implementation and how it is possible to extract data and get results. The first two screenshots are made from the Cisco Unified Communications Manager command line. The Call manager is installed on a virtual machine running on VMware Workstation.



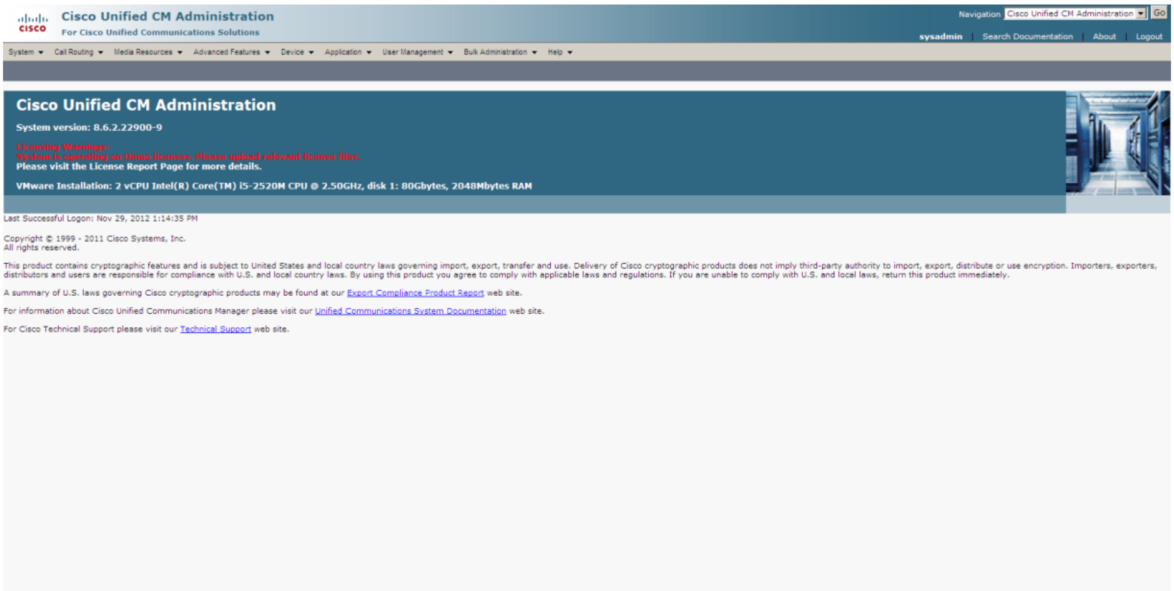
```
Cisco Unified Communications Manager 8.6.2.22900-9
TESTIPTCCM86 login: webadmin
Password:
Last login: Wed Jun 26 09:46:29 on tty1
Command Line Interface is starting up, please wait ...
_
```

Figure 7.9: Cisco Unified Communications Manager 8.6.2.22900-9 Command Line interface



```
      show network all
      show network cluster
      show network dhcp*
      show network eth0
      show network failover
      show network ip_conntrack
      show network ipprefs*
      show network ipv6*
      show network max_ip_conntrack
      show network route
      show network status

admin:show network eth0
Ethernet 0
DHCP          : disabled           Status      : up
IP Address    : 172.26.130.250     IP Mask     : 255.255.255.000
Link Detected: yes                 Mode        : Auto disabled, Full, 1000 Mbits/s
Duplicate IP : no

DNS
Not configured.
Gateway       : none


admin:_
```

Figure 7.10: Cisco Unified Communications Manager Network settings


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
sysadmin | Search Documentation | About | Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help

Cisco Unified CM Administration

System version: 8.6.2.22900-9

Licensing Warnings:
System is operating on Demo licenses. Please upload relevant license files.
Please visit the License Report Page for more details.

VMware Installation: 2 vCPU Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz, disk 1: 80Gbytes, 2048Mbytes RAM

Last Successful Logon: Nov 29, 2012 1:14:35 PM

Copyright © 1999 - 2011 Cisco Systems, Inc.
All rights reserved.

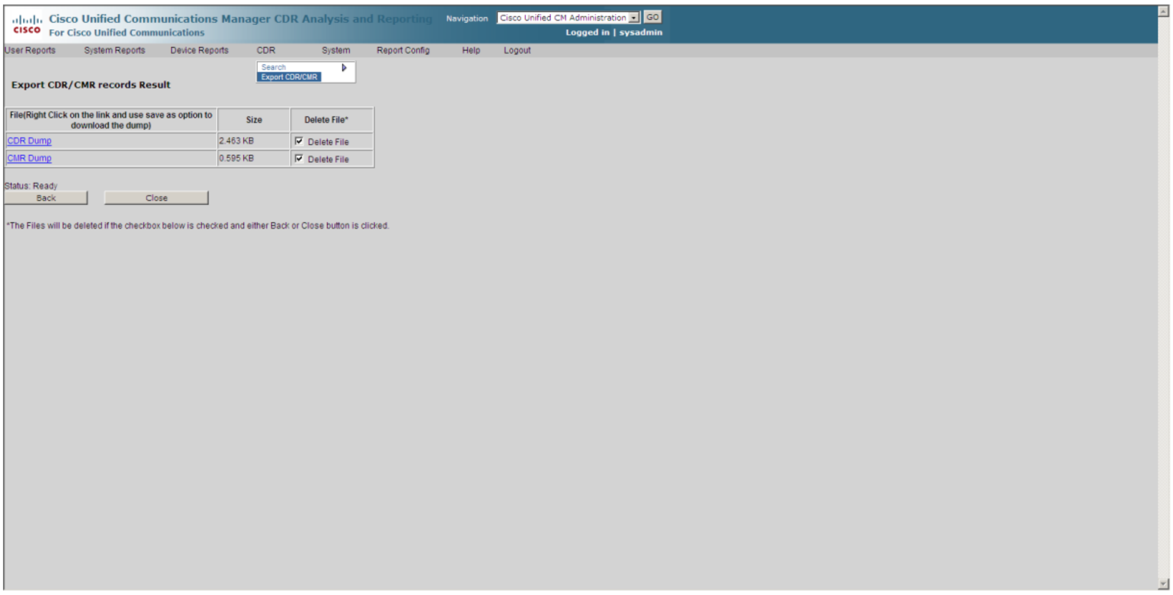
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

Figure 7.11: Cisco Unified CM Administration System version 8.6.2.22900-9 GUI



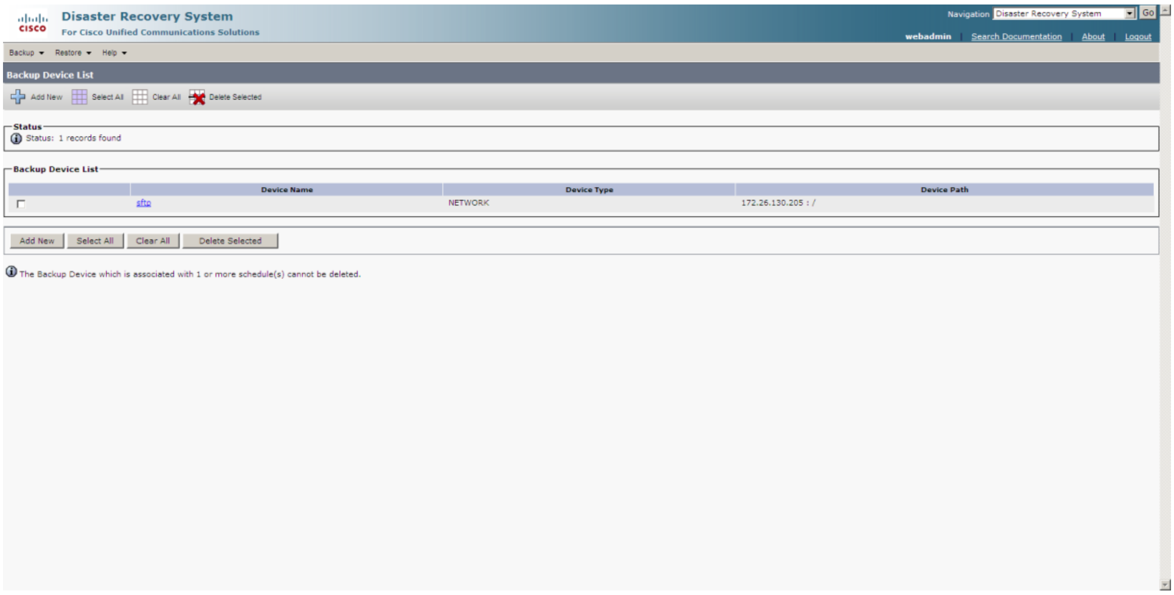
Export CDR/CMR records Result

File(Right Click on the link and use save as option to download the dump)	Size	Delete File*
CDR Dump	2.463 KB	☑ Delete File
CMR Dump	0.595 KB	☑ Delete File

Status: Ready

*The Files will be deleted if the checkbox below is checked and either Back or Close button is clicked.

Figure 7.12: Cisco Unified Communications Manager CDR Analysis and Reporting Export



Status

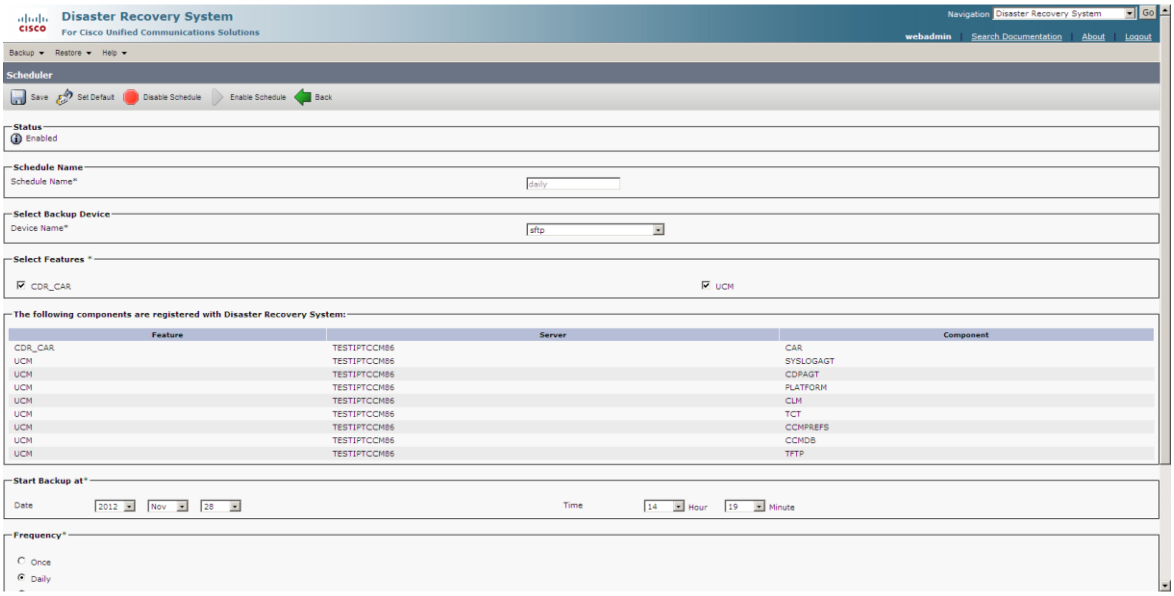
Status: 1 records found

Backup Device List

	Device Name	Device Type	Device Path
□	sftp	NETWORK	172.26.130.205 : /

The Backup Device which is associated with 1 or more schedule(s) cannot be deleted.

Figure 7.13: Cisco Unified Communications Manager Disaster Recovery Backup Device


Disaster Recovery System
For Cisco Unified Communications Solutions
Navigation Disaster Recovery System Go
webadmin | Search Documentation | About | Logout
Backup Restore Help
Scheduler
Save Set Default Disable Schedule Enable Schedule Back

Status
Enabled

Schedule Name
Schedule Name* daily

Select Backup Device
Device Name* sftp

Select Features *
☑ CDR_CAR ☑ UCM

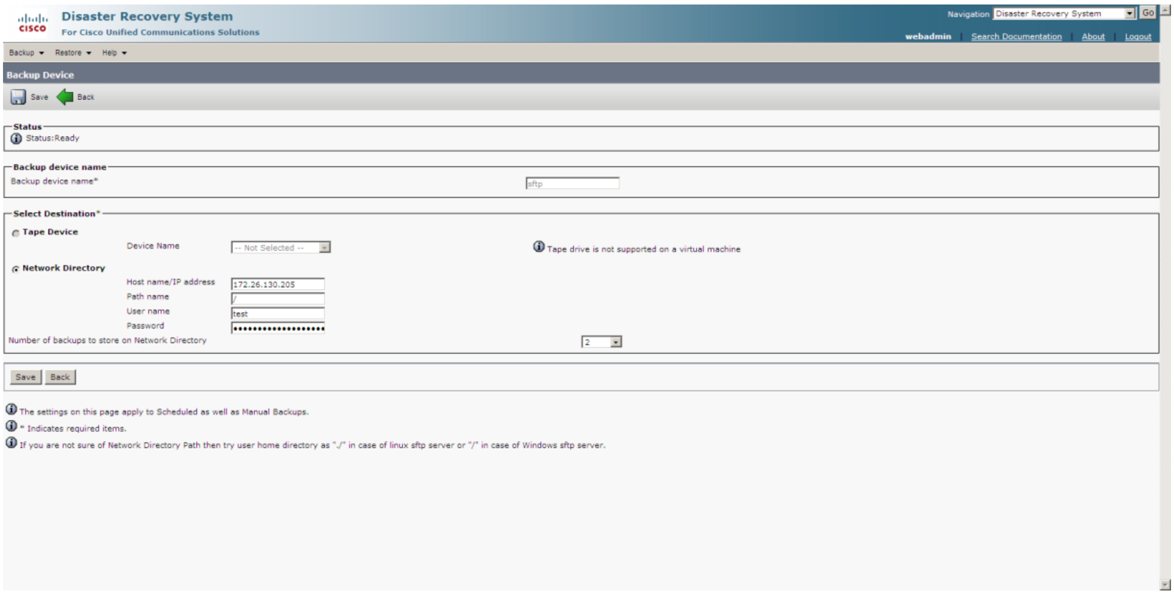
The following components are registered with Disaster Recovery System:

Feature	Server	Component
CDR_CAR	TESTIPTCCM86	CAR
UCM	TESTIPTCCM86	SYSLOGAGT
UCM	TESTIPTCCM86	CDPAGT
UCM	TESTIPTCCM86	PLATFORM
UCM	TESTIPTCCM86	CLM
UCM	TESTIPTCCM86	TCT
UCM	TESTIPTCCM86	CCMPREFS
UCM	TESTIPTCCM86	CCMDB
UCM	TESTIPTCCM86	TFTP

Start Backup at*
Date 2012 Nov 28 Time 14 Hour 19 Minute

Frequency*
○ Once
● Daily

Figure 7.14: Cisco Unified Communications Manager Backup Schedule


Disaster Recovery System
For Cisco Unified Communications Solutions
Navigation Disaster Recovery System Go
webadmin | Search Documentation | About | Logout
Backup Restore Help
Backup Device
Save Back

Status
Status:Ready

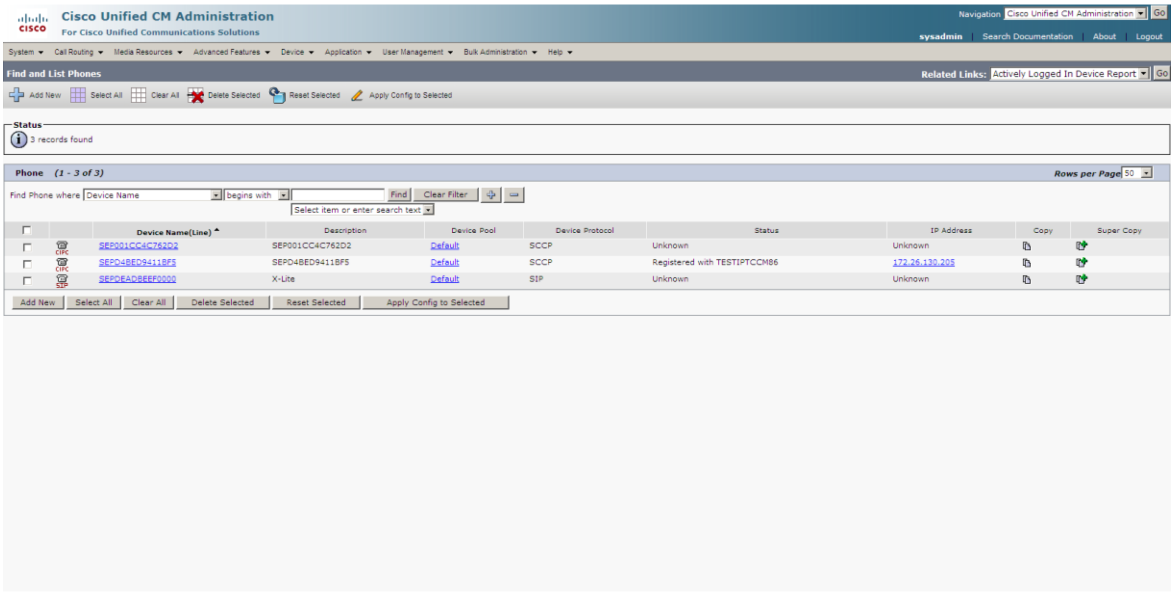
Backup device name
Backup device name* sftp

Select Destination*
○ Tape Device
Device Name -- Not Selected --
Tape drive is not supported on a virtual machine
● Network Directory
Host name/IP address 172.26.130.205
Path name /
User name test
Password ••••••••••••••••••••
Number of backups to store on Network Directory 2

Save Back

The settings on this page apply to Scheduled as well as Manual Backups.
* Indicates required items.
If you are not sure of Network Directory Path then try user home directory as "./" in case of linux sftp server or "/" in case of Windows sftp server.

Figure 7.15: Cisco Unified Communications Manager Backup Device Settings


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Find and List Phones
Related Links: Actively Logged In Device Report Go
Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Status
3 records found

Phone (1 - 3 of 3) Rows per Page 50

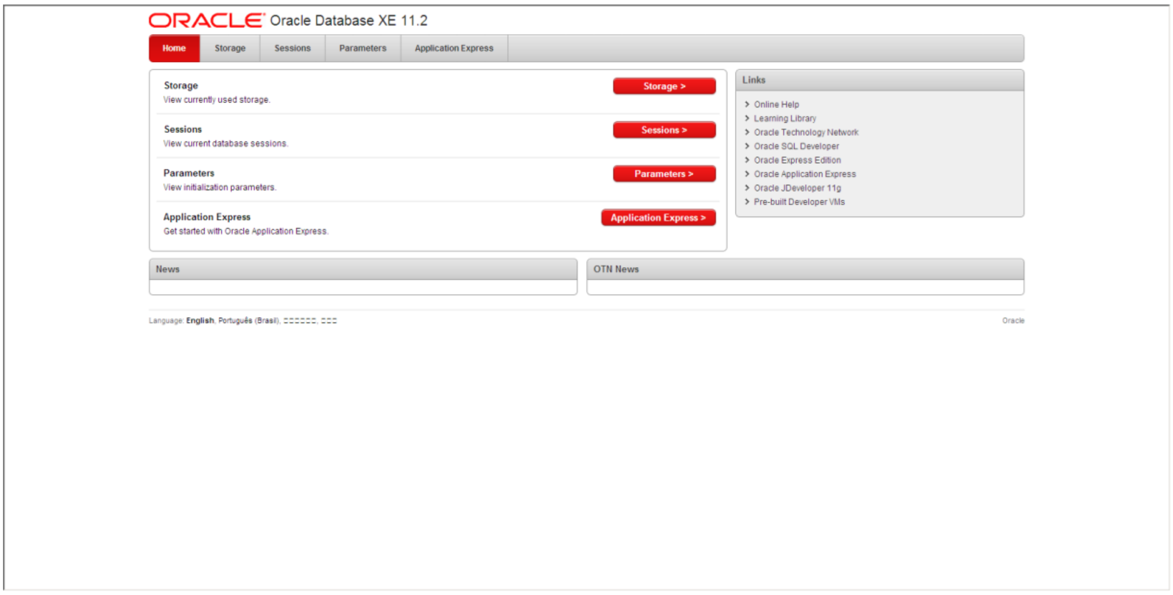
Find Phone where Device Name begins with Find Clear Filter
Select item or enter search text

□		Device Name(Line) ▲	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
□	☎ CIPC	SEP001CC4C762D2	SEP001CC4C762D2	Default	SCCP	Unknown	Unknown	⎘	⎘
□	☎ CIPC	SEPD4BED9411BF5	SEPD4BED9411BF5	Default	SCCP	Registered with TESTIPTCCM86	172.26.130.205	⎘	⎘
□	☎ SIP	SEPDEADBEEF0000	X-Lite	Default	SIP	Unknown	Unknown	⎘	⎘

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Figure 7.16: Cisco Unified Communications Manager Phone Devices

The following screenshots are taken from the local database of the management PC. After extracting the CDRs, the files are imported and analyzed in the free Oracle database.



Storage
View currently used storage.

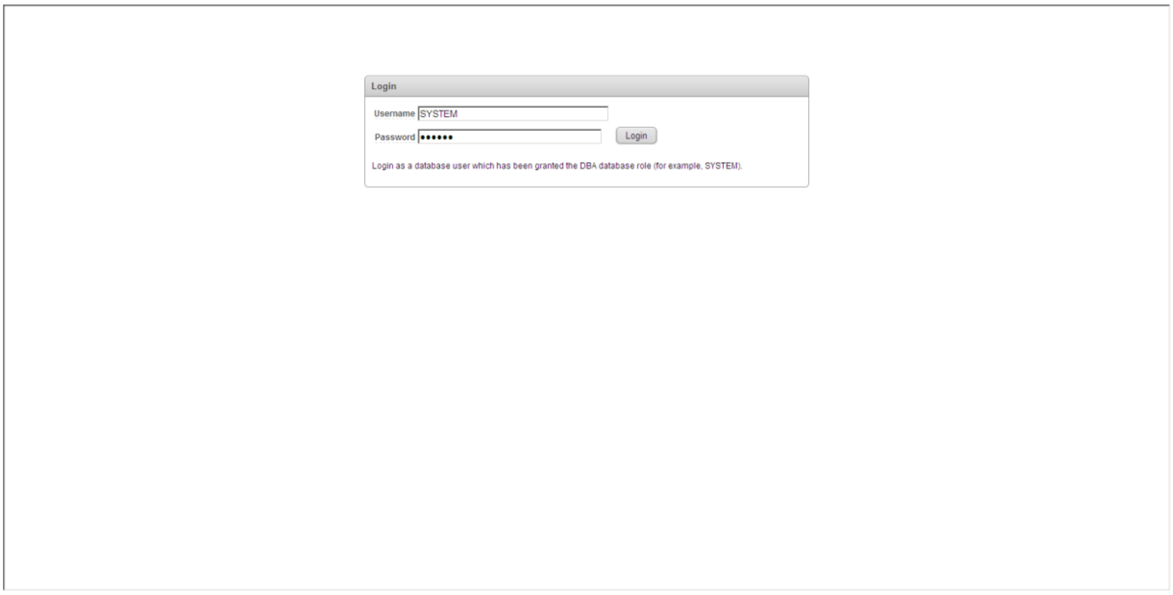
Sessions
View current database sessions.

Parameters
View initialization parameters.

Application Express
Get started with Oracle Application Express.

Language: English, Português (Brasil), □□□□□□, □□□

Figure 7.17: Oracle Database Application Express XE 11.2 GUI

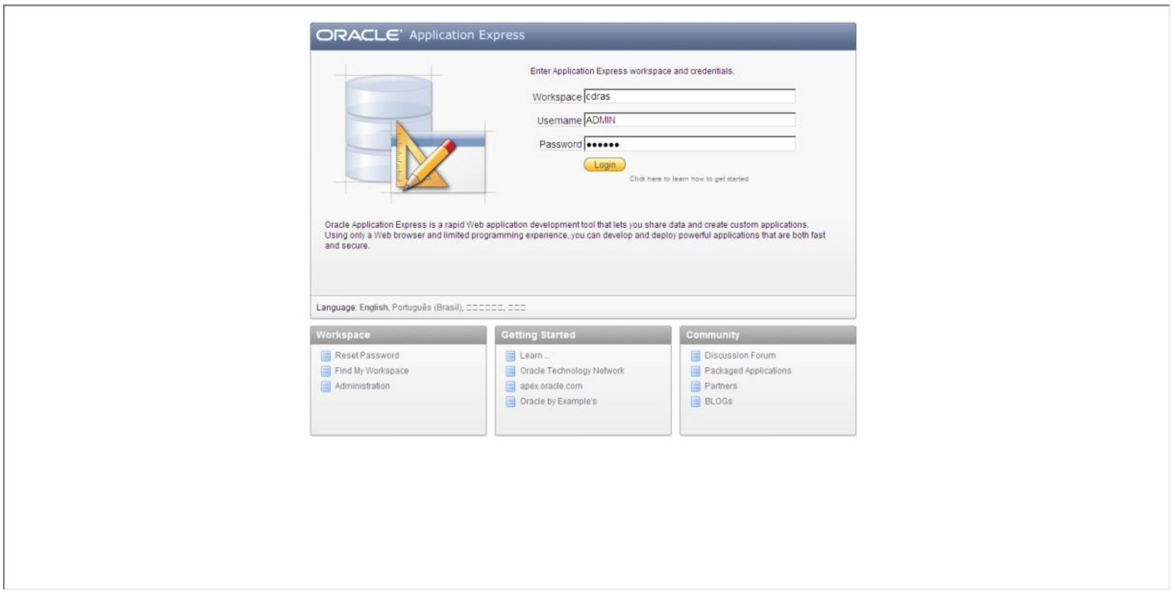


Username SYSTEM

Password ••••••

Login as a database user which has been granted the DBA database role (for example, SYSTEM).

Figure 7.18: Login Oracle Database Application Express



Enter Application Express workspace and credentials.

