NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USING VOICE OVER INTERNET PROTOCOL TO CREATE TRUE END-TO-END SECURITY

by

Philip J. Starcovic

September 2011

Thesis Co-Advisors:	Rex Buddenberg Don McGregor
Second Reader:	Raymond Buettner

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Using Voice Over Internet Protocol to Create True End-to-End Security		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Philip J. Starcovic			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

In 2010, there were approximately 260,000 classified messages released to the general public via the website Wikileaks. The classified information was gathered by a "trusted" military member who had the right level of clearance to view the documents in question, but did not have a need-to-know. This easily illustrates the flaw in trusted enclaves and computing bases that secure the data lower than Layer 7 of the OSI Reference Model. Once a spy, hacker, or "trusted" member is inside the enclave, they have access to any and all information they wish to see.

The goal of this thesis is to convey the need for security solutions that are developed at layer 7 of the OSI Reference Model. VOIP/SIP clients that use TLS and SRTP in conjunction with PKI will show that there are already solutions that exist at Layer 7. Additionally, clients that take advantage of ZRTP will provide the best examples of protecting data instead of just an infrastructure. Because only small amounts of source code will see unprotected data, thorough analysis of this code is achievable mitigating security vulnerabilities within the code.

14. SUBJECT TERMS VOIP, Voice Over Internet Protocol, RTP, SRTP, SIP, TLS, ZRTP, Session Initiation Protocol, End-to-End Security, Network Security, Software Engineering, SIP Server			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

USING VOICE OVER INTERNET PROTOCOL TO CREATE TRUE END-TO-END SECURITY

Philip J. Starcovic
Lieutenant, United States Navy
B.S., The Ohio State University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2011

Author: Philip J. Starcovic

Approved by: Rex Buddenberg
Thesis Co-Advisor

Don McGregor
Thesis Co-Advisor

Raymond Buettner
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In 2010, there were approximately 260,000 classified messages released to the general public via the website Wikileaks. The classified information was gathered by a “trusted” military member who had the right level of clearance to view the documents in question, but did not have a need-to-know. This easily illustrates the flaw in trusted enclaves and computing bases that secure the data lower than Layer 7 of the OSI Reference Model. Once a spy, hacker, or “trusted” member is inside the enclave, they have access to any and all information they wish to see.

The goal of this thesis is to convey the need for security solutions that are developed at layer 7 of the OSI Reference Model. VOIP/SIP clients that use TLS and SRTP in conjunction with PKI will show that there are already solutions that exist at Layer 7. Additionally, clients that take advantage of ZRTP will provide the best examples of protecting data instead of just an infrastructure. Because only small amounts of source code will see unprotected data, thorough analysis of this code is achievable mitigating security vulnerabilities within the code.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APCO	Association of Public-Safety Communications Officials-International
CA	Certificate Authority
CAC	Common Access Card
CIA	Confidentiality, Integrity, Authenticity
CIO	Chief Information Officer
CNSSI	Committee on National Security Systems Instruction
CVS	Concurrent Versioning System
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DoN	Department of the Navy
DoS	Denial of Service
GUI	Graphical User Interface
HAIPE	High Assurance Internet Protocol Encryptor
IA	Information Assurance
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
ISO	International Organization for Standardization
MAC	Message Authentication Code
MAINGATE	Mobile Ad-Hoc Interoperable Network GATEway
MUOS	Mobile User Objective System

NGO	Non-Governmental Organization
OS	Operating System
OSI	Open Systems Interconnection
P25	Project 25
PDA	Personal Digital Assistant
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RDF	Resource Description Framework
RFC	Request For Comments
RSS	RDF Site Summary
RTP	Real-time Transport Protocol
SD	Secure Digital
SIP	Session Initiation Protocol
SMS	Short Message Service
SRTP	Secure RTP
SSL	Secure Sockets Layer
STE	Secure Terminal Equipment
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
USB	Universal Serial Bus
VOIP	Voice Over Internet Protocol

VPN	Virtual Private Network
WEP	Wired Equivalent Privacy

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Rex Buddenberg for your patience and guidance through the entire process of writing my thesis. Additional thanks go to Don McGregor and Ray Buettner for helping me out on such short notice.

I would also like to thank The Average Joes, the Del Monte Brass, the Beer and Ale Research Foundation in the Bay, and a certain other group of people that I associate myself with for giving me the much needed reprieves from my work. You helped me keep my sanity when it would have been easy to lose it.

Thanks go to my parents, Liz and Perry, my brothers and sisters, Brad, Monica, Patrick, and Rosemary, and my in-laws, Don and Linda for their never-ending support. Thank you all, I love you.

Special thanks go to Mike Clement for helping me with setting up the SIP server, the network, and generally letting me nerd out with you when Susan could not listen anymore.

Lastly, I would like to thank my beautiful and loving wife, Susan. You have been so patient with me while I ignored you to work on my thesis. Even when you needed me around, you were willing let me work on my thesis. You are wonderful and I will love you forever!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

A. THE SECURITY PROBLEM

In 2010, there were approximately 260,000 classified messages released to the general public via the website Wikileaks (Fildes, 2010). These sets were not made public by any foreign spy or even a teenager hacking into classified networks out of curiosity or malice. The classified information was gathered by a "trusted" military member. While said person had the right level of clearance to view the documents in question, he did not necessarily have a need-to-know. This easily illustrates the flaw in secured enclaves that secure the data lower than layer 7 of the Open Systems Interconnection (OSI) model. Once a spy, hacker, or "trusted" member is inside the enclave, they, with few exceptions, have access to any and all information they wish to see.

End-to-end security is often said to be the solution, but what the term describes protected transmission from one computer to another. Once the data is stored on a hard drive or server within an enclave, it is typically stored without any encryption or integrity mechanism. This is end-to-end security in the sense of computer-to-computer. However, it is infeasible to believe that only one person will have access any given computer. The Department of Defense (DoD), like most civilian institutions, is relying on its network security (layer 3 of the OSI model), physical security (layer 1), and the clearance process or background investigations to prevent information theft. This removes two thirds of the threat, but it still leaves the disgruntled employee able to carry out his/her nefarious plans or simple accidents.

Applications that protect data in a way that only the people that have a need-to-know can access it, allow the other security measures already in place to be an added layer of protection. Therefore, if network security, physical security, and/or the clearance process fail, the application level (layer 7) security will still be intact, rendering the data useless without the proper authorization. This will become more important as sensitive/classified data is used on mobile devices such as laptops and smartphones where

physical security will be almost non-existent. It is paramount that the data stay secured not just until it reaches the computer, but until it reaches the person authorized to use the data and thus creating true end-to-end security.

In order to work on the organizations' information systems, Information Technology (IT) personnel are required to have a level of access at or above that which is required to see the data on these systems. The largest reason to have the IT personnel cleared at such a high level is because they may accidentally see information on the systems. If the data were secured while at rest at layer 7, there would be no need to give clearances to every IT person, thus saving a large sum of money by reducing the amount of people without a need-to-know who have access to classified information.

Finally, by protecting the data at layer 7, the majority of the software, communications infrastructure, and storage will never see the data in an unprotected form. Because of this, very little code will have to be scrutinized for security vulnerabilities thus minimizing the space where malware can attack.

VOIP is an example of data being transmitted over the network at the application layer. It is clear that voice over internet protocol (VOIP) is overtaking a lot of single-segment or voice-network-only voice applications (such as law enforcement radios). VOIP can also be seen in phone service as applications on some smartphones. Because of VOIP's rapid growth, there is a need to analyze VOIP security.

B. PROBLEM FRAMEWORK

1. Security Definitions

In order to discuss the matter of information security in an organized and succinct manner, a few terms need to be defined. These terms will be used throughout the thesis with the associated definitions in mind.

- Confidentiality: The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information (Committee on National Security Systems, 2010).
- Integrity: The property whereby an entity has not been modified in an unauthorized manner (Committee on National Security Systems, 2010).

- Availability: The property of being accessible and useable upon demand by an authorized entity (Committee on National Security Systems, 2010).

The idea of confidentiality, integrity, and availability (CIA) collectively creating information assurance (IA) is commonly referred to as the CIA Triad. This thesis is concerned with the confidentiality and the integrity (which, as later discussed, includes authentication and non-repudiation) of the data. The availability of the data is assumed and will not be discussed in this thesis. While the CIA Triad is arguably the most recognized of the IA models, there is another model, the Five Pillars of IA, which needs to be briefly discussed.

The Five Pillars of IA model begins with the CIA Triad and adds authenticity and non-repudiation. Many argue that because authenticity and non-repudiation are not attributes of information, but a way to ensure the integrity of the data that these two terms are actually implied and encompassed by the term integrity. Though references to this model can be seen throughout DoD publications including the CNSSI (Committee on National Security Systems Instruction) 4009, DoD Directive 8500.01E section 4.7 states, "The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation" (Assistant Secretary of Defense for Networks & Information Integration andDepartment of Defense Chief Information Officer, 2007). When discussing public key infrastructure (PKI), having integrity as a subset of authenticity makes more sense. However, according to United States Code, Title 44, Section 3542, "integrity … means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" (Definitions, 2006). For the above reasons, the definition of integrity will imply authenticity and non-repudiation throughout this thesis.

2. Other Definitions

a. User Agent

There are many different signaling protocols used for VOIP. Session initiation protocol (SIP) is arguably the most recognized and therefore the most widely

used of the VOIP signaling protocols. For this reason, VOIP with a concentration on SIP will be the focus of this thesis

SIP uses the model of a client-server network. The user agent (UA) exists on the clients as an application that implements SIP. The term UA will be used extensively throughout this study and will indicate the application and not the person (Rosenberg, et al., 2002).

b. SIP Server

The SIP server is the entity that negotiates the call setup for the UAs. Figure 1 is a diagram of a simple VOIP/SIP network. An UA will send SIP or transport layer security (TLS) traffic, which is a secure version of SIP to request a call be established with a second UA. The server and second UA will also use SIP/TLS traffic to establish the call. Once the call is connected, very little SIP/TLS traffic is sent.

Once the call is established, the voice data is not sent over SIP, but real-time transport protocol (RTP) or secure RTP (SRTP). Depending on how the UA was created, the SIP server will not be included in the RTP/SRTP traffic as seen in Case #1 in Figure 1. If case #1 does not happen, then SIP server will stay in the conversation and work as a layer 7 gateway relaying the RTP/SRTP traffic from one UA to the other as seen in Case #2 of Figure 1. This means that the SIP server will need to be part of the end-to-end security solution.

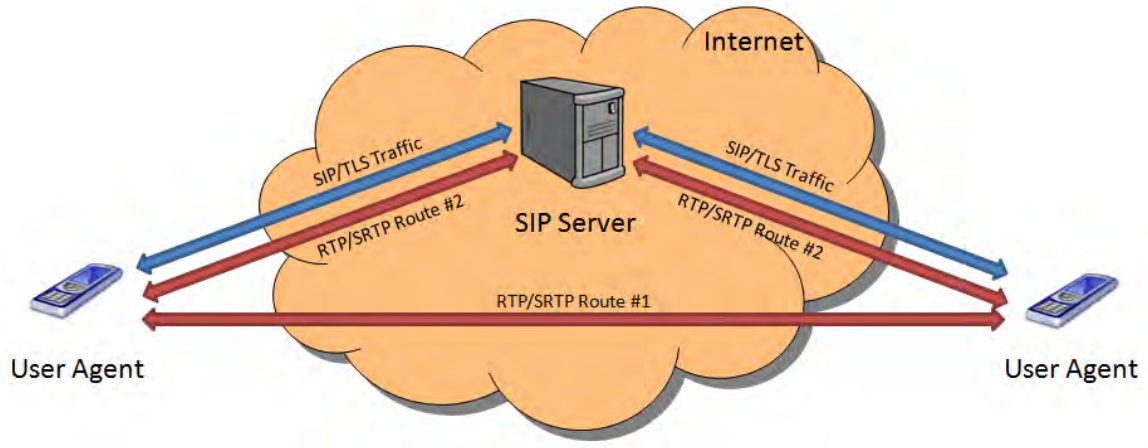


Figure 1. SIP and RTP possible traffic routes

c. Protected Data

For the purposes of this thesis, protected data will be considered to be data that has both confidentiality and integrity. This will typically be seen in the form of encryption (to ensure confidentiality) and a digital signature (to ensure integrity). Additionally, the protection will be applied to the data and not the communications infrastructure.

d. Covert Channel

Covert channels are methods of transmitting data in a way that was not intended to be an information path and thus violates the security policy (Harris, 2008).

e. Trusted Computing Base

According to the DoD Department of Defense Trusted Computer System Evaluation Criteria (commonly referred to as the Orange Book), a trusted computing base (TCB):

> ….contains all of the elements of the system responsible for supporting the security policy and supporting the isolation of objects (code and data) on which the protection is based. The bounds of the TCB equate to the "security perimeter" referenced in some computer security literature. In the interest of understandable and maintainable protection, a TCB should be as simple as possible consistent with the functions it has to perform. Thus, the TCB includes hardware, firmware, and software critical to protection and must be designed and implemented such that system elements excluded from it need not be trusted to maintain protection. (Department of Defense, 1985)

The DoD's intent was to focus on just the individual computer and not the entire network. The TCB definition given will be appropriate for the purposes of this thesis. However, the scope will be extended beyond the computer and will include the network components as well.

f. True End-to-End Security

True end-to-end security is defined as data that is protected throughout the transmission, receiving, and storage such that only layer 7 applications will see the data in unprotected form. Specifically, only the user and the tools used to relay the information to the user will see the data in an unprotected form. Essentially, the data will be protected from speaker to listener and vice versa.

g. Layer 7 Security Solution

The phrase "layer 7 security solution" will be used throughout this thesis referring to an application providing VOIP at the security standards previously discussed. A security solution that resides at layer 6 or 7 can provide true end-to-end security. Though video, short message service (SMS) (also known as text messages), and chat can be provided via VOIP, this thesis will strictly focus on voice.

3. International Organization for Standardization's (ISO) OSI Reference Model

All security discussions throughout this thesis will be conducted in reference to the ISO's OSI Reference Model. The purpose of this model as described by the ISO is to "provide a conceptual and functional framework" that allows developers of a specific layer to work independently of the other layers' developers. Additionally, this reference model is not intended to be "an implementation specification" and therefore does not exist in a real-world example. Instead, it is meant to have other "existing standards be placed into perspective within the overall model" (International Organization for Standardization and International Electrotechnical Commission, 1996). For these reasons, the OSI Reference Model will serve as a logical way to discuss data security solutions. Figure 2 is a visual representation of the OSI Reference Model.

