國立交通大學

資訊學院　資訊學程

碩 士 論 文

在 VoIP 環境中的彈性化監聽方案

Flexible Interception in VoIP Environment

研 究 生：顏士哲

指導教授：蔡文能　教授

中 華 民 國 九 十 七 年 五 月

在 VoIP 環境中的彈性化監聽方案
Flexible Interception in VoIP Environment

研 究 生：顏士哲 Student：Shih-Che Yen

指導教授：蔡文能教授 Advisor：Dr. Wen-Nung Tsai

國 立 交 通 大 學
資訊學院 資訊學程
碩 士 論 文

A Thesis
Submitted to College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of

Master of Science
in

Computer Science

May 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年五月

在 VoIP 環境中的彈性化監聽方案

學生：顏士哲　　　　指導教授：蔡文能教授

國立交通大學　資訊學院　資訊學程碩士班

摘　要

由於 IP 網路的蓬勃發展，再加上更便宜的通訊費用和更多樣化的加值服務，VoIP 的技術成為傳統 PSTN 網路的替代方案。但是在提供通訊服務之外，電信業者也必須提供合法的監聽管道，提供政府能夠執行合法的監聽。本篇論文在現行的網路基礎架構下，提供彈性化的 VoIP 監聽方案。我們提供了一套名為 FIVE System 的彈性化監聽方案，提供五種不同的監聽模式，並針對不同的模式做評估與分析。

我們提供的五種監聽方式分別為：The Rogue Back to Back Interception, The Rogue SIP Proxy Interception, The SIP Proxy attached Interception, Remote Attack Interception and Port Mirroring Interception。每一種不同的監聽模式都可應用在某一種網路區域，而且各有其優點。藉由我們 FIVE System 的協助下，政府單位可以選擇最適合的方式來做合法的監聽。我們也建構了 VoIP 的環境來驗證我們的 FIVE System，所得到的實驗結果更可以提供未來使用 FIVE System 的參考。而各種彈性化的方案，提供使用者根據不同的網路類型選擇方案，或者使用混合的方式得到最佳的網路監聽效果。

Flexible Interception in VoIP Environment

student：Shih-Che Yen Advisors：Dr.Wen-Nung Tasi

Degree Program of Computer Science
National Chiao Tung University

ABSTRACT

The VoIP is growing rapidly due to the popular of the Internet network. The VoIP can provide the cheaper communication fee and various values-add services. It can replace the traditional PSTN network. But the VoIP network should also provide the lawful interception function for government. This thesis based on the current network architecture to provide a Flexible Interception in VoIP Environment. We name this system as FIVE system.

The FIVE system is a flexible interception system. It provides five different interception models for interception. The five models are Rogue Back to Back Interception, Rogue SIP Proxy Interception, SIP Proxy attached Interception, Remote Attack Interception, and Port Mirroring Interception. All interception models have their advantages. The government can do the flexible interception by using the FIVE system. We also setup the VoIP environment to do the experiment according to our experimental results. Government can choose the best solution to adapt the different network environment. And the hybrid mode can provide the best VoIP lawful interception.

誌　　　　謝

在交大求學的這段期間很感謝各位師長的諄諄教誨，和各位同學的相互勉勵之下，讓我可以順利的完成課業，和論文的相關研究。首先要感謝蔡文能教授擔任我們的指導教授，對於我們的論文研究和專業知識都不辭辛勞的給予許多的指導和協助。在論文研究的學習過程中，我們不但得到了許多專業的知識，並且學習到了做學問的方法。再來是感謝和我一起努力的同學們，雖然大家都是以在職的身份同時忙於工作和課業，但是在我們的相互激勵和幫助之下，我們在課業方便都得到了不錯的結果。最後是感謝我的內人李佳倩小姐。在這兩年的求學過程中，總是辛勤的幫我扶持家務，讓我能沒有後顧之憂的努力於事業與課業之上。也感謝交大能提供這樣的環境和機會，讓我在出社會之後仍有進修的機會。今天我以身為交大人為榮，希望他日交大也會以我為榮。

Contents

FIGURE CONTENTS

TABLE CONTENTS

Chapter 1 Introduction

Traditional PSTN (Public Switched Telephone Network) telecommunication service provides stable services for years. It can reach the five nines service quality. But circuit switching network always costs a lot in the network architecture construction. It is hard to do the cost down. But by the arising of the Internet network, we have chances to choose VoIP (Voice over Internet Protocol) to make a phone call. And VoIP can support more value added services. Video call is one of the new features. That will bring us to a more modern life style.