Workspace cdras

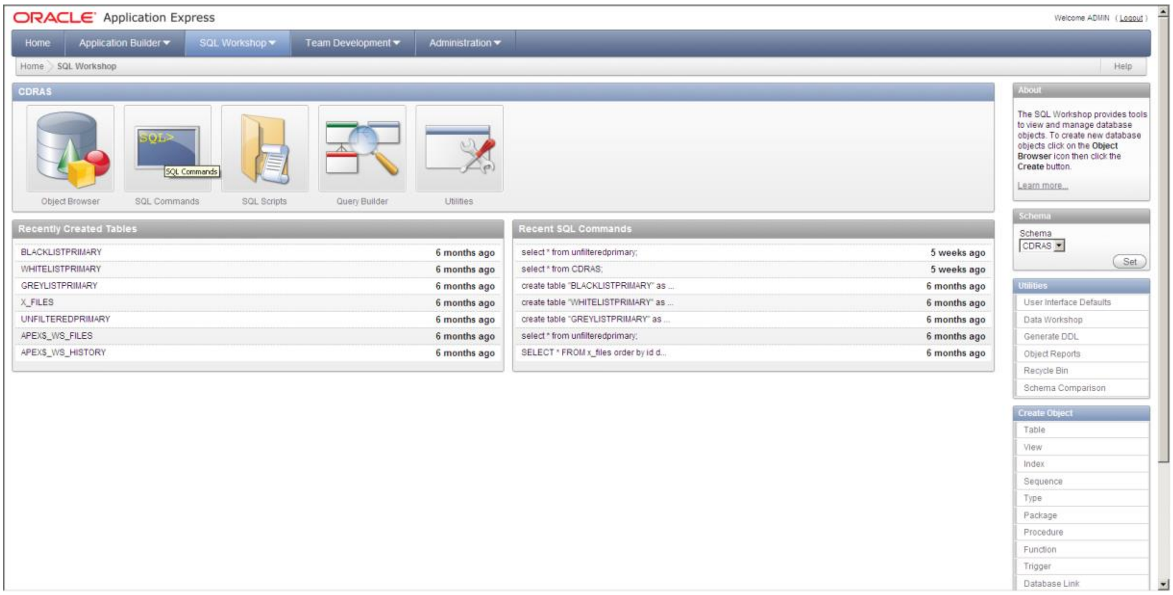
Username ADMIN

Password ••••••

Oracle Application Express is a rapid Web application development tool that lets you share data and create custom applications. Using only a Web browser and limited programming experience, you can develop and deploy powerful applications that are both fast and secure.

Language: English, Português (Brasil), □□□□□□, □□□

Figure 7.19: Enter Oracle Application Express Workspace



About

The SQL Workshop provides tools to view and manage database objects. To create new database objects click on the Object Browser icon then click the Create button.

Learn more...

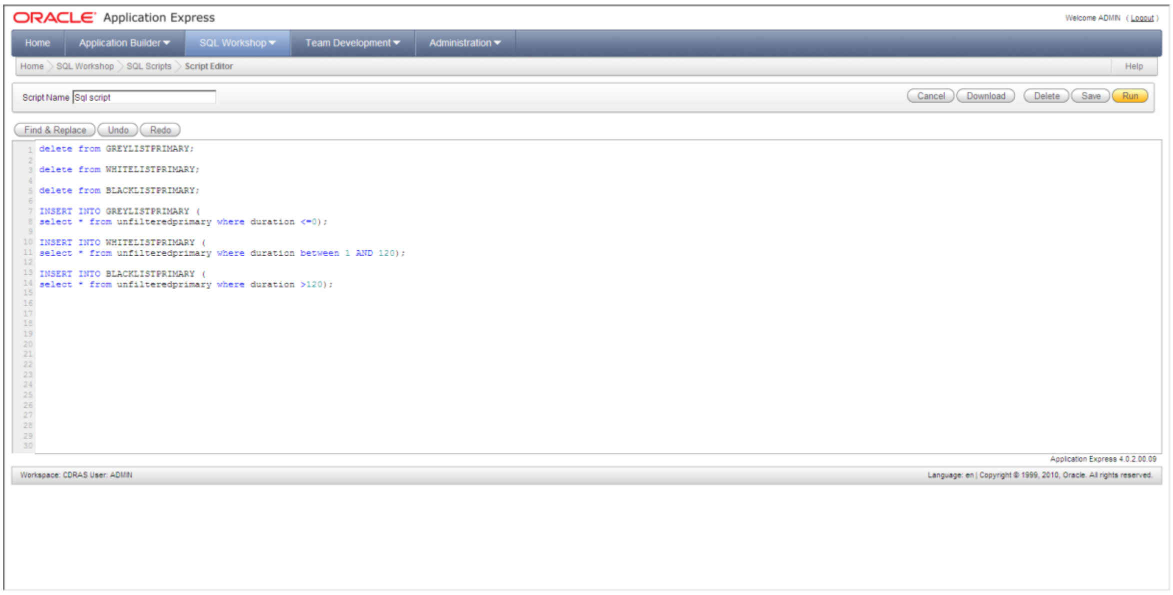
Schema: CDRAS

Recently Created Tables	
BLACKLISTPRIMARY	6 months ago
WHITELISTPRIMARY	6 months ago
GREYLISTPRIMARY	6 months ago
X_FILES	6 months ago
UNFILTEREDPRIMARY	6 months ago
APEX$_WS_FILES	6 months ago
APEX$_WS_HISTORY	6 months ago

Recent SQL Commands	
select * from unfilteredprimary;	5 weeks ago
select * from CDRAS;	5 weeks ago
create table "BLACKLISTPRIMARY" as ...	6 months ago
create table "WHITELISTPRIMARY" as ...	6 months ago
create table "GREYLISTPRIMARY" as ...	6 months ago
select * from unfilteredprimary;	6 months ago
SELECT * FROM x_files order by id d...	6 months ago

Figure 7.20: Oracle Application Express Database Tables and SQL commands

The following screenshot is representing the attack patterns in terms of duration and filters out possible attacks.



Script Name: Sql script

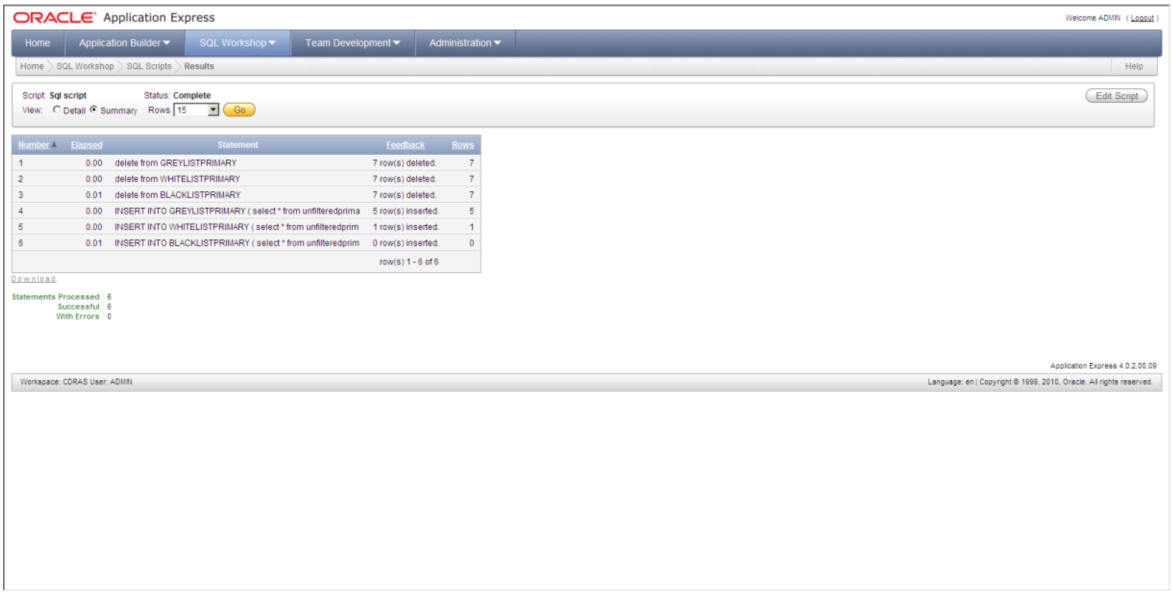
```
delete from GREYLISTPRIMARY;

delete from WHITELISTPRIMARY;

delete from BLACKLISTPRIMARY;

INSERT INTO GREYLISTPRIMARY (
select * from unfilteredprimary where duration <=0);

INSERT INTO WHITELISTPRIMARY (
select * from unfilteredprimary where duration between 1 AND 120);

INSERT INTO BLACKLISTPRIMARY (
select * from unfilteredprimary where duration >120);
```

Application Express 4.0.2.00.09

Workspace: CDRAS User: ADMIN

Language: en | Copyright © 1999, 2010, Oracle. All rights reserved.

Figure 7.21: Oracle Application Express SQL script editor


ORACLE Application Express
Welcome ADMIN (Logout)
Home
Application Builder
SQL Workshop
Team Development
Administration
Home > SQL Workshop > SQL Scripts > Results
Help
Edit Script
Go
Download
Application Express 4.0.2.00.09
Language: en | Copyright © 1999, 2010, Oracle. All rights reserved.

Script: Sql script Status: Complete

View: ○ Detail ● Summary Rows 15

Number	Elapsed	Statement	Feedback	Rows
1	0.00	delete from GREYLISTPRIMARY	7 row(s) deleted.	7
2	0.00	delete from WHITELISTPRIMARY	7 row(s) deleted.	7
3	0.01	delete from BLACKLISTPRIMARY	7 row(s) deleted.	7
4	0.00	INSERT INTO GREYLISTPRIMARY (select * from unfilteredprima	5 row(s) inserted.	5
5	0.00	INSERT INTO WHITELISTPRIMARY (select * from unfilteredprim	1 row(s) inserted.	1
6	0.01	INSERT INTO BLACKLISTPRIMARY (select * from unfilteredprim	0 row(s) inserted.	0
			row(s) 1 - 6 of 6	

Statements Processed	6
Successful	6
With Errors	0

Workspace: CDRAS User: ADMIN

Figure 7.22: Oracle Application Express Script Execution

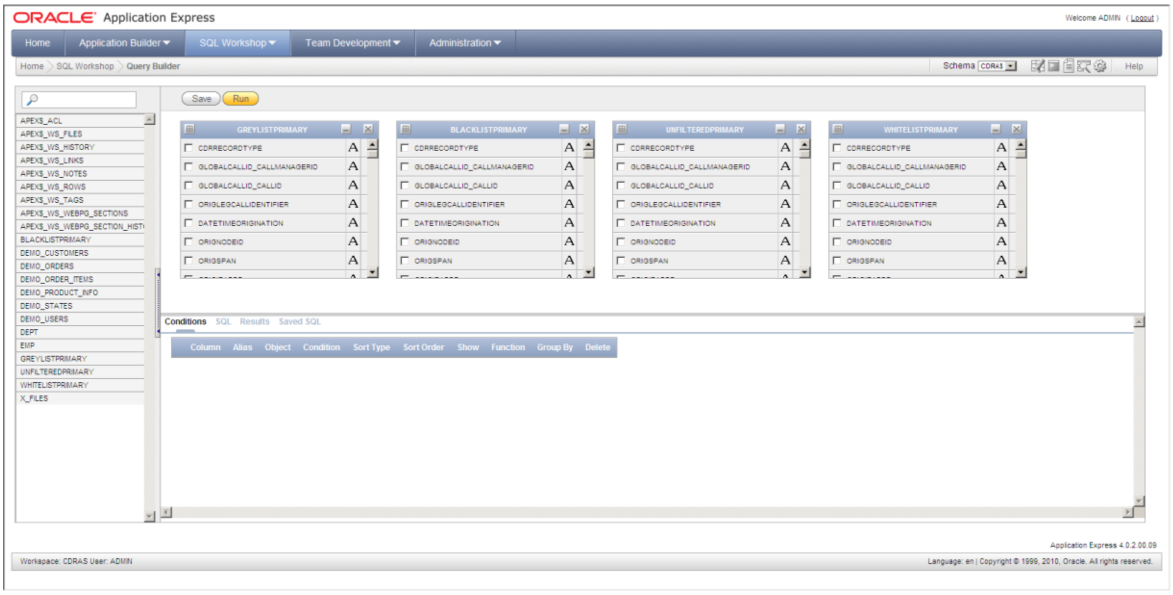
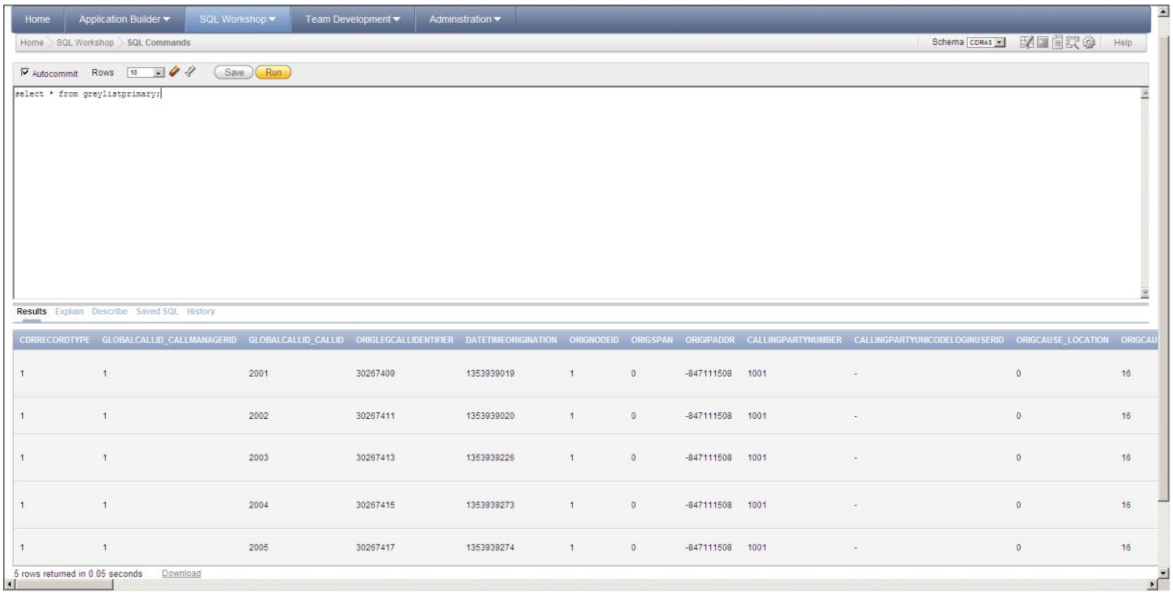


Figure 7.23: Oracle Application Express Databases



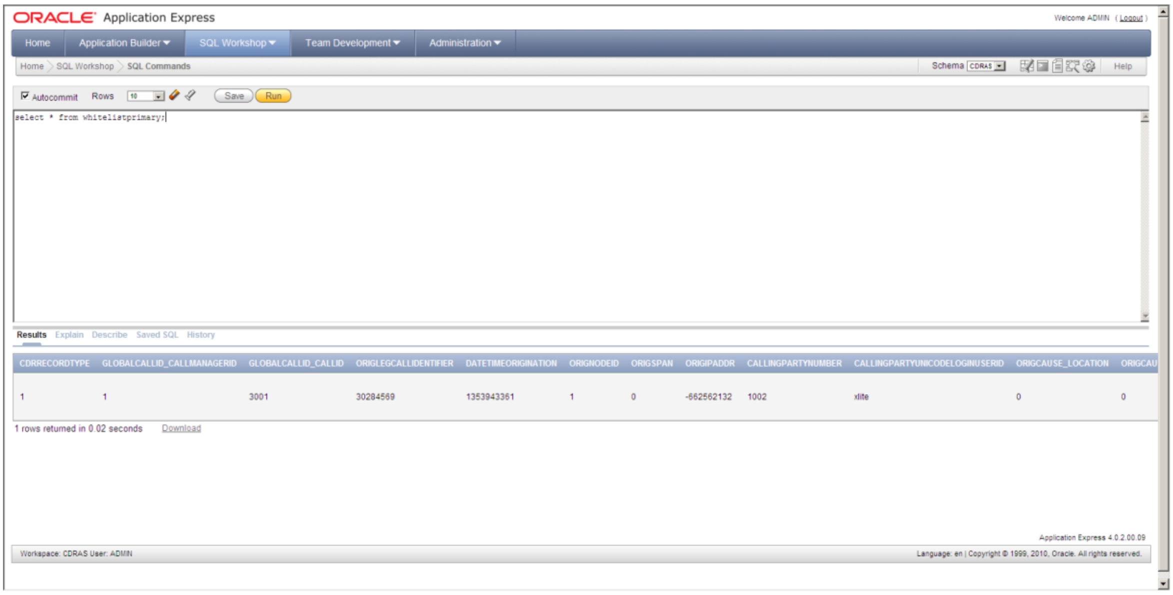
```
select * from greylistprimary;
```

CDRRECORDTYPE	GLOBALCALLID_CALLMANAGERID	GLOBALCALLID_CALLID	ORIGLEGCALLIDENTIFIER	DATETIMEORIGINATION	ORIGNODEID	ORIGSPAN	ORIGIPADDR	CALLINGPARTYNUMBER	CALLINGPARTYUNICODELOGINUSERID	ORIGCAUSE_LOCATION	ORIGCAU
1	1	2001	30267409	1353939019	1	0	-847111508	1001	-	0	16
1	1	2002	30267411	1353939020	1	0	-847111508	1001	-	0	16
1	1	2003	30267413	1353939226	1	0	-847111508	1001	-	0	16
1	1	2004	30267415	1353939273	1	0	-847111508	1001	-	0	16
1	1	2005	30267417	1353939274	1	0	-847111508	1001	-	0	16

5 rows returned in 0.05 seconds

Figure 7.24: Oracle Application Express Content of table greylistprimary

Different database queries are verifying the system status and health. These checks have to be done on a regular basis and to carry out possible corrective mechanisms.

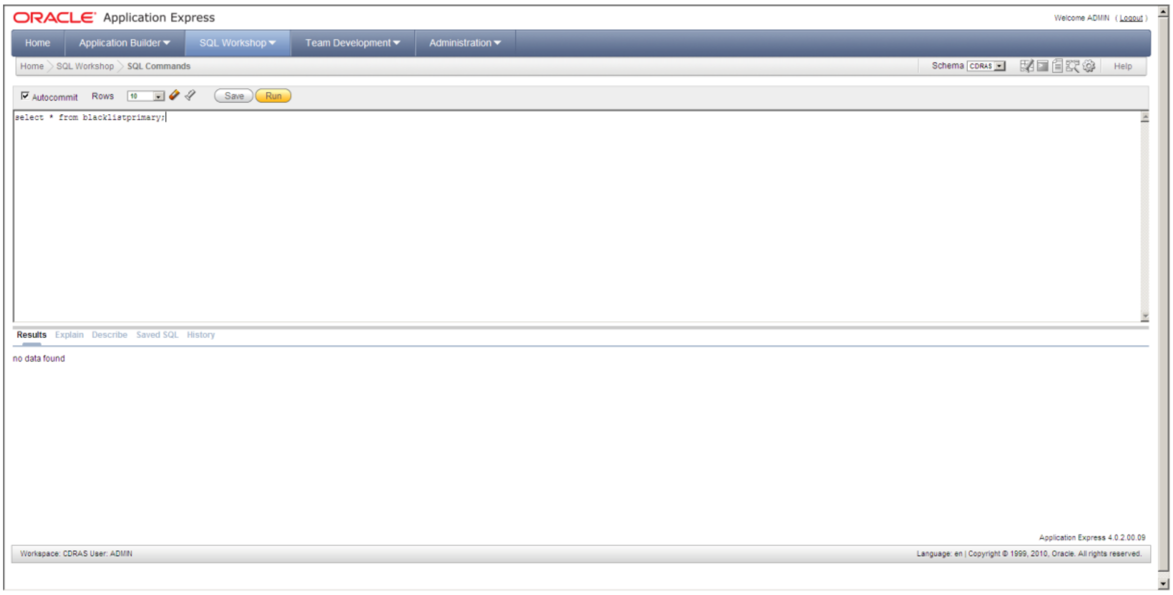

ORACLE Application Express
Welcome ADMIN (Logout)
Home
Application Builder
SQL Workshop
Team Development
Administration
Home > SQL Workshop > SQL Commands
Schema CDRAS
Help
☑ Autocommit
Rows 10
Save
Run
Results
Explain
Describe
Saved SQL
History
Download
Application Express 4.0.2.00.09
Workspace: CDRAS User: ADMIN
Language: en | Copyright © 1999, 2010, Oracle. All rights reserved.

```
select * from whitelistprimary;
```

CDRRECORDTYPE	GLOBALCALLID_CALLMANAGERID	GLOBALCALLID_CALLID	ORIGLEGCALLIDENTIFIER	DATETIMEORIGINATION	ORIGNODEID	ORIGSPAN	ORIGIPADDR	CALLINGPARTYNUMBER	CALLINGPARTYUNICODELOGINUSERID	ORIGCAUSE_LOCATION	ORIGCAU
1	1	3001	30284569	1353943361	1	0	-662562132	1002	xlite	0	0

1 rows returned in 0.02 seconds

Figure 7.25: Oracle Application Express Content of table whitelistprimary



```
select * from blacklistprimary;
```

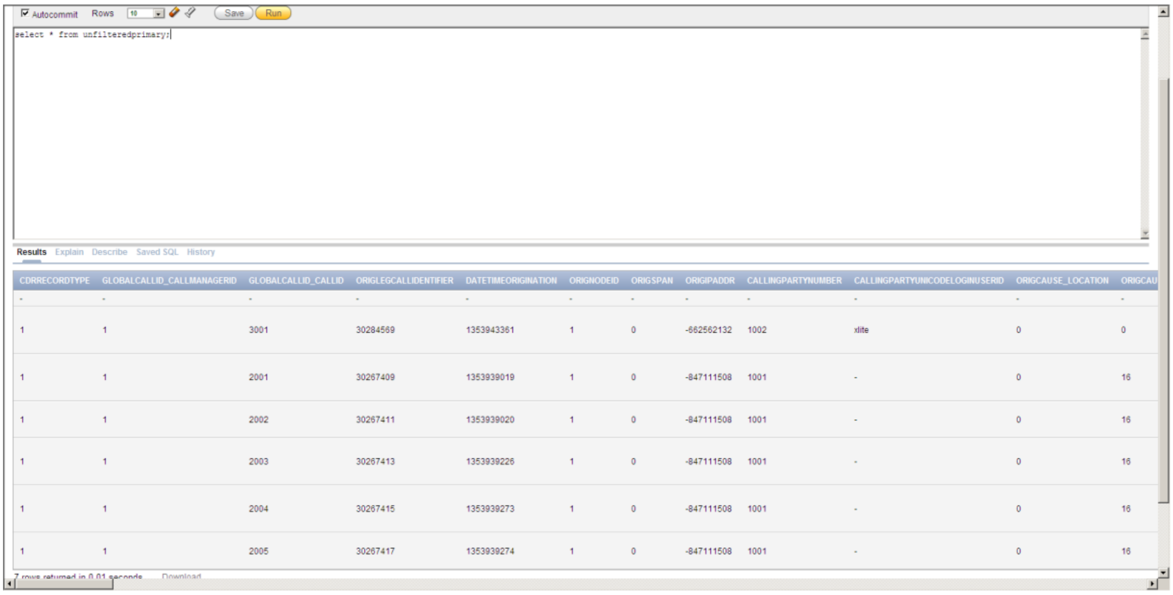
no data found

Application Express 4.0.2.00.09

Workspace: CDRAS User: ADMIN

Language: en | Copyright © 1999, 2010, Oracle. All rights reserved.

Figure 7.26 Oracle Application Express Content of table blacklistprimary



```
select * from unfilteredprimary;
```

CDRRECORDTYPE	GLOBALCALLID_CALLMANAGERID	GLOBALCALLID_CALLID	ORIGLEGCALLIDENTIFIER	DATETIMEORIGINATION	ORIGNODEID	ORIGSPAN	ORIGIPADDR	CALLINGPARTYNUMBER	CALLINGPARTYUNICODELOGINUSERID	ORIGCAUSE_LOCATION	ORIGCAU
-	-	-	-	-	-	-	-	-	-	-	-
1	1	3001	30284569	1353943361	1	0	-662562132	1002	xlite	0	0
1	1	2001	30267409	1353939019	1	0	-847111508	1001	-	0	16
1	1	2002	30267411	1353939020	1	0	-847111508	1001	-	0	16
1	1	2003	30267413	1353939226	1	0	-847111508	1001	-	0	16
1	1	2004	30267415	1353939273	1	0	-847111508	1001	-	0	16
1	1	2005	30267417	1353939274	1	0	-847111508	1001	-	0	16

7 rows returned in 0.01 seconds

Figure 7.27: Oracle Application Express Content of table unfilteredprimary

Normally, administrators will first have a look at blacklisted hosts, to make fast corrections and then inspect the greylist for manual intervention and further analysis. Detailed code examples for SQL code and example CDRs can be seen in Appendix I and Appendix II.

8 Test of the prototype

This chapter looks more at the practical implementation of the prototype and how to verify and analyze it.

Real life cases of toll fraud cost organization losses ranging from a few thousand dollars to hundreds of thousands of dollars [FEMA08, FRA10, and TFA09]. Three kinds of VoIP providers are distinguished. First, there are VoIP providers, who only provide the service to their own company. Second there are providers, who are only offering services to customers who they have a contract with. And third, there are open providers, whose services can be used by anyone, as long as he/she will pay for it. The last example is of course highly vulnerable against toll fraud, where high costs are caused by misuse of calling into the PSTN, as well as satellite mobile phones. It is presented how these attacks could have been avoided via this method.