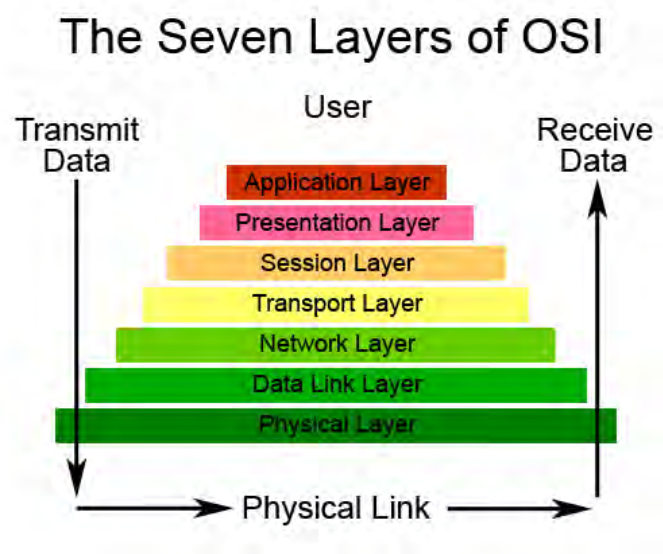


Figure 2. ISO's OSI Reference Model (From WindowsNetworking.com)

The bottom two layers of Figure 2 are the physical (layer 1) and data-link (layer 2) layers. The physical layer provides the initiation, maintenance, and closure of physical connections for the transmission of bits (International Organization for Standardization and International Electrotechnical Commission, 1996). These bits are then assembled into units called data frames. (Institute for Telecommunications Sciences, 1996) For proper routing to the data frame's destination, the addressing portion of the data frames must be opened by other devices, which in turn creates a vulnerability to traffic analysis.

Layer 3 is the network layer. The network layer is responsible for routing packets between network segments. Though there are many protocols used at this layer, Internet Protocol (IP) is the most prevalent and will be the only protocol discussed in reference to this layer in this study. Because packets in internet protocol (IP) are connectionless (does not rely "on prior exchanges between equipment and network"), they are called datagrams (Institute for Telecommunications Sciences, 1996). Each router will have to read the headers of the IP datagram in order to route to the proper destination (International Organization for Standardization and International Electrotechnical Commission, 1996).

Layers 4 and 5 are called the transport and session layers, respectively. The transport layer's primary responsibility is to ensure the information is transferred correctly. This assurance is accomplished by error control and sequence checking among other factors. The transport layer provides reliable end-to-end data transfer via segments for session control (Institute for Telecommunications Sciences, 1996). The session layer established and terminates data transfers within the network (Held, 2001).

Layers 6 and 7 are called the presentation and application layers, respectively. The presentation layer's primary function is data transformation. Data transformation can include data compression/decompression and data encryption/decryption. The application layer is the way that the application accesses any service within the rest of the model (Held, 2001).

4. Security Implications

In order for data to be considered secure, it must have confidentiality and integrity. To ensure data is confidential, encryption must be applied to obscure the true meaning of the data. However, confidential data is worthless unless the recipient can authenticate the sender and be assured the message was unaltered. Therefore, it is also important to apply a digital signature to the data. A digital signature is a hash computed from the message that is encrypted with the sender's private key. The digital signature is then decrypted with the sender's public key. The hash ensures that the data was unaltered (intentionally or unintentionally) and the encryption with the private key ensures that no other entity could have sent the data (authenticity).

The layer of the OSI Reference Model that these protections occur at defines the resulting scope of the protection. Wired Equivalent Privacy (WEP), which occurs at layers 1/2, is an encryption implementation that protects the frames over a single network segment. Virtual private networks (VPN), which occur at layer 3, protect the datagrams while outside of an enclave. Secure sockets layer (SSL), occurring at layers 4/5, protects the connection providing end-to-end security over the internet. Each of these protections must be removed and reapplied before moving onto the next segment, enclave, or operating system (OS). However, if there are multiple users on the same OS, these

protections do not secure the data. Only with the encryption of data objects at layers 6/7 will true end-to-end security be accomplished. With true end-to-end security only allowing members with a need-to-know access to the data, situations like Wikileaks will not be able to happen as easily and certainly the extent of damage will be less. Additionally, true end-to-end security will prevent sensitive data from reaching unintended users without the originator knowing.

The Internet Engineering Task Force's (IETF) main goal "is to make the internet work better" (The Internet Engineering Task Force, n.d.). The standards (and best practices as some are not technically standards) that are contained in the requests for comment (RFC) attempt to standardize the internet. Compliance of these RFCs focuses on what happens within the network and the internet. This leaves very little standardization once inside the client at layers 6 and 7. The IETF views this as a local matter that is left up to the developer of the UA. This is a very serious gap that, once thoroughly understood as end-to-end, should be encompassed by some standardization activity. Though this would be standarization that the entire world could benefit from, the Department of the Navy's (DoN) Chief Information Officer (CIO) would be an example of the type of organization that would be interested in this within the Navy. Perhaps another task force like the IETF would be a way to have international standardization.

C. THESIS GOAL

The goal of this thesis is to assess the use of VOIP (with a focus on SIP) as a communications protocol that can provide true end-to-end security (through confidentiality and integrity) at layer 6 or 7 of the OSI Reference Model. By protecting the data at layer 6 or 7, the data will not only be protected from entities outside of the trusted network, but also from entities that are inside that do not have a need-to-know. Layer 6 and 7 security solutions protect the data all the way to the end user (not just the computer). Security solutions at any level less than 6 only protect the infrastructure and not actually the data. These types of security solutions have their place, but using only

these solutions to protect data leaves gaps in the security of the information. VOIP has the ability to provide true end-to-end security.

This thesis promotes the extension of the application of existing standards. The standard would shift the focus from enclave-base security solutions to a layer 7-based solution that could be provided by VOIP in concert with a PKI-like technology. Such a solution would provide true end-to-end security:

- Providing data confidentiality, in transit and at rest, through VOIP/TLS and SRTP encryption
- Providing data integrity, in transit and at rest, through VOIP/TLS and SRTP message authentication codes
- Providing a way to reduce the TCB size
- Enforcing the "need-to-know" and mitigating the social engineering vulnerability.

D. THESIS ORGANIZATION

1. Chapters II and III: Sampling of Current Technologies' Security and Analysis

How different technologies secure their data, both in transmission and storage, will be discussed in this section. This will provide an idea of the inadequacies and advantages of these current systems and practices. This information will later be used to determine the applicability of the current VOIP/SIP technologies.

2. Chapters IV and V: Testing

In the first section of these chapters, the confidentiality and integrity of the calls are tested with multiple VOIP/SIP UAs. Only looking at the inputs and outputs of the UA determines how the UA transmits and stores the data without examining how the UA manipulates the data in an unprotected form prior to transmission and storage.

In the second section, the source code of two VOIP/SIP UAs is parsed to determine what portions of code handle unprotected data and what does not. This prevents the portions of code that only handle protected data from needing to be tested

for malicious code. If sensitive/classified, but protected data is released to entities that do not have a need-to-know, no compromise of the information has occurred. This makes the amount of source code that needs to be tested manageable.

3. Chapter VI: Conclusion

This chapter will discuss the end results and implications of the experiment. Additionally, suggestions for future work in this area of study will be included. Finally, recommendations on actions to be taken based on the results of the experiment will be discussed.

E. ITEMS BEYOND THE SCOPE OF STUDY

1. Cryptographic Algorithms

The unbreakability of cryptographic hashes and encryption/decryption keys is of the utmost importance to the security of data. Arguably, all cryptographic algorithms, given enough time, are breakable. However, the importance is that the algorithms are strong enough to be computationally infeasible to break. Without the cryptographic algorithms being sufficiently strong, even protected data will be vulnerable to attack. For this thesis, the strength of the cryptographic algorithms will be assumed to be sufficient to prevent successful attack on the algorithms. Because of this assumption, encrypted data seen by any entity is assumed to be uncompromised.

2. Security and Trust within PKI

PKI provides a means by which the appropriate users can successfully gain access to protected data. Though PKI is an integral part of ensuring proper protection of VOIP/SIP data in transit and at rest, it is not required for VOIP/SIP technologies to operate. Because the focus of this thesis is VOIP/SIP and not PKI, the integrity of all keys and certificates and the confidentiality of the private keys will be assumed for the duration of the thesis.

The way in which the keys and certificates are distributed may be vulnerability within a PKI-based system. Because of the assumptions already made regarding the integrity and confidentiality of the keys and certificates, the distribution methods will also be beyond the scope of this study.

F. BENEFITS OF THE STUDY

This thesis will provide a look at existing VOIP/SIP technologies as a way to provide true end-to-end security. The applicable protocols used in VOIP/SIP will also be examined ensuring that regardless of the abilities of the UAs that were assessed, the standards allow for implementation of true end-to-end security. The results can be used within the DoD and private sector enhancing voice and, as VOIP matures, other types of data security and providing a framework by which other technologies can be analyzed.

II. SAMPLING OF CURRENT TECHNOLOGIES' SECURITY

A. ASSOCIATION OF PUBLIC-SAFETY COMMUNICATIONS OFFICIALS-INTERNATIONAL (APCO) PROJECT 25 (P25)

APCO's P25 "…is a suite of wireless communications protocols used in the US and elsewhere for public safety two-way (voice) radio systems" and is used by public safety agencies at the federal, state, and local government levels (Clark, Goodspeed, Metzger, Wasserman, Xu, & Blaze, 2011). P25 is supposed to provide secure communications among public safety responders to enable enhanced coordination and timely response; however, this is not the case.

Clark et al. explain that in this type of system, integrity is often provided by a message authentication code (MAC). Due to the way the system's error correction was designed, MACs cannot be used. This allows an unauthorized user to inject false traffic and replay captured traffic even when the radios are operating in encrypted mode. Another flaw is that the metadata is not encrypted which allows for easy traffic analysis. Finally, the design allows radios with encryption enabled to interact with radios that do not have encryption enabled. Obviously, the radio that is unencrypted will be able to be intercepted, but if encryption was accidentally disabled, it is unlikely that the user will ever notice. (Clark, Goodspeed, Metzger, Wasserman, Xu, & Blaze, 2011)

P25 "does not provide clean separation of layers and lacks a clearly stated set of requirements against which it can be tested" (Clark, Goodspeed, Metzger, Wasserman, Xu, & Blaze, 2011). Unfortunately,

> many of the security problems in P25 arise from basic protocol design and architectural decisions that cannot be altered without a substantial, top-to-bottom redesign of the protocols and of the assumptions under which it operates. (Clark, Goodspeed, Metzger, Wasserman, Xu, & Blaze, 2011)

In properly layered systems, problems with confidentiality and integrity occur at layer 7 of the OSI reference model. Because the P25 standard is only for the radios and

not the rest of the network, and that the standard is unlayered, the security, even if perfectly implemented, would only be good for the P25 part of a wider internetwork.

B. MAINGATE

The Defense Advanced Research Projects Agency's (DARPA) Mobile Ad-Hoc Interoperable Network GATEway (MAINGATE) is a program that was created to develop and demonstrate the communication technologies and capabilities required to execute network centric warfare between the US military, coalition forces, Non-Governmental Organizations (NGO) and First Responders. Such a system requires a way to interface with the multitude of technologies and capabilities that may be used. Often times interfacing multiple systems together is an extremely difficult task. However, when the systems are used to carry classified communications, security between the end users becomes the most essential task (Defense Advanced Research Projects Agency, 2010).

DARPA has not publicly announced how MAINGATE will secure the data. It is important that through its design, MAINGATE secures the data and not just the infrastructure. Without the layer 7 integrity or confidentiality, the radios connected to MAINGATE cannot be assured that their data is protected. Additionally, this rather large vulnerability becomes even more emphasized when considering MAINGATE is intended to be a mobile gateway. If the device is lost or stolen while in use, the information that is routed through the gateway will not be protected.

C. SECURE TERMINAL EQUIPMENT (STE)

The STE phone system is used in many different settings throughout the U.S. government. It has the ability to secure classified communications via a crypto card. The card and STE individually are unclassified making them accountable items only for cost, not classification. When the card is inserted and the correct personal identification number for the card is entered, the STE has the ability to provide confidentiality and integrity (The National Security Telecommunications and Information Systems Security Committee, 2001). To provide authenticity, the authentication information is "embedded

as part of the key" (U.S. Naval Academy, 2011). The authentication information is then displayed on the opposite user's phone for verification. The authentication information includes the classification level, identification of the user, a five digit key identification number, and a key expiration date (U.S. Naval Academy, 2011). This is an excellent example of a system that creates true end-to-end security.

Unfortunately, certain practices may preclude the assurance of true end-to-end security. The cards are typically distributed in such a way that multiple users are able to use a single card. While this assures the authenticity of the organization that owns the card, the individual user is not authenticated. Each organization is then dependent on the opposite organization's STE physical security measures. Without cards for individual users, there is no method for ensuring the user is who (s)he says (s)he is.

D. MOBILE USER OBJECTIVE SYSTEM (MUOS)

MUOS is a "narrowband tactical satellite communications system" designed by Lockheed Martin for use by U.S. ground forces (Lockheed Martin, 2011). It is meant to be a replacement for the Ultra High Frequency Follow-On system. This communications system is designed with the intent of protecting the data from one user to another user (end-to-end).

HAIPE devices are used to protect the network traffic and information systems from exploitation while on the terrestrial links (Green, 2007). HAIPE devices are layer 3 encryption devices and therefore do not provide end-to-end security. This highlights a security gap between the layer 3 device and the user located at layer 7. Additionally, because the HAIPE is strictly an encryption device, there is no assurance of integrity and therefore authenticity.

E. SUMMARY

The discussion in this chapter provides a brief look at some of the voice technologies and the process in which they secure the voice data. There are many systems available that can be analyzed for best and worst practices. The important item

here is that the system protects the data at layer 7 of the OSI reference model to ensure true end-to-end security. Without this level of protection, there is a portion of the path the data travels that is unprotected and therefore vulnerable to exploitation.

III. ANALYSIS OF TECHNOLOGIES AND PROCESSES

A. EXISTING PHILOSOPHY LIMITATION

Initially, computers were standalone and were not networked. If the computer was kept physically secure, there was no way to reach the data without proper authorization. With networked computers and the advent of the internet, physical security could only provide data protection if the entire network was physically secure; often times due to size and distance this was not feasible as was the case with the internet thus requiring network security. The object of protection (in theory) is the data, however in practice the actual object has been the computer. Because of this implementation of security, if the physical or network security fails, the data is compromised.

Over the last decade, mobile computing has increased thanks to increase in popularity of cellular phones and personal digital assistants (PDA) evolving into smartphones and wireless networks. If physical security could be relied upon before, it certainly cannot be now. The increase in mobility means that laptops and smartphones (and the data contained within) are more likely to be lost or stolen. Additionally, social engineering attempts frequently occur and when the user fails to recognize them, the current security philosophy is further circumvented.

B. WEAKNESS IN THE PHILOSOPHY

Simple information systems had one communications path, so link security equaled end-to-end security. As networks become internetworks, the end-to-end security does not exist in the same scale. The secured enclave approach creates many authorized users that do not have a need-to-know for all data contained within the enclave. Additionally, it allows unintentional disclosure of data during a social engineering attack.

1. A Gap in Security with Lower Layer Protection Schemes

The goal of data protection is to ensure that the data has confidentiality and integrity between the authorized sending and receiving entities. When discussing content

data, it must be protected between the people using the data and therefore needs to be protected at layer 7. As discussed in Chapter I, providing data protection at any layer less than 7 will not ensure confidentiality and integrity for a portion of the transit less than user-to-user. To ensure user-to-user (true end-to-end) security, a layer 7 security solution must be in place.

2. Minimal Protection for Data at Rest

Because the majority of data stored by the UAs is secured at a layer less than 7, the data while at rest on a server, hard drive, internal memory, or any other media is not protected. Without proper protection, any entity that can physically get the data will have the ability to read the data. A simple example is removing the secure digital (SD) card from a smartphone and reading it from a computer. Without layer 7 protection, there is no assurance that the user is authorized to use that SD card. Again, the goal of data protection is to ensure the data's confidentiality and integrity between authorized users.