The VoIP is used to transport the voice by using the Internet Protocol. For the growing volume of the Internet users, and the complete Internet Network construction, the trend will push us to next generation communication network. The NGN (Next Generation Network) is going to replace the current PSTN network. It will provide us a cheaper charge of the communication fee, as well as much add-value services. But before this technique being matured, there are still many security concerns.

1.1 Motivation

After working in a telecomm company for years, we understand to provide a total solution is very important. The best advantage of the VoIP is that the technique is based on the widely used IP network. The service provider didn't need to construct their own network infrastructure. But it also brings up many the security issues. And to modify the current infrastructure to a complete new one will be impossible. The cost will be incredible.

So there will be two major reasons that we choose this topic. The first reason is that the VoIP network security is very important. If we didn't secure the security, it will lead to more problems, such as quality, privacy even the crime. For example, if someone uses the credit card by phone, the credit card pin number might be stolen by the voice interception. These issues will lead to serious crime problems. The security issues in VoIP are not only the IP protocol layer problems. But also the VoIP protocols, the applications and the Operation

System flaws. The internet is an open space for everyone to access, so all of the security issues should be concerned. We can review the security issue by the concept of OSI network models; it could be some flaws in each layer. The protection should be well concerned in any aspect of it.

And another reason is the government always requests the telecomm service provider to provide a lawful interception function for the government. But this is another big problem for the service providers. We know that the packet switching network always didn't have a fix routing path and you can't easily wiretap your target machine. Even the soft switch only management the signaling messages. So if you can't wiretap your target in LAN, you should wiretap the specific equipment or to do the interception in some specific access points. Our study will provide a solution of it.

1.2 Object

Due to the cost of reconstruct the IP network infrastructure will be incredible. So we'll base on the original infrastructure to provide a software based solution to do the interception. The application should be individual, and running in an individual sever or attach in a server without modify or recompile the VoIP protocol stack in the server.

First of all, we will introduce all of the VoIP security vulnerabilities in different points of view, and then to study how to attack the VoIP network countermeasures. Based on the studies, we will implement a VoIP network program that can support varies lawful interception models. And build a test environment to verify our solution.

1.3 Emphasis

There are two emphases in this thesis. The first one is the analysis of the VoIP security issues. And the one second is the VoIP interception system.

The current VoIP protocol is based on the IP network, so it inherits all of the problems in the IP network. Unsecured VoIP network may bring up many serious problems. The users have to protect from various kinds of denial of service attacks. And their private information might be stolen. So the security issues are a major part that we want to study.

The second part is the lawful VoIP interception. For the security issue, the government needs to intercept the specific people or phone. But the call routing in VoIP is not the same as traditional PSTN phone, so we need a new solution for the VoIP interception. It is better to keep the current VoIP architecture. So we'll provide a software based solution to achieve this goal.

1.4 "FIVE" System Introduction

We build a software based system to do the interception, and we name this system "FIVE" system. This name has two meanings; the first is the "Flexible Interception in VoIP Environment". It is the target of the system. Another reason is our system provides 5 different interception models. The interception server has different locating in these five different in the VoIP network. And use different mechanisms to process the interception. We will descript the details about how to implement them, and also do the compare and analysis the result of experiment.

Chapter 2 Background

The VoIP signaling and voice packet will be transport in the Internet. So the Internet protocol is the basic of the VoIP protocols, and there are still other protocols and equipments to construct the VoIP environment. In this chapter, we will introduce all of the background knowledge of VoIP.