Three vulnerabilities that lead to VoIP toll fraud are:

- *”Telecom Connectivity Vulnerabilities: Enterprises that use Session Border Controllers (SBC) to secure VoIP and unified communications traffic risk a breach caused by configuration errors, SBC vulnerabilities or functional limitations*
- *Application-level vulnerabilities: Many communications systems are vulnerable to fraud because they have weak passwords and authentication systems*
- *End-point vulnerabilities: Enterprises haven’t instituted much security on users’ devices, especially as unified communications applications are extended to mobile devices, which are much easier to lose than a laptop [SIP09].”*

As Cisco is still commanding close to a third of the worldwide market [CIS11], the example is based on Cisco enterprise routers. “The default behavior for IOS voice gateways is to accept call setups from all sources. As long as voice services are running on the router, the default configuration will treat a call setup from any source IP address as a legitimate and trusted source to set a call up for. Also, FXO ports and inbound calls on ISDN circuits will present secondary-dial tone for inbound calls, allowing for two-stage dialing. This assumes a proper inbound dial-peer is being matched [TFP10]. ”

”Starting with Cisco IOS software version 15.1(2)T, the router’s default behavior is to not trust a call setup from a VoIP source. This feature adds an internal application named TOLLFRAUDAPP to the default call control stack, which checks the source IP of the call setup before routing the call. If the source IP does not match an explicit entry in the configuration as a trusted VoIP source, the call is rejected. The router automatically adds any destinations that are defined as an ipv4 target in a VoIP dial-peer to the trusted source list [TFP10].”

One possibility to stop such toll fraud calls is changing the international dial peer on the voice gateway. It is also not a good idea to have an Internet reachable router with port 5060 (SIP) TCP or UDP and port 1720 (H323) TCP open. These ports can be shut down on the outside interface of the router. Access lists on the voice router should be applied as well, for security reasons. Another possibility is using a dedicated device for the outbound facing functions, a CUBE in Cisco’s world, or SBC with other vendors. The CUBE or SBC is placed between the voice gateway (router) and PBX and therefore knows about every session. Access lists are applied on the voice gateway to block the aforementioned SIP and H.323 ports from external sources.

”The wireless networks, VoIP, and mobile communications pose a variety of novel challenges to the traditional network traffic detection techniques, in terms of the flexibility and adaptability to the particular characteristics of the traffic data. The peculiar characteristics include, but are not limited to, multimedia data, heterogeneous data from multi-standard cyber infrastructures, an influx of high streaming traffic flows, novel noises largely involved in traffic traces, and the short period for updating of cyber infrastructures. A variety of companies can provide services through mobile networks, including the traditional mobile phone and Voice over Internet protocol (VoIP) infrastructures. The good calling quality and reliable service entices more companies to offer mobile services and attract more customers to use them. The investigations have shown that even financial transactions appear in mobile services. These services on mobile devices provide a number of opportunities for hackers to steal valuable information from the digital voice communication [DD11]”.

Real life cases of toll fraud cost organization losses ranging from a few thousand dollars to hundreds of thousands of dollars [COL08, VOI10, and ITP09]. The model shown in chapter 7 is instantiated in Figure 7.3 and Figure 7.4: The PBX is instantiated with Cisco hardware, since Cisco has a significant market share [TEL11]. Hence, the PBX is a Cisco enterprise router as voice gateway and a Cisco Unified Communication Manager (Call manager). In addition, the proposed solution CDRAS and an IDS placed in this call flow, between the PBX and the IP phone, will effectively detect and block the attacker.

8.1 An Example Attack Vector

A possible attack vector for toll fraud is a high frequency of calls to expensive destinations within a short time frame. In this scenario the following call flow is used: IP phone - PBX - Gateway – PSTN [SIP02]. The attacker uses a SIP IP phone. The PBX is owned by a VoIP provider with whom the attacker has a SIP connection. The gateway's duty is to route SIP calls from the PBX to the PSTN network. In addition, the proposed solution CDRAS and an IDS are placed in this call flow, between the PBX and the gateway, which will effectively detect and block the attacker. If a toll fraud attack is underway, numerous SIP messages will be generated from the attacker in a short time frame and, thus, the thresholds in this system will be exceeded. This is because the attacker violates the threshold for timings between call initiations.

It is a matter of the system's configuration. Also the units (seconds or milliseconds) can be chosen. Before a call is sent to the destination and the destination rings, the call is filtered through CDRAS and the IDS. The sequence diagram is instantiated in Figure 5.3 as follows: the initiateCall() method consists of two SIP INVITE messages, the connectCall() consists of SIP 200 OK messages, the denyCall() of SIP 480 Temporarily Unavailable messages or SIP 486 User Busy messages, the forbidCall() with a SIP 603 Decline message and allowCall() with RTP messages, which contain the voice data. The fact that more than the default two SIP INVITE messages are sent, is characteristic for a timing attack. The messages in Figure 5.3, matchPattern(), issueHostLists(), updateHostLists(), intrusionDetected(), and noIntrusionDetected() between the PBX and CDRAS and vice versa and CDRAS and the IDS and vice versa are Extensible Markup Language (XML)-based messages [XML98]. The format makes it easy to edit and add or delete entries of the lists and patterns. Part of the messages will be the number of sessions (numeric number, e.g. 200), the duration of the calls (time interval, e.g. 60 seconds) and the time between the calls (time interval, e.g. 4 milliseconds). The messages are ordered by the time, the messages are arriving.

In addition, the correct configuration of the devices in the call flow is part of this approach. The standard configuration of the PBX involved opens a gateway connection from the SIP network to the PSTN gateway on specific ports per default.

This behavior needs to be modified, before the CDRAS approach is integrated into the call flow. Real world traffic tests are currently conducted with an industry partner. The test results give an answer to the question how good the approach is and against which attacks it can defend. The prototype is implemented with test data of an industry partner and attack patterns are built into the test data. From run-time perspective, there have not been any problems analyzing the data so far. The overall performance is good.

”The wireless networks, VoIP, and mobile communications pose a variety of novel challenges to the traditional network traffic detection techniques, in terms of the flexibility and adaptability to the particular characteristics of the traffic data. The peculiar characteristics include, but are not limited to, multimedia data, heterogeneous data from multi-standard cyber infrastructures, an influx of high streaming traffic flows, novel noises largely involved in traffic traces, and the short period for updating of cyber infrastructures. A variety of companies can provide services through mobile networks, including the traditional mobile phone and VoIP infrastructures. The good call quality and reliable service entices more companies to offer mobile services and attract more customers to use them. The investigations have shown that even financial transactions appear in mobile services. These services on mobile devices provide a number of opportunities for hackers to steal valuable information from the digital voice communication [DD11]”.

8.2 Example Attack Scenario

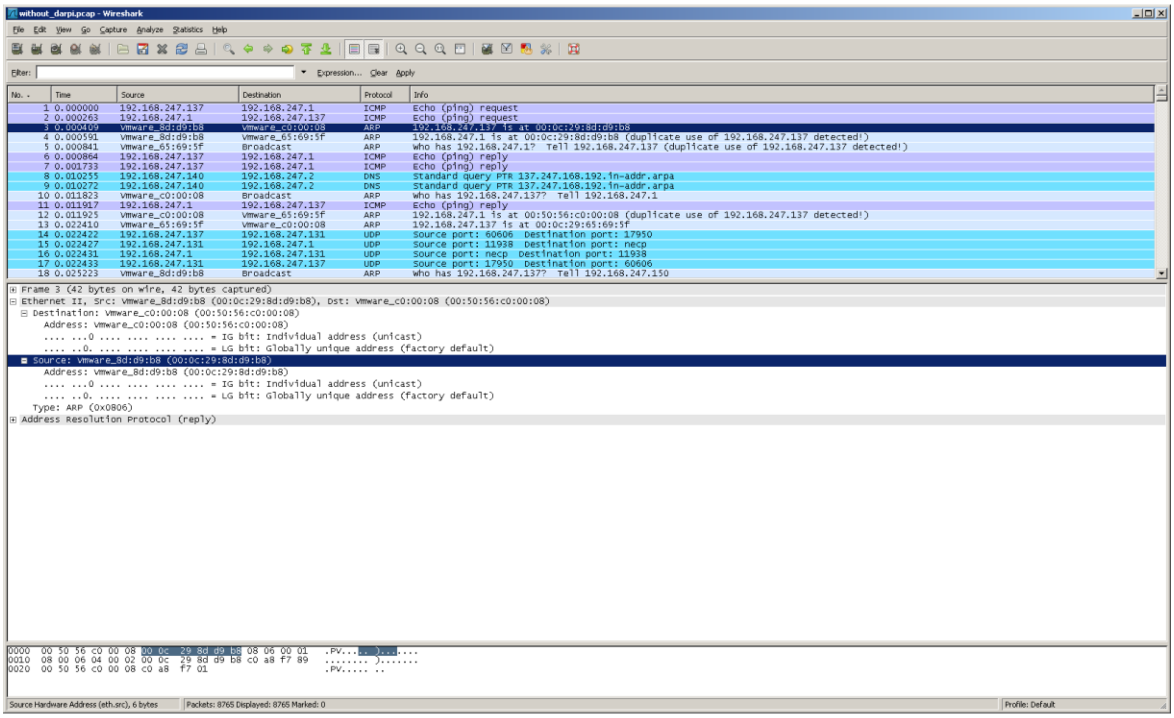
A typical attack is not discovered easily and it takes quite some time to take appropriate countermeasures. From experience, it can be told that there are different possibilities to handle an attack. From the rerouting of voice traffic to the active mitigation of the attack till the power cycling of affected devices. Which decision is made, depends on the nature of the attack and the parties involved. An attack is always stressful and means that there is a known security hole for the attacker, which can be used. To sort out this security hole takes some time as well as fixing it.

If only little fees are abused, it can be that these attacks are not discovered at all. So from all recorded attacks, there are quite a high number of not discovered attacks. It is the same with a botnet, where not all affected PCs know that they are affected. This makes it even more difficult, because it is hard to guess which equipment is safe and which not.

Regular scans and ethical hacking might help companies in being confident to stay secure. During an attack, there is only one victim needed to exploit a whole company. On the other hand, if one attack try is stopped, it does not mean that the company will not get attacked again.

8.2.1. Traffic analysis without DARPI inspection

Without DARPI inspection it is clearly shown that RTP packets (user data) are sent over the network, which can be easily tapped when the attacker has a machine within the same network or has gained access to a machine within the same network through a bot or Trojan horse.


without_darpi.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

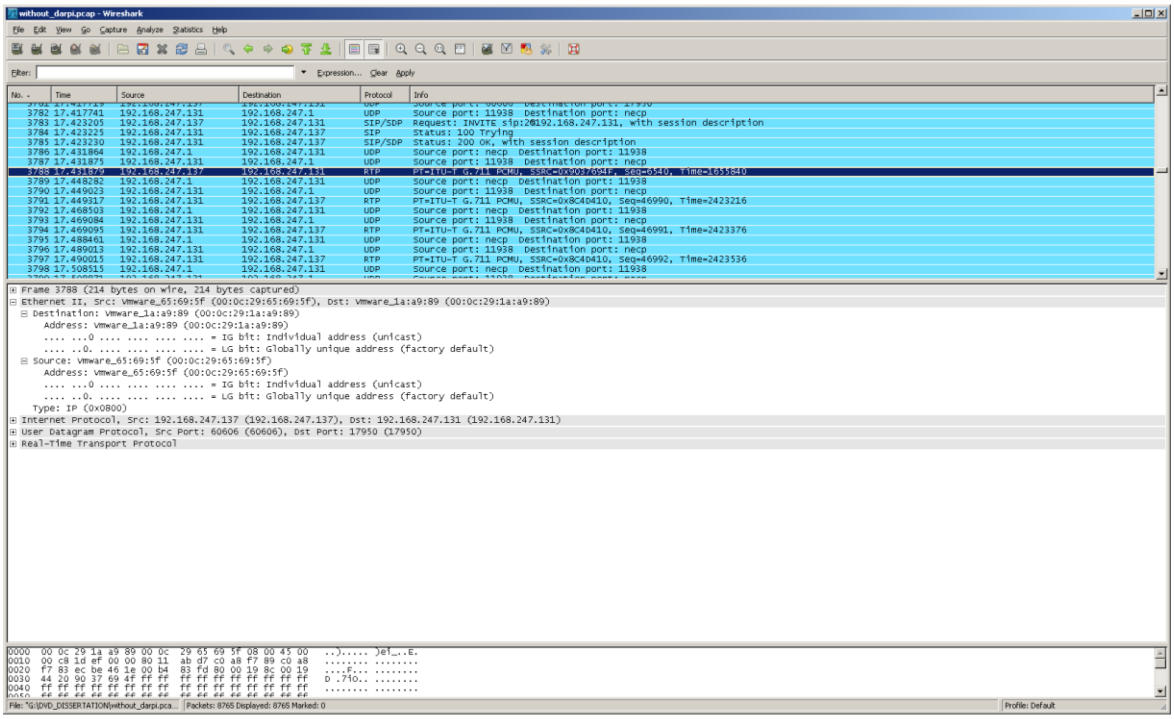
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.247.137	192.168.247.1	ICMP	Echo (ping) request
2	0.000263	192.168.247.1	192.168.247.137	ICMP	Echo (ping) request
3	0.000409	Vmware_8d:d9:b8	Vmware_c0:00:08	ARP	192.168.247.137 is at 00:0c:29:8d:d9:b8
4	0.000591	Vmware_8d:d9:b8	Vmware_65:69:5f	ARP	192.168.247.1 is at 00:0c:29:8d:d9:b8 (duplicate use of 192.168.247.137 detected!)
5	0.000841	Vmware_65:69:5f	Broadcast	ARP	Who has 192.168.247.1? Tell 192.168.247.137 (duplicate use of 192.168.247.137 detected!)
6	0.000864	192.168.247.137	192.168.247.1	ICMP	Echo (ping) reply
7	0.001733	192.168.247.137	192.168.247.1	ICMP	Echo (ping) reply
8	0.010255	192.168.247.140	192.168.247.2	DNS	Standard query PTR 137.247.168.192.in-addr.arpa
9	0.010272	192.168.247.140	192.168.247.2	DNS	Standard query PTR 137.247.168.192.in-addr.arpa
10	0.011823	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.247.137? Tell 192.168.247.1
11	0.011917	192.168.247.1	192.168.247.137	ICMP	Echo (ping) reply
12	0.011925	Vmware_c0:00:08	Vmware_65:69:5f	ARP	192.168.247.1 is at 00:50:56:c0:00:08 (duplicate use of 192.168.247.137 detected!)
13	0.022410	Vmware_65:69:5f	Vmware_c0:00:08	ARP	192.168.247.137 is at 00:0c:29:65:69:5f
14	0.022422	192.168.247.137	192.168.247.131	UDP	Source port: 60606 Destination port: 17950
15	0.022427	192.168.247.131	192.168.247.1	UDP	Source port: 11938 Destination port: necp
16	0.022431	192.168.247.1	192.168.247.131	UDP	Source port: necp Destination port: 11938
17	0.022433	192.168.247.131	192.168.247.137	UDP	Source port: 17950 Destination port: 60606
18	0.025223	Vmware_8d:d9:b8	Broadcast	ARP	Who has 192.168.247.137? Tell 192.168.247.150

```
⊞ Frame 3 (42 bytes on wire, 42 bytes captured)
⊟ Ethernet II, Src: Vmware_8d:d9:b8 (00:0c:29:8d:d9:b8), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
  ⊟ Destination: Vmware_c0:00:08 (00:50:56:c0:00:08)
      Address: Vmware_c0:00:08 (00:50:56:c0:00:08)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Vmware_8d:d9:b8 (00:0c:29:8d:d9:b8)
      Address: Vmware_8d:d9:b8 (00:0c:29:8d:d9:b8)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
⊞ Address Resolution Protocol (reply)
```

```
0000  00 50 56 c0 00 08 00 0c  29 8d d9 b8 08 06 00 01   .PV..... )......
0010  08 00 06 04 00 02 00 0c  29 8d d9 b8 c0 a8 f7 89   ........ )......
0020  00 50 56 c0 00 08 c0 a8  f7 01                     .PV..... ..
```

Source Hardware Address (eth.src), 6 bytes | Packets: 8765 Displayed: 8765 Marked: 0 | Profile: Default

Figure 8.1: Wireshark analyzing ARP packets without DARPI inspection

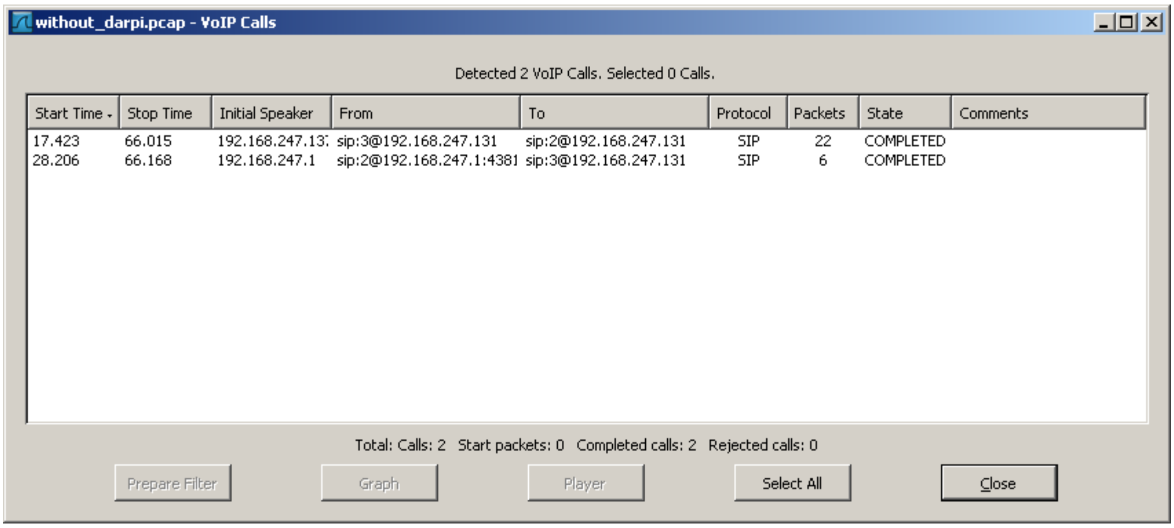

without_darpi.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No.  Time      Source           Destination      Protocol Info
3782 17.417741 192.168.247.131  192.168.247.1    UDP      Source port: 11938  Destination port: necp
3783 17.423205 192.168.247.137  192.168.247.131  SIP/SDP  Request: INVITE sip:2@192.168.247.131, with session description
3784 17.423225 192.168.247.131  192.168.247.137  SIP      Status: 100 Trying
3785 17.423230 192.168.247.131  192.168.247.137  SIP/SDP  Status: 200 OK, with session description
3786 17.431864 192.168.247.1    192.168.247.131  UDP      Source port: necp  Destination port: 11938
3787 17.431875 192.168.247.131  192.168.247.1    UDP      Source port: 11938  Destination port: necp
3788 17.431879 192.168.247.137  192.168.247.131  RTP      PT=ITU-T G.711 PCMU, SSRC=0x9037694F, Seq=6540, Time=1655840
3789 17.448282 192.168.247.1    192.168.247.131  UDP      Source port: necp  Destination port: 11938
3790 17.449023 192.168.247.131  192.168.247.1    UDP      Source port: 11938  Destination port: necp
3791 17.449317 192.168.247.131  192.168.247.137  RTP      PT=ITU-T G.711 PCMU, SSRC=0x8C4D410, Seq=46990, Time=2423216
3792 17.468503 192.168.247.1    192.168.247.131  UDP      Source port: necp  Destination port: 11938
3793 17.469084 192.168.247.131  192.168.247.1    UDP      Source port: 11938  Destination port: necp
3794 17.469095 192.168.247.131  192.168.247.137  RTP      PT=ITU-T G.711 PCMU, SSRC=0x8C4D410, Seq=46991, Time=2423376
3795 17.488461 192.168.247.1    192.168.247.131  UDP      Source port: necp  Destination port: 11938
3796 17.489013 192.168.247.131  192.168.247.1    UDP      Source port: 11938  Destination port: necp
3797 17.490015 192.168.247.131  192.168.247.137  RTP      PT=ITU-T G.711 PCMU, SSRC=0x8C4D410, Seq=46992, Time=2423536
3798 17.508515 192.168.247.1    192.168.247.131  UDP      Source port: necp  Destination port: 11938

⊞ Frame 3788 (214 bytes on wire, 214 bytes captured)
⊟ Ethernet II, Src: Vmware_65:69:5f (00:0c:29:65:69:5f), Dst: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
  ⊟ Destination: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
      Address: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Vmware_65:69:5f (00:0c:29:65:69:5f)
      Address: Vmware_65:69:5f (00:0c:29:65:69:5f)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.247.137 (192.168.247.137), Dst: 192.168.247.131 (192.168.247.131)
⊞ User Datagram Protocol, Src Port: 60606 (60606), Dst Port: 17950 (17950)
⊞ Real-Time Transport Protocol