3. Minimal Integrity

Finally, even if all of the data is encrypted and therefore confidential, most UAs do not have integrity implemented into their design. Without integrity there is no way to ensure that the data is from the authentic sender. Additionally, the data may have been altered, intentionally by an attacker or unintentionally by electromagnetic anomalies, during transmission or while at rest and the recipient may not know otherwise. It is easy to see how important authenticity, and integrity as a whole, is in a military setting. The recipient wants to know for sure that the orders came from the commander and that the orders were unaltered.

C. THE LAYER 7 SECURITY SOLUTION

A layer 7 security solution based on VOIP/SIP has the ability to provide true end-to-end security. The current protocols and their standards can provide confidentiality and integrity protection of the signaling and voice data while in transit over the network. This can easily be extended beyond just the network to the UAs. Using PKI in concert with

VOIP/SIP can provide a solution that will protect not only the infrastructure, but the content as well. Implementing a way to listen to recordings within the UA can provide protection for the data at rest on the file system. A layer 7 security solution can be employed in addition to the existing infrastructure protection that is provided by physical security, WEP, VPNs, and SSL at the lower layers.

1. Digital Signature Provides Integrity

The digital signature provides integrity (which includes authentication) by encryption with a private key of a hash and therefore only the public key of the sender will decrypt the hash. Because the key is private, authentication is guaranteed because no other entity has that specific private key; therefore it must have come from that sender. Additionally, the message can be guaranteed to not have been altered between the sender and receiver if the hash matches because no entity could have altered the message, rehashed it, and signed it with the private key of the sender. Since the digital signature guarantees authenticity and non-alteration, complete integrity is provided.

2. Encryption Provides Confidentiality

VOIP/SIP UAs that properly implement TLS and SRTP will provide confidentiality of the data (both signaling and voice) while in transit. If the data is intercepted or lost while in transit, the data will be not be compromised and a simple resend is all that is required. The appropriate key to decrypt the data will be the only way to make the data useful. Additionally, the confidentiality will ensure that the data is protected while at rest on the file system.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTING METHODOLOGY

A. UNPROTECTED TESTING: CONTROL PHASE

At the outset of the experiment, no data protection (confidentiality or integrity) measures were used. Calls were made between two clients (using the same UA, but on different OSs). (This was repeated for each UA.) Additionally, recordings were made by each client (provided the UA had an organic recording capability) to see how the recordings were stored within the file system. The following UAs were used for this portion of the testing:

- Linphone[1]
- Blink[2]
- Jitsi (formerly known as SIP Communicator)[3]

Using port mirroring on the switch, Wireshark[4] was used to intercept all traffic flowing through the network. Wireshark can detect, filter, and assemble VOIP/SIP related traffic for further analysis including playback of the conversations. Because the calls were made without any protection, the data is in an unencrypted state and susceptible to unauthorized interception while in transit. Also, the data is susceptible to spoofing and alterations without any type of integrity mechanism. If no digital signature or other authentication mechanism is in use, a simple man-in-the-middle attack would have the ability to change pertinent routing information without any user knowing that an unauthorized entity was making changes. This test showed how vulnerable the VOIP/SIP calls are without the use of any confidentiality or integrity protection.

Depending on how the UA was designed (this is not configurable), the content may or may not pass through the server once the call is established. Additionally, the

[1] Linphone is an open source audio/video and text messaging client that uses SIP

[2] Blink is an open source audio SIP client that is available for Mac, Windows, and Linux.

[3] Jitsi is an open source audio/video and chat client that supports SIP, XMPP/Jabber, AIM/ICQ, Windows Live, Yahoo!, Bonjour, and others.

[4] Wireshark is a network protocol analyzer that captures and interactively browses the traffic running on a computer network.

recorded data was stored without protection on the file system which means the data at rest was vulnerable to illegitimate access, alteration, and may not have been authentic. Because the VOIP was unencrypted, playback of the voice data was successful. This control phase revealed that without any type of protection, the data was vulnerable both in transit over the network(s) and at rest within the file systems and the identity of the source UA may not be authentic.

B. PROTECTED TESTING: BLACK-BOX TESTING

Knowing that the data in transit and at rest was not secure and that sender was not authenticated, TLS and SRTP were used in place of SIP and RTP, respectively, for each UA (exceptions explained later). With protection of the voice data, Wireshark was able to assemble the VOIP/SIP call, but because the contents were encrypted, the playback was unintelligible. The RFCs for both TLS and SRTP specify sender authentication, integrity of the message, and confidentiality of the message (Dierks, Certicom, & Allen, 1999) (Baugher, M.; McGrew, D.; Cisco Systems; Naslund, M.; Carrara, E.; Norrman, K.; Ericsson Research, 2004). The following UAs were used for this portion of the testing:

- Linphone (with Zfone[5] activated)
- Blink
- Jitsi
- Skype[6]

Each UA differs on how it implements signaling and data protection. Some require previously created PKI certificates. Asterisk was the server software used and it has a script, ast_tls_cert, which created a self-signed certificate authority (CA) certificate and private key. The script then used this certificate and created public certificates and private keys for the server and each of the two clients.

[5] Zfone is an open source VOIP phone software product that established SRTP using ZRTP.

[6] Skype is a VOIP application that makes use of the Skype Protocol

All of the certificates and private keys were distributed via a universal serial bus (USB) flash drive. While this is a relatively secure method of distributing private keys, it is not the most ideal. It is recognized that this method of key distribution works for the experiment, but it is not scalable to the real world. The integrity of the PKI is an absolute must in order for the data to be secured and the identities of the UAs to be authentic. If the private keys are not kept a secret from everybody except for the appropriate user, the PKI is compromised and therefore no assurance can be made on the confidentiality and integrity of the calls. The proper distribution of private keys and the strength of cryptographic algorithms are outside of the scope of this thesis. For this reason, a few assumptions will be made:

- All private keys are kept private
- All certificates are authentic
- All cryptographic algorithms are sufficiently strong to prevent unauthorized decryption

After the distribution of the public certificates and private keys, the black-box testing began. Calls were made between the two clients (using the same UA, but different OSs) with some form of protection being implemented. (Interoperability between the different UAs is outside the scope of this thesis and therefore was not tested.) This was repeated for each UA. This protection secured the signaling data, the voice data, or both. Wireshark captured all traffic within the network for analysis. Recordings were made to assess the security of the voice data at rest.

C. SOURCE CODE REVIEW: WHITE-BOX TESTING

The final portion of testing was to look at the source code of Blink and Jitsi. The purpose of this was to preliminarily determine the portions of code that would see unprotected data which included both signaling and voice data. Unprotected data was considered to be any data (both signaling and voice) that did not have a digital signature appended to ensure integrity or was not encrypted and therefore not ensuring confidentiality.

Depending on the program in question, it may have millions of lines of code. To know exactly how the data is being used and accessed in every procedure within the program is virtually impossible. If such an undertaking is required, many man-hours would be spent looking at every single line of code to ensure there is no malicious code inserted. An example of such malicious code could be a covert channel. The covert channel would be built into the code that would handle the unprotected data. Then the channel would send the unprotected data from the trusted portion of code to an area that the attacker would be able to access at a later time.

Because scrubbing an entire program for any such malicious code can require so much manpower, it is financially and time-wise beneficial to limit the amount of code located within the TCB boundary. Knowing what portions of the source code deal with unprotected data can limit the amount of code that is required to be in the TCB. If data protection is applied at all times, the size of the TCB continues to shrink.

Every file of the Blink and Jitsi UA source codes was categorized into one of three groups:

- Files that dealt with unprotected data (red code)
- Files that possibly dealt with unprotected data (gray code)
- Files that only dealt with protected data (black code)

Separating the files of both UAs into these categories provided a basic estimate of how much of the source code would be considered part of the TCB and therefore need to be scrutinized for covert channels and other such attacks. This showed that if the data is in a protected state as much as possible, the data is protected within the computer with exactly the same protections as it has over the network.

The naming convention and rudimentary analysis of the actual lines of code were used for this preliminary categorization into red, gray, and black code. Looking for specific keywords within the names and code helped to divide the files into their proper category. This portion of the experiment was very basic and would need to be revisited

in a much more detailed manner to provide an extremely accurate TCB analysis. Nonetheless, this will provide crucial groundwork that will help redefine the size of the TCB.

D. SUMMARY

The completed experiment illustrated the importance of creating a layer 7 security solution. The black-box testing of the different UAs showed the ability of the existing open source VOIP/SIP technologies to provide a layer 7 security solution through the use of TLS and SRTP. The white-box testing of two open source UAs helped to demonstrate the critical need for TCB analysis that does not require the entire program to be analyzed.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TESTING RESULTS

A. UNPROTECTED TESTING: CONTROL PHASE

This was the first phase of the testing that was conducted. While this phase was primarily used to ensure the proper setup of the network, Asterisk server, and the clients with the UAs, this also provided a baseline to see how the UAs managed the signaling and voice data without any protection mechanisms.

1. Control, In-Transit Testing

While calls were made from one client to another, Wireshark captured all traffic traveling through the switch. The voice that was transmitted between the two clients represented sensitive/classified conversations. There are six possible points within the network where valuable information could be captured:

- Signaling data sent between the initiating client and the server
- Signaling data sent between the server and called client(s)
- Voice data sent between the initiating client and the server
- Voice data sent between the the server and called client(s)
- Voice data sent from the initiating client to the called client(s)
- Voice data sent from the called client(s) to the initiating client

Figure 3 shows Linphone actively connected to a VOIP/SIP call. Figure 4 shows the initiation and negotiation of a call between the clients and the server. As soon as the connection between the two users is fully established, very little signaling occurs and the majority of the traffic is voice data carried over RTP.

Figure 3. Linphone UA connected to a VOIP/SIP call (From Linphone, 2010)

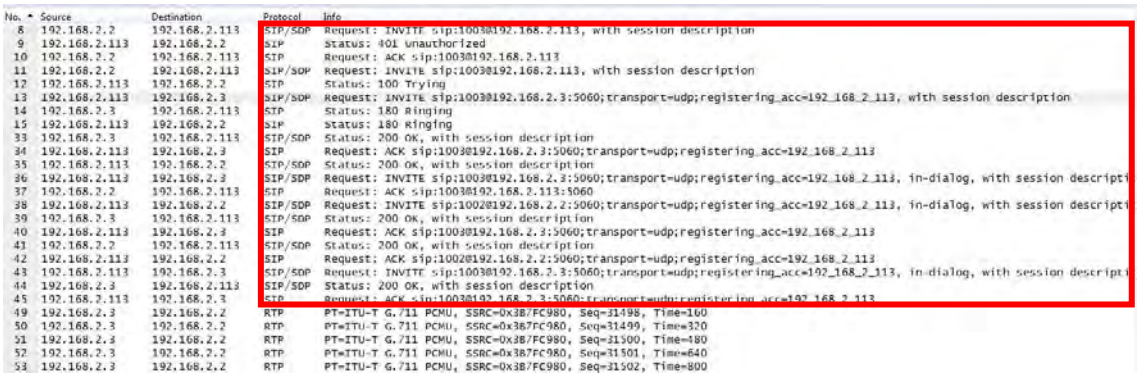


Figure 4. Wireshark capture: Call initiation (From Wireshark, 1998)

a. Signaling/SIP Data

Once the signaling to setup the call was finished, the server stepped out of the conversation until termination of the call for Jitsi and Linphone. Blink passed all RTP traffic through the server for the duration of the call. Skype will be covered in a separate section. All of the SIP traffic can easily be seen to be without any protection. Figure 5 shows who the request was from, who it was to, and what UA was being used among other pieces of information. Without PKI encryption, neither client can truly be authenticated without other non-electronic means (i.e., using a pre-shared passphrase that has never been previously used). If the server stays in the middle, as was the case with Blink, PKI will only provide authentication between the server and each UA. Because authentication is not associative, the UAs are not authenticated to each other.

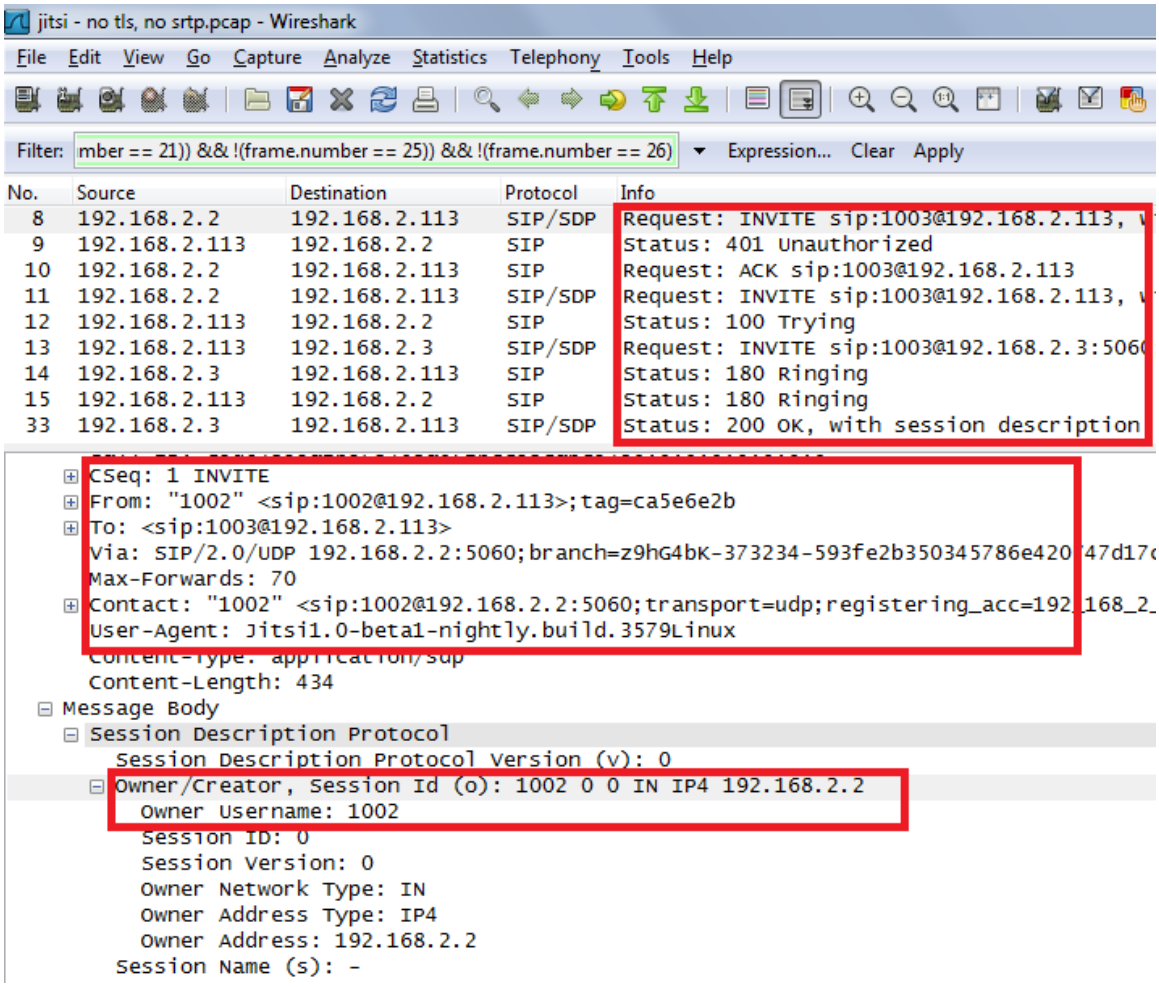


Figure 5. Wireshark capture: Unencrypted SIP data (From Wireshark, 1998)

b. Voice/RTP Data

Figure 6 shows what the frequency spectrum of the two sides of the conversation looked like once Wireshark reassembled the RTP data. The top spectrum is going from the receiving user to the initiating user and bottom in the opposite direction. The voice within the spectrum was very clear which will not be the case when the data is encrypted. Using the playback feature on Wireshark allowed both sides of the conversation to be listened to in their entirety.