The first is the overview of VoIP network. We'll introduce the architecture of the VoIP network. And then is the VoIP related protocols, there are various VoIP related protocols that support different functions. Most important of all, the signaling protocols is what we need to take care. The call setup procedure is defined in the signaling protocols. So we'll also introduce a standard call setup flow of SIP, because we need the standard flow for our, and to compare with the modifications.

2.1 Overview of VoIP

VoIP is a packet switching telecommunication technique, different from the traditional PSTN circuit switching network. The analog voice signal will be convert into digital datagram. And the packet will be transported by the IP network. And the receiver side will receive the data packet and roll back to the analog voice. The routing of the packet will depends on the router's decision, the voice packet maybe not arrive in order. The VoIP will need some mechanism to deal with these issues. Traditional PSTN will create a lease-line for one call, will cost more than VoIP. But the quality is stable and good.

The packet switching technique will bring up the reliability issues. Besides the low cost and many value-added services, the VoIP also bring up many problems. The unreliability transmission may lead to jitter, packet loss and delay. The NAT (Network Address Transfer) and emergency call will also be the problems that the service providers have to handle. So the quality and security are both very important.

2.2 VoIP Architecture

The traditional telephony network is PSTN (Public Switched Telephone Network) network. When someone makes a phone call will reserve a lease line for the communication. But circuit switching is costly, the VoIP provide a packet switching solution based on the current IP network. A call will be divided into two streams, one is the signaling stream for transmit the call setup command. And another one is the audio stream for the voice packet. The streams didn’t have the fix routing rules, so the packet will follow the normal IP network routing rule to the destination. The following figure is a simple VoIP network example. The signaling stream will carry the signaling protocols such as SIP, MGCP, MEGACO and H.323. And the audio stream will carry the voice data by Real-time Transport Protocol.

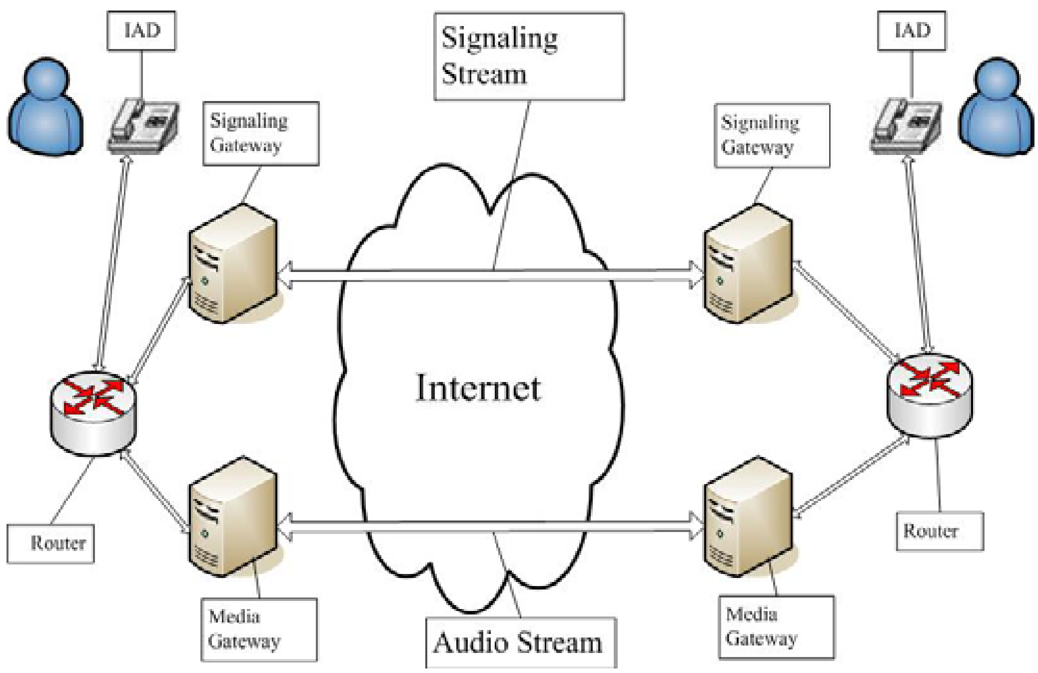


Figure 1. A Simple VoIP Network

The VoIP network can also connect to the current PSTN network. We just need a Signaling Gateway to convert the call processing signal into the SS7 signal. And also need a Media Gateway to convert the audio stream into the analog data, and send it to a Class 5 switch, and then new VoIP network and old PSTN network can connect together.