0000  00 0c 29 1a a9 89 00 0c  29 65 69 5f 08 00 45 00   ..)..... )ei_..E.
0010  00 c8 1d ef 00 00 80 11  ab d7 c0 a8 f7 89 c0 a8   ........ ........
0020  f7 83 ec be 46 1e 00 b4  83 fd 80 00 19 8c 00 19   ....F... ........
0030  44 20 90 37 69 4f ff ff  ff ff ff ff ff ff ff ff   D .7io.. ........
0040  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff   ........ ........
```

File: "G:\DVD_DISSERTATION\without_darpi.pca... Packets: 8765 Displayed: 8765 Marked: 0 Profile: Default

Figure 8.2: Wireshark analyzing RTP packets without DARPI inspection

In this screenshot two SIP calls have been captured, which can be decoded and replayed immediately.

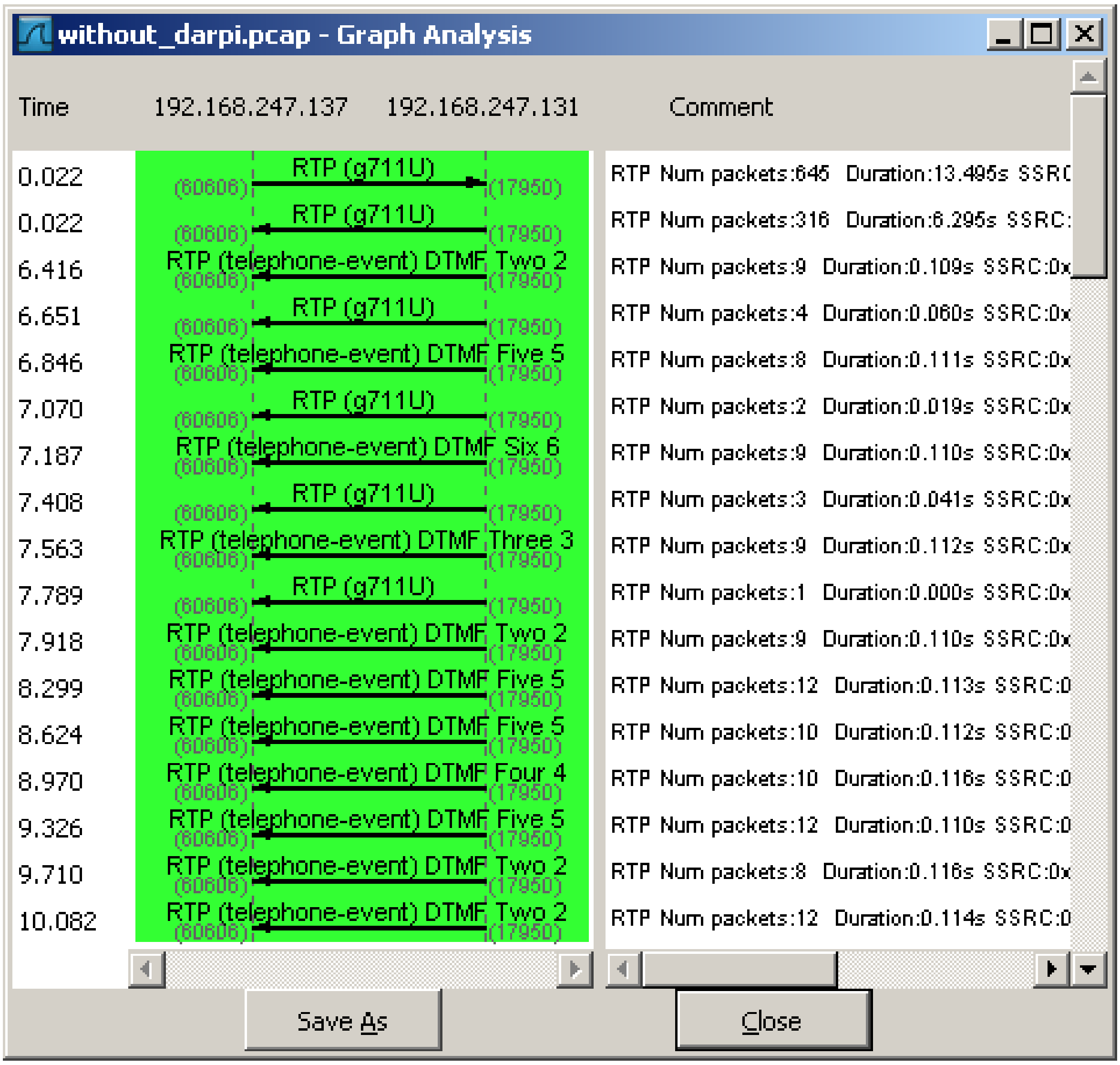


Detected 2 VoIP Calls. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
17.423	66.015	192.168.247.13	sip:3@192.168.247.131	sip:2@192.168.247.131	SIP	22	COMPLETED	
28.206	66.168	192.168.247.1	sip:2@192.168.247.1:4381	sip:3@192.168.247.131	SIP	6	COMPLETED	

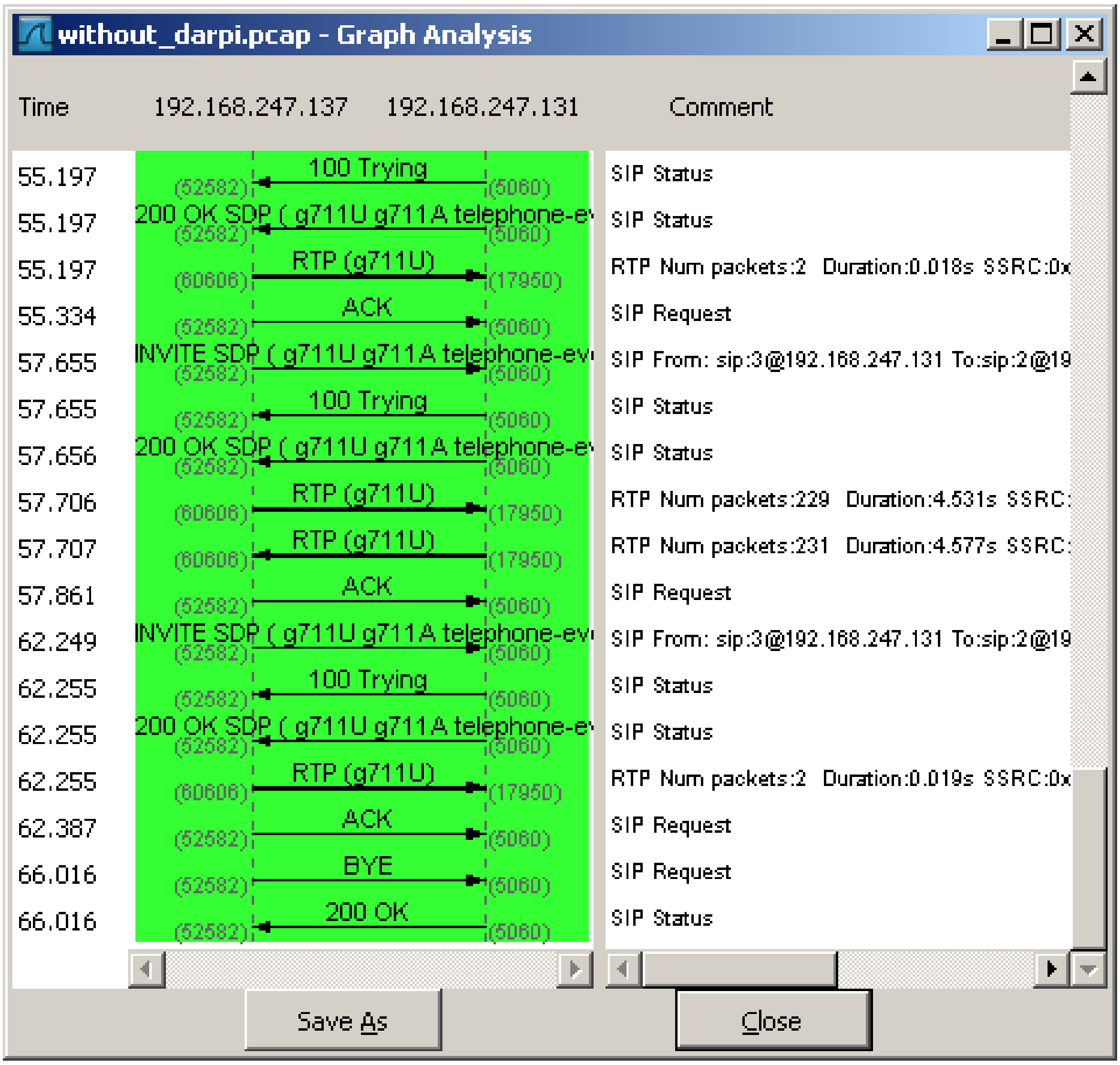
Total: Calls: 2 Start packets: 0 Completed calls: 2 Rejected calls: 0

Figure 8.3: Detected VoIP calls with Wireshark



Time	192.168.247.137		192.168.247.131	Comment
0.022	(60606)	RTP (g711U) →	(17950)	RTP Num packets:645 Duration:13.495s SSRC
0.022	(60606)	← RTP (g711U)	(17950)	RTP Num packets:316 Duration:6.295s SSRC:
6.416	(60606)	← RTP (telephone-event) DTMF Two 2	(17950)	RTP Num packets:9 Duration:0.109s SSRC:0x
6.651	(60606)	← RTP (g711U)	(17950)	RTP Num packets:4 Duration:0.060s SSRC:0x
6.846	(60606)	← RTP (telephone-event) DTMF Five 5	(17950)	RTP Num packets:8 Duration:0.111s SSRC:0x
7.070	(60606)	← RTP (g711U)	(17950)	RTP Num packets:2 Duration:0.019s SSRC:0x
7.187	(60606)	← RTP (telephone-event) DTMF Six 6	(17950)	RTP Num packets:9 Duration:0.110s SSRC:0x
7.408	(60606)	← RTP (g711U)	(17950)	RTP Num packets:3 Duration:0.041s SSRC:0x
7.563	(60606)	← RTP (telephone-event) DTMF Three 3	(17950)	RTP Num packets:9 Duration:0.112s SSRC:0x
7.789	(60606)	← RTP (g711U)	(17950)	RTP Num packets:1 Duration:0.000s SSRC:0x
7.918	(60606)	← RTP (telephone-event) DTMF Two 2	(17950)	RTP Num packets:9 Duration:0.110s SSRC:0x
8.299	(60606)	← RTP (telephone-event) DTMF Five 5	(17950)	RTP Num packets:12 Duration:0.113s SSRC:0
8.624	(60606)	← RTP (telephone-event) DTMF Five 5	(17950)	RTP Num packets:10 Duration:0.112s SSRC:0
8.970	(60606)	← RTP (telephone-event) DTMF Four 4	(17950)	RTP Num packets:10 Duration:0.116s SSRC:0
9.326	(60606)	← RTP (telephone-event) DTMF Five 5	(17950)	RTP Num packets:12 Duration:0.110s SSRC:0
9.710	(60606)	← RTP (telephone-event) DTMF Two 2	(17950)	RTP Num packets:8 Duration:0.116s SSRC:0x
10.082	(60606)	← RTP (telephone-event) DTMF Two 2	(17950)	RTP Num packets:12 Duration:0.114s SSRC:0

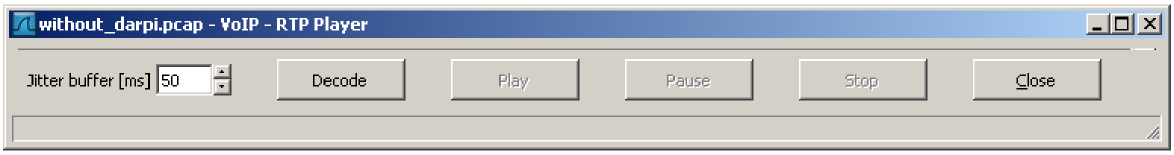
Figure 8.4: Graph analysis of RTP packets



```
Time     192.168.247.137        192.168.247.131      Comment
55.197   (52582) <- 100 Trying (5060)                SIP Status
55.197   (52582) <- 200 OK SDP ( g711U g711A telephone-e (5060)   SIP Status
55.197   (60606) -> RTP (g711U) (17950)              RTP Num packets:2  Duration:0.018s SSRC:0x
55.334   (52582) -> ACK (5060)                       SIP Request
57.655   (52582) -> INVITE SDP ( g711U g711A telephone-ev (5060)  SIP From: sip:3@192.168.247.131 To:sip:2@19
57.655   (52582) <- 100 Trying (5060)                SIP Status
57.656   (52582) <- 200 OK SDP ( g711U g711A telephone-e (5060)   SIP Status
57.706   (60606) -> RTP (g711U) (17950)              RTP Num packets:229  Duration:4.531s SSRC:
57.707   (60606) <- RTP (g711U) (17950)              RTP Num packets:231  Duration:4.577s SSRC:
57.861   (52582) -> ACK (5060)                       SIP Request
62.249   (52582) -> INVITE SDP ( g711U g711A telephone-ev (5060)  SIP From: sip:3@192.168.247.131 To:sip:2@19
62.255   (52582) <- 100 Trying (5060)                SIP Status
62.255   (52582) <- 200 OK SDP ( g711U g711A telephone-e (5060)   SIP Status
62.255   (60606) -> RTP (g711U) (17950)              RTP Num packets:2  Duration:0.019s SSRC:0x
62.387   (52582) -> ACK (5060)                       SIP Request
66.016   (52582) -> BYE (5060)                       SIP Request
66.016   (52582) <- 200 OK (5060)                    SIP Status
```

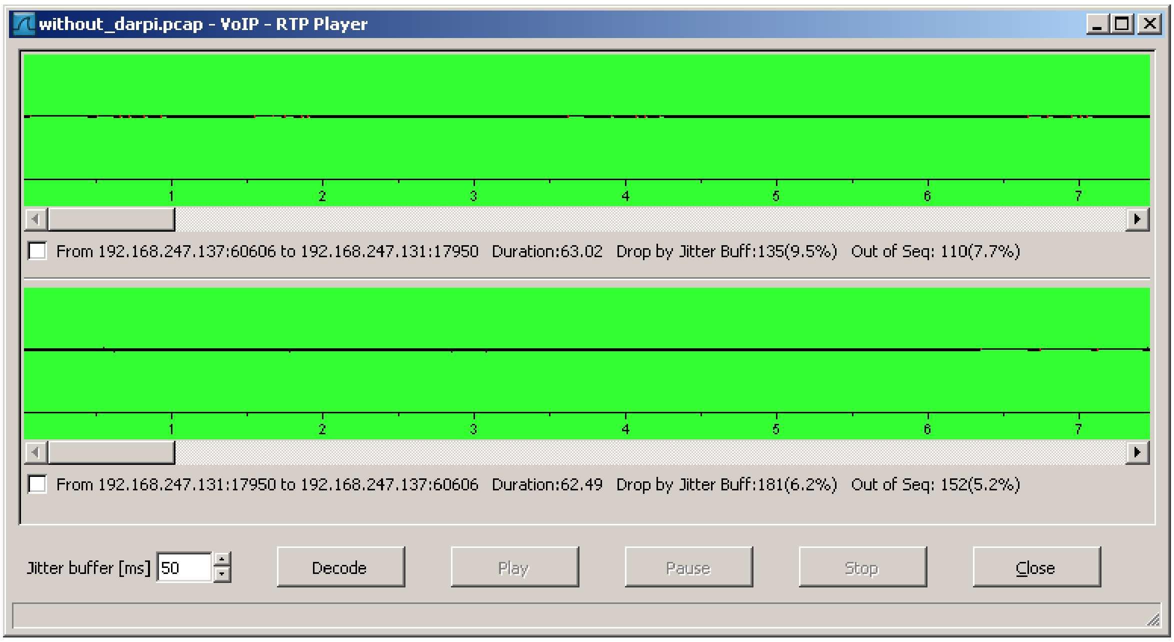
Figure 8.5: Graph analysis of session ending

There is not much processing power needed to decode the voice streams and replay the streams.



Jitter buffer [ms] 50

Figure 8.6: Decoding of RTP streams

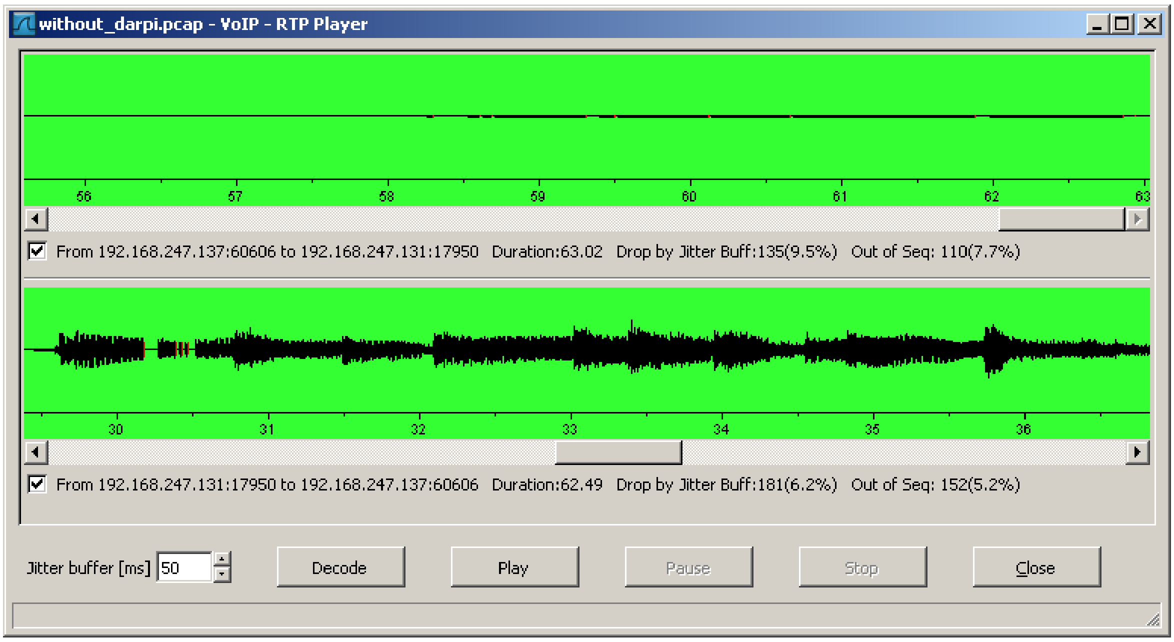


☐ From 192.168.247.137:60606 to 192.168.247.131:17950 Duration:63.02 Drop by Jitter Buff:135(9.5%) Out of Seq: 110(7.7%)

☐ From 192.168.247.131:17950 to 192.168.247.137:60606 Duration:62.49 Drop by Jitter Buff:181(6.2%) Out of Seq: 152(5.2%)

Jitter buffer [ms] 50

Figure 8.7: Voice capture of two channels



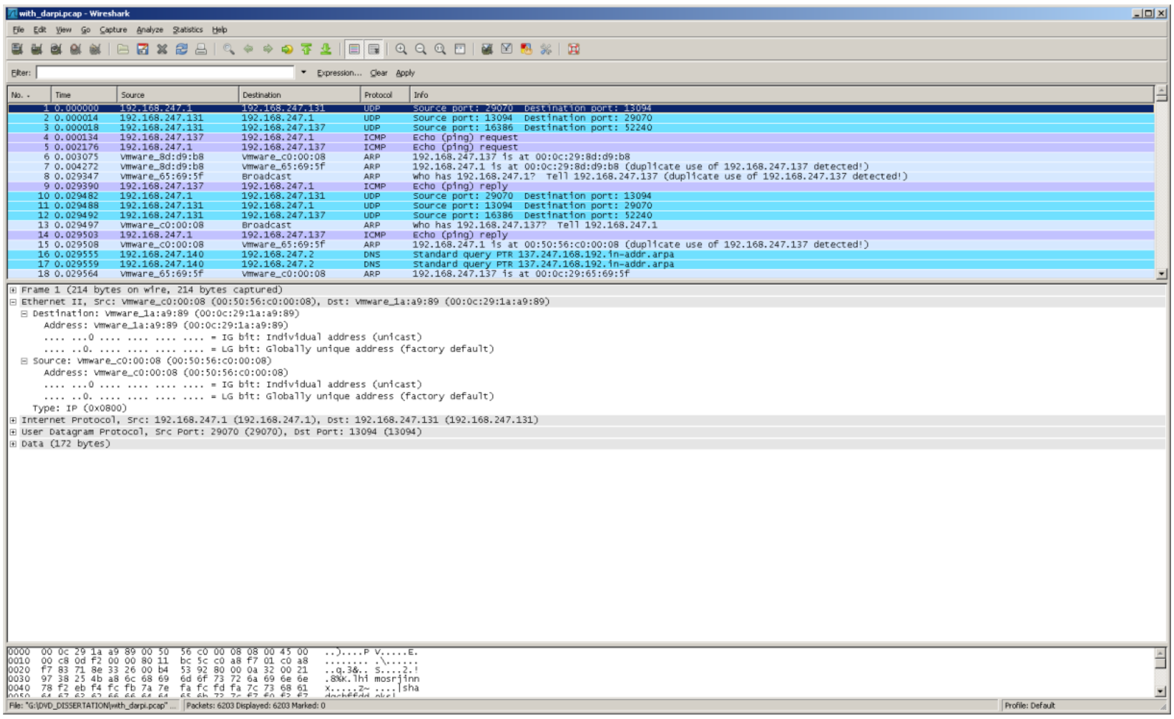
☑ From 192.168.247.137:60606 to 192.168.247.131:17950 Duration:63.02 Drop by Jitter Buff:135(9.5%) Out of Seq: 110(7.7%)

☑ From 192.168.247.131:17950 to 192.168.247.137:60606 Duration:62.49 Drop by Jitter Buff:181(6.2%) Out of Seq: 152(5.2%)

Figure 8.8: Actual voice detection

8.2.2. Traffic analysis with DARPI inspection

With the use of DARPI inspection, RTP data is not seen on the network, which makes it impossible for an attacker to hijack voice data.


with_darpi.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

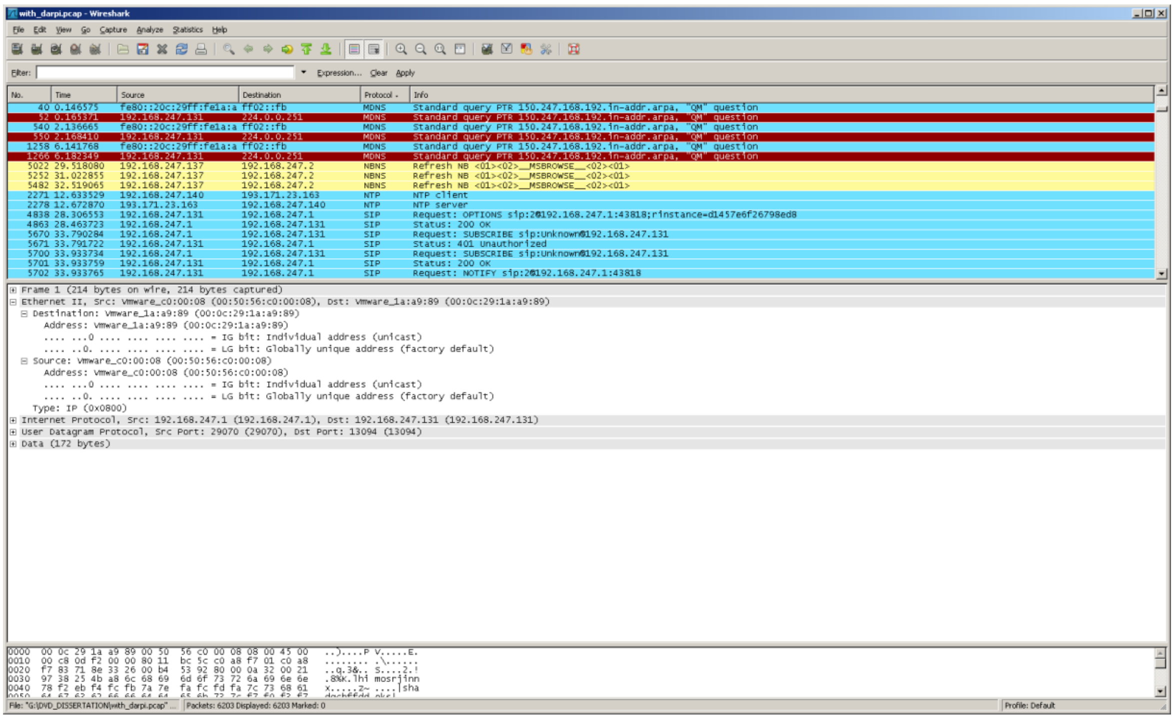
```
No. .  Time      Source             Destination        Protocol  Info
    1 0.000000  192.168.247.1      192.168.247.131    UDP       Source port: 29070  Destination port: 13094
    2 0.000014  192.168.247.131    192.168.247.1      UDP       Source port: 13094  Destination port: 29070
    3 0.000018  192.168.247.131    192.168.247.137    UDP       Source port: 16386  Destination port: 52240
    4 0.000134  192.168.247.137    192.168.247.1      ICMP      Echo (ping) request
    5 0.002176  192.168.247.1      192.168.247.137    ICMP      Echo (ping) request
    6 0.003075  Vmware_8d:d9:b8    Vmware_c0:00:08    ARP       192.168.247.137 is at 00:0c:29:8d:d9:b8
    7 0.004272  Vmware_8d:d9:b8    Vmware_65:69:5f    ARP       192.168.247.1 is at 00:0c:29:8d:d9:b8 (duplicate use of 192.168.247.137 detected!)
    8 0.029347  Vmware_65:69:5f    Broadcast          ARP       Who has 192.168.247.1?  Tell 192.168.247.137 (duplicate use of 192.168.247.137 detected!)
    9 0.029390  192.168.247.137    192.168.247.1      ICMP      Echo (ping) reply
   10 0.029482  192.168.247.1      192.168.247.131    UDP       Source port: 29070  Destination port: 13094
   11 0.029488  192.168.247.131    192.168.247.1      UDP       Source port: 13094  Destination port: 29070
   12 0.029492  192.168.247.131    192.168.247.137    UDP       Source port: 16386  Destination port: 52240
   13 0.029497  Vmware_c0:00:08    Broadcast          ARP       Who has 192.168.247.137?  Tell 192.168.247.1
   14 0.029503  192.168.247.1      192.168.247.137    ICMP      Echo (ping) reply
   15 0.029508  Vmware_c0:00:08    Vmware_65:69:5f    ARP       192.168.247.1 is at 00:50:56:c0:00:08 (duplicate use of 192.168.247.137 detected!)
   16 0.029555  192.168.247.140    192.168.247.2      DNS       Standard query PTR 137.247.168.192.in-addr.arpa
   17 0.029559  192.168.247.140    192.168.247.2      DNS       Standard query PTR 137.247.168.192.in-addr.arpa
   18 0.029564  Vmware_65:69:5f    Vmware_c0:00:08    ARP       192.168.247.137 is at 00:0c:29:65:69:5f
```

```
⊞ Frame 1 (214 bytes on wire, 214 bytes captured)
⊟ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
  ⊟ Destination: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
      Address: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Vmware_c0:00:08 (00:50:56:c0:00:08)
      Address: Vmware_c0:00:08 (00:50:56:c0:00:08)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.247.1 (192.168.247.1), Dst: 192.168.247.131 (192.168.247.131)
⊞ User Datagram Protocol, Src Port: 29070 (29070), Dst Port: 13094 (13094)
⊞ Data (172 bytes)
```

```
0000  00 0c 29 1a a9 89 00 50  56 c0 00 08 08 00 45 00   ..)....P V.....E.
0010  00 c8 0d f2 00 00 80 11  bc 5c c0 a8 f7 01 c0 a8   ........ .\......
0020  f7 83 71 8e 33 26 00 b4  53 92 80 00 0a 32 00 21   ..q.3&.. S....2.!
0030  97 38 25 4b a8 6c 68 69  6d 6f 73 72 6a 69 6e 6e   .8%K.lhi mosrjinn
0040  78 f2 eb f4 fc fb 7a 7e  fa fc fd fa 7c 73 68 61   x.....z~ ....|sha
```

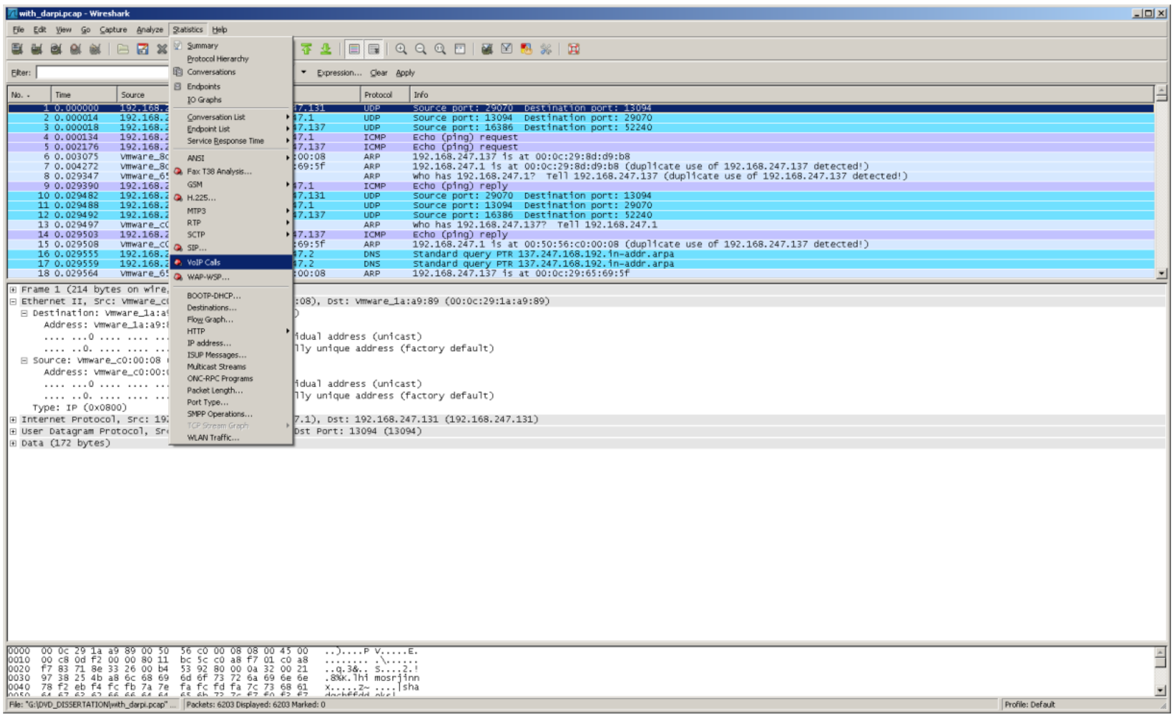
File: "G:\DVD_DISSERTATION\with_darpi.pcap" ...
Packets: 6203 Displayed: 6203 Marked: 0
Profile: Default

Figure 8.9: Wireshark analyzing ARP packets with DARPI inspection


with_darpi.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No.  Time        Source                    Destination      Protocol  Info
  40 0.146575    fe80::20c:29ff:fe1a:a     ff02::fb         MDNS      Standard query PTR 150.247.168.192.in-addr.arpa, "QM" question
  52 0.165371    192.168.247.131           224.0.0.251      MDNS      Standard query PTR 150.247.168.192.in-addr.arpa, "QM" question
 540 2.136665    fe80::20c:29ff:fe1a:a     ff02::fb         MDNS      Standard query PTR 150.247.168.192.in-addr.arpa, "QM" question
 550 2.168410    192.168.247.131           224.0.0.251      MDNS      Standard query PTR 150.247.168.192.in-addr.arpa, "QM" question
1258 6.141768    fe80::20c:29ff:fe1a:a     ff02::fb         MDNS      Standard query PTR 150.247.168.192.in-addr.arpa, "QM" question
1266 6.182349    192.168.247.131           224.0.0.251      MDNS      Standard query PTR 150.247.168.192.in-addr.arpa, "QM" question
5022 29.518080   192.168.247.137           192.168.247.2    NBNS      Refresh NB <01><02>__MSBROWSE__<02><01>
5252 31.022855   192.168.247.137           192.168.247.2    NBNS      Refresh NB <01><02>__MSBROWSE__<02><01>
5482 32.519065   192.168.247.137           192.168.247.2    NBNS      Refresh NB <01><02>__MSBROWSE__<02><01>
2271 12.633529   192.168.247.140           193.171.23.163   NTP       NTP client
2278 12.672870   193.171.23.163            192.168.247.140  NTP       NTP server
4838 28.306553   192.168.247.131           192.168.247.1    SIP       Request: OPTIONS sip:2@192.168.247.1:43818;rinstance=d1457e6f26798ed8
4863 28.463723   192.168.247.1             192.168.247.131  SIP       Status: 200 OK
5670 33.790284   192.168.247.1             192.168.247.131  SIP       Request: SUBSCRIBE sip:Unknown@192.168.247.131
5671 33.791722   192.168.247.131           192.168.247.1    SIP       Status: 401 Unauthorized
5700 33.933734   192.168.247.1             192.168.247.131  SIP       Request: SUBSCRIBE sip:Unknown@192.168.247.131
5701 33.933759   192.168.247.131           192.168.247.1    SIP       Status: 200 OK
5702 33.933765   192.168.247.131           192.168.247.1    SIP       Request: NOTIFY sip:2@192.168.247.1:43818

⊞ Frame 1 (214 bytes on wire, 214 bytes captured)
⊟ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
  ⊟ Destination: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
      Address: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Vmware_c0:00:08 (00:50:56:c0:00:08)
      Address: Vmware_c0:00:08 (00:50:56:c0:00:08)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.247.1 (192.168.247.1), Dst: 192.168.247.131 (192.168.247.131)
⊞ User Datagram Protocol, Src Port: 29070 (29070), Dst Port: 13094 (13094)
⊞ Data (172 bytes)

0000  00 0c 29 1a a9 89 00 50  56 c0 00 08 08 00 45 00   ..).....P V.....E.
0010  00 c8 0d f2 00 00 80 11  bc 5c c0 a8 f7 01 c0 a8   ........ .\......
0020  f7 83 71 8e 33 26 00 b4  53 92 80 00 0a 32 00 21   ..q.3&.. S....2.!
0030  97 38 25 4b a8 6c 68 69  6d 6f 73 72 6a 69 6e 6e   .8%K.lhi mosrjinn
0040  78 f2 eb f4 fc fb 7a 7e  fa fc fd fa 7c 73 68 61   x.....z~ ....|sha

File: "G:\DVD_DISSERTATION\with_darpi.pcap" ...   Packets: 6203 Displayed: 6203 Marked: 0   Profile: Default
```