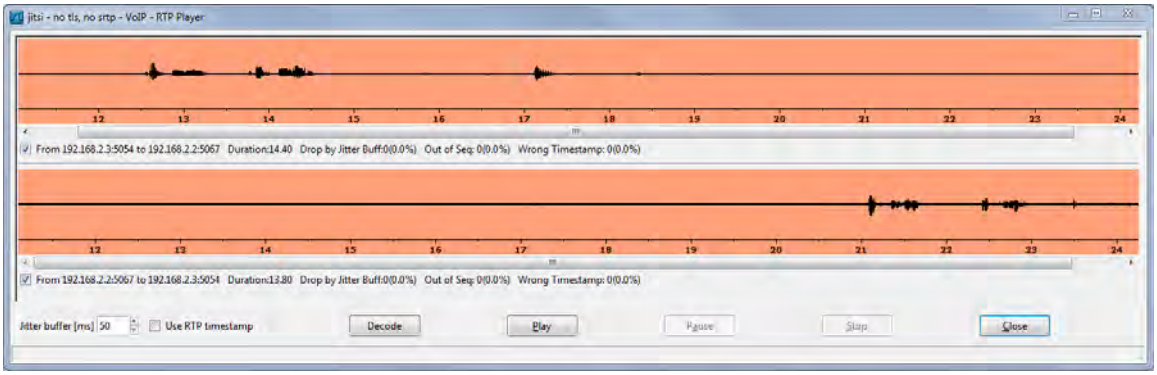


Figure 6. Frequency spectrum of voice between Jitsi UAs (From Wireshark, 1998)

2. Control, at Rest Testing

A recording was made with the organic capability of Blink and Jitsi. (Linphone does not have an organic recording capability therefore no recording was made with this UA). Blink only gives the option of recording the conversation in the .wav format. Jitsi offers the option to save the recording in any of the following formats:

- .aiff
- .au
- .gsm
- .mp3
- .wav

In the interest of keeping the experiment as similar as possible among the different UAs, all recordings were made using the .wav format.

Looking at the frequency spectrum of the two recordings in Figure 7, it is clear that no encryption was implemented. These recordings are able to be accessed by anybody that has (authorized or unauthorized) access to the file system that the recording was created on.

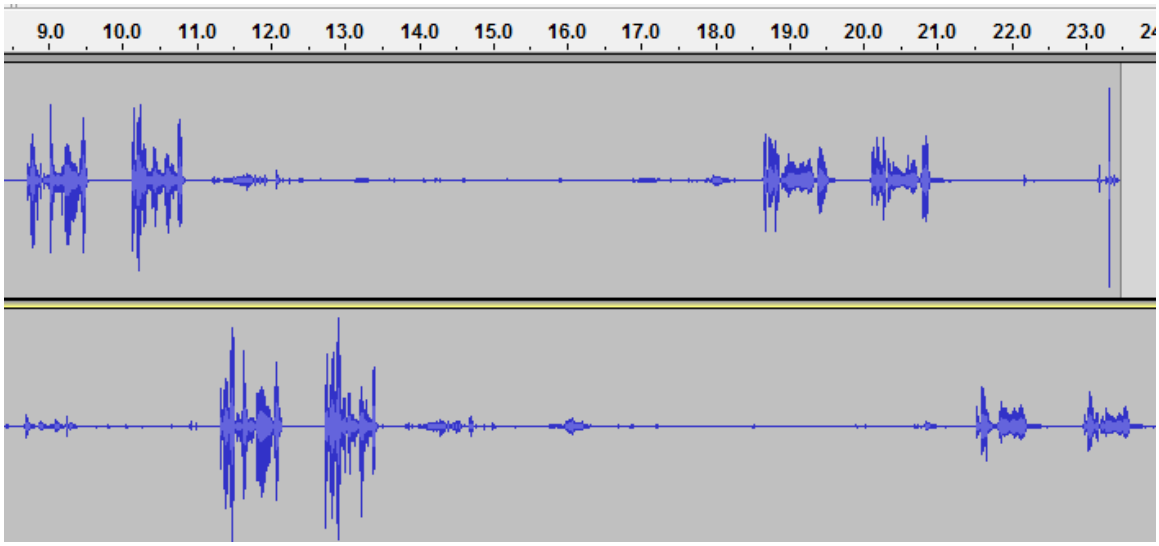


Figure 7. Visual inspection of the Linux and Windows Jitsi recordings (From Audacity, 1999)

B. PROTECTED TESTING: BLACK-BOX TESTING

This was the second phase of the experiment. The first step was to enable only the signaling protection. Afterwards, only the voice protection was enabled. Finally, both types of protection were enabled and at this time a recording was made to test the security of recordings made during a "completely" secured call.

1. Black-Box, In-Transit Testing

As discussed in the control, in-transit testing section, there were six vulnerabilities within the network where sensitive data could be collected, the signaling data between the UAs and the server, the voice data between the UAs and the server (Blink), and the voice data between the UAs. The assessment of the four UAs used in this portion of the testing follows.

a. Signaling/SIP Data

The top red box in Figure 8 shows a series of messages sent between the initiating user and the server using TLS. It was identified as encrypted in the second red

box of Figure 8. Packet 15 was the first packet of the call and therefore was an INVITE request. Once the call was completely established, the server removed itself until the call is terminated by one of the users in both Blink and Jitsi. Figure 9 shows that even though the signaling data is encrypted via TLS[7], the voice data is still unencrypted and using RTP. Jitsi and Blink implemented TLS in the same way.

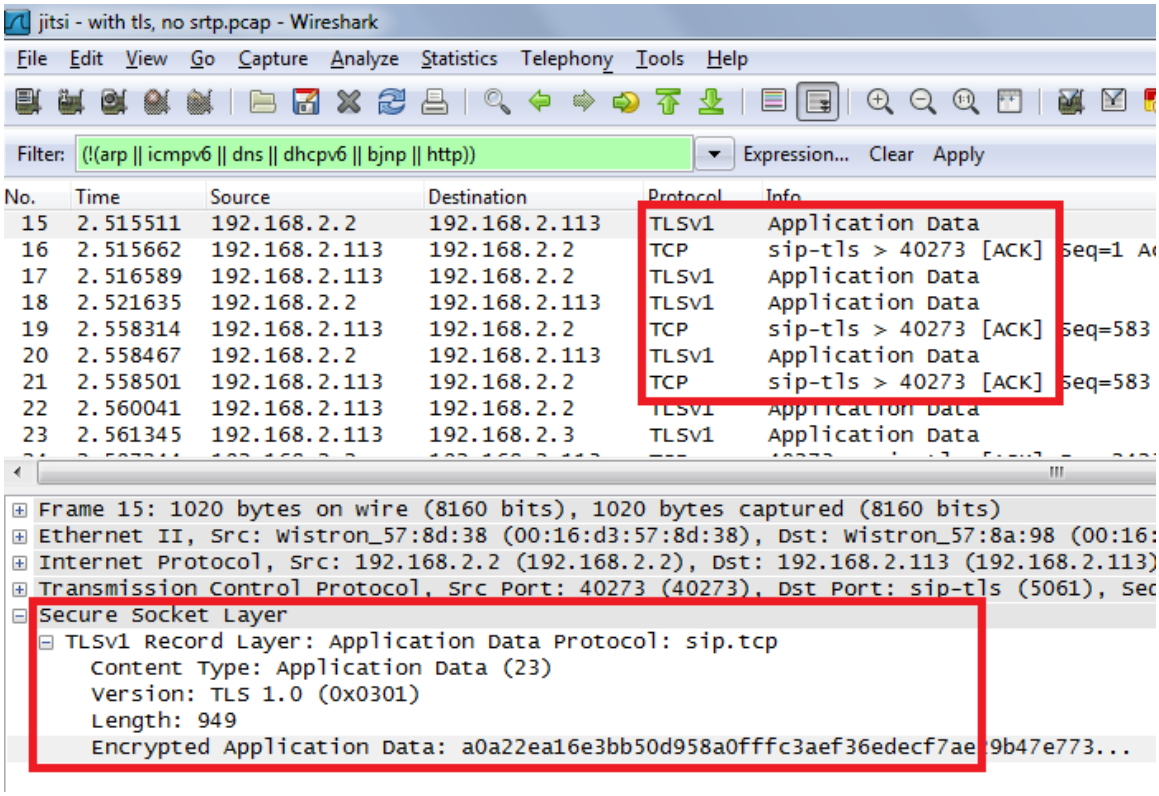


Figure 8. Wireshark capture: Jitsi using TLS to secure SIP (From Wireshark, 1998)

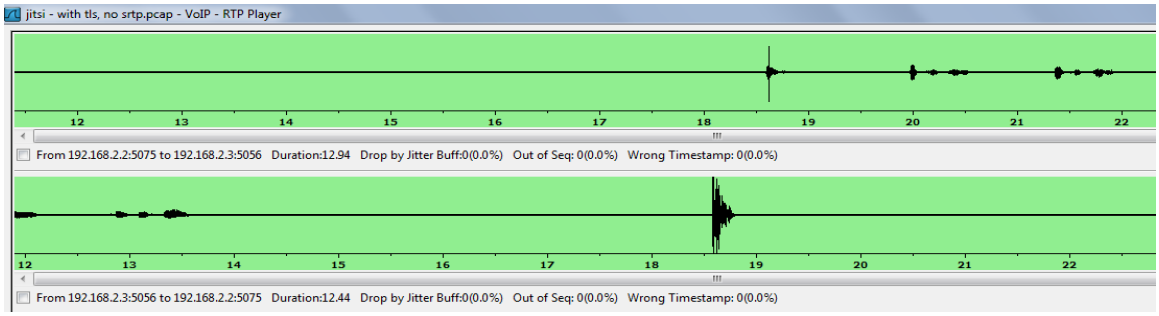


Figure 9. Frequency spectrum of voice between Jitsi UAs using TLS (From Wireshark, 1998)

[7] TLS provides signaling security between the TCP sockets on both end clients. It is still vulnerable to malware within each client.

TLS has the potential to ensure that the identity of the user is authentic because it requires PKI-based keys. However, Blink did not require any form of authentication (i.e., username and password) except for initially setting up the account. After the account has been created, the username and password are stored, not ensuring true authentication each time the user logs on. Jitsi gives the option of "remembering the password" and it is defaulted to yes. See Figure 10 for a screenshot of the Jitsi account menu. Therefore, neither UA is defaulted to protect against imposter user users.

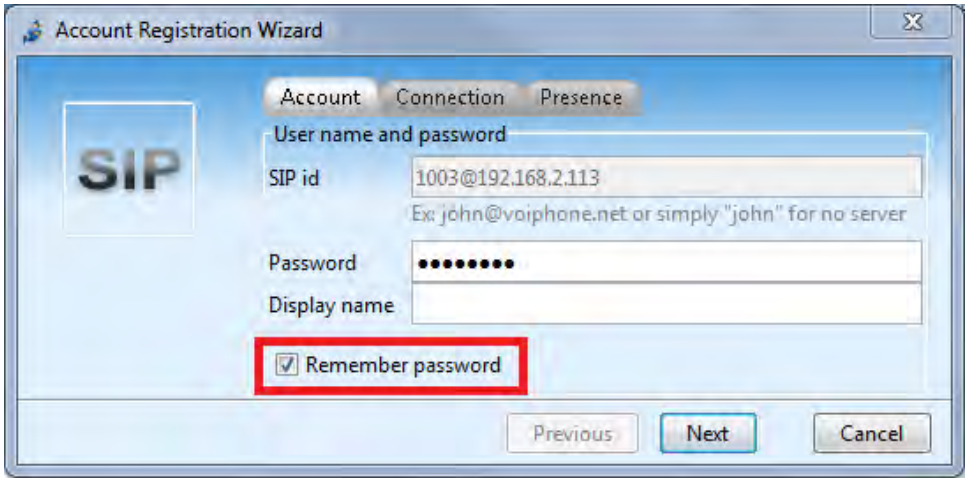


Figure 10. Jitsi account registration window (From Jitsi, 2011)

Because Linphone does not have an organic ability to provide signaling or voice protection, the Zfone program was used to give Linphone this ability. Unfortunately, it only protects the voice data and not the signaling data. According to the ZRTP FAQ, "ZRTP cannot automatically authenticate the end-users, this is task of the users once they can talk to each other" (ZRTP FAQ - GNU Telephony, 2011). However, ZRTP can work in concert with PKI-backed digital signatures to automatically authenticate the end-users (Zimmerman, P.; Zfone Project; Johnston, A.; Avaya; Callas, J.; Apple, Inc., 2011) as will be seen in the following sections. This direct user authentication, independent of the SIP server, is a good thing.

b. Voice/RTP Data

The second red box in Figure 11 shows that Blink successfully employed SRTP encrypting the payload. Figure 12 shows a very noisy spectrum further indicating the success of the encryption. The first red box in Figure 11 shows traffic going from one user, to the server, and then to the second user. This is also why there are four voice spectrums in Figure 12. This transfer of voice to the server in the middle shows the key vulnerability in SRTP; it requires the server to be trusted. This does not allow any UA strictly using SRTP to provide end-to-end security.