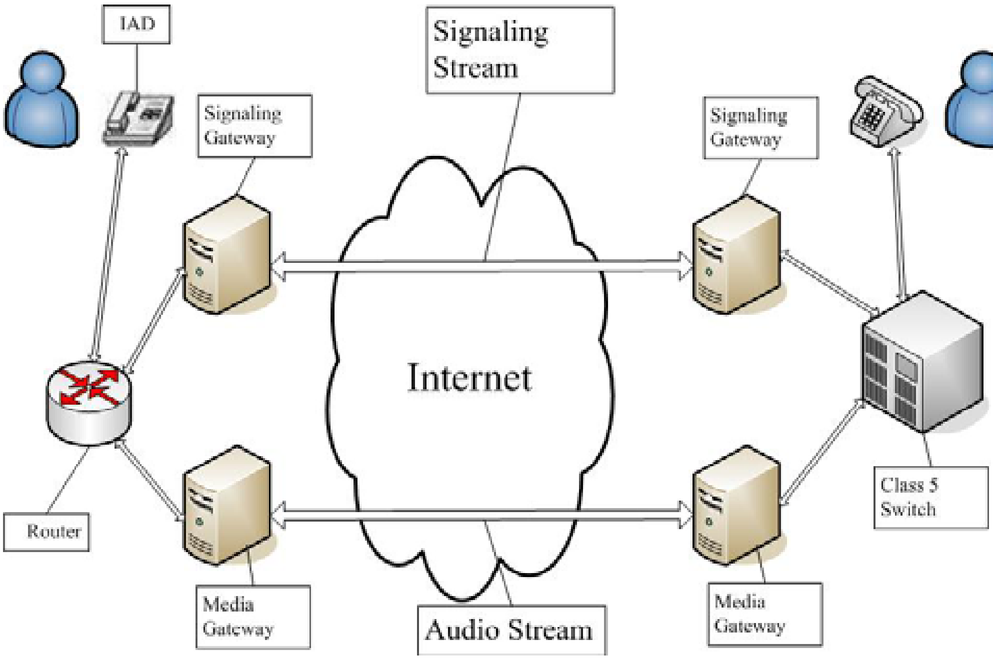


Figure 2. VoIP network with PSTN network

2.3 VoIP Protocols

The VoIP protocols support the functions of call setup, control message delivery, and resource allocation. So we'll introduce the various important VoIP protocols in the VoIP and their functions. All of them are the important elements to construct the VoIP network, and we have to familiar with these protocols.

2.3.1 SIP

The SIP (Session Initiation Protocol) is a VoIP signaling protocol. Designed for create Internet sessions for audio or multimedia data transmission. It was developed by Columbia University and University College London, and the latest version defines in the RFC 3261 from the IETF SIP working group. SIP controls the call setup progress in the VoIP; it can setup or tear down a call by SIP signaling, or even create a conference call party. SIP is a peer-to-peer protocol, different from MGCP and MEGACO. In VoIP, SIP works as a carrier of SDP to create the RTP stream to do the communication.

2.3.2 MGCP

MGCP (Media Gateway Control Protocol) is a signaling protocol within a VoIP system. The detailed definition of MGCP is defined in RFC 3435. And still many other RFC to describe the other details of MGCP. In MGCP architecture, there will be one Media Gateway to convert the audio to data packet, and a Signaling Gateway to create the connection of two end points. And the Call Agents is handled by the Media Gateway. MGCP messages are a series of commands that handles the call processing.

2.3.3 MEGACO

The MEGACO (Media Gateway Control Protocol) or H.248 protocol is also a VoIP signaling control protocol. The protocol was developed by both IETF and ITU, so the details of this protocol are defined in RFC 3525 of IETF and H.248-1 of ITU-T. The protocol provides the ability for the Media Gateway Controller to control the gateway to process the call processing. It contains the concept of context, and the command format is quite different from SIP and MGCP.