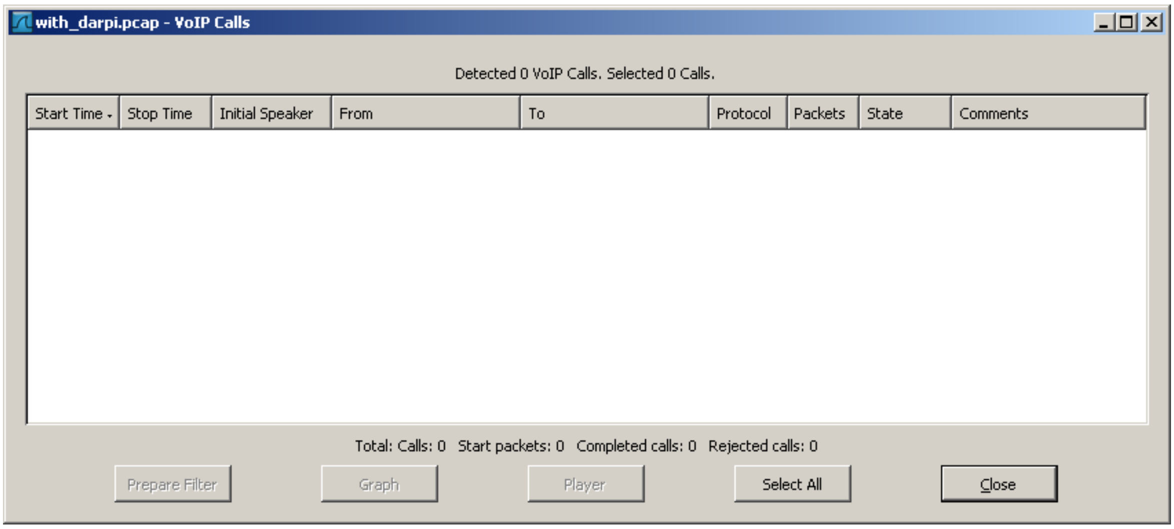
Figure 8.10: Wireshark cannot detect RTP packets with DARPI inspection



```
No.  Time       Source        Protocol  Info
  1 0.000000   192.168.2   7.131    UDP   Source port: 29070  Destination port: 13094
  2 0.000014   192.168.2   7.1      UDP   Source port: 13094  Destination port: 29070
  3 0.000018   192.168.2   7.137    UDP   Source port: 16386  Destination port: 52240
  4 0.000134   192.168.2   7.1      ICMP  Echo (ping) request
  5 0.002176   192.168.2   7.137    ICMP  Echo (ping) request
  6 0.003075   Vmware_8c   :00:08   ARP   192.168.247.137 is at 00:0c:29:8d:d9:b8
  7 0.004272   Vmware_8c   :69:5f   ARP   192.168.247.1 is at 00:0c:29:8d:d9:b8 (duplicate use of 192.168.247.137 detected!)
  8 0.029347   Vmware_65            ARP   Who has 192.168.247.1?  Tell 192.168.247.137 (duplicate use of 192.168.247.137 detected!)
  9 0.029390   192.168.2   7.1      ICMP  Echo (ping) reply
 10 0.029482   192.168.2   7.131    UDP   Source port: 29070  Destination port: 13094
 11 0.029488   192.168.2   7.1      UDP   Source port: 13094  Destination port: 29070
 12 0.029492   192.168.2   7.137    UDP   Source port: 16386  Destination port: 52240
 13 0.029497   Vmware_c0            ARP   Who has 192.168.247.137?  Tell 192.168.247.1
 14 0.029503   192.168.2   7.137    ICMP  Echo (ping) reply
 15 0.029508   Vmware_c0   :69:5f   ARP   192.168.247.1 is at 00:50:56:c0:00:08 (duplicate use of 192.168.247.137 detected!)
 16 0.029555   192.168.2   7.2      DNS   Standard query PTR 137.247.168.192.in-addr.arpa
 17 0.029559   192.168.2   7.2      DNS   Standard query PTR 137.247.168.192.in-addr.arpa
 18 0.029564   Vmware_65   :00:08   ARP   192.168.247.137 is at 00:0c:29:65:69:5f

⊞ Frame 1 (214 bytes on wire,
⊟ Ethernet II, Src: Vmware_c0   :08), Dst: Vmware_1a:a9:89 (00:0c:29:1a:a9:89)
  ⊟ Destination: Vmware_1a:a9   )
      Address: Vmware_1a:a9:8
      .... ...0 .... .... ...   idual address (unicast)
      .... ..0. .... .... ...   lly unique address (factory default)
  ⊟ Source: Vmware_c0:00:08 (
      Address: Vmware_c0:00:0
      .... ...0 .... .... ...   idual address (unicast)
      .... ..0. .... .... ...   lly unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 19   7.1), Dst: 192.168.247.131 (192.168.247.131)
⊞ User Datagram Protocol, Sr   Dst Port: 13094 (13094)
⊞ Data (172 bytes)

0000  00 0c 29 1a a9 89 00 50  56 c0 00 08 08 00 45 00   ..).....P V.....E.
0010  00 c8 0d f2 00 00 80 11  bc 5c c0 a8 f7 01 c0 a8   ........ .\......
0020  f7 83 71 8e 33 26 00 b4  53 92 80 00 0a 32 00 21   ..q.3&.. S....2.!
0030  97 38 25 4b a8 6c 68 69  6d 6f 73 72 6a 69 6e 6e   .8%K.lhi mosrjinn
0040  78 f2 eb f4 fc fb 7a 7e  fa fc fd fa 7c 73 68 61   x.....z~ ....|sha

File: "G:\DVD_DISSERTATION\with_darpi.pcap" ...   Packets: 6203 Displayed: 6203 Marked: 0   Profile: Default
```

Figure 8.11: Wireshark statistics of VoIP calls

It is impressive that with the protection, no voice calls can be detected anymore. The protection is implemented and verified.



Detected 0 VoIP Calls. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments

Total: Calls: 0 Start packets: 0 Completed calls: 0 Rejected calls: 0

Figure 8.12: Wireshark cannot detect VoIP calls with DARPI

Chapter 9 rules out the need for VoIP protection and the difference between this approach and others.

9 Comparison of achieved results with existing work

Here, achieved results are compared against existing work. This means, how existing work can contribute to achieve results with this approach.

Many people are using Skype for communicating with each other over the Internet, but it bears two great problems. First, with Skype you do not know which data is transmitted, and second, Skype uses UDP which is fast but has no security implemented. A scenario within Skype is that one believes talking to someone he or she knows, but in fact the callee is someone else. Because of the belief in talking to someone one knows, one is willing to give away secrets. The Skype network, based on SIP, is distributed worldwide and therefore no common secure authentication is possible.

The following graph shows the trend of worldwide VoIP, especially using Skype:

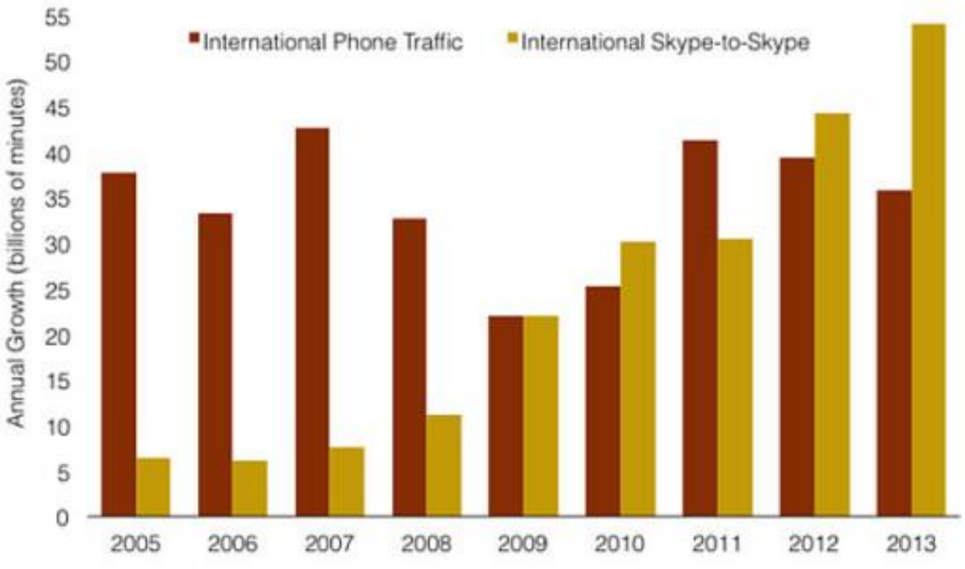


Figure 9.1: Skype's worldwide traffic continues to grow, 214 billion minutes on VoIP in 2013, taken from http://www.trutower.com/2014/01/13/skype-voip-app-calling-statistics-telegeography/

Improvements in the protocol of H.323 and SIP have to be done. The SIP protocol is favored for optimization. As SIP is an open, extendable protocol, there are many extensions available. SIP is a subset of the multimedia communication.

There are five tasks of SIP:

These tasks, also known as activities, are named user location, user availability, user capability, session setup and session management.

SIP network elements:

The SIP network elements, also known as roles, are called proxy server, redirect server, registrar server, gateway server, back to back user agents and user agents, the clients.

Often, many functions are combined in one SIP server, like proxy server, redirect server and gateway server. For secure VoIP connections SRTP is used. Encryption proves the confidentiality of the data. Authentication is guaranteed by authenticating the requestor.

Altered packets are identified by checking the integrity. Anti-Replay protection makes it impossible for attackers to read VoIP packets and use this information to establish new sessions and get information from the endpoint.

"SRTP supports symmetric VoIP data encryption with AES to avoid tapping, authentication of the sender to avoid identity-spoofing, integrity checks to avoid unauthorized changes and anti-replay functionality to avoid unauthorized access. All of the provided features (such as encryption and authentication) are optional and can be separately enabled or disabled. For using the encryption functionality, SRTP needs a Public Key Infrastructure (PKI). In cryptography, a PKI is an arrangement that provides for trusted third party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried out by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates.

The term is used for two meanings , the certificate authority and related arrangements as well as, more broadly and somewhat confusingly, the use of public key algorithms in electronic communications. The latter sense is erroneous since PKI methods are not required to use public key algorithms. PKI arrangements enable users to be authenticated to each other, and to use the information in identity certificates (i.e., each other's public keys) to encrypt and decrypt messages traveling to and from. In general, a PKI consists of client software, server software such as a certificate authority, hardware (e.g., smart cards) and operational procedures. A user may digitally sign messages using his private key, and another user can check that signature (using the public key contained in that user's certificate issued by a certificate authority within the PKI). This enables two (or more) communicating parties to establish confidentiality, message integrity and user authentication without having to exchange any secret information in advance. A PKI is a complex structure that is necessary to make secure VoIP phone calls using SRTP. Therefore it is no alternative for private users, because normally only companies can afford to setup this structure to use it with their VoIP phone calls. Private users have to look for alternatives like Zfone[Mu06].“

Confidentiality and data integrity in SRTP are realized using encryption and HMAC. HMAC is known as relatively secure in combination with SHA-1 and SHA-2. These are only two points of Confidentiality, Integrity, Availability, Privacy, Authorization, Accounting, Authentication and Identification (CIAPAAAI).

There are some protocols for the media key exchange within SRTP to establish encrypted telephone calls. These include MIKEY, Pre Shared Key (PSK), RSA, DH, DHHMAC, RSA-R, Session Description Protocol Security Descriptions (SDES), Encrypted Key Transport (EKT) and ZRTP by Phil Zimmermann.

ZRTP has two working modes:

- Preshared mode (authentication relies only on previously shared secrets)
- DH mode (authentication relies on DH exchange and on previously shared secrets)

ZRTP generates SRTP master keys and salt using a HMAC function. The overall key and security negotiation is purely peer-to-peer realized by ZRTP. Cipher Feedback (CFB), an algorithm, is an encrypted transmission of the SAS verified flag. If a fake trusted server is used with SAS, the user will recognize it.

The Conf2Ack message is a confirmation sent by Alice upon receipt of a Conf2 message. ZRTP provides means like strong secrecy (having a pool of possible valid keys) or SAS for the key exchange to detect a MITM attack. It is important to carry out a SAS authentication when contacting somebody for the first time and checking the SAS verified flag for connection with which the SAS has already been carried out.

The theoretical Achilles heel of the ZRTP protocol is the SAS endpoint authentication. SAS, which requires a trusted server, also makes the server resistant against DOS attacks and can blacklist IP addresses. ZRTP is designed to provide authentication between parties, secrecy, and end-to-end PFS between sessions. AES is used for payload encryption and the SRTP packet including headers is authenticated using SHA-1.

ZRTP is vulnerable to adversaries with strong capabilities. Some experts advise for modifying the protocol to include a randomized start time for the conversation. This method is called pseudonymization. A practical example is the Zfone software installation of a SIP phone that has encryption already implemented. Hardware SIP phones are not so vulnerable than software phones. Where software phones are attackable on the guest operating system, hardware phones run on proprietary operating systems with limited network services.

MD5 is commonly used for 802.1X, certificates for authentication, IPSec, TLS and SIPS for the signaling security, SRTP for media security and MIKEY-RSA for the media key exchange.

Security relevant parameters between the clients are exchanged by parameters and a secret key is generated with the Key Management Protocol (KMP). IKE is used in IP networks and MIKEY for VoIP connections. The secret key, which must be known for both sides but must not be sent across the network, is supplied by the DH process. For encrypting the user data, session keys are applied, which are derived from the DH-process created master key. The authentication check is done with HMAC.

Testing of hard-phones, Wi-Fi phones and terminal adapters shows that many have weak security:

- open ports, default passwords, weak provisioning, weak cryptography
- defective software
- low tolerance for fuzzing and flooding

VoIP attacks are either aimed at the service itself (e.g. DDOS, spoofing) or the customer (SPIT, fraud, call-hijacking) or the service provider (e.g. SQL-injection). Already observed have been attacks, such as REGISTER / INVITE flooding, multi-source flooding, unresolvable DNS names and unintentional misbehavior / misconfiguration.

"Though SIP offers various flexible mechanisms for managing communications between different User Identities, it still does not offer the flexibility to the User to federate and use information/rights from one Identity to another. Users are still required to subscribe or configure each service individually at each of their different identities. SIP would also need a solution for providing mobility across multiple user identities [M06]."

To prevent additional use as disadvantage for the user, a central user identity management should be implemented with strong identities. Reputation systems can also be used to build up a white list of an allowed network. Address books and buddy lists are examples for white lists.

9.1 State of the art models

There are several state-of-the-art models dealing with the interception of messages, which have been looked at during the literature research phase of this thesis.

- AVISPA model (a cryptographic protocol verifier)
- PROVERIF model (a cryptographic protocol verifier)
- Dolev-Yao model (intruder can do whatever he pleases with the exchanged messages)
- Murphi model (ciphered, by Andrew Schwartz)

Currently, secure SIP services offer signaling links secured by TLS and media data security transport realized by SRTP. As there are many VoIP protocols, like SIP, RTP/RTCP, SRTP, ZRTP and many more, chaos exists.

9.2 Summary

So far, many contributions have been made, but the gaps are still not closed. Variants of attacks are a struggle for every IT administrator and they persist. Sensitive information is tapped and makes it possible to get to know insider information. New approaches are needed to come up with existing and new evolving attack scenarios. Attacks are getting more complex nowadays and it often takes long time to recover. The financial losses and frequency of attacks have also risen in the last few years.

Often these attacks are also politically motivated, which makes it even more dangerous and difficult to handle. A combination of different attacks has led to a methodological new approach closing some of the existing gaps. But still there is lot of work to do and the fight against the attackers is not yet won. It is doubtful that this fight can be ever won. It is thought that there will always be attacks. The motivation and the attack itself have changed, but not the parties involved. Patches get released faster, but viruses and new attacks are carried out even faster. So it is a matter how fast a company can keep pace with this increased speed. Some companies still do not invest into security and do not minimize the risks. It must be made clear for the companies what it means to be under the radar of the attackers and be a victim. Often, these companies are not attacked once, but regularly and even without notice.

A successful attack can have many consequences. From the closure of a company to temporal service disruptions, everything is possible. Bad reputation can also be the case if the attack is aimed at points, where externals are involved or aimed against, for instance the CEO or CFO of a company, where sensitive data relies. Social engineering is another attack, which makes it easy for attackers to gain information, if carried out right. It is difficult to be recognized and affected people feel secure and do not know that they have just given away sensitive information, because they think they give the information to a valid person. This is not only the case with externals but with externals, hiding as spies, getting internal by applying for certain positions.

This makes it even worse, because it is difficult to be identified and to not trust internals. Regular audits and scans can help here and an open mindset is to always watch out for threats.

The next chapter gives an overview of limitations concerning the approach and which legal considerations must be cared for, while fulfilling the privacy requirements.

10 Achieved results and remaining limitations

In this chapter, a number of laws are presented to stay within the law and further solutions are presented to fulfill the privacy requirements.

As telecommunication is protected by several laws, instances of surveillance or filtering calls can result in several legal consequences (for example imprisonment). Therefore, it is very important not only to construct technical filtering mechanisms, but also to consider implications with regard to telecommunication or privacy protection laws and regulations. The CDRAS tool will be open source and make a contribution in the fight against hackers.

10.1 Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained. No data revealing the content of the communication may be retained pursuant to this Directive [DIR10].

The thesis author’s opinion of logging CDR’s of a PBX is that the CDRAS tool can be considered as lawful. The CDRs for instance of Cisco Unified Communication Manager (Cisco Call manager) are also recorded and can be analyzed. The possibility and access to analyze this sensitive information should of course be limited to few persons and only presented to those, who are authorized.

It is the same with a firewall or a URL & content filter, where sensitive information is stored and analyzed. But it can help, in case of police investigations to defend this information against hackers and unwanted people.

The analysis of VoIP data has to obey numerous laws for telecommunication. These restrictions increase the difficulty of analyzing it. In the following sections the rights of callers and callers in a telephone conversation in the US and in Germany, which have two fundamentally different legal systems, are displayed.

Section 88 of the German Telecommunications Act (TKG) states that the content and the connection data of a phone call are personal data. Thus, the BDSG is relevant for this data. Telecommunications companies are only allowed to store start and end of a call, resulting costs and participants, due to Section 3a of the BDSG. The entire connection data including IP address of electronic communications have to be deleted after the call terminates according to Section 96 of the TKG. IP addresses are considered as personal data in Germany, because a link between the IP address and a person can be established using reasonable amounts of time and money [WIT11].

Section 15 of the German Telemedia Act (TMG) states that log files are personal data if they contain information that is not needed for a business transaction, e.g., billing. Thus, communication records that are not required for billing purposes are personal data and have to be deleted after the service finishes according to Section 13 of the German Telemedia Act (TMG). However, Section 110 and 113 of the German Telecommunications Act (TKG) and Section 16 and 17 of the German telecommunications monitoring regulation (TKUEV) have to store communication records for six month for the German authorities. These laws are an implementation of the EU Directive 2006/24/EC, the so-called Data Retention Directive (EUDRD), where Section 3 of the BDSG states that telecommunications laws outrank the BDSG [WIT11]. Thus, storing communication records according to TKG and TKUEV is legal and in accordance with the BDSG. However, communication records of persons with a confidentiality constraint due to their profession, e.g., doctors and psychologists, are never allowed to be stored according to Section 203 of the German penal code (StGB) [ARES12].

The Australian *Telecommunications (Interception and Access) Act* makes it an offence to record, use or disclose intercepted information, stored communication information, or information about an interception or stored communication warrant, except in certain circumstances. For example, this type of information can be recorded, used or disclosed for the purpose of applying for a warrant or for investigating certain offences [ALRC13].

Westin defines privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” [WES67].

Nissenbaum [NIS04] adds the notion of context to privacy and the role of agents receiving the information, relationship to information subjects; on what terms the information is shared by the subject and the terms of further distribution.

A number of guidelines for privacy are available, the FIPs [OEC80] are widely accepted, which state that a person’s informed consent is required before the data is collected and the collection should be limited to the task it is required for and erased as soon as this is not the case anymore. The collector of the data shall keep the data secure and shall be held accountable for any violation of these principles. In the European Union the EU Data Protection Directive, Directive 95/46/EC, doesn’t permit processing personal data at all, except when a specific legal basis explicitly allows it or when the individuals concerned consented prior to the data processing [EUD95]. The Directive 2002/58/EC specifies and complements the EU Data Protection Directive and stresses the importance of consent for processing telecommunications data and that electronic communication has to be kept confidential [EUD02].

The US has no central data protection law, but separate privacy laws, e.g., HIPAA for medical information and COPPA for data related to children [HSC08]. The Telecommunications Act of 1996 in the US distinguishes between telecommunications services, which are the primary subject of regulation in the US, and information services. The former offers telephony for a fee directly to the public. Information services offer a capability for using telecommunications for information exchange, e.g., email services. In the US the classification of VoIP technology is not decided. VoIP technology can be classified as telecommunications services, as well as information services [LEI06]. The VoIP Regulatory Freedom Act of 2004 in the US demands that VoIP providers offer several services that fixed phone line providers offer, e.g., 911-service requirements (emergency calls). In the case that telecommunications providers use VoIP technology, for calls that originate and terminate on the PSTN, these calls are regulated as telecommunications services. Every other combination remains open to interpretation, e.g., calls that originate at a VoIP service and terminate on the PSTN [LEI06]. Sect. 702 of the Telecommunications Act concerns the privacy of customer information. They have to be kept confidential. Otherwise the law refers to the Electronic Communications Privacy Act (ECPA). The ECPA of 1986 (US Code, title 18, chapter 121, section 2510-2522), concerns the protection of electronic communications while in transit. The Stored Communications

Act (SCA) of 1986 (US Code, title 18, chapter 121, section 2701-2712) is considered a part of the ECPA and prohibits access to records of electronic communications. Nevertheless, section 2712 allows, with the lawful consent of the call participants, to divulge a communication record.

Otherwise the record has to be kept confidential. ECPA and SCA concern information services. The Telecommunications Act concerning telecommunications services, however, also refers to ECPA.

To sum up, in the US and the EU, telecommunication has to be kept confidential and any usage of telecommunications data requires the informed consent of the participants. They have to be in possession of all the facts, implications, and future consequences of an action in order to give an informed consent. In addition, the facts, implications, and future consequences have to be understood entirely and in every detail at the time consent is given. Telecommunications records may only be stored as long as they are required for and the purpose they were recorded for, e.g., billing.

The privacy requirements presented in the beginning of this section only apply as long as personal information is stored in the communication records. If the records are anonymized, the personal information is replaced with other content, the storage and analysis would not be affected by the law. However, these would render the records useless for attack prevention, since attacks could no longer be identified and blocked. A compromise between these two is the pseudonymization of the CDRs. In this case the personal information in these records is replaced with other content.

However, the relations between the original and the replaced content still exist in a database. This database has to be kept confidential via mechanism like access control or encryption. In this scenario a pseudonymization technique applies to the CDRs fields: callingPartyNumber, callingPartyUnicodeLoginUserID, originalCalled PartyNumber, dateTimeConnect and dateTimeDisconnect. For example, their values could be exchanged with random values and the real values can be stored in a separate database that is encrypted. Hence, only in case of a detected intrusion the second database would be queried for the identity of the caller. Additionally, only system administrators would be authorized to execute this query. An alternative solution is the protection of the CDRs. This can be accomplished via applying an access control system for the systems processing the CDRs. In this example these are the PBX, CDRAS, IDS, and the destination. These systems or devices possess access control systems that need to be configured adequately. An issue with access control is that physical access to the devices may provide access to data storage. An attacker could access the data on these physical devices directly and, thus, bypass the access control mechanism. Hence, if access control is used without encryption, the physical security of the devices has to be ensured as well.