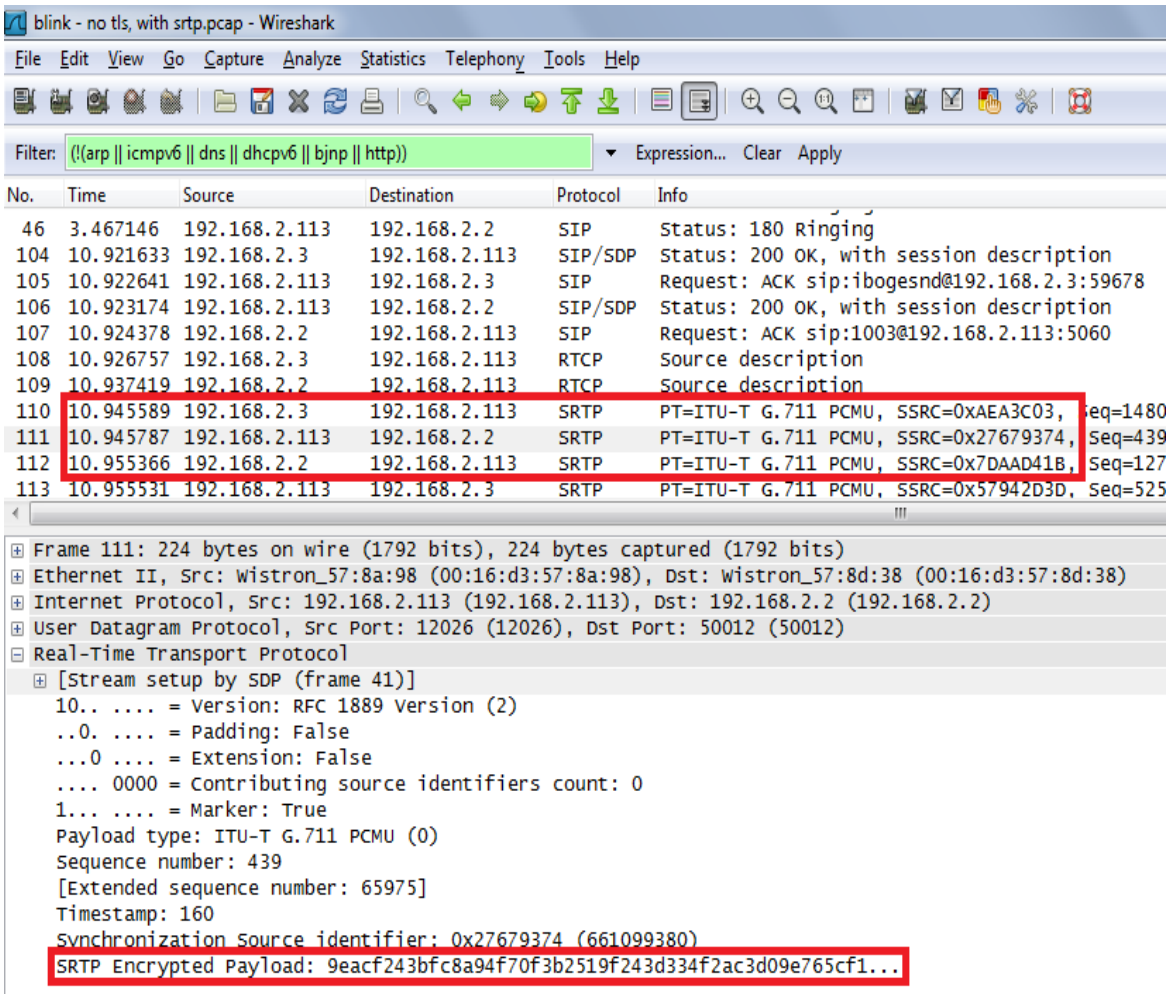


Figure 11. Wireshark capture: Blink using SRTP (From Wireshark, 1998)

Figure 12. Frequency spectrum of voice between Blink UAs using SRTP (From Wireshark, 1998)

Jitsi employed ZRTP to setup the SRTP. Once the connection between the two clients was fully established, ZRTP messages were used to exchange the encryption keys allowing the UAs to secure the RTP. Figure 13 shows the information contained in a ZRTP packet. Notice that the ZRTP messages were sent directly from one user to the other. ZRTP does not require a server to negotiate the encryption keeping the server out of the trusted computing base.

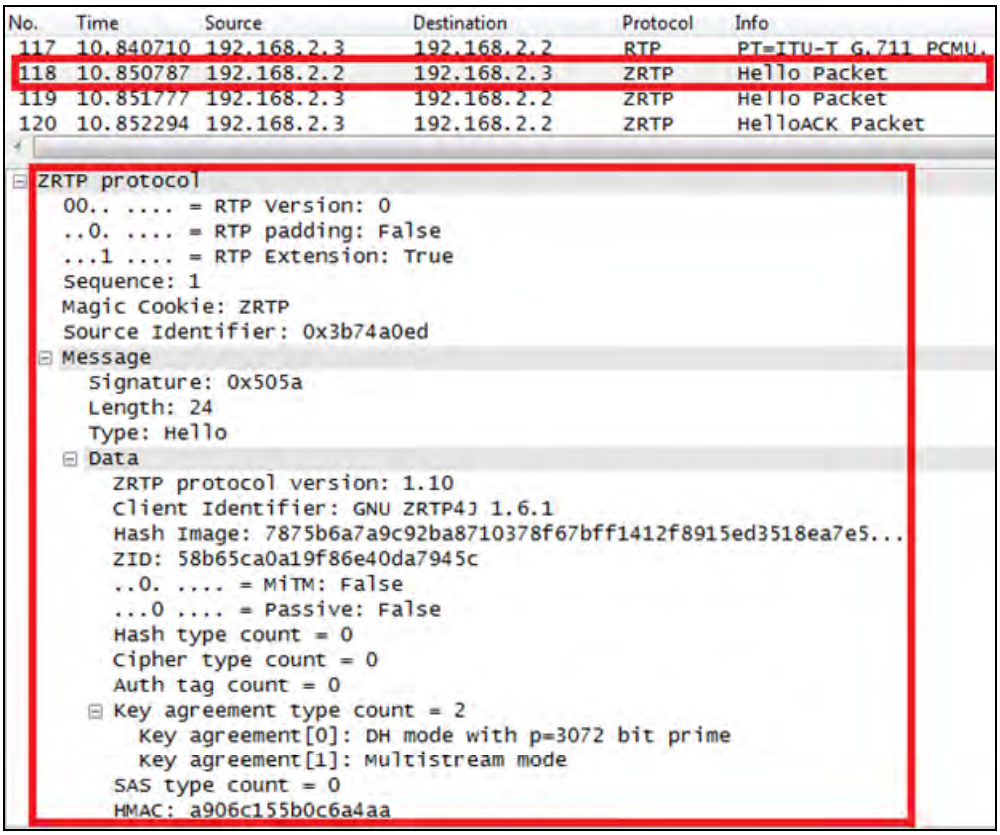


Figure 13. ZRTP packet (From Wireshark, 1998)

Jitsi connects the call as soon as possible. Because the exchange of ZRTP messages takes time, there is actually a period of time that the call is unsecure. Figure 14 shows the voice spectrum of the call. It is easy to see one portion of the call is not encrypted and the other is encrypted.

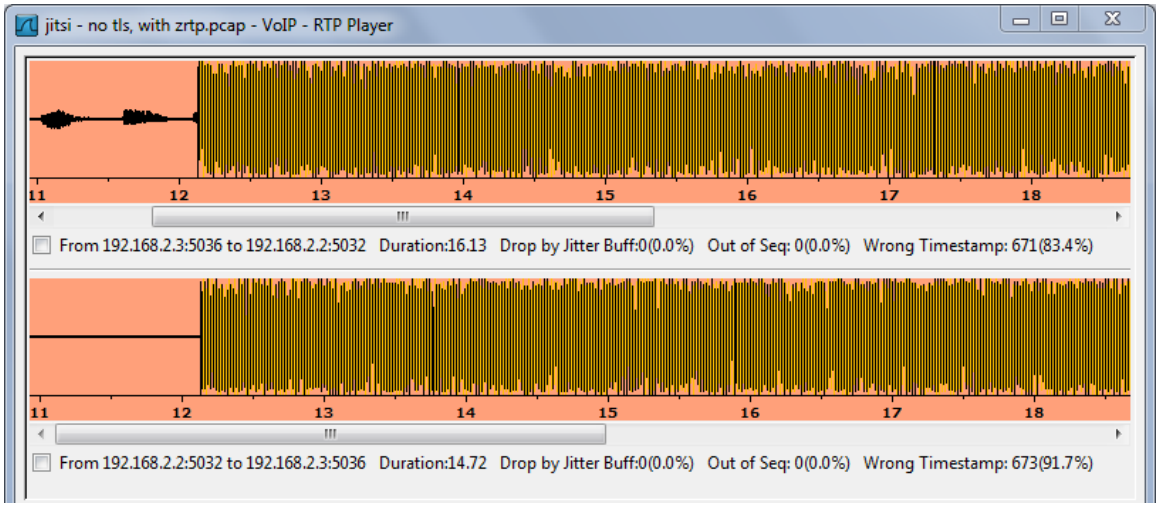


Figure 14. Frequency spectrum of voice between Jitsi UAs using ZRTP enabled SRTP (From Wireshark, 1998)

Once Linphone established a call with the other UA, Zfone determined that the other user was also using Zfone. Since both users were using Zfone, a series of ZRTP messages (see Figure 15) were sent between the users to setup the protection of the RTP packets. As with Jitsi, establishment of ZRTP takes some time and the first portion of the call was unencrypted (see Figure 16). Though the call was clearly encrypted, Wireshark still read the data as RTP and not SRTP. It is not even identified as being encrypted (see the red box in Figure 15). Regardless, Linphone using Zfone provided encrypted voice without another entity, such as a server, in the middle.

No.	Time	Source	Destination	Protocol	Info
363	6.984836	192.168.2.3	192.168.2.2	ZRTP	Commit Packet
364	7.067599	192.168.2.2	192.168.2.3	ZRTP	DHPart1 Packet
365	7.132251	192.168.2.3	192.168.2.2	ZRTP	DHPart2 Packet
366	7.225062	192.168.2.3	192.168.2.2	ZRTP	DHPart2 Packet
367	7.249530	192.168.2.2	192.168.2.3	ZRTP	Confirm1 Packet
368	7.249532	192.168.2.2	192.168.2.3	ZRTP	Confirm1 Packet
369	7.250011	192.168.2.3	192.168.2.2	ZRTP	Confirm2 Packet
370	7.252493	192.168.2.2	192.168.2.3	ZRTP	Conf2ACK Packet
371	7.256982	192.168.2.2	192.168.2.3	RTP	PT=ITU-T G.711 PCMU,
372	7.258843	192.168.2.3	192.168.2.2	RTP	PT=ITU-T G.711 PCMU,

```
⊞ Frame 371: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
⊞ Ethernet II, Src: Wistron_57:8d:38 (00:16:d3:57:8d:38), Dst: Wistron_57:53:5
⊞ Internet Protocol, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.3 (192.168
⊞ User Datagram Protocol, Src Port: 7078 (7078), Dst Port: 7078 (7078)
⊟ Real-Time Transport Protocol
  ⊞ [Stream setup by SDP (frame 126)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 81
    [Extended sequence number: 65617]
    Timestamp: 12960
    Synchronization Source identifier: 0x3e8e81b0 (1049526704)
    Payload: fe9ec3008fc1844275b687e42b3e7954e1e4190c591d2657...
```

Figure 15. Wireshark capture: Linphone using Zfone (From Wireshark, 1998)

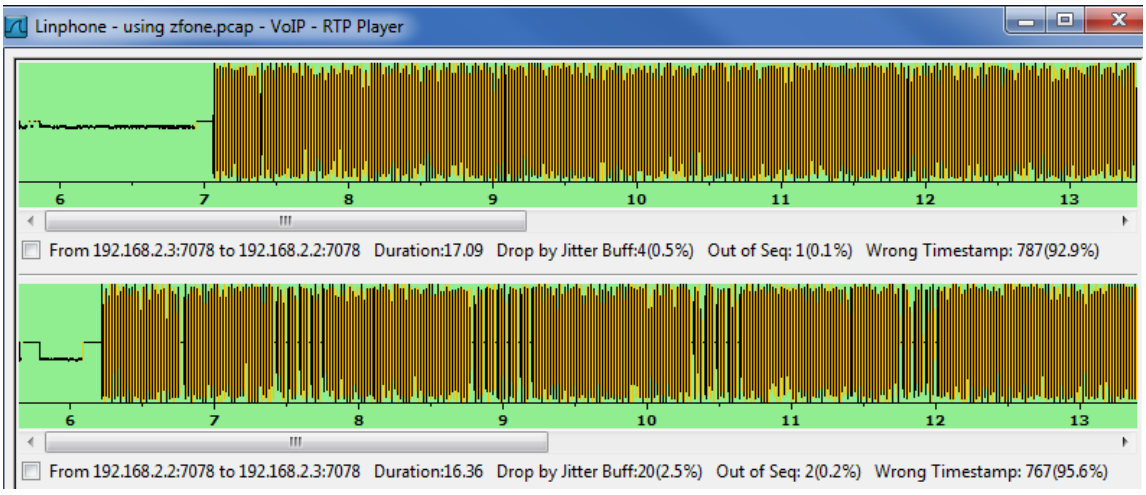


Figure 16. Frequency spectrum of voice between Linphone UAs using Zfone (From Wireshark, 1998)

2. Skype

The discussion could not be complete without a discussion on arguably the most well known VOIP client, Skype. There is little information publicly available on how Skype employs its Skype Protocol. Skype uses strictly transmission control protocol (TCP) for signaling data and a combination of TCP and user datagram protocol (UDP) for media traffic (Baset & Schulzrinne, 2004). Figure 17 shows one side of a Skype conversation showing only TCP and UDP traffic.

Identity authentication occurs by properly logging into the Skype UA with a username and password. While the username can be seen in unencrypted form, the password is never sent in the clear. The authenticity of a user is guaranteed assuming the user has not checked the "Sign me in when Skype starts" option as can been seen in Figure 18. If it has been checked, having to logon to the OS will help to mitigate an incorrectly authenticated user.

All of the data contained in the TCP and UDP traffic associated with Skype does not follow the standards of any publicly known protocol (see the red box in Figure 17). One can reasonably assume that most data, including the username and password, in the TCP and UDP traffic are encrypted. However, not all traffic is encrypted. Specfically, the very first UDP packet sent by skype is not encrypted (Biondi & Desclaux, 2006). Skype should improve their security model by implementing a trusted security scheme to ensure all packets are confidential and have integrity.

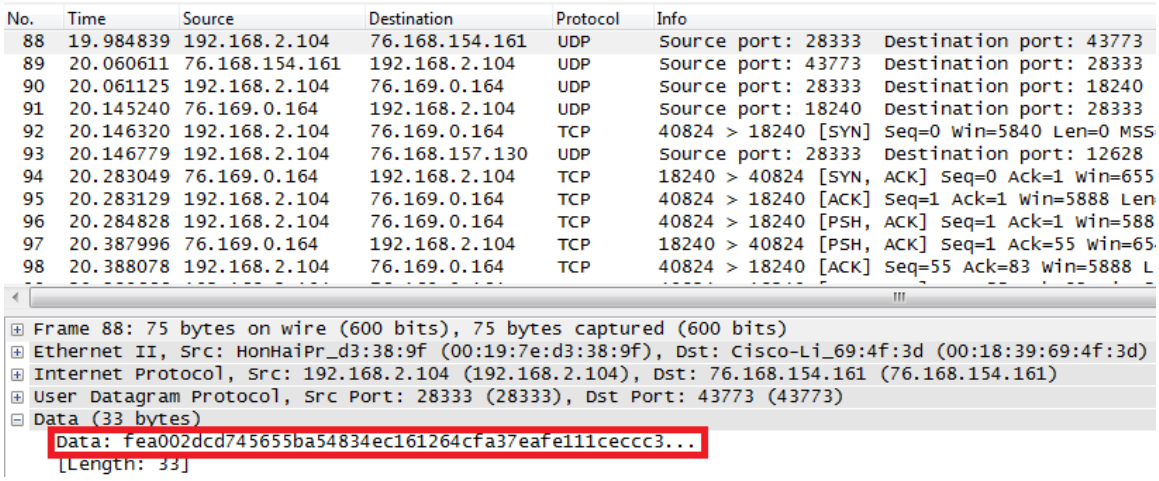


Figure 17. Wireshark capture: Skype traffic (From Wireshark, 1998)