2.3.4 H.323

H.323 is created by the ITU-T for the multimedia transmission in LAN. And it is the first VoIP standard to serve the VoIP call processing. H.323 is not only used in VoIP, but also the IP based video conference, such as the NetMeeting. The H.323 call processing is defined in the ITU-T Q.931, and similar to the standard ISDN call setup. We will need to setup a H.323 Gatekeeper if we want to run the H.323 protocol in the VoIP network.

2.3.5 RTP

RTP (Real-time Transport Protocol) is a network transport protocol, developed by the Audio-Video Transport Working Group of IETF. RTP defines a standard datagram format of the audio and video. The RTP didn't define the specific port for the transmission, and can support both unicast and multicast transmission. Using RTP in VoIP is as a unicast streaming media transmission.

2.3.5 RTCP

RTCP (Real-time Transport Control Protocol) defines in RFC 3550. RTCP provides the out of band control of RTP media stream, but with no media payload on it. The main function of the RTCP is to provide the QoS (Quality of Service) information of the RTP stream. Such as the transmitted octets, received octets, packet loss, jitter. The RTCP packet will be periodically send out for the terminal to measure the quality of the conversation.

2.4 SIP standard call flow

We were taking SIP as a sample signaling protocol to discuss how to implement the VoIP interception. We'll introduce the SIP call processing flow in this section. The following tables are the descriptions of the SIP request commands. The command sequence will establish the call setup procedure.

SIP Request Command	Command Description
INVITE	To initial a call
BYE	To terminate a call
ACK	The acknowledge of a command
OPTIONS	Query some information
CANCEL	To cancel a request
REGISTER	To register location information

Table 1. SIP Request Commands

The response commands always carry an integer to indicate the status of the result. The following table is the roughly definitions of the different numbers. For example, the 100 is trying, 180 is ringing. 200 is means ok, and 202 is accepted.

SIP Response Command	Command Description
100 ~ 199	Information
200 ~ 299	OK
300 ~ 399	Redirection
400 ~ 499	Client Error
500 ~ 599	Server Error
600 ~ 699	Global Error

Table 2. SIP Response Commands

The following diagram is an example of a sample SIP call. User A wants to call User B. The call setup command will send to the proxy sever to process. And the location of user B will be resolved by a location server. The Proxy Server will redirect the invite command to the correct Proxy Server. The Proxy Server will send the command to the user B. After some call setup procedure, the VoIP call will be established between user A and user B.

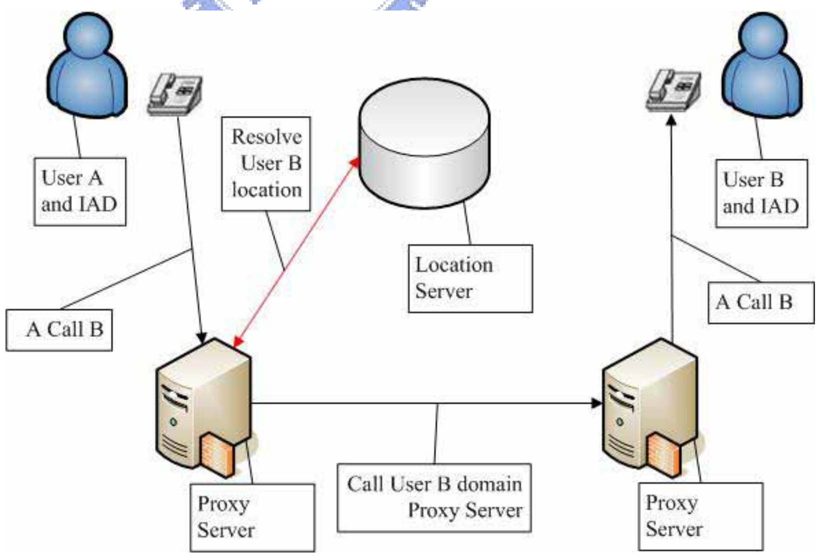


Figure 3. SIP VoIP network topology

The following diagram is a standard call setup flow of the SIP call, the black flow is the call setup from the user A, the red flow is the call terminate from user A. After the user A off hook the phone and dial a number. The IAD sends the invite command to the SIP Proxy. SIP

Proxy will try to route the message to the correct SIP Proxy, and transmit the invite command to the user B. When the user B answers this call, the IAD will send the OK acknowledgement back to the caller. After some call setup process, a RTP stream will be create to transmit the voice data between the users.