The privacy requirements state that users shall be informed, if their personal information in CDRs is used for a purpose that differs from the purpose these were collected for. In this case users should be allowed not to participate.

The source and the destination are user telephones. Hence, users are located at these locations in our scenario. The destination is assumed to be users inside a company. These can be informed in a meeting before using the telephone system for the first time and their informed consent can be collected or they deny their consent and the system is not used for these destinations. This step is omitted in Figure 5.3 for simplicities sake. Collecting an informed consent from the source, however, is difficult. For practical reasons, not every source can be queried.

However, there are alternative options: the PBX can repeat an automated recorded message for callers calling the first time that informs the caller of the usage of CDRAS and asks for his/her agreement or disagreement. Alternatively, the callers could be asked by their respective providers, and a PBX could include a list of providers who ask for that consent.

Further, the confidentiality requirements for CDRs are addressed. This requires the configuration of access control measures in VoIP hard- and soft phones, as well as the PBX, the IDS and CDRAS. The configuration has to reflect that only administrators are allowed to investigate CDRs and that the access to the CDRs is recorded in, e.g., log files. These files have to reflect the names of the persons that accessed the CDRs. Hence, non-repudiation of access to CDRs is guaranteed. Otherwise it is not possible to prove that the privacy requirement, confidentiality, is fulfilled.

An HMAC algorithm is used as specified in RFC 2104 [IET97] and based on [JJQ07] in order to generate the pseudonyms for all the CDRs fields containing primary personal information. These are the original IP address, calling party number, calling party Unicode login user ID, original Media Transport Address IP and port, destination IP address, original called party number, final called party number, destination media transport address IP and port. HMAC is used, because it uses a hash function that gets the data in the CDRs as input and it gets a hash value as output. It is unlikely that two different inputs result in the same output. HMAC also gets a key that has an impact on the output. Thus, an attacker cannot simply use the hash algorithm and try to guess the input and check the output. For an attack, the attacker also has to guess the key, which makes the problem more complex.

One problem that pseudonymization however cannot solve, is the prevention of a statistical attack on the technical call details.

10.2 Fulfilling the Privacy Requirements

As can be seen in Figure 10.1 there are different solutions for the mentioned privacy requirements. They are derived from user and system requirements in order to meet the law.

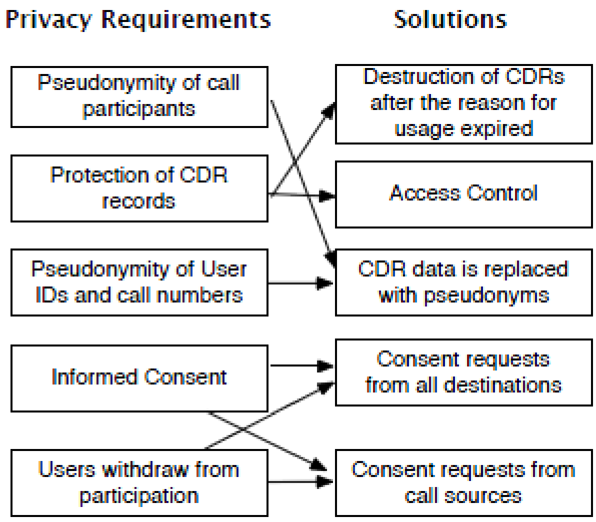

Privacy Requirements
Solutions
Pseudonymity of call participants
Protection of CDR records
Pseudonymity of User IDs and call numbers
Informed Consent
Users withdraw from participation
Destruction of CDRs after the reason for usage expired
Access Control
CDR data is replaced with pseudonyms
Consent requests from all destinations
Consent requests from call sources

Figure 10.1: Relations between privacy requirements and chosen solutions

There is an increasing need for privacy, as the amount of data is rising and the users get more global. There are for instance mobile devices, carrying CDRs. The security of all kinds of devices and its data must be maintained.

The last chapter summarizes the contributions and benefits of this approach, also in respect to the privacy questions. Conclusions and possible future work rounds it up.

11 Summary of contributions and conclusion

This chapter gives an overview of the contributions provided and some concluding thoughts about the thesis and its results.

11.1 Summary of contributions

In essence the following contributions have been made:

- Introduction of a new model, based on a defense algorithm
- Semi-automatic generation of white-, grey- and black-lists
- Using a hybrid IDS (signature based and anomaly detection system)
- Considering privacy for CDRs analysis (privacy compliant analysis)
- Effective blocking of calls and sending feedback to the calling party

These contributions can serve as inspiration for further research in this area. The used model is a base model, which can be extended by two to three points. The model extension can be built on this thesis.

11.2 Conclusion

The question about the existence of privacy always plays an integral part in the usage of a communication media.

Regarding the research question, privacy concerns have been identified in respect to the MITM and toll fraud problems in VoIP. Only few solutions have privacy considerations in their solutions.

Therefore the PIA approach has been integrated in this work, which makes it possible to make a privacy compliant CDRs analysis of the provided data. The PIA approach seamlessly fits into the model and even can be enlarged.

So what are the lessons learned and how was it able to come up with the challenges? Of course there will always be parts, which cannot be taken under control with a technical system alone. Therefore, a combination of technical and organizational approaches is proposed as a holistic view on this topic.

It is not so much that the signaling with SIP has to be secured but that the data, the voice and video traffic, need to be transferred with the SRTP protocol. Although there are mechanisms to secure SIP and encrypt multimedia packets for secure transport with SRTP, the security features are often not used by the users. Neither the communication partners authenticate at the beginning of the conversation, nor are the multimedia packets encrypted and secured against manipulation.

SRTP was developed to maintain the confidentiality and integrity of VoIP data. The integrity is forced by SHA-1 signing of the packet. Another advantage is that SRTP is tolerant against packet loss. So how can a company best protect its VoIP network from these sorts of threats?

It should protect itself on three levels: network architecture, security protocols and user interaction. At the network level, hosting VoIP on a VPN does a good job of separating VoIP's security holes from the underlying data network. Like all computer systems exposed to outside vulnerabilities, a VoIP network should be covered by firewalls, anti-virus programs and a sturdy IPS.

At the user level, company employees should be trained and instructed not to use high security risk applications, such as Google Talk [GOO10], Skype [SKY10] or other hosted IP voice technologies that could expose the company's VoIP network to outside attacks. A new generation of firewalls, called SBC addresses most of these problems, concerning QOS parameters such as packet delay, packet loss and packets jitter. [BD06] Finally, the complex nature of VoIP infrastructure demands a different approach to security. A VoIP network consists of a wide range of components and applications such as telephone handsets, conferencing units, mobile units, call processors/call managers, gateways, routers, firewalls and specialized protocols. As a result, a system-level approach where security is built into all of the infrastructure layers and coordinated via a centralized control center is required [MITM18].

CDRAS prevents unauthorized access to voice systems and a further objective of the tool is that of providing a method which allows for the selective application of custom filters to the whitelist. This will make it even harder for attackers and we can be more secure again.

A lightweight VoIP security method has been established that prevents attacks via analyzing communication records. The approach can be integrated into existing VoIP systems with little effort. The method also incorporates privacy requirements elicited from laws and regulations in the US and EU.

11.3 Main benefits of this approach

- A structured method to provide VoIP security using communication records
- Systematic identification of relevant privacy threats and determining privacy mechanisms for communication records
- Improving the security of existing VoIP communication systems by adding security for communication records analysis
- Support lawful operating communication security systems via fulfilling legal privacy requirements

Future work is a system-based approach that combines network and host-based security devices, as well as applications with sophisticated, systems level threat mitigation systems. In the future, the approach can be extended to protect VoIP infrastructures from further attacks. The approach will consider the privacy requirements presented in this thesis for all further types of attacks.

The method includes also a structured privacy engineering approach that prevents privacy violations during the communication data records analysis. Thereby the contribution is to prevent VoIP attacks on VoIP systems on the one hand and preserve the privacy of the call participants on the other hand.

11.4 Privacy relevant benefits of this Approach

- A structured method to prevent VoIP attacks
- Systematic identification of relevant privacy threats and determining privacy mechanisms for communication records
- Improving the outcome of communication systems implementations by adding security from communication records analysis
- Re-using the structured techniques of privacy engineering methods for the analysis and elicitation of privacy requirements to support lawful operating communication security systems

Also the legal situation in the US and Germany has been presented. In addition, several existing privacy guidelines, e.g., from the OECD and the common criteria have been shown. Further an approach that analyses the privacy requirements and choosing mechanisms to preserve it.

Choosing and implementing privacy mechanisms is a complex task and should be considered as early in system design as possible. Moreover, the engineers building a system that considers privacy should always consider if there is a way around the collection of personal information. Unfortunately, this is very difficult concerning communication data records, because almost every data set in these can be classified as personal information.

The work presented here will be extended with a privacy preserving VoIP systems approach. An approach to design a privacy preserving system depends upon the requirements of a given system. These include the requirements of laws from the country the system operates in and the different goals from the stakeholders involved. It is planned to extend this approach with a structured analysis method that allows a more fine grained elicitation of privacy requirements.

In addition, a set of configurations of the CDRAS system will be provided that restrict the use of the personal information according to given laws and stakeholders involved.

A structured method to conduct a privacy impact analysis has been established, for example when analyzing communication records for security purposes. The approach provides a structured analysis of privacy requirements from users and laws.

11.5 Overall benefits of the approach

A structured method to conduct a PIA, considering privacy requirements from users and laws, systematic pattern-based identification of privacy requirements for communication records, ease the burden of identifying privacy measures that fulfill the requirements, improve the privacy preservation of call participants during security analysis of communication records, systematic identification of relevant privacy threats and determining privacy mechanisms for communication records, improve the outcome of communication systems implementations by adding security from communication record analysis, re-use the structured techniques of privacy engineering methods for analyzing and elicitation of privacy requirements to support the lawful operation of communication security systems. For future work, the systematic privacy analysis can be extended to further security analysis, for instance, the usage of cloud computing services.

The thesis has already been input for research in other domains, as can be seen in the latest submission to ARES 2013 conference with the paper "A Method for Re-Using existing ITIL processes for creating and ISO27001 Information Security Management System (ISMS) process applied to a high availability video conferencing cloud scenario.

Many companies have already adopted their business processes to be in accordance with defined and organized standards. Two standards that are sought after by companies are ITIL and ISO 27001. Often companies start certifying their business processes with ITIL and continue with ISO 27001. For small and medium-sized businesses, it is difficult to prepare and maintain the ISO 27001 certification. The IT departments of these companies often do not have the time to fully observe standards as part of their daily routine. ITIL and

ISO 27001 perfectly fit into companies and help reduce errors through the standardization and comparability of products and services between themselves and other companies and partners. ISO 27001 specifically looks at security risks, countermeasures and remedial actions.

Processes need to be in place for implementing ITIL in an organization's business processes. A cloud service provider is used as a running example and compares ITIL processes with ISO 27001 processes. It is identified which aspects of these two standards can be better executed.

A mapping between ITIL and ISO 27001 is proposed that makes them easier to understand and assists with the certification process. It is further shown how to prepare for audits as well as re-certification. Often, these two processes are seen separately and not in conjunction, where synergies can be exploited. Legal requirements, compliance and data security play an integral part in this process. In essence, checklists and guidelines for companies, who want to prepare for standardization or that are already certified, but want to improve their business processes, are presented.

The move towards cloud services is accelerating the rate at which companies develop, and the use of such service requires the sharing of large amounts of data in a secure and scalable way. ITIL and ISO 27001 help companies to achieve customer friendliness and high quality services and support. Without standardization, a lot of manual effort, growing cost and complexity for an organization arise, as the number of their service partners grows.

An organization should definitely start with certifying ITIL and proceed with the ISO 27001 security afterwards. The basis for the ITIL certification is an understanding of ITIL itself, quality assurance and knowledge of the business processes in place. Capacity management assures that there is no capacity shortage on the provider side, as well as on the customer side. Regular checks and warnings, based on defined thresholds help to meet the capacity requirements and plan for expected growth. Exceptionally fast growth or the adding of resources must be planned, organized and scheduled, with the cloud provider service manager. This is an important step towards supporting the client or customer. At the base of the organizational hierarchy is the first level desk, then the technical engineers, the service manager and a department manager or even CEO. The involvement of these roles depends on the defined SLAs and the target-, reaction time to solve incidents.

The ISO 27001 standard defines the requirements for establishing and maintaining an Information Security Management System (ISMS) [ISO05]. In particular, the standard describes the process of creating a model of the entire business risks of a given organization and specific requirements for the implementation of security controls. The ISO 27001 standard is structured according to the "Plan-Do-Check-Act" (PDCA) model, the so-called ISO 27001 process [ISO05]. In the Plan phase an ISMS is established, in the Do phase the ISMS is implemented and operated, in the Check phase the ISMS is monitored and reviewed, and in the Act phase the ISMS is maintained and improved. In the Plan phase, the scope and boundaries of the ISMS, its interested parties, environment, assets, and all the technology involved are defined. In this phase also the ISMS policies, risk assessments, evaluations, and controls are defined. Controls in the ISO 27001 are measures to modify risk.

The ISO 27001 standard demands the creation of a set of documents and the certification of an ISO 27001 compliant ISMS is based upon these documents. Changes in the organization or technology also have to comply with the documented ISMS requirements. Furthermore, the standard demands periodic audits towards the effectiveness of an ISMS. These audits are also conducted using documented ISMS requirements.

In addition, the ISO 27001 standard demands that management decisions, providing support for establishing and maintaining an ISMS, are documented as well. This support has to be documented via management decisions, which has to be proven.

ITIL [ITI12] is a collection of best practices for implementing an IT service management. The standard provides example processes for typical tasks regarding IT management. The standard also provides tools of how to consider planning, establishing, supporting and optimizing of IT services in order to achieve business goals. ITIL is a de facto standard for the creation, establishment and management of critical processes. ITIL contains generic descriptions and is independent of vendors or technology. ITIL provides a set of process that contain: basic requirements for the process, goals of the process, pattern for procedures and roles, interfaces for different processes, hints for critical success factors, suggestions for measuring key performance indicators (KPI) and knowledge about success criteria for deploying the process.

Cost, flexibility and ease of operation are driving more and more organizations into the cloud. We differentiate here between the public cloud, with cloud services of providers such as Amazon or Salesforce and the private cloud of virtualized services running on an organization’s privately run hardware and software. It is not easy for a huge organization to transition everything over to the cloud at once, because then parts of the business critical systems and services are already transitioned into the cloud and some are not. Cloud integration platform help solve this issue and help unite those services. With the cloud integration platform it becomes much easier for global cloud players to sell cloud services to their partners.

The two standards, ITIL and ISO 27001 are capable of mappings between them. We are using steps from the ITIL process as input for the ISO 27001 process. With these inputs, an output can be generated, which means that the result of the ITIL process serves as input for the ISO 27001 activities. There are different action items regarding countermeasures within the ITIL and ISO 27001 standards. So how can the company compliance still be assured after the mapping between the ITIL and ISO 27001 processes took place? It is a matter of compliance regarding the privacy and legislation of the involved participants and entities. ITIL and ISO 27001 have in common that they are both based on the PDCA model. From ITIL point of view, nearly all security controls in ISO 27001 are part of ITIL service management. It is also in the ITIL standard, chapter on service design that there is a reference on ISO 27001. The advantage of this approach is that the company's information security department is in line with the risk management department, regarding which ITIL processes have been implemented through ISO 27001. The information security department can also easily identify which ISO 27001 objectives are already met through the use of ITIL and which still must be handled.

Using this hybrid approach, considering ITIL and ISO 27001 together, companies can save a lot of time and money using mutual synergies and knowledge in this area. The need to use both standards at the same time is to establish a well-known information security process that covers all relevant aspects. If doing so, a company can rely on acceptable security levels, effectively manage risks and reduce overall risk levels.

Only with a thorough configured monitoring and alerting system it is possible to conduct effective risk management. The goal is to mitigate risks and be aware of new risks. A classification of the monitored assets is important to easily identify the severity of an incident. Reaction times, escalation times, contact with partners and producers and time to recover are heavily dependent on the severity of an incident. The higher the severity is, the faster is the required reaction times, escalation times, communication with partners and producers and recovery time. Only if an organization is certified in its core business areas, can it be able to embark upon business continuity and disaster recovery planning. Certified personnel as well as experience and knowledge in the matter of subjects are a plus. Input for this is the documentation of all necessary information and changes. The documentation must be extended and kept up to date at every chance. It is important to define boundaries to stakeholders and produce a control list consisting of action items as well. The boundaries to stakeholders serve as input for Annex A of the ISO 27001 standard.

The cloud providers of course will get the chance to improve their offer in the second phase towards the customer. A feedback process from the cloud customer to the cloud provider after the first phase is recommended. The services provided to the customer are defined in a contract between the two parties involved. In this contract the service levels are expressed in SLA, as well as the response times during business hours and after business hours are defined. A high customer satisfaction rate is assured through security, availability and confidence in the cloud provider. The cloud provider has established processes and policies that maintain the security of the customer data. A confident handling of customer information and infrastructure is based on the consequent implementation of rules and processes, which are embedded in policies and specified in standards and operational guidelines. Implementing these guidelines is the duty of the cloud providers' employees. Based on these policies, responsibilities, roles, behavior, process definitions and supporting technologies are derived.

For the change log within the service delivery, all changes in the productive environment must be logged. The structure of the change log is as follows: The first column is filled with an incremental ID, followed by the name of the change owner. The initiator of the change, which can vary, comes next. After that, the change cause, described in words or referring to a support ticket is listed. Next is the hostname, where the change is carried out, following the change description in descriptive language as well as the configuration changes itself in computer language. The category of the change is classified in regular, emergency and standard changes. It has to be defined, which duties belong to a standard change. If a change is non-standard, it is qualified by the engineer as a non-standard change. All productive changes have to be scheduled and appropriate configuration and fallback procedures in place prior to executing the change.

The last possibility is a non-operational relevant change. This means changes in non-productive environments and no scheduling of the change is needed. The risk of the change can vary from low to medium to high. At the end, a control check is performed, where the name of the change approver as well as the date the change was approved and the date the change was carried out, are documented.

Last, but not least, a flag is inserted stating whether the change was successful or not. Changes are executed, following a four eye principle. With this feature, errors can be minimized and the overall availability and customer satisfaction is high. Urgent changes or emergency changes can be delivered faster, but require the consent of the Change Advisory Board (CAB).

List of Figures

List of Tables

Appendix I: SQL Code

Create tables in Oracle Apex, Oracle Database 11g Express Edition:

```
delete from GREYLISTPRIMARY;

delete from WHITELISTPRIMARY;

delete from BLACKLISTPRIMARY;

create table whitelistprimary
(
    cdrRecordType        varchar (50),
    globalCallID_callManagerID   varchar (50),
    globalCallID_callId      varchar (50),
    origLegCallIdentifier      varchar (50),
    dateTimeOrigination      varchar (50),
    origNodeId       varchar (50),
    origSpan         varchar (50),
    origIpAddr        varchar (50),
    callingPartyNumber      varchar (50),
    callingPartyUnicodeLoginUserID   varchar (50),
    origCause_location       varchar (50),
    origCause_value        varchar (50),
    origPrecedenceLevel      varchar (50),
    origMediaTransportAddress_IP    varchar (50),
    origMediaTransportAddress_Port   varchar (50),
    origMediaCap_payloadCapability   varchar (50),
    origMediaCap_maxFramesPerPacke   varchar (50),
    origMediaCap_g723BitRate     varchar (50),
    origVideoCap_Codec      varchar (50),
    origVideoCap_Bandwidth      varchar (50),
    origVideoCap_Resolution      varchar (50),
    origVideoTransportAddress_IP     varchar (50),
    origVideoTransportAddress_Port   varchar (50),
    origRSVPAudioStat      varchar (50),
    origRSVPVideoStat      varchar (50),
    destLegIdentifier      varchar (50),
    destNodeId        varchar (50),
    destSpan          varchar (50),
    destIpAddr        varchar (50),
    originalCalledPartyNumber   varchar (50),
    finalCalledPartyNumber      varchar (50),
    finalCalledPartyUnicodeLoginUs   varchar (50),
    destCause_location       varchar (50),
    destCause_value         varchar (50),
    destPrecedenceLevel       varchar (50),
    destMediaTransportAddress_IP    varchar (50),
    destMediaTransportAddress_Port   varchar (50),
    destMediaCap_payloadCapability   varchar (50),
    destMediaCap_maxFramesPerPacke   varchar (50),
    destMediaCap_g723BitRate     varchar (50),
    destVideoCap_Codec     varchar (50),
    destVideoCap_Bandwidth     varchar (50),
    destVideoCap_Resolution     varchar (50),
    destVideoTransportAddress_IP    varchar (50),
    destVideoTransportAddress_Port   varchar (50),
    destRSVPAudioStat     varchar (50),
    destRSVPVideoStat     varchar (50),
    dateTimeConnect         varchar (50),
    dateTimeDisconnect       varchar (50),
    lastRedirectDn         varchar (50),
    pkid            varchar (50),
    originalCalledPartyNumberParti   varchar (50),
    callingPartyNumberPartition    varchar (50),
    finalCalledPartyNumberPartitio   varchar (50),
    lastRedirectDnPartition       varchar (50),
    duration        varchar (50),
    origDeviceName        varchar (50),
    destDeviceName        varchar (50),
    origCallTerminationOnBehalfOf    varchar (50),
    destCallTerminationOnBehalfOf    varchar (50),
    origCalledPartyRedirectOnBehal    varchar (50),
    lastRedirectRedirectOnBehalfOf    varchar (50),
    origCalledPartyRedirectReason    varchar (50),
    lastRedirectRedirectReason   varchar (50),
    destConversationId       varchar (50),
    globalCallId_ClusterID     varchar (50),
    joinOnBehalfOf        varchar (50),
    commentonit       varchar (50),
    authCodeDescription      varchar (50),
    authorizationLevel     varchar (50),
    clientMatterCode     varchar (50),
    origDTMFMethod       varchar (50),
    destDTMFMethod       varchar (50),
    callSecuredStatus      varchar (50),
    origConversationId      varchar (50),
    origMediaCap_Bandwidth      varchar (50),
    destMediaCap_Bandwidth      varchar (50),
    authorizationCodeValue      varchar (50),
    outpulsedCallingPartyNumber   varchar (50),
    outpulsedCalledPartyNumber    varchar (50),
    origIpv4v6Addr      varchar (50),
    destIpv4v6Addr      varchar (50),
    origVideoCap_Codec_Channel2    varchar (50),
    origVideoCap_Bandwidth_Channel    varchar (50),
    origVideoCap_Resolution_Channe   varchar (50),
    origVideoTransportAddress_IP_C    varchar (50),
    origVideoTransportAddress_P_C2   varchar (50),
    origVideoChannel_Role_Channel2   varchar (50),
    destVideoCap_Codec_Channel2    varchar (50),
    destVideoCap_Bandwidth_Channel    varchar (50),
    destVideoCap_Resolution_Channe   varchar (50),
    destVideoTransportAddress_IP_C    varchar (50),
        destVideoTransportAddress_P_C2   varchar (50),
        destVideoChannel_Role_Channel2   varchar (50),
        incomingProtocolID     varchar (50),
        incomingProtocolCallRef      varchar (50),
        outgoingProtocolID      varchar (50),
        outgoingProtocolCallRef       varchar (50),
        currentRoutingReason      varchar (50),
        origRoutingReason       varchar (50),
        lastRedirectingRoutingReason   varchar (50),
        huntPilotDN        varchar (50),
        huntPilotPartition       varchar (50),
        calledPartyPatternUsage      varchar (50),
        outpulsedOriginalCalledPartyNu    varchar (50),
        outpulsedLastRedirectingNumber   varchar (50)
    );

    create table greylistprimary
    (
        cdrRecordType        varchar (50),
        globalCallID_callManagerID   varchar (50),
        globalCallID_callId      varchar (50),
        origLegCallIdentifier      varchar (50),
        dateTimeOrigination      varchar (50),
        origNodeId       varchar (50),
        origSpan        varchar (50),
        origIpAddr       varchar (50),
    callingPartyNumber      varchar (50),
    callingPartyUnicodeLoginUserID   varchar (50),
    origCause_location       varchar (50),
    origCause_value         varchar (50),
    origPrecedenceLevel       varchar (50),
    origMediaTransportAddress_IP    varchar (50),
    origMediaTransportAddress_Port   varchar (50),
    origMediaCap_payloadCapability   varchar (50),
    origMediaCap_maxFramesPerPacke   varchar (50),
    origMediaCap_g723BitRate     varchar (50),
    origVideoCap_Codec      varchar (50),
    origVideoCap_Bandwidth      varchar (50),
    origVideoCap_Resolution      varchar (50),
    origVideoTransportAddress_IP    varchar (50),
    origVideoTransportAddress_Port   varchar (50),
    origRSVPAudioStat      varchar (50),
    origRSVPVideoStat      varchar (50),
    destLegIdentifier      varchar (50),
    destNodeId        varchar (50),
    destSpan         varchar (50),
    destIpAddr        varchar (50),
    originalCalledPartyNumber   varchar (50),
    finalCalledPartyNumber      varchar (50),
    finalCalledPartyUnicodeLoginUs   varchar (50),
    destCause_location       varchar (50),
    destCause_value         varchar (50),
    destPrecedenceLevel      varchar (50),
    destMediaTransportAddress_IP    varchar (50),
    destMediaTransportAddress_Port   varchar (50),
    destMediaCap_payloadCapability   varchar (50),
    destMediaCap_maxFramesPerPacke   varchar (50),
    destMediaCap_g723BitRate    varchar (50),
    destVideoCap_Codec     varchar (50),
    destVideoCap_Bandwidth     varchar (50),
    destVideoCap_Resolution     varchar (50),
    destVideoTransportAddress_IP    varchar (50),
    destVideoTransportAddress_Port   varchar (50),
    destRSVPAudioStat     varchar (50),
    destRSVPVideoStat     varchar (50),
    dateTimeConnect         varchar (50),
    dateTimeDisconnect       varchar (50),
    lastRedirectDn         varchar (50),
    pkid            varchar (50),
    originalCalledPartyNumberParti   varchar (50),
    callingPartyNumberPartition    varchar (50),
    finalCalledPartyNumberPartitio   varchar (50),
    lastRedirectDnPartition       varchar (50),
    duration        varchar (50),
    origDeviceName        varchar (50),
    destDeviceName        varchar (50),
    origCallTerminationOnBehalfOf    varchar (50),
    destCallTerminationOnBehalfOf    varchar (50),
    origCalledPartyRedirectOnBehal    varchar (50),
    lastRedirectRedirectOnBehalfOf    varchar (50),
    origCalledPartyRedirectReason    varchar (50),
    lastRedirectRedirectReason   varchar (50),
    destConversationId       varchar (50),
    globalCallId_ClusterID     varchar (50),
    joinOnBehalfOf         varchar (50),
    commentonit       varchar (50),
    authCodeDescription      varchar (50),
    authorizationLevel     varchar (50),
    clientMatterCode     varchar (50),
    origDTMFMethod       varchar (50),
    destDTMFMethod       varchar (50),
    callSecuredStatus       varchar (50),
    origConversationId       varchar (50),
    origMediaCap_Bandwidth       varchar (50),
    destMediaCap_Bandwidth       varchar (50),
    authorizationCodeValue      varchar (50),
    outpulsedCallingPartyNumber   varchar (50),
    outpulsedCalledPartyNumber    varchar (50),
    origIpv4v6Addr       varchar (50),
    destIpv4v6Addr       varchar (50),
    origVideoCap_Codec_Channel2     varchar (50),
    origVideoCap_Bandwidth_Channel    varchar (50),
    origVideoCap_Resolution_Channe   varchar (50),
    origVideoTransportAddress_IP_C    varchar (50),
        origVideoTransportAddress_P_C2   varchar (50),
        origVideoChannel_Role_Channel2   varchar (50),
        destVideoCap_Codec_Channel2     varchar (50),
        destVideoCap_Bandwidth_Channel    varchar (50),
        destVideoCap_Resolution_Channe   varchar (50),
        destVideoTransportAddress_IP_C    varchar (50),
        destVideoTransportAddress_P_C2   varchar (50),
        destVideoChannel_Role_Channel2   varchar (50),
        incomingProtocolID     varchar (50),
        incomingProtocolCallRef      varchar (50),
        outgoingProtocolID      varchar (50),
        outgoingProtocolCallRef       varchar (50),
        currentRoutingReason      varchar (50),
        origRoutingReason       varchar (50),
        lastRedirectingRoutingReason   varchar (50),
        huntPilotDN        varchar (50),
        huntPilotPartition       varchar (50),
        calledPartyPatternUsage      varchar (50),
        outpulsedOriginalCalledPartyNu    varchar (50),
        outpulsedLastRedirectingNumber   varchar (50)
    );

    create table blacklistprimary
    (
        cdrRecordType        varchar (50),
        globalCallID_callManagerID   varchar (50),
    globalCallID_callId     varchar (50),
    origLegCallIdentifier     varchar (50),
    dateTimeOrigination     varchar (50),
    origNodeId      varchar (50),
    origSpan        varchar (50),
    origIpAddr      varchar (50),
    callingPartyNumber     varchar (50),
    callingPartyUnicodeLoginUserID   varchar (50),
    origCause_location      varchar (50),
    origCause_value       varchar (50),
    origPrecedenceLevel     varchar (50),
    origMediaTransportAddress_IP    varchar (50),
    origMediaTransportAddress_Port   varchar (50),
    origMediaCap_payloadCapability   varchar (50),
    origMediaCap_maxFramesPerPacke   varchar (50),
    origMediaCap_g723BitRate    varchar (50),
    origVideoCap_Codec     varchar (50),
    origVideoCap_Bandwidth     varchar (50),
    origVideoCap_Resolution     varchar (50),
    origVideoTransportAddress_IP    varchar (50),
    origVideoTransportAddress_Port   varchar (50),
    origRSVPAudioStat     varchar (50),
    origRSVPVideoStat     varchar (50),
    destLegIdentifier     varchar (50),
    destNodeId      varchar (50),
    destSpan        varchar (50),
    destIpAddr        varchar (50),
    originalCalledPartyNumber   varchar (50),
    finalCalledPartyNumber      varchar (50),
    finalCalledPartyUnicodeLoginUs   varchar (50),
    destCause_location      varchar (50),
    destCause_value        varchar (50),
    destPrecedenceLevel      varchar (50),
    destMediaTransportAddress_IP   varchar (50),
    destMediaTransportAddress_Port   varchar (50),
    destMediaCap_payloadCapability   varchar (50),
    destMediaCap_maxFramesPerPacke   varchar (50),
    destMediaCap_g723BitRate    varchar (50),
    destVideoCap_Codec     varchar (50),
    destVideoCap_Bandwidth     varchar (50),
    destVideoCap_Resolution     varchar (50),
    destVideoTransportAddress_IP    varchar (50),
    destVideoTransportAddress_Port   varchar (50),
    destRSVPAudioStat     varchar (50),
    destRSVPVideoStat     varchar (50),
    dateTimeConnect        varchar (50),
    dateTimeDisconnect      varchar (50),
    lastRedirectDn        varchar (50),
    pkid           varchar (50),
    originalCalledPartyNumberParti   varchar (50),
    callingPartyNumberPartition    varchar (50),
    finalCalledPartyNumberPartitio   varchar (50),
    lastRedirectDnPartition       varchar (50),
    duration        varchar (50),
    origDeviceName        varchar (50),
    destDeviceName        varchar (50),
    origCallTerminationOnBehalfOf    varchar (50),
    destCallTerminationOnBehalfOf    varchar (50),
    origCalledPartyRedirectOnBehal    varchar (50),
    lastRedirectRedirectOnBehalfOf    varchar (50),
    origCalledPartyRedirectReason    varchar (50),
    lastRedirectRedirectReason   varchar (50),
    destConversationId       varchar (50),
    globalCallId_ClusterID     varchar (50),
    joinOnBehalfOf         varchar (50),
    commentonit       varchar (50),
    authCodeDescription      varchar (50),
    authorizationLevel     varchar (50),
    clientMatterCode     varchar (50),
    origDTMFMethod       varchar (50),
    destDTMFMethod       varchar (50),
    callSecuredStatus      varchar (50),
    origConversationId      varchar (50),
    origMediaCap_Bandwidth      varchar (50),
    destMediaCap_Bandwidth      varchar (50),
    authorizationCodeValue      varchar (50),
    outpulsedCallingPartyNumber   varchar (50),
    outpulsedCalledPartyNumber    varchar (50),
    origIpv4v6Addr       varchar (50),
    destIpv4v6Addr       varchar (50),
    origVideoCap_Codec_Channel2     varchar (50),
    origVideoCap_Bandwidth_Channel    varchar (50),
    origVideoCap_Resolution_Channe   varchar (50),
    origVideoTransportAddress_IP_C    varchar (50),
    origVideoTransportAddress_P_C2   varchar (50),
    origVideoChannel_Role_Channel2   varchar (50),
    destVideoCap_Codec_Channel2     varchar (50),
    destVideoCap_Bandwidth_Channel    varchar (50),
    destVideoCap_Resolution_Channe   varchar (50),
    destVideoTransportAddress_IP_C    varchar (50),
    destVideoTransportAddress_P_C2   varchar (50),
    destVideoChannel_Role_Channel2   varchar (50),
    incomingProtocolID     varchar (50),
    incomingProtocolCallRef      varchar (50),
    outgoingProtocolID      varchar (50),
    outgoingProtocolCallRef       varchar (50),
    currentRoutingReason      varchar (50),
    origRoutingReason       varchar (50),
    lastRedirectingRoutingReason   varchar (50),
    huntPilotDN        varchar (50),
    huntPilotPartition       varchar (50),
    calledPartyPatternUsage      varchar (50),
    outpulsedOriginalCalledPartyNu    varchar (50),
    outpulsedLastRedirectingNumber   varchar (50)
```

```
);
```

SQL code run in SQL Developer:

```
INSERT INTO WHITELISTPRIMARY (
select * from unfilteredprimary where duration between 1 AND 120);

INSERT INTO GREYLISTPRIMARY (
select * from unfilteredprimary where duration <=0);

INSERT INTO BLACKLISTPRIMARY (
select * from unfilteredprimary where duration >120);
```

Appendix II: Example CDRs

Example CDRs taken from Cisco Callmanager, Version 8.6:

```
cdrRecordType,globalCallID_callManagerId,globalCallID_callId,origLegCallIdentifier,dateTimeOrigination,origNodeId,origSpan,origIpAddr,callingPartyNumber,callingPartyUnicodeLoginUserID,origCause_location,origCause_value,origPrecedenceLevel,origMediaTransportAddress_IP,origMediaTransportAddress_Port,origMediaCap_payloadCapability,origMediaCap_maxFramesPerPacket,origMediaCap_g723BitRate,origVideoCap_Codec,origVideoCap_Bandwidth,origVideoCap_Resolution,origVideoTransportAddress_IP,origVideoTransportAddress_Port,origRSVPAudioStat,origRSVPVideoStat,destLegIdentifier,destNodeId,destSpan,destIpAddr,originalCalledPartyNumber,finalCalledPartyNumber,finalCalledPartyUnicodeLoginUserID,destCause_location,destCause_value,destPrecedenceLevel,destMediaTransportAddress_IP,destMediaTransportAddress_Port,destMediaCap_payloadCapability,destMediaCap_maxFramesPerPacket,destMediaCap_g723BitRate,destVideoCap_Codec,destVideoCap_Bandwidth,destVideoCap_Resolution,destVideoTransportAddress_IP,destVideoTransportAddress_Port,destRSVPAudioStat,destRSVPVideoStat,dateTimeConnect,dateTimeDisconnect,lastRedirectDn,pkid,originalCalledPartyNumberPartition,callingPartyNumberPartition,finalCalledPartyNumberPartition,lastRedirectDnPartition,duration,origDeviceName,destDeviceName,origCallTerminationOnBehalfOf,destCallTerminationOnBehalfOf,origCalledPartyRedirectOnBehalfOf,lastRedirectRedirectOnBehalfOf,origCalledPartyRedirectReason,lastRedirectRedirectReason,destConversationId,globalCallId_ClusterID,joinOnBehalfOf,comment,authCodeDescription,authorizationLevel,clientMatterCode,origDTMFMethod,destDTMFMethod,callSecuredStatus,origConversationId,origMediaCap_Bandwidth,destMediaCap_Bandwidth,authorizationCodeValue,outpulsedCallingPartyNumber,outpulsedCalledPartyNumber,origIpv4v6Addr,destIpv4v6Addr,origVideoCap_Codec_Channel2,origVideoCap_Bandwidth_Channel2,origVideoCap_Resolution_Channel2,origVideoTransportAddress_IP_Channel2,origVideoTransportAddress_Port_Channel2,origVideoChannel_Role_Channel2,destVideoCap_Codec_Channel2,destVideoCap_Bandwidth_Channel2,destVideoCap_Resolution_Channel2,destVideoTransportAddress_IP_Channel2,destVideoTransportAddress_Port_Channel2,destVideoChannel_Role_Channel2,incomingProtocolID,incomingProtocolCallRef,outgoingProtocolID,outgoingProtocolCallRef,currentRoutingReason,origRoutingReason,lastRedirectingRoutingReason,huntPilotDN,huntPilotPartition,calledPartyPatternUsage,outpulsedOriginalCalledPartyNumber,outpulsedLastRedirectingNumber
```

```
1,1,3001,30284569,1353943361,1,0,-662562132,1002,xlite,0,0,4,-
662562132,16176,4,20,0,0,0,0,0,0,0,0,30284570,1,0,-847111508,1001,1001,\        ,0,16,4,-
847111508,24578,4,20,0,0,0,0,0,0,0,0,1353943369,1353943387,1001,a3086e83-a4dc-
4e51-a25f-
32e5868031e9,,,,,18,SEPDEADBEEF0000,SEPD4BED9411BF5,0,12,0,0,0,0,0,StandAlon
eCluster,0,,,0,,2,3,0,0,64,64,,,,172.26.130.216,172.26.130.205,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,,
0,0,0,,,2,,


1,1,2001,30267409,1353939019,1,0,-
847111508,1001,,0,16,4,0,0,0,0,0,0,0,0,0,0,0,0,30267410,0,0,0,,,,0,0,4,0,0,0,0,0,0,0,0,0,0,0
,0,0,1353939019,,e5e11c2d-5392-4ac0-8a32-
f4154d530f11,,,,,0,SEPD4BED9411BF5,,12,0,0,0,0,0,0,StandAloneCluster,0,,,0,,3,0,0,0,0,
0,,,,172.26.130.205,,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,,0,0,0,,,2,,


1,1,2002,30267411,1353939020,1,0,-
847111508,1001,,0,16,4,0,0,0,0,0,0,0,0,0,0,0,0,30267412,1,0,-
662562132,1002,1002,xlite,0,0,4,0,0,0,0,0,0,0,0,0,0,0,0,0,1353939037,1002,13ab0592-
f016-494b-ae29-
5517e0bce053,,,,,0,SEPD4BED9411BF5,SEPDEADBEEF0000,12,0,0,0,0,0,0,StandAlone
Cluster,0,,,0,,3,0,0,0,0,0,,,,172.26.130.205,,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,,0,0,0,,,2,,


1,1,2003,30267413,1353939226,1,0,-
847111508,1001,,0,16,4,0,0,0,0,0,0,0,0,0,0,0,0,30267414,1,0,-
662562132,1002,1002,xlite,0,0,4,0,0,0,0,0,0,0,0,0,0,0,0,0,1353939272,1002,a87b86b1-
cc16-4837-9a7c-
ae60e18d1a67,,,,,0,SEPD4BED9411BF5,SEPDEADBEEF0000,12,0,0,0,0,0,0,StandAlone
Cluster,0,,,0,,3,0,0,0,0,0,,,,172.26.130.205,,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,,0,0,0,,,2,,


1,1,2004,30267415,1353939273,1,0,-
847111508,1001,,0,16,4,0,0,0,0,0,0,0,0,0,0,0,0,30267416,0,0,0,,,,0,0,4,0,0,0,0,0,0,0,0,0,0,0
,0,0,1353939274,,05e6c638-9219-4e58-b35e-
7d43ff276314,,,,,0,SEPD4BED9411BF5,,12,0,0,0,0,0,0,StandAloneCluster,0,,,0,,3,0,0,0,0,
0,,,,172.26.130.205,,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,,0,0,0,,,2,,
1,1,2005,30267417,1353939274,1,0,-
847111508,1001,,0,16,4,0,0,0,0,0,0,0,0,0,0,0,0,30267418,0,0,0,,,,0,0,4,0,0,0,0,0,0,0,0,0,0,0
,0,0,1353939278,,0fd83ede-2203-48ea-b9f3-
6d339e72e9c1,,,,,0,SEPD4BED9411BF5,,12,0,0,0,0,0,0,StandAloneCluster,0,,,0,,3,0,0,0,0
,0,,,,172.26.130.205,,0,0,0,0,0,0,0,0,0,0,0,0,,0,,0,0,0,,,2,,
```

Appendix III: Example toll fraud attack

```
show isdn active

------------------------------------------------------------------------------

                    ISDN ACTIVE CALLS

------------------------------------------------------------------------------

Call   Calling     Called       Remote  Seconds Seconds Seconds Charges

Type   Number      Number       Name    Used    Left    Idle    Units/Currency

------------------------------------------------------------------------------

Out   40000000 +7165779386            +26242      0      0     0

Out      10000 +7165779386            +26164      0      0     0

Out      20000 +7165779388            +13197      0      0     0

Out      20000 +7165779388            +13190      0      0     0

Out         10 +7165779382            49559      0      0     0

Out         10 +7165779382            49556      0      0     0

Out         10 +7165779382            49534      0      0     0

Out         10 +7165779382            49532      0      0     0

Out         10 +7165779382            49529      0      0     0

Out         10 +7165779382            49521      0      0     0

Out    8066666 +7165779382               49491      0      0     0

Out    8066666 +7165779382               49488      0      0     0

Out    8066666 +7165779382               49484      0      0     0

Out    8066666 +7165779382               49481      0      0     0

Out    8066666 +7165779382               49479      0      0     0

Out    8066666 +7165779382               49448      0      0     0

Out    8066666 +7165779382               49446      0      0     0
Out     8066666 +7165779382              49446     0      0     0
Out     8066666 +7165779382              49446     0      0     0
Out     8066666 +7165779382              49446     0      0     0
Out     8066666 +7165779382              49432     0      0     0
Out     8066666 +7165779382              49431     0      0     0
Out     8066666 +7165779382              47890     0      0     0
Out     8066666 +7165779382              47886     0      0     0
Out       88800 +7165779384             43185     0      0     0
Out       88800 +7165779384             43184     0      0     0
Out     8066666 +7165779384                931     0      0     0
Out     8066666 +7165779384                930     0      0     0
Out     8066666 +7165779384                927     0      0     0
Out     8066666 +7165779384                926     0      0     0
```

```
show isdn active
-------------------------------------------------------------------------------
                          ISDN ACTIVE CALLS
-------------------------------------------------------------------------------
Call    Calling      Called       Remote  Seconds Seconds Seconds Charges
Type    Number       Number       Name    Used    Left    Idle    Units/Currency
-------------------------------------------------------------------------------
Out         232 +6308423348               145     0      0     0
```

```
show isdn active

--------------------------------------------------------------------------------

                        ISDN ACTIVE CALLS

--------------------------------------------------------------------------------

Call    Calling     Called      Remote  Seconds Seconds Seconds Charges

Type    Number       Number      Name    Used    Left    Idle    Units/Currency

--------------------------------------------------------------------------------

Out       amer +2599692169            185      0      0     0

Out       amer +0140496982            125      0      0     0
```

Appendix IV: Cisco Call manger 8.6 VMware Template

```
.encoding = "windows-1252"
config.version = "8"
virtualHW.version = "7"
scsi0.present = "TRUE"
scsi0.virtualDev = "lsilogic"
memsize = "2048"
scsi0:0.present = "TRUE"
scsi0:0.fileName = "CUCM86-000001.vmdk"
ide1:0.present = "TRUE"
ide1:0.fileName = "H:\CISCO\Bootable_UCSInstall_UCOS_8.6.2.22900-9.sgn.iso"
ide1:0.deviceType = "cdrom-image"
floppy0.startConnected = "FALSE"
floppy0.fileName = ""
floppy0.autodetect = "TRUE"
ethernet0.present = "TRUE"
ethernet0.connectionType = "bridged"
ethernet0.wakeOnPcktRcv = "FALSE"
ethernet0.addressType = "generated"
usb.present = "TRUE"
ehci.present = "TRUE"
sound.present = "TRUE"
sound.fileName = "-1"
sound.autodetect = "TRUE"
serial0.present = "TRUE"
serial0.fileType = "thinprint"
pciBridge0.present = "TRUE"
pciBridge4.present = "TRUE"
pciBridge4.virtualDev = "pcieRootPort"
pciBridge4.functions = "8"
pciBridge5.present = "TRUE"
pciBridge5.virtualDev = "pcieRootPort"
pciBridge5.functions = "8"
pciBridge6.present = "TRUE"
pciBridge6.virtualDev = "pcieRootPort"
pciBridge6.functions = "8"
pciBridge7.present = "TRUE"
pciBridge7.virtualDev = "pcieRootPort"
pciBridge7.functions = "8"
vmci0.present = "TRUE"
roamingVM.exitBehavior = "go"
displayName = "CUCM86"
guestOS = "rhel5"
nvram = "CUCM86.nvram"
virtualHW.productCompatibility = "hosted"
printers.enabled = "TRUE"
```

```
extendedConfigFile = "CUCM86.vmxf"

ethernet0.generatedAddress = "00:0c:29:d1:e9:e9"

tools.syncTime = "FALSE"

uuid.location = "56 4d ef ae 52 a9 f1 ef-65 36 5f 75 76 d1 e9 e9"

uuid.bios = "56 4d ef ae 52 a9 f1 ef-65 36 5f 75 76 d1 e9 e9"

cleanShutdown = "FALSE"

replay.supported = "FALSE"

replay.filename = ""

scsi0:0.redo = ""

pciBridge0.pciSlotNumber = "17"

pciBridge4.pciSlotNumber = "21"

pciBridge5.pciSlotNumber = "22"

pciBridge6.pciSlotNumber = "23"

pciBridge7.pciSlotNumber = "24"

scsi0.pciSlotNumber = "16"

usb.pciSlotNumber = "32"

ethernet0.pciSlotNumber = "33"

sound.pciSlotNumber = "34"

ehci.pciSlotNumber = "35"

vmci0.pciSlotNumber = "36"

vmotion.checkpointFBSize = "33554432"

ethernet0.generatedAddressOffset = "0"

vmci0.id = "1450432146"
```

```
checkpoint.vmState = ""

softPowerOff = "FALSE"

gui.exitOnCLIHLT = "FALSE"

numvcpus = "2"

tools.remindInstall = "FALSE"
```

Appendix V: Cisco Call manger 8.6 VMware OVF File

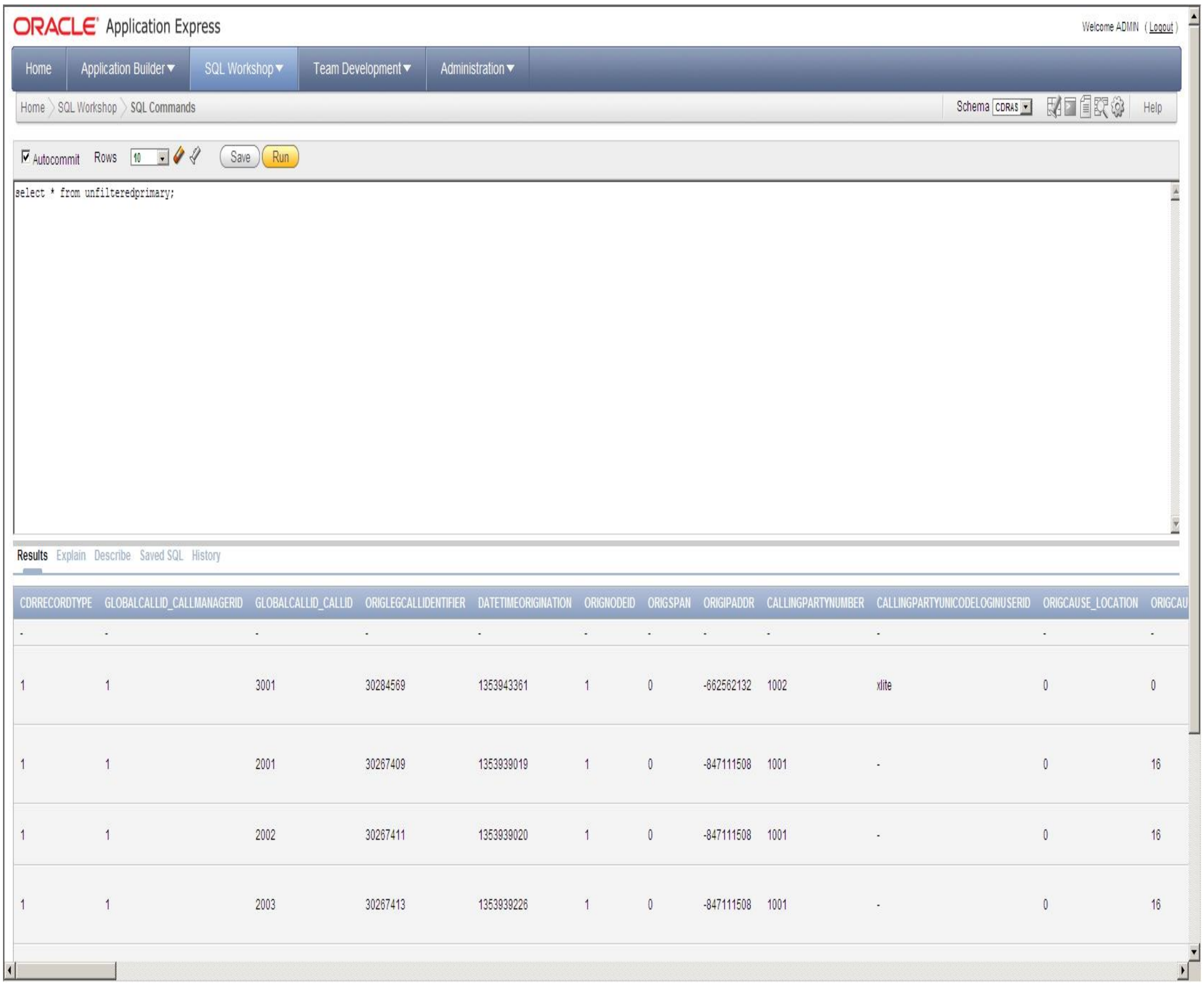
```
<?xml version="1.0" encoding="UTF-8"?>

<!--Generated by VMware ESX Server, User: root, UTC time: 2012-11-
21T01:59:03.165259Z-->

<Envelope vmw:buildId="build-469512" xmlns="http://schemas.dmtf.org/ovf/envelope/1"
xmlns:cim="http://schemas.dmtf.org/wbem/wscim/1/common"
xmlns:ovf="http://schemas.dmtf.org/ovf/envelope/1"
xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/CIM_ResourceAllocationSettingData"
xmlns:vmw="http://www.vmware.com/schema/ovf"
xmlns:vssd="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/CIM_VirtualSystemSettingData"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <References>

    <File ovf:href=" CUCM86.vmdk" ovf:id="file1" ovf:size="8066748416" />

    <File ovf:href="CUCM86.iso" ovf:id="file2" ovf:size="4819529728" />

  </References>

  <DiskSection>

    <Info>Virtual disk information</Info>

    <Disk ovf:capacity="160" ovf:capacityAllocationUnits="byte * 2^30"
ovf:diskId="vmdisk1" ovf:fileRef="file1"
ovf:format="http://www.vmware.com/interfaces/specifications/vmdk.html#streamOptimiz
ed" ovf:populatedSize="15668150272" />

  </DiskSection>

  <NetworkSection>

    <Info>The list of logical networks</Info>

    <Network ovf:name="VLAN_100">

      <Description>The VLAN_100 network</Description>

    </Network>

  </NetworkSection>
```

```
<VirtualSystem ovf:id="CUCM86">
  <Info>A virtual machine</Info>
  <Name> CUCM86</Name>
  <OperatingSystemSection ovf:id="79" ovf:version="5" vmw:osType="rhel5Guest">
    <Info>The kind of installed guest operating system</Info>
  </OperatingSystemSection>
  <VirtualHardwareSection>
    <Info>Virtual hardware requirements</Info>
    <System>
      <vssd:ElementName>Virtual Hardware Family</vssd:ElementName>
      <vssd:InstanceID>0</vssd:InstanceID>
      <vssd:VirtualSystemIdentifier> CUCM86</vssd:VirtualSystemIdentifier>
      <vssd:VirtualSystemType>vmx-08</vssd:VirtualSystemType>
    </System>
    <Item>
      <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
      <rasd:Description>Number of Virtual CPUs</rasd:Description>
      <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
      <rasd:InstanceID>1</rasd:InstanceID>
      <rasd:ResourceType>3</rasd:ResourceType>
      <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
    </Item>
    <Item>
      <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
      <rasd:Description>Memory Size</rasd:Description>
      <rasd:ElementName>2048MB of memory</rasd:ElementName>
  <rasd:InstanceID>2</rasd:InstanceID>
  <rasd:ResourceType>4</rasd:ResourceType>
  <rasd:VirtualQuantity>2048</rasd:VirtualQuantity>
</Item>
<Item>
  <rasd:Address>0</rasd:Address>
  <rasd:Description>SCSI Controller</rasd:Description>
  <rasd:ElementName>SCSI Controller 0</rasd:ElementName>
  <rasd:InstanceID>3</rasd:InstanceID>
  <rasd:ResourceSubType>lsilogic</rasd:ResourceSubType>
  <rasd:ResourceType>6</rasd:ResourceType>
</Item>
<Item>
  <rasd:Address>1</rasd:Address>
  <rasd:Description>IDE Controller</rasd:Description>
  <rasd:ElementName>VirtualIDEController 1</rasd:ElementName>
  <rasd:InstanceID>4</rasd:InstanceID>
  <rasd:ResourceType>5</rasd:ResourceType>
</Item>
<Item>
  <rasd:Address>0</rasd:Address>
  <rasd:Description>IDE Controller</rasd:Description>
  <rasd:ElementName>VirtualIDEController 0</rasd:ElementName>
  <rasd:InstanceID>5</rasd:InstanceID>
  <rasd:ResourceType>5</rasd:ResourceType>
</Item>
```

```
<Item>
  <rasd:AddressOnParent>0</rasd:AddressOnParent>
  <rasd:ElementName>Hard Disk 1</rasd:ElementName>
  <rasd:HostResource>ovf:/disk/vmdisk1</rasd:HostResource>
  <rasd:InstanceID>6</rasd:InstanceID>
  <rasd:Parent>3</rasd:Parent>
  <rasd:ResourceType>17</rasd:ResourceType>
</Item>
<Item>
  <rasd:AddressOnParent>0</rasd:AddressOnParent>
  <rasd:AutomaticAllocation>true</rasd:AutomaticAllocation>
  <rasd:ElementName>CD-ROM 1</rasd:ElementName>
  <rasd:HostResource>ovf:/file/file2</rasd:HostResource>
  <rasd:InstanceID>7</rasd:InstanceID>
  <rasd:Parent>4</rasd:Parent>
  <rasd:ResourceType>15</rasd:ResourceType>
</Item>
<Item>
  <rasd:AddressOnParent>7</rasd:AddressOnParent>
  <rasd:AutomaticAllocation>true</rasd:AutomaticAllocation>
  <rasd:Connection>VLAN_100</rasd:Connection>
  <rasd:Description>PCNet32 ethernet adapter on "VLAN_100"</rasd:Description>
  <rasd:ElementName>Ethernet 1</rasd:ElementName>
  <rasd:InstanceID>8</rasd:InstanceID>
  <rasd:ResourceSubType>PCNet32</rasd:ResourceSubType>
  <rasd:ResourceType>10</rasd:ResourceType>
```

```
   </Item>
   <Item ovf:required="false">
    <rasd:AddressOnParent>0</rasd:AddressOnParent>
    <rasd:AutomaticAllocation>false</rasd:AutomaticAllocation>
    <rasd:Description>Floppy Drive</rasd:Description>
    <rasd:ElementName>Floppy 1</rasd:ElementName>
    <rasd:InstanceID>9</rasd:InstanceID>
    <rasd:ResourceType>14</rasd:ResourceType>
   </Item>
  </VirtualHardwareSection>
 </VirtualSystem>
</Envelope>
```

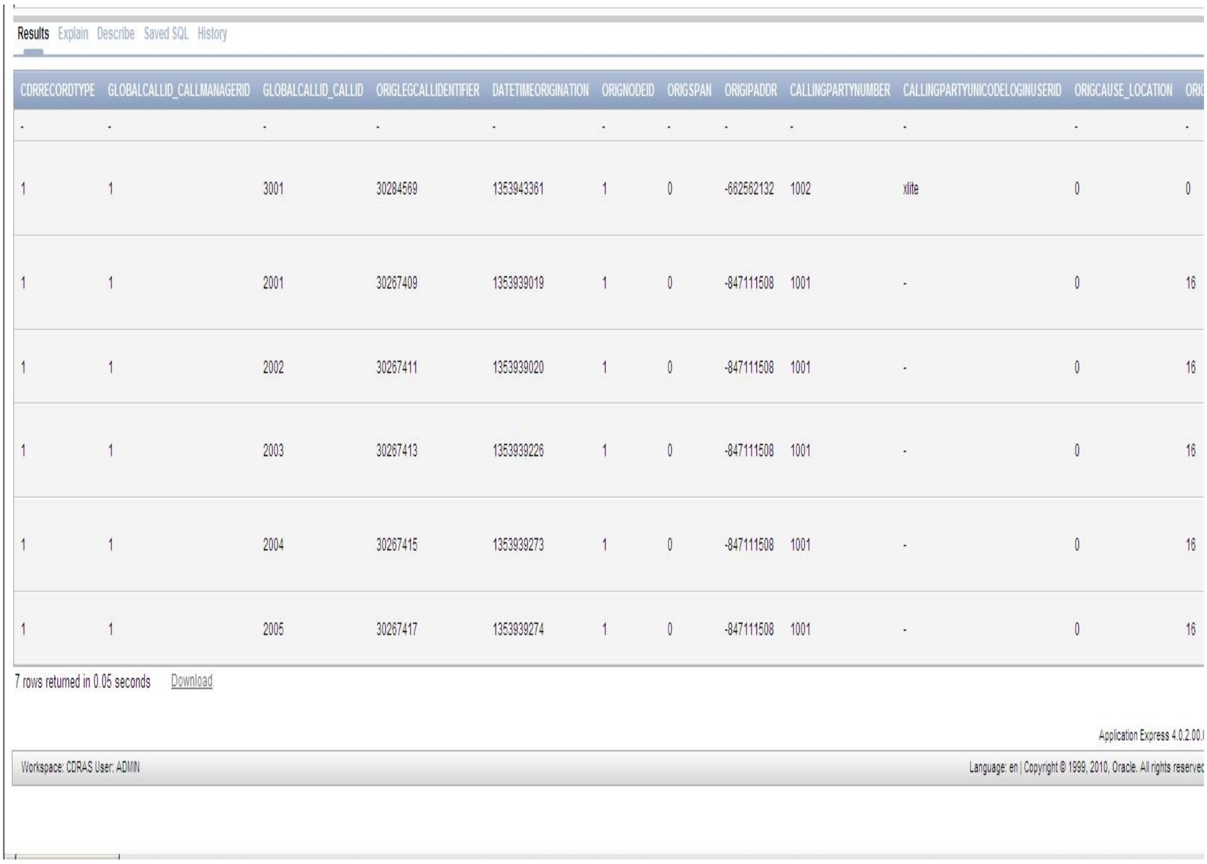
Appendix VI: Oracle Apex Workspace Query



```
select * from unfilteredprimary;
```

CDRRECORDTYPE	GLOBALCALLID_CALLMANAGERID	GLOBALCALLID_CALLID	ORIGLEGCALLIDENTIFIER	DATETIMEORIGINATION	ORIGNODEID	ORIGSPAN	ORIGIPADDR	CALLINGPARTYNUMBER	CALLINGPARTYUNICODELOGINUSERID	ORIGCAUSE_LOCATION	ORIGCAU
-	-	-	-	-	-	-	-	-	-	-	-
1	1	3001	30284569	1353943361	1	0	-662562132	1002	xlite	0	0
1	1	2001	30267409	1353939019	1	0	-847111508	1001	-	0	16
1	1	2002	30267411	1353939020	1	0	-847111508	1001	-	0	16
1	1	2003	30267413	1353939226	1	0	-847111508	1001	-	0	16

Figure A1: Sample results from database query



CDRRECORDTYPE	GLOBALCALLID_CALLMANAGERID	GLOBALCALLID_CALLID	ORIGLEGCALLIDENTIFIER	DATETIMEORIGINATION	ORIGNODEID	ORIGSPAN	ORIGIPADDR	CALLINGPARTYNUMBER	CALLINGPARTYUNICODELOGINUSERID	ORIGCAUSE_LOCATION	ORIG
-	-	-	-	-	-	-	-	-	-	-	-
1	1	3001	30284569	1353943361	1	0	-662562132	1002	xlite	0	0
1	1	2001	30267409	1353939019	1	0	-847111508	1001	-	0	16
1	1	2002	30267411	1353939020	1	0	-847111508	1001	-	0	16
1	1	2003	30267413	1353939226	1	0	-847111508	1001	-	0	16
1	1	2004	30267415	1353939273	1	0	-847111508	1001	-	0	16
1	1	2005	30267417	1353939274	1	0	-847111508	1001	-	0	16

7 rows returned in 0.05 seconds Download

Application Express 4.0.2.00.

Workspace: CDRAS User: ADMIN

Language: en | Copyright © 1999, 2010, Oracle. All rights reservec

Figure A2: Sample results from database query continued

Bibliography

[ALRC13] Australian Law Reform Commission (ALRC), Telecommunications (Interception and Access) Act, http://www.alrc.gov.au/publications/73.%20Other%20Telecommunications%20Privacy%20Issues/telecommunications-interception-and-access-, 2013.

[ANS04] American National Standards Institute (ANSI), American national standard for information technology – role based access control, ANSI, ANSI INCITS 359-2004, 2004.

[AST10] Asterisk - The Open Source Telephony Projects, URL: http://www.asterisk.org/, 2010.

[AUS10] Australian Government - Office of the Privacy Commissioner, Privacy Impact Assessment Guide, Australian Government, 2010, http://www.privacy.gov.au/materials/types/download/9509/6590 , 2010.

[BAC10] BackTrack Linux - Penetration Testing Distribution, URL: http://www.backtrack-linux.org/ , 2010.

[BD06] Biondi, B., Desclaux, F., Silver Needle in the Skype, EADS Corporate Research Center, France, 2006.

[BHQS12] Beckers, K., Hofbauer, S., Quirchmayr, G., Sorge, C.: A process for the automatic generation of white-, grey-, and black-lists from Call Detail Records to prevent VoIP attacks while preserving privacy, In: Availability, Reliability and Security, 2012. ARES ’12. International Conference on (August 2012), 2012.

[BLG07] D. Butcher, X. Li, and J. Guo, “Security challenge and defense in voip infrastructures,” Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. 37, no. 6, pp. 1152 –1162, November 2007, 2007.

[BW10] Businesswire, A Berkshire Hathaway Company, “Number of Mobile VoIP Users Will Approach 300 Million by 2013, In-Stat Reports, Scottsdale, Arizona, 2010.

[CDR10] Cisco Call Detail Records Field Descriptions. [Online]. Available: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/8_5_1/cdrdef/cdrfdes.html , 2010.

[CG03] Carnut, M. A. and Gondim J. J, Arp spoofing detection on switched Ethernet networks: A feasibility study, Simposio Segurancaem Informatica (Symposium Security in Informatics, November 2003, 2003.

[CIS10] Cisco Systems Inc., Cisco Unified Communications Manager Version 7.0, Cisco Systems Inc., 2010, http://www.cisco.com/en/US/products/ ps9517/index.html, 2010.

[CIS11] Cisco loses market share as router/switch market up. [Online]. Available: http://www.telecomreseller.com/2011/08/26/cisco-loses-market-share-as routerswitch-market-up/ , 2011.

[CKK05] Clauß, S., Kesdogan D., and Koelsch T., Privacy enhancing identity management: protection against re-identification and profiling, in Proceedings of the 2005 workshop on Digital identity management, ser. DIM ’05. ACM, 2005, pp. 84–93, 2005.

[COL08] Collier, M., http://voipsecurityblog.typepad.com/marks voip security blog/2008/08/library-voip-sy.html , 2008.

[DD11] Dua, S. and Du, X., Data Mining and Machine Learning in Cybersecurity. Boca Raton, FL, USA: Taylor and Francis Group, LLC, 2011.

[DG11] Danezis G. and Guerses, S., A critical review of 10 years of privacy technology, in Proceedings of Surveillance Cultures: A Global Surveillance Society?, UK, 2011. [Online]. Available: http://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf , 2011.

[DIR10] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, URL: http://eurlex europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF , 2010.

[DR07] Dunte, M., Ruland, C., Secure Voice-over-IP, Germany, 2007.

[DRO05] Dropped VoIP Calls: http://www.voipmechanic.com/droppedcalls.htm , 2005.

[DSNE08] d'Heureuse, N., Seedorf, J., Niccolini, S. and Ewald T., Protecting sip-based networks and services from unwanted communications, in GLOBECOM. IEEE, 2008, pp. 1–5, 2008.

[DWSPJ11] Deng, M., Wuyts, K., Scandariato, R., Preneel, B. and Joosen, W., A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements, Requir. Eng., vol. 16, pp. 3–32, March 2011, 2011.

[ETT10] Ettercap, URL: http://ettercap.sourceforge.net/, 2010.

[EUD02] ——, "Directive 2002/58/EC of European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," European Community(EU), Tech. Rep., 2002. [Online]. Available: http://www.dataprotection.ie/documents/legal/directive2002 58.pdf , 2002.

[EUD95] EU, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," European Community(EU), Tech. Rep., 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML , 1995.

[EWMS08] Ehlert, S., Wang, C., Magedanz, T. and Sisalem, D., Specification-based denial-of-service detection for sip voiceover-ip networks, in Internet Monitoring and Protection, 2008. ICIMP '08. The Third International Conference on, 29 2008-july 5 2008, pp. 59 –66, 2008.

[FEMA08] FEMA/Library VoIP Systems Hacked - Toll Fraud. [Online]. Available: http://voipsecurityblog.typepad.com/marks_voip_security_blog/2008/08/library-voip-sy.html , 2008.

[FPL07] Fernandez, E. B., Pelaez J. C. and Larrondo-Petrie, M. M., Security patterns for voice over ip networks, in Proceedings of the International Multi-Conference on Computing in the Global Information Technology. Washington, DC, USA: IEEE Computer Society, 2007, pp. 19–29, pp. 33–, 2007.

[FRA10] VoIP Fraudster and Fugitive Edwin Pena pleads guilty. [Online]. Available: http://voipsa.org/blog/2010/02/19/voipfraudster-and-fugitive-edwin-pena-pleads guilty/ , 2010.

[GAR10] Gartner Magic Quadrant for Unified Communications 2010. [Online]. Available: http://msunified.net/2010/08/09/gartnermagic-quadrant-for-unified-communications 2010/ , 2010.

[GL07] Geneiatakis,D. and Lambrinoudakis, C., An ontology description for SIP security flaws, University of the Aegean, Karlovassi, Samos, Greece, 2007.

[GOO10] Google Talk, URL: http://www.google.com/talk/index.html , 2010.

[HCCQ07] Hwang, K., Cai, M., Chen, Y. and Qin M., Hybrid intrusion detection with weighted signature generation over anomalous internet episodes, IEEE Trans. Dependable Secure Comput., pp. 6–14, 2007.

[HM06] Hung P. C. and Martin M. V., Security issues in VoIP applications, in Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on, may 2006, pp. 2361–2364 , 2006.

[HQW11] Hofbauer, S., Quirchmayr, G. and Wills, C. C., An approach to dealing with Man-in-the-Middle attacks in the context of Voice over IP, ARES 2011 Proceedings, pp. 249–255, 2011.

[HSC08] Hansen, M., Schwartz, A. and Cooper A., Privacy and identity management, IEEE Security and Privacy, vol. 6, no. 2, pp. 38–45, 2008.

[IET97] IETF, HMAC: Keyed-hashing for message authentication, Internet Engineering Task Force (IETF), IETF RFC 2104, 1997. [Online]. Available: http://tools.ietf.org/rfc/rfc2104.txt , 1997.

[ISO05] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC 27001 (2005), 2005.

[ISO09] ISO and IEC, “Common Criteria for Information Technology Security Evaluation,” International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 15408, 2009.

[ITI12] Government, H.: It infrastructure library (ITIL) (2012) http://www.itilofficialsitecom/home/home.aspx, 2012.

[ITP09] ITProPortal: http://www.itproportal.com/2009/01/28/voip-toll-fraudattack-racks-57k-bill-two-days/ , 2009.

[JC07] Jackson, B., Clark, C., Asterisk Hacking, Syngress Media, 2007, ISBN: 978-1597491518, 2007.

[JJQ07] Jorns, O., Jung, O. and Quirchmayr, G., Transaction pseudonyms in mobile environments, in EICAR 2007 Best Academic Paper, 2007, pp. 49–58 , 2007.

[KKG08] Kalloniatis, C., Kavakli E. and Gritzalis, S. Addressing privacy requirements in system design: the pris method, Requir. Eng., vol. 13, pp. 241–255, August 2008, 2008.

[KN11] Korb, K. B. and Nicholson, A. E., Bayesian Artificial Intelligence. Boca Raton, FL, USA: Taylor and Francis Group, LLC, 2011.

[KP11] Kalajdzic, K. and Patel, A., Active detection and prevention of sophisticated ARP-poisoning Man-in-the-Middle attacks on switched Ethernet LANs, WDFIA 2011 Proceedings, July 2011, 2011.

[LAW07] Lawecki, P., VoIP Security in Public Networks, University of Technology, Poznan, Poland, 2007.

[LBL10] Arpwatch by LBL Network Research Group, URL: http://www.securityfocus.com/tools/142, 2010.

[LEI06] Leisinger, A. L., If it looks like a duck: The need for regulatory parity in VoIP telephony, Washburn Law Journal, vol. 45, no. 3, pp. 585–624, 2006.

[M06] Materna, B., A proactive approach to VoIP security: Understanding VoIP security requirements, threats and architectures, Canada, 2006.

[M10] Xarp by Mayer C., URL: http://www.securityfocus.com/tools/3517, 2010.

[Mu06] Muncan,M., Secure telephony: SIP / SRTP (PKI) vs. Zfone vs. Skype, Germany, 2006.

[NIS04] Nissenbaum, H., Privacy as contextual integrity, Washington Law Review, vol. 79, no. 1, pp. 101–139, 2004.

[OAS05]. OASIS, eXtensible Access Control Markup Language TC v2.0 (XACML), OASIS, (2005), http://docs.oasis-open.org/xacml/2.0/access-control-xacml-2.0-core-spec-os.pdf , 2005.

[OEC80] OECD, OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, Organization for Economic Cooperation and Development (OECD), Tech. Rep., 1980. [Online]. Available: http://www.oecd.org/document/18/0,3746,en 2649_34255_1815186_1_1_1_1,00&&en-USS 01DBC.html, 1980.

[ONYS08] Ormazabal, G., Nagpal, S., Yardine, E., Schulzrinne, H., Secure SIP: A scalable prevention mechanism for DOS attacks on SIP based VoIP systems, IPTComm, Heidelberg, 2008.

[OS09] Opdahl, A. L. and Sindre, G., Experimental comparison of attack trees and misuse cases for security threat identification, Inf. Softw. Technol., vol. 51, pp. 916–932, 2009.

[P3P02]. Platform for privacy preferences project, W3C, (2002), http://www.w3.or/TR/P3P/ , 2002.

[PH11] Pfitzmann, A. and Hansen, M., A terminology for talking about privacy by data minimization: Anonymity, unlinkability, unobservability, pseudonymity, and identity management - version v0.34, TU Dresden and ULD Kiel, Tech. Rep., 2011. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology v0.34.pdf , 2011.

[PK09]. Patil, S and Kobsa, A: Privacy considerations in awareness systems. Designing with privacy in mind, in Awareness Systems, ser. Human-Computer Interaction Series, Markopoulos P., De Ruyter B., and Mackay W., Eds. Springer London, (2009), 187-206, 2009.

[PP07] Pfleeger, C. P. and Pfleeger, S. L., Security In Computing, 4th ed. Prentice Hall PTR, 2007.

[QNTS07] Quittek, J., Niccolini, S., Tartarelli, S., Stiemerling, M., Brunner, M. and Ewald, T., Detecting spit calls by checking human communication patterns, in ARES 2007 Proceedings. IEEE, 2007, pp. 1–6, 2007.

[RS06] Robin, J. and Schwartz, A., Analysis for ZRTP, CS259 Final Project, 2006.

[SAS06] Shin, D., Ahn, J. and Shim,C., Progressive multi gray-leveling: A voice spam protection algorithm, IEEE Network, vol. 9, no. 1, pp. 18–24, 2006.

[SC09] Spiekermann, S. and Cranor, L. F., Engineering Privacy, IEEE Transactions on Software Engineering, vol. 35, no. 1, pp. 67–82, Jan. 2009.

[SIP02] Session Initiation Protocol (SIP): http://www.ietf.org/rfc/rfc3261.txt, 2002.

[SIP09] Sipera: VoIP Toll Fraud On The Rise. [Online]. Available: http://www.darkreading.com/securityservices/167801101/security/vulnerabilities/217800061/index.html , 2009.

[SKY10] Skype, URL: http://www.skype.com , 2010.

[SNS10] Sorge, C., Niccolini, S. and Seedorf, J., The legal ramifications of call filtering solutions, IEEE Security and Privacy, vol. 8, pp. 45–50, 2010.

[SRT04] SRTP, URL: http://www.ietf.org/rfc/rfc3711.txt, 2004.

[TDN10] Tartarelli, S., d'Heureuse N., and Niccolini, S., Lessons learned on the usage of call logs for security and management in IP telephony, Communications Magazine, IEEE, vol. 48, no. 12, pp. 76 –82, 2010.

[TEL11] TelecomReseller UCNetworks: http://www.telecomreseller.com/2011/08/26/cisco-loses-market-share-as-routerswitch-market-up/ , 2011.

[TFA09] VoIP toll fraud attack racks up a 57K pound bill in two days. [Online]. Available: http://www.itproportal.com/2009/01/28/voip-toll-fraud-attack-racks-57k-bill-two-days/ , 2009.

[TFP10] Cisco, Toll Fraud Prevention Feature in IOS Release 15.1(2)T, Cisco Systems Inc., Tech. Rep., 2010. [Online]. Available: http://www.cisco.com/en/US/tech/tk652/tk90/technologies tech note09186a0080b3e123.shtml , 2010.

[UML10] Unified Modeling Language (UML): http://www.omg.org/spec/UML/2.3/ , 2010.

[US08] United States Patent Application, Crume, Detecting and Defending Against Man-in-the-Middle Attacks, Pub. No.: US 2008/0295169 A1, Pub. Date: Nov. 27, 2008, 2008.

[VOI05] VoIP Security Alliance Threat Taxonomy: http://www.voipsa.org/ Activities/taxonomy.php, 2005.

[VOI10] VoIP Security Alliance: http://voipsa.org/blog/2010/02/19/voipfraudster-and-fugitive-edwin-pena-pleads-guilty/ , 2010.

[VR10] Voznak, M. and Rezac, F., Threats to Voice over IP Communication Systems, Wseas Transaction on Computers, Issue 11, Volume 9, November 2010, 2010.

[WES67] Westin, A. F., Privacy and Freedom. New York: Atheneum, 1967.

[WIR10] Wireshark - the world's foremost network protocol analyzer, URL:http://www.wireshark.org/ , 2010.

[WIT11] Witt, B. C., Datenschutz kompakt und verstaendlich, 2nd ed. Vieweg+Teubner, 2011.

[WSDJ09] Wuyts, K., Scandariato, R., De Decker, B. and Joosen, W., Linking privacy solutions to developer goals, in Availability, Reliability and Security, 2009. ARES '09. International Conference on, march 2009, pp. 847 –852, 2009.

[WT03] Wieser, C., Takanen, A., Robustness testing of SIP implementations, Finland, 2003.

[WZYJW08] Wang, X., Zhang, R., Yang, X., Jiang, X., Wijesekera, D., Voice Pharming Attack and the Trust of VoIP, SecureComm, Istanbul, 2008.

[XML98] Extensible Markup Language (XML): http://www.w3.org/XML/ , 1998.

[ZRT10] The ZRTP Protocol: http://tools.ietf.org/html/draft-zimmermann-avtzrtp-22, 2010.

[ZZH08] Zhang, J., Zulkernine, M. and Haque, A., Random-forest-based network intrusion detection systems, IEEE Trans. Syst. Man Cybernet. C Appl. Rev, pp. 84–93, 2008.

Curriculum Vitae

Education

2008 – 2014 PhD in Computer Science, University of Vienna

2006 – 2008 MSc in Computer Security, University of Applied Sciences Technikum Vienna

2002 – 2006 Diploma Engineer in Information Management, University of Applied Sciences Technikum Vienna

Professional Experience

2012 – present Network Architect

Amadeus Data Processing GmbH, Erding, Germany

2010 – 2012 Network Engineer

Danube Data Center GmbH, Vienna, Austria

2009 – 2010 IT Administrator

Inform GmbH, Vienna, Austria

2006 – 2009 Network & Security Engineer

Duropack AG, Vienna, Austria