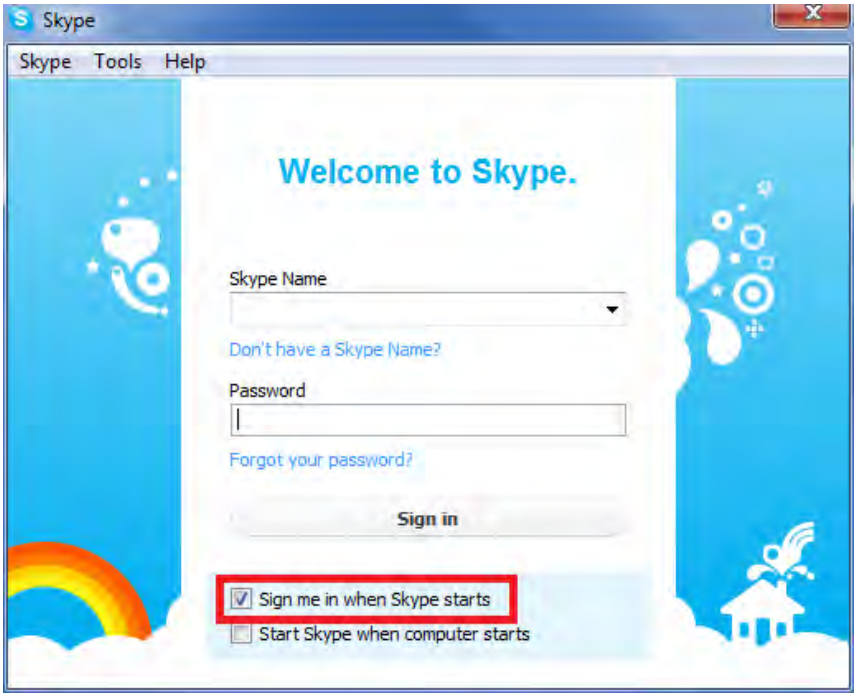


Figure 18. Skype Logon Window (From Skype, 2003)

3. Black-Box, at Rest Testing

Neither Skype nor Linphone have organic recording capabilities and therefore were not included in this test. As discussed before, Blink and Jitsi have organic call recording capabilities. Recordings were taken while both UAs were in a "completely"

secure mode; that is they had TLS and SRTP enabled. For both Blink and Jitsi, these recordings are not stored in an encrypted form. Figure 19 clearly shows that the waveform of both the Linux and Windows recordings are not encrypted. RFC 3711, which defines SRTP, is concerned with data transmission over the network and not storage. These implementations of SRTP are RFC-compliant; however because of their lack of storage protection, they do not create true end-to-end security. In order to implement secure storage of the recordings, the UAs would most likely have to incorporate a recording player in order to decrypt the recordings properly and still be in the confines of the TCB within the UA. Additionally, UAs that allow the use of the pipe command in Unix environments[8] would create a (not so) covert channel to siphon data out of the protocol enclave.

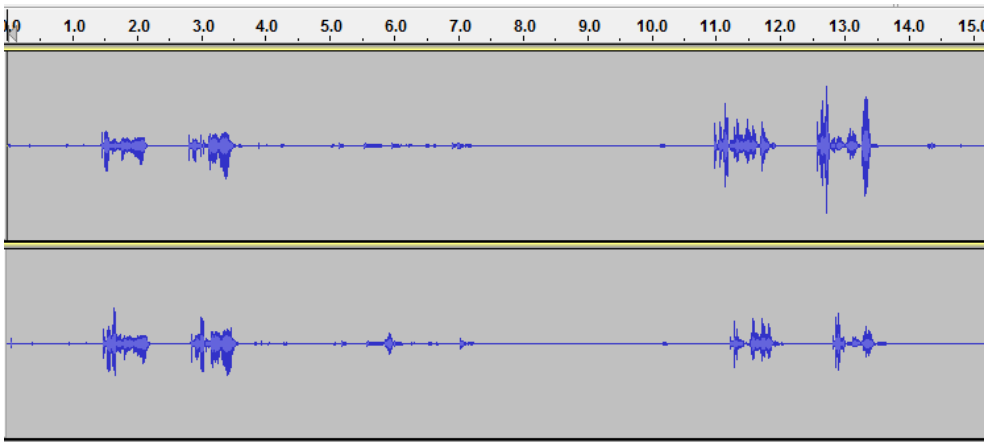


Figure 19. Visual inspection of the Linux and Windows Blink recordings (From Audacity, 1999)

4. Black-Box Testing Summary

The black-box portion of the experiment tested the ability of multiple VOIP/SIP UAs to handle voice calls in a secure manner. This demonstrated that there are current layer 7 security solutions that provide confidentiality and integrity of the calls while in transit. Specifically, the use of TLS and SRTP prevented the unauthorized access to:

[8] The pipe command allows the data handled by a particular program to be outputted into a receiving file.

- Signaling data sent between the initiating client and the server
- Signaling data sent between the server and called client(s)
- Voice data sent between the initiating client and the server
- Voice data sent between the the server and called client(s)
- Voice data sent from the initiating client to the called client(s)
- Voice data sent from the called client(s) to the initiating client

Though no UAs that store a recording of the call in a protected state were examined, the technology could be easily implemented into current VOIP/SIP UAs thus adding the capability of protecting the recordings while at rest on the file system.

a. Man (that must be) in the Middle

For each entity (i.e., SIP server) that handles the data in an unprotected form, the risk of compromise increases. It is important to reduce the amount of time that the data spends with entities other than the users. Not only does this increase security, it also decreases the amount of code that the data is exposed to in an unprotected form.

The VOIP/SIP infrastructure relies on a SIP server to negotiate the terms of the calls and therefore will be in the middle of all signaling traffic. For this reason, it is impossible to have a VOIP/SIP call without a server that is in the middle for the call setup. Registration redirection, server impersonation, denial of service (DoS) and traffic amplification, and forged session teardown are all examples of attacks that can target the SIP server remotely. The use of TLS mitigates these attacks (Dobson, 2010). Even with the use of TLS to avoid the remote attacks, the server must be trusted.

These attacks could just as easily come from an authentic server whose security has been breached. These attacks are a nuisance and can be serious if availability is crucial to time-sensitive data (e.g., emergency services). With TLS and SRTP enabled, if the SIP server cannot be trusted, traffic analysis can be conducted, however, as long as the voice data is protected, it has not been compromised and maintains its confidentiality and integrity. For this reason, it is extremely important that SIP server involvement be limited to just signaling data.

The involvement of the SIP server boils down to one of three cases.

- Case 1: The SIP server is used for call setup and does not act as a layer 7 gateway.
- Case 2: The SIP server is used for call setup and stays in the middle for layer 7 translation (i.e., translate from one codec to another for user interoperability).
- Case 3: The SIP server is used for call setup and stays in the middle for no reason (i.e., no codec translation is required).

Case 1 is the ideal case. Case 2 occurs when two UAs are using different codecs. This then requires the SIP server to translate between the two. For interoperability, this is good, but it requires the SIP server to see the data in an unprotected form. This may also be the case in which a conference call would be required to fall into. It will be important to design UAs that warn the user that they are operating in a situation like case 2. Case 3 occurs due to poor design and should be avoided at all costs. Table 1 is a summary of the UAs examined and what cases that UA uses. Additionally, the table shows if it possible to achieve end-to-end security while in transit during case 1.

UA	Server in the Middle?	Confidentiality and Integrity End-to-End for Case 1?
Linphone (with Zphone)	Case 1, 2	Yes
Blink	Case 2, 3	N/A
Jitsi	Case 1, 2	Yes
Skype	Case 1	Yes

Table 1. Summary of UA requirement of server in the middle

C. SOURCE CODE REVIEW: WHITE-BOX TESTING

The black-box testing of multiple VOIP/SIP UAs demonstrated the security capabilities of current open-source VOIP/SIP UAs. Because of the way VOIP/SIP technologies have been implemented, the server is not required to have access to the data

in order to route the data properly. This ensures the data is secure while in-transit between the two clients. However, the data is not necessarily completely protected. The possibility still exists that malicious code creating a covert channel may exist within the UA. This malicious code could then send the unprotected data outside of the TCB completely circumventing any of the security already in place.

Because of the size of the source code of many programs, it does not take an expert programmer to hide a covert channel in an otherwise well-intentioned application. An analysis of the files within the source code was conducted in an effort to separate the files into red, gray, or black files. A search for specific keywords within the title and the text itself plus internet searches for the files in question helped to correctly determine if the file handles unprotected data or not.

1. Blink

The Blink 0.2.7 source code was downloaded using the Darcs concurrent versioning system (CVS). The size of the source code was 5.67 MB in total. Figure 20 is a top level view of the source code. Looking at the folders' names gave very little indication of the functionality and therefore most files needed to be opened to determine the possibly of handling unprotected data.

Name	Size	Type	Date Modified
bin	1 item	folder	Thu 04 Aug 2011 01:00:55 PM
blink	14 items	folder	Thu 04 Aug 2011 02:13:31 PM
_darcs	8 items	folder	Thu 04 Aug 2011 01:00:55 PM
debian	15 items	folder	Thu 04 Aug 2011 01:00:55 PM
doc	5 items	folder	Thu 04 Aug 2011 01:00:55 PM
resources	14 items	folder	Thu 04 Aug 2011 01:00:55 PM
MANIFEST.in	381 bytes	plain text document	Thu 04 Aug 2011 01:00:55 PM
run	30 bytes	shell script	Thu 04 Aug 2011 01:00:55 PM
setup.py	1.4 KB	Python script	Thu 04 Aug 2011 01:00:55 PM
TODO	455 bytes	plain text document	Thu 04 Aug 2011 01:00:55 PM

Figure 20. Blink source code top directory

a. Red Files

Due to the size of the source code, there were not many files that were considered to be handling unprotected data. Specifically, Atom[9] and GData[10] files were considered red because they are used for Resource Description Framework (RDF) Site Summary (RSS) feeds. It must be noted that there are many "lib" files that would be required to handle unprotected data such as codecs that are not provided in the source code. Blink relies on the lib files that are organic to the OS. If these types of files were present, they would be considered red. The graphical user interface (GUI) used for the handling and recording of connected calls was labeled as red because it would definitely see data in an unprotected form.

The accounts window was also considered red. It was noted earlier that Blink actually stores the password of the VOIP/SIP account. The accounts window is where this actually happens. Though the accounts window does not actually see unprotected data related to the calls, it sees the account password that may be used as verification of authenticity therefore requiring a thorough scrub for any malicious code.

b. Gray Files

Gray files were considered to be files that may handle unprotected data, but could not be determined without a more detailed analysis. The four files in this category were GUIs that included:

- add_account.ui
- blink.ui
- preferences.ui
- session.ui

These four were thought to have the possibility of seeing unprotected or sensitive data, but it could not be determined with 100 percent certainty. Regardless, it would be a good idea to scrub these files for malicious code.

---

[9] Atom refers to a pair of related standards that are used for web feeds and resources.

[10] GData is a protocol used reading and writing data on the internet.

c. Black Files

The rest of the files not already covered were labeled as black. These files included the entire "_darcs" directory. This folder contains patches and inventories used for the Darcs CVS that would never see unprotected data. Also, all of the graphics and sound files were considered to be black since these are files that will not be able to execute code on their own.

d. Blink Totals

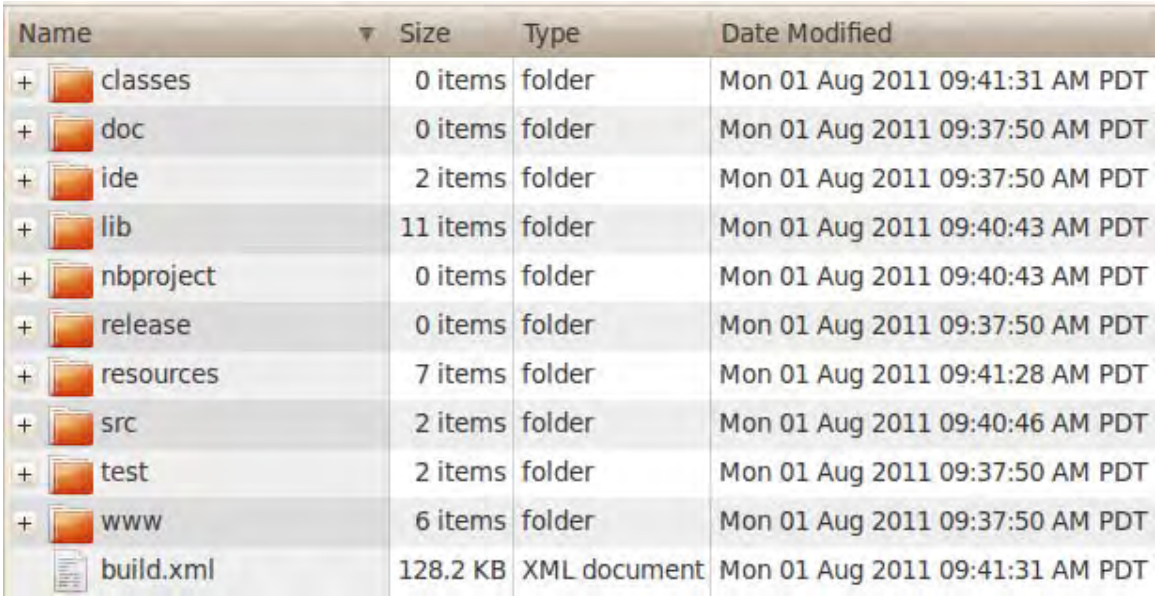
Table 2 shows a breakdown of the size (in MB) and the percentage of the overall size of each category.

Category	Size (MB)	Percentage
Red	0.44	7.80%
Gray	0.17	2.95%
Black	5.06	89.25%
Total	5.67	100%

Table 2. Blink source code totals

2. Jitsi

The Jitsi 1.0-beta1-nightly.build.3579 source code was downloaded using the Subversion CVS. The size of the source code was 108.24 MB in total. Figure 21 is a top level view of the source code. Again, looking at the folders' names did not help much and therefore a deeper look at the individual files was required to determine the possibly of handling unprotected data.



Name	Size	Type	Date Modified
classes	0 items	folder	Mon 01 Aug 2011 09:41:31 AM PDT
doc	0 items	folder	Mon 01 Aug 2011 09:37:50 AM PDT
ide	2 items	folder	Mon 01 Aug 2011 09:37:50 AM PDT
lib	11 items	folder	Mon 01 Aug 2011 09:40:43 AM PDT
nbproject	0 items	folder	Mon 01 Aug 2011 09:40:43 AM PDT
release	0 items	folder	Mon 01 Aug 2011 09:37:50 AM PDT
resources	7 items	folder	Mon 01 Aug 2011 09:41:28 AM PDT
src	2 items	folder	Mon 01 Aug 2011 09:40:46 AM PDT
test	2 items	folder	Mon 01 Aug 2011 09:37:50 AM PDT
www	6 items	folder	Mon 01 Aug 2011 09:37:50 AM PDT
build.xml	128.2 KB	XML document	Mon 01 Aug 2011 09:41:31 AM PDT

Figure 21. Jitsi source code top directory

a. Red Files

The red files included anything that handled credentials (passwords), SRTP, crypto, and codecs. The source code for Jitsi included the codecs for each OS that is compatible. Because of the amount of OS specific files, the amount of red files is much larger than what was seen in Blink. Many of the red files most likely would not need to be in the source code and could depend on the native OS files. Many of these files are part of the lib directory. There will be two sets of totals at the end show with and without lib files

Jitsi has the ability to connect via audio, video, and other services such as Jabber and Yahoo Messenger adding to the abnormally large section of red in comparison to Blink. Additionally, the spellchecker files were included in this section. Several GUIs including those for chat, audio calling, video calling, and desktop sharing were also determined to be red.

b. Gray Files

The gray files consisted of the implementations of many events. A few GUIs that were only somewhat likely to see unprotected data were put into this category. Additionally, geolocation, message history, and some protocol data were all included in this category.

c. Black Files

For the same reasons as listed in the Blink results, the graphics and sound files were categorized as black. The plug-ins that would not carry sensitive data were also put into this category.

d. Jitsi Totals

Table 3 shows the totals of the source code as categorized into the three groupings. As mentioned before, there is a very large section that is considered red. Because it was expected that the red portion would be smaller than the black, the lib files that are OS specific were removed to see how this would affect the totals. The totals without the lib files can be seen in Table 4.