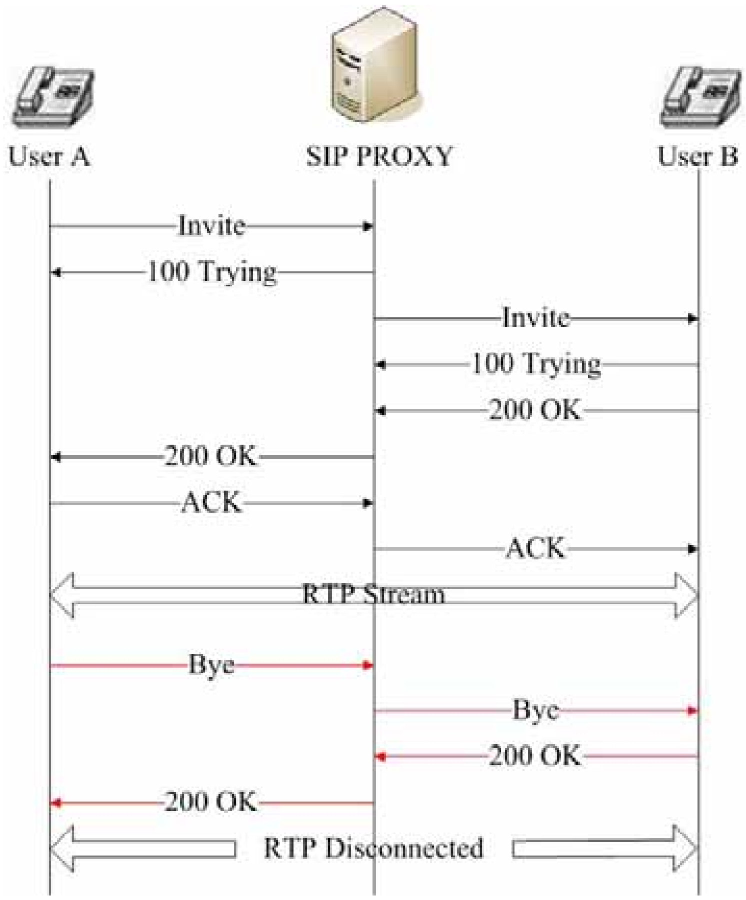


Figure 4. SIP call flow

Chapter3 Related Work

There are various VoIP study publications that focus on different points of view. We have to reference these studies to get the necessary information to attack the VoIP vulnerabilities. There are a lot VoIP vulnerability studies for us to reference. We'll use the vulnerabilities to do the interception in this thesis especially in the remote attack interception model. About the VoIP interception related studies also provide us many ideas about how to design a better mechanism to do the VoIP interception. And our target is to provide a better solution.

3.1 VoIP Security

The VoIP have various security issues. And also many studies in this domain. Within the different motivation and different target, they have different points of views in this subject. Some of them will analysis the issues, and some of them will discuss how to avoid them. The following is the keys of the related studies that we have referenced.

3.1.1 VoIP Security Analysis

To analysis the VoIP security issues, we can divide the issues into different classification to discuss. In "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems [1]" the authors provided a VoIP security matrix for our reference. All of the issues can be filled into the matrix. The issues could be happened in the Network Interface Layer, Network Layer, Transport Layer or Application Layer. And the vulnerabilities will affect three major areas as the following table. This thesis provides us an idea to classify our interception mechanism. Our interception mechanism will break the confidentiality by the vulnerabilities of different network layers. The following table is the VoIP vulnerabilities classification. Our study will break the confidentiality and integrity and to do the interception.

Vulnerabilities