Category	Size (MB)	Percentage
Red	59.93	55.37%
Gray	8.45	7.80%
Black	39.87	36.83%
Total	108.24	100.00%

Table 3. Jitsi source code totals

Category	Size (MB)	Percentage
Red	18.66	29.43%
Gray	8.45	13.32%
Black	36.31	57.26%
Total	63.41	100.00%

Table 4. Jitsi source code totals without lib files

3. Source Code Review Summary

The white-box testing shows that large sections of both sets of source code will only handle protected data. By cordoning off the much smaller red portions of code, the TCB is drastically reduced making the job of scrutinizing the code that will deal with unprotected data much more possible. The TCB would be further reduced through the detailed analysis of the gray category.

The source code review provided a basic analysis of the amount of source code that would need to be thoroughly tested for malicious code. Using the VOIP/SIP technologies that currently exist as a layer 7 security solution and analyzing the red sections of source code would provide a very effective start to reducing the TCB. The reduction of the TCB would in turn reduce the possibility of unauthorized access to classified data while in transit or at rest in the file system.

No white-box testing of the SIP server was conducted. Some VOIP/SIP UAs require the SIP server to be in the middle of the conversation acting as a layer 7 gateway which would indicate the necessity to conduct a TCB analysis of the SIP server. However, there are also UAs that do not require the SIP server to act as a gateway. This lack of layer 7 gateway configuration is preferred to avoid the requirement of a trusted SIP server.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. SUMMARY

It is clear that voice over internet protocol (VOIP) is overtaking a lot of single-segment or voice-network-only voice applications (such as law enforcement radios). VOIP can also be seen in phone service as applications on some smartphones. Because of VOIP's rapid growth, there is a need to analyze VOIP security.

This thesis focused on the feasibility of using VOIP/SIP as a means of achieving true end-to-end security. Current military and civilian technologies and processes and how they protect the confidentiality and integrity of data were explored. How data was protected between users and a server during and after a call and how this was implemented in different UAs was examined. Finally, a discussion on the amount of code that would need to be scrubbed during a TCB evaluation to remove vulnerabilities in the code was conducted.

1. Data Protection with VOIP/SIP

The majority of the world has tried to protect data by applying encryption at the lower levels of OSI Reference Model. While protecting the infrastructure over which the data rides is important and necessary, this will not provide true end-to-end security. The end result must protect not only the network, servers, machines, etc., but it must also protect the data. By protecting the data, the infrastructure can fail without the data being compromised.

As the world becomes increasingly mobile, the ability to protect the infrastructure will become more difficult. The consumers refuse to give up functionality for security, as is shown by the amount of smartphone users that conduct purchasing, banking, and other such sensitive functions on their almost entirely unsecure phone. Since functionality

cannot go by the wayside, there must be a different way in which developers attack the security solution. That way is via layer 7 security solutions (including data at rest protection) such as VOIP. VOIP has the ability to:

- Provide data confidentiality, in transit and at rest, through VOIP/TLS and SRTP encryption
- Provide data integrity, in transit and at rest, through VOIP/TLS and SRTP message authentication codes
- Provide a way to reduce the TCB size
- Enforce the "need-to-know" and mitigate the social engineering vulnerability.

With a layer 7 security solution, only the VOIP application and peripheral applications authorized by the VOIP application will have access to unprotected data at rest or in transit.

2. Testing

The black-box study tested the data protection of a few VOIP UAs. Without any data protection enabled, where the data was vulnerable within the network was determined. Wireshark was able to capture all VOIP traffic, reassemble it, and play it back without any problems. Additionally, the recordings were stored in an unprotected format and were able to be played by any program that plays mp3s.

Adding signaling and voice data protection showed that VOIP has the ability to be a layer 7 security solution that provides true end-to-end security. The UAs provided secured signaling and voice data through layers 6 and 7. The one in transit vulnerability that remained was that depending on the UA, the SIP server acted as a layer 7 gateway (this will be further explained in the next section). The UAs that were tested did not have an organic ability to play recordings, thus the data at rest was not protected. The addition of organic recording and playback ability would be simple and would provide true end-to-end security for not only data in transit, but also at rest.

B. AREAS FOR FUTURE RESEARCH

1. Secure Multicast (also known as Conferencing)

VOIP/SIP has been very focused on the unicast/peer-to-peer configuration. However, as VOIP becomes more prevalent, multicast will be a feature that will be desired in VOIP/SIP UAs. This is particularly true of emergency services and the military as much of their data is multicast in nature. Additionally, as the frequency spectrum continues to get more crowded, efficient use of the spectrum will be very necessary. Exploiting multicast to enable delivery of a message to more than one destination for the price of a single transit will create efficient use of the spectrum. With multicast the protection problem becomes much more complex.

Unless each UA has the ability to directly send its data to the other UAs involved in the conversation, the SIP server will likely need to act as a layer 7 gateway to relay all parts of the conversation to all parties involved. An area of research would be how to protect the data with the SIP server in the middle to act as a relay station for the voice data.

If there is no need for the SIP server to stay in the middle, then the UAs will have to handle all PKI certificates. PKI is unicast in nature, therefore it may be somewhat difficult for the UAs to handle all of the certificates. Using PKI to distribute a symmetric session key may make more sense. During an extended conversation, users may be gained and/or dropped while the conversation continues. How the session key is managed during these types of events will be important to ensure only authorized users have access to the conversation. The use of PKI for multicast security will need to be another area of future research.

2. SIP Server Vulnerabilities

Securing the voice data is, without a doubt, the most important aspect of VOIP security. Removing the SIP server from the middle of the voice traffic significantly reduces the number of data vulnerabilities and the amount of code—the entire SIP

server—that will be required to go through a TCB evaluation. While using protocols such as ZRTP prevents the server from remaining in the middle of a conversation there may be reasons that the server is forced back into the middle. For example, if the UAs are using different codecs for the voice, ZRTP will not connect and the server will be required to serve as a codec translator for the now unprotected voice data. This situation becomes even more complex when discussing multicast. Naturally, demanding that all UAs involved use the same codec will solve a large portion of this problem, but that may not always be possible.

Another example is network address translation. The SIP server is often required to send the voice data to a specific port so that the receiving router can translate the request and route it to the proper private destination IP address. This was outside of the scope of the thesis, but is certainly an area that needs to be researched in order to remove the SIP server from the conversation as much as possible.

The SIP server is responsible for the setup, maintenance, and termination of VOIP calls. Much research has been conducted to determine how vulnerable a SIP server is to a DoS attack, but there is a lack of research emphasis on how the SIP server handles the (un)protected signaling data, what the repercussions of an intercept would be, and how to mitigate this. Traffic analysis has the ability to produce information that is just as useful as listening to the actual conversation making this research area a must.

Reliance on the SIP server to connect the calls means that the server needs to be available at all times. This thesis did not discuss availability, but if the SIP server is not available, calls cannot be made. Availability of the SIP server along with the ability to gain or drop parties on the fly will need to be studies in detail.

3. Analysis of ZRTP Vulnerabilities

ZRTP is a relatively new protocol. The first draft was submitted to the IETF in 2006 and the final draft was published in April of 2011. The publishing of papers such as “Security and Usability Aspects of Man-in-the-Middle Attacks on ZRTP” by Petraschek

et al. demonstrates that ZRTP is not flawless. More research needs to be conducted to ensure the integrity of this new protocol and how to mitigate/defend against known vulnerabilities.

4. Detailed UA Code Review and TCB Evaluation

The white-box testing provided a basic analysis of the amount of source code that would need to be thoroughly tested for malicious code. A thorough review of the source code is necessary to validate the categorization. The detailed review would remove the "gray" category. After this review is complete, a comprehensive TCB evaluation must be conducted to remove the possibility of vulnerabilities in the "red" code.

5. Move Beyond Voice

Though VOIP stands for *Voice* Over IP, there are many other types of communications that can be carried over SIP and RTP which include video, fax, SMS, instant messaging, RSS feeds, and others. Many of these are already being implemented in some UAs such as Jitsi that also supports other messengers such as XMPP/Jabber, AIM/ICQ, Windows Live, Yahoo!, and Bonjour. The same security principles already discussed throughout this thesis will need to apply to all features.

VOIP has the ability to replace and improve upon some existing systems used throughout the Department of the Navy, and DoD in general. Much like STEs, voice communications over traditional radio nets do not provide authentication of a specific user. Most traditional radio nets are single segment only. Each user is authorized on the net by virtue that they have the proper encryption/decryption keys, but there is no way to authenticate each user individually. It is assumed that they are who they say they are. VOIP has the ability to enforce true end-to-end security by ensuring that the confidentiality and integrity (and authenticity) of the conversation would be intact.

C. RECOMMENDATIONS

As discussed in Chapter I, the standards (or best practices) that are available from the IETF do not extent to the user. Their scope stops with the internet creating a gap of

standardization between the internet and the user. In order to create standards, implementation recommendations will need to be made and then evaluation criteria created.

1. UA Implementation Recommendations

The current VOIP UAs depend on the SIP server for a lot more functionality than should be allowed. Putting the SIP server in the middle of everything is poor design and leaves gaps in security. The server only needs to be in the middle for signaling; for many UAs this is not the case.

New UAs need to be developed so that all functionality (except call setup) can be moved away from the server and toward the UAs. The functionality that currently resides with the server (depending on the UA) that can be moved to the UAs includes codec translation, temporary key distribution, RTP security. Additionally, ZRTP-like technology is a must to ensure the encryption keys are remade for each conversation and to keep the server out of the conversation.

The ability to use public key cryptography (PKC) must also be included in the UA. Without this, a large amount of symmetric key infrastructure will be required to ensure confidentiality *and* integrity of the conversations. With the SIP server no longer in the middle, the UAs will need to authenticate each other. This requirement will be helped by the implementation of PKC.

Using PKC, the UAs need to have the ability to store protected recordings of the conversation on the file system with the confidentiality and integrity intact. None of the UAs tested had this ability therefore any entity with (un)authorized access to the file system could access the recordings in an unprotected form. Confidentiality and integrity of the conversation, in transit and at rest, are the keys to true end-to-end security.

As previously discussed, there may be times that the SIP server will be required to be in the middle for the voice (i.e., to translate between different codecs). The vulnerability created by having the SIP server in the middle may be acceptable. If this is not true, it is important that the users be clearly notified that the SIP server *is* in the

middle and that true end-to-end security has not been achieved. Now UA evaluation criteria can be created to ensure these recommendations have been added to future UAs.

2. End-to-End Standards

Standards for how UAs implement protocols like SIP, TLS, RTP, SRTP, and ZRTP need to be created. The IETF provides standards that focus on the behavior of the protocols while on the internet, however, handling of data within the gap between the user and the internet, which is the UA, is not standardized and has been shown to possibly be handled insecurely. Standardization would ensure that vulnerabilities would be limited to those that are flaws of the protocol and not the implementation. It needs to be noted that standards are not easy to create. Because of this, it is important that at a minimum, best practices that adhere to the evaluation criteria be drafted.

As end-to-end standards are created, it is important to ensure there is an organization to codify the standards. This organization would be very similar to the IETF, but its scope would extend beyond the internet. Without this type of organization, developers will be able to claim that their software meets the standards, but no assurance would be provided. In addition to an international organization, U.S. government organizations may want to ensure the software is developed to their standards as well. DoN entities such as CIO and Fleet Cyber Command/10th Fleet may have a special interest in this organization.

3. Education on Public Key Cryptography Technologies

VOIP applications require PKC to create true end-to-end security. The DoD has already implemented PKI with the use of common access cards (CAC). Despite having the CACs, many members of the DoD still do not use the PKI to encrypt and sign their unclassified but sensitive e-mails. Policy may dictate the use of PKI to ensure confidentiality and integrity, but without enforcement, there are no consequences for not using the PKI.

It is recommended that as more VOIP UAs are created, particularly for the DoD, that PKC be required for use. This along with education on the vulnerabilities of not using PKC will prevent the disclosure of unclassified, but sensitive data.

D. FINAL THOUGHTS

This thesis has analyzed existing VOIP applications as a secure technology that has the ability to create true end-to-end security. After testing four VOIP UAs, it was apparent that while communications in transit were secure, how the UA handles data at rest needs to be reevaluated. With the above future areas of research and recommendations, VOIP will create confidentiality and integrity for secure communications throughout the DoD and the world.

APPENDIX NETWORK SETUP DETAILS

This appendix is provided for purposes of replicating the stand-alone network experiment, if desired.

A. HARDWARE AND SOFTWARE USED

Four laptops and a Dell Powerconnect 2716 switch were used to create the network. The following is the how the laptops were configured.

- Monitoring laptop
  - Manufacturer: ACER
  - OS: Ubuntu 10.04
  - Extra programs installed: Wireshark
  - Description: This laptop was used to monitor all traffic on the network. Its IP address was statically set to 192.168.2.6
- Server
  - Manufacturer: ACER
  - OS: Ubuntu 10.04
  - Extra programs installed: Asterisk 1.8
  - Description: This laptop was used as the SIP server. Its IP address was statically set to 192.168.2.113
- UA – User 1002
  - Manufacturer: ACER
  - OS: Ubuntu 10.04
  - Extra programs installed: Blink, Jitsi, Linphone, Skype, Zfone
  - Description: This laptop was used as one of the two UAs. For SIP server registration purposes, this laptop was known as user 1002.
- UA – User 1003
  - Manufacturer: Dell
  - OS: Windows 7
  - Extra programs installed: Blink, Jitsi, Linphone, Skype, Zfone

- Description: This laptop was used as one of the two UAs. For SIP server registration purposes, this laptop was known as user 1003.

B. NETWORK SETUP

Port mirroring was enabled so that all network traffic would be sent to the monitoring laptop. All networked components were given a static IP address (see Table 5).

Component	Switch Port	IP Address
Switch	N/A	192.168.2.1
SIP Server	1	192.168.2.113
UA – 1002	3	192.168.2.2
UA – 1003	5	192.168.2.3
Monitoring Laptop	16	192.168.2.6

Table 5. Physical Network Setup

C. USER AGENT SETUP

As already mentioned, the UA laptops were setup with Blink, Jitsi, Linphone, Skype, and Zfone. One laptop was user 1002 and the other 1003. To add an account, all UAs required the username and password. Both usernames were 100X@192.168.2.113, where X is either a "2" or "3" and their password was "testtest". The rest of the setup was different for each UA, but as an example, screenshots of Blink will be provided.

To avoid the need for codec translation, all UAs were forced to use the PCMU audio codec (see Figure 22). Also on this screen is the ability to turn on SRTP encryption. Jitsi and Linphone (with Zfone) use ZRTP and the setup is similar.

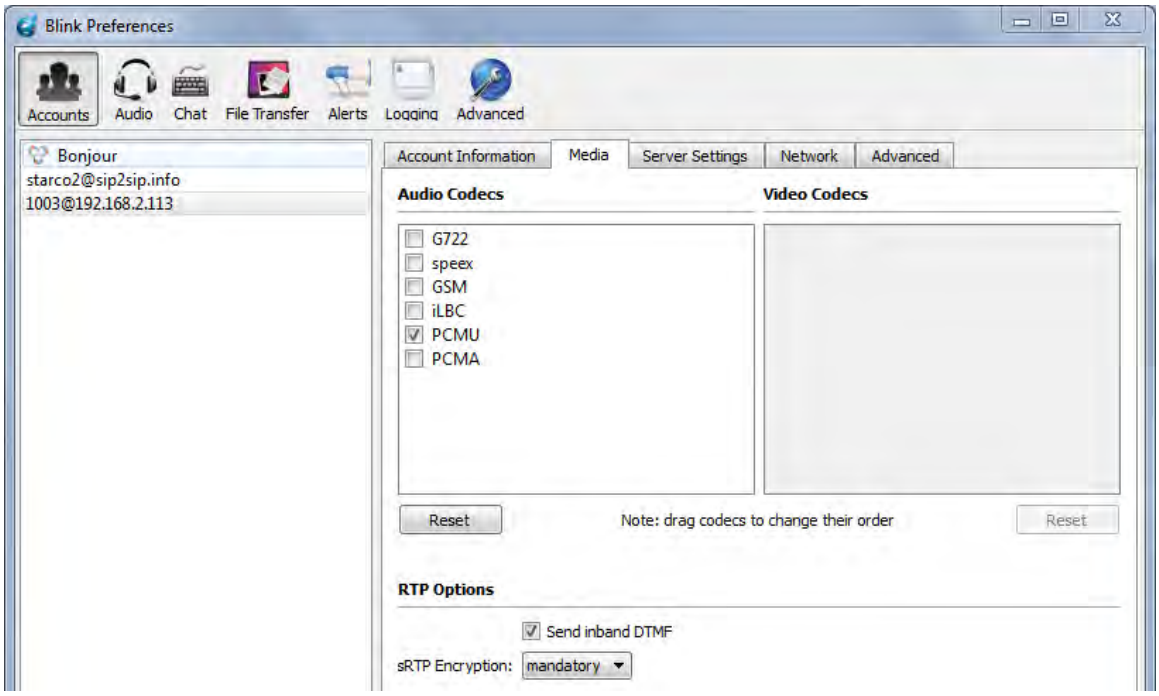


Figure 22. Blink media settings (From Blink, n.d.)

The SIP proxy settings needed to direct the UAs to the SIP server. The outbound proxy was filled in as can be seen in Figure 23. The port used was 5060 if the transport was UDP. If the transport was TLS, then port 5061 was used.

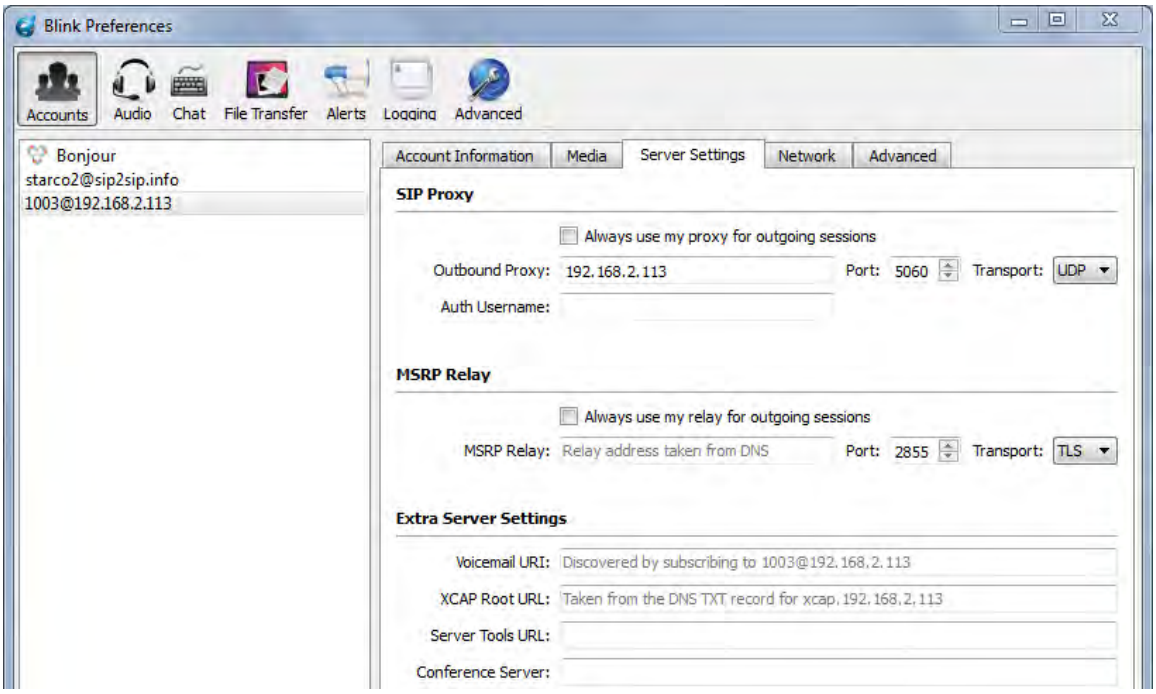


Figure 23. Blink server settings (From Blink, n.d.)

Finally, in order to use TLS, the UA had to be directed to the appropriate certificate file. This can be seen in the bottom of Figure 24.

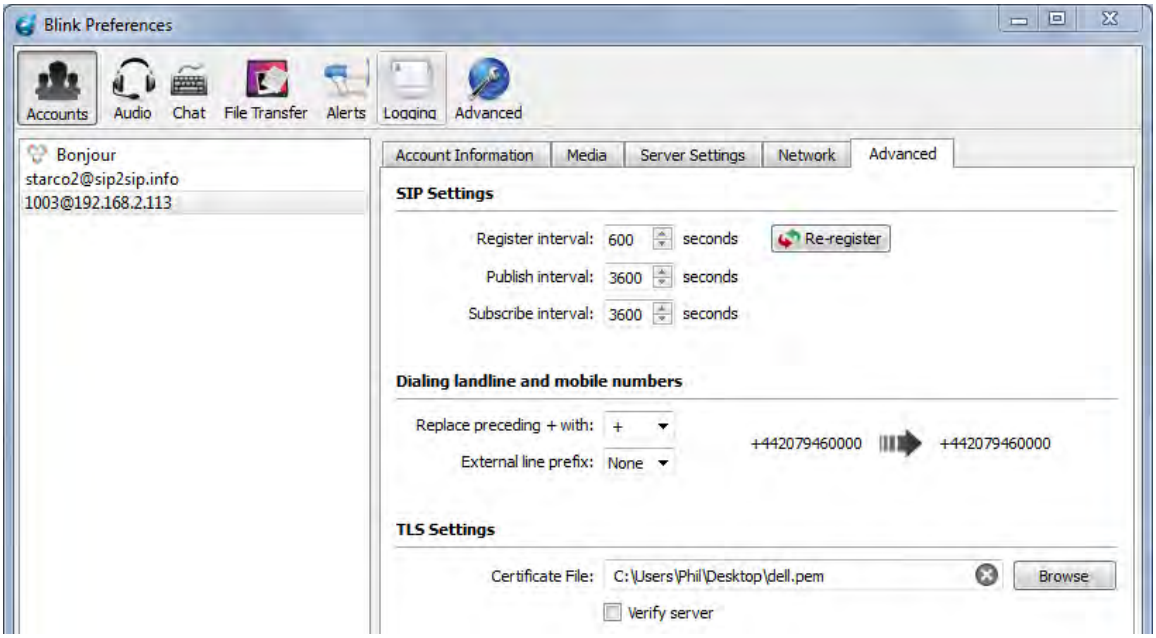


Figure 24. Blink advanced settings (From Blink, n.d.)

D. SIP SERVER SETUP

Asterisk was installed onto the server computer and all files were left as on the default settings with the exception of two. The two files were edited with a text editor. Note that a ';' denotes a comment line. The comments indicate what sections needed to be uncommented in order for TLS and SRTP support to work correctly.

Filename: sip.conf

```
[general]

;;;;;;;;;;;;; This is all for TLS support ;;;;;;;;;;;;;
transport=tls
tlsenable=yes
tlsbindaddr=0.0.0.0
tlscertfile=/etc/asterisk/keys/asterisk.pem
tlscafile=/etc/asterisk/keys/ca.crt
tlscipher=ALL
tlsclientmethod=tlsv1
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

[sets](!)
type=friend
context=from-sip
host=dynamic
allow=all
dtmfmode=rfc2833

;;;;;;;;;;;;; This is for SRTP support ;;;;;;;;;;;;;;;;
encryption=yes
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; 1
[1002](sets)
secret=testtest

; 2
[1003]( sets)
secret=testtest
```

Filename: extensions.conf

```
[general]

[from-sip]
exten => 1002,1,Dial(SIP/1002)
exten => 1003,1,Dial(SIP/1003)
```

Once the files were edited to their final form, the server was restarted and it worked as intended.

LIST OF REFERENCES

A.G. Projects. (n.d.). Blink: A state of the art, easy to use SIP client (Version 0.2.7) [Software]. Available from http://icanblink.com/download.phtml

Assistant Secretary of Defense for Networks & Information Integration andDepartment of Defense Chief Information Officer. (2007). *DoD Directive 8500.01E.*

Baset, S. A., & Schulzrinne, H. (2004, September 15). An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Retrieved from http://arxiv.org/ftp/cs/papers/0412/0412017.pdf

Baugher, M.; & McGrew, D.; Cisco Systems; Naslund, M.; Carrara, E.; Norrman, K.; Ericsson Research. (2004, March). *RFC 3711 - The Secure Real-time Transport Protocol (SRTP)*. Retrieved from http://www.ietf.org/rfc/rfc3711.txt

Biondi, P. & Desclaux, F. (2006, March). *Silver Needle in the Skype*. Presentation at BlackHat Europe, Retrieved from http://www.secdev.org/conf/skype_BHEU06.handout.pdf

Clark, S., Goodspeed, T., Metzger, P., Wasserman, Z., Xu, K., & Blaze, M. (2011, August 12). *Why (Special Agent) Johnny (Still) Can't Encrypt:A Security Analysis of the APCO Project 25 Two-Way Radio System.* Retrieved from http://online.wsj.com/public/resources/documents/p25sec08102011.pdf

Combs, Gerald. (1998). Wireshark: Network Protocol Analyzer (Version 1.6.1) [Software]. Available from http://www.wireshark.org/download.html

Committee on National Security Systems. (2010). *National Information Assurance (IA) Glossary.*

Dannenberg, R., & Mazzoni, D. (1999). Audacity: The Free, Cross-Platform Sound Editor (Version 1.2.6) [Software]. Available from http://audacity.sourceforge.net/download/

Defense Advanced Research Projects Agency. (2010, December 22). *MAINGATE Provides ISR Data Dissemination and C2 Networking.* Retrieved from www.darpa.mil/WorkArea/DownloadAsset.aspx?id=1804

Definitions, 44 U.S.C. §3542 (2006).

Department of Defense. (1985). *DoD 5200.28-STD - Department of Defense Trusted Computer System Evaluation Criteria.* Washington D.C.: United States Government Printing Office.

Dierks, T., Certicom, & Allen, C. (1999, January). *RFC 2246 - The TLS Protocol*. Retrieved from http://www.ietf.org/rfc/rfc2246.txt

Dobson, L. E. (2010). *Security Analysis of Session Initiation Protocol*. (Master's thesis, Naval Postgraduate School, 2010). Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2010/Jun/10Jun_Dobson.pdf

Fildes, J. (2010, June 8). *BBC News - Wikileaks site unfazed by arrest of US army 'source'*. Retrieved from http://www.bbc.co.uk/news/10265430

Friis, J., & Zennström, N. (2003). Skype (Version 5.5) [Software]. Available from http://www.skype.com/intl/en-us/get-skype/

Green, L., & Mackowick, F. (2007, October). *Experimental Results of Routing Protocol Convergence in a HAIPE Protected Fault Tolerant Network.* Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4454805&isnumber=4454733

Harris, S. (2008). *CISSP All-in-One Exam Guide.* Ney York: McGraw-Hill.

Held, G. (2001). *Understanding Data Communications: From Fundamentals to Networking.* West Sussex: John Wiley & Sons.

Institute for Telecommunications Sciences. (1996, August 23). *Definition: datagram*. Retrieved from http://www.its.bldrdoc.gov/fs-1037/dir-010/_1464.htm

Institute for Telecommunications Sciences. (1996, August 23). *Definition: frame*. Retrieved from http://www.its.bldrdoc.gov/fs-1037/dir-016/_2313.htm

Institute for Telecommunications Sciences. (1996, August 23). *Definition: protocol data unit (PDU)*. Retrieved from http://www.its.bldrdoc.gov/fs-1037/dir-028/_4199.htm

International Organization for Standardization and International Electrotechnical Commission. (1996, June 15). *ISO/IEC 7498-1 - Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.* Retrieved from http://standards.iso.org/ittf/licence.html

The Internet Engineering Task Force. (n.d.). *Internet Engineering Task Force*. Retrieved from http://www.ietf.org/

Ivov, E. (2011). Jitsi: Open Source Video Calls and Chat (Version 1.0-beta1 stable) [Software]. Available from http://jitsi.org/index.php/Main/Download

Linphone Development Team. (2010). Linphone: Free SIP VOIP Client (Version 3.4.3) [Software]. Available from http://www.linphone.org/eng/download/

The National Security Telecommunications and Information Systems Security Committee. (2001). *Operational Security Doctrine for the FORTEZZA User PCMCIA Card* (NSTISSI No. 3028). Retrieved from http://www.cnss.gov/Assets/pdf/nstissi_3028.pdf

Rosenberg, J.; dynamicsoft; Schulzrinne, H.; Columbia University; Camarillo, G.; Ericsson; Johnston, A.; WorldCom; Peterson, J.; Neustar; Sparks, R.; Handley, M.; ICIR; Schooler, E.; AT&T. (2002, June). *RFC 3261 - SIP: Session Initiation Protocol.* Retrieved from http://tools.ietf.org/html/rfc3261

U.S. Naval Academy. (2011).*Secure Telephone Equipment Terminal* (USNAINST 2210.1C). Retrieved from http://www.usna.edu/AdminSupport/Instructions/2000-2999/2210.1C.pdf

WindowsNetworking.com. (n.d.). *image0011210155736818.jpg.* Retrieved from http://www.windowsnetworking.com/img/upl/image0011210155736818.jpg

Zimmerman, P.; Zfone Project; Johnston, A.; Avaya; Callas, J.; Apple, Inc. (2011, April). *RFC 6189 - ZRTP: Media Path Key Agreement for Unicast Secure RTP*. Retrieved from http://tools.ietf.org/html/rfc6189

ZRTP FAQ - GNU Telephony. (2011, March 22). Retrieved July 29, 2011, from GNU Telephony: http://www.gnutelephony.org/index.php/ZRTP_FAQ

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

4. Dr. Dan Boger
   Chair, Department of Operation and Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Dr. Ray Buettner
   Naval Postgraduate School
   Monterey, California

6. Mr. Don McGregor
   Naval Postgraduate School
   Monterey, California

7. LT Philip Starcovic
   Naval Postgraduate School
   Monterey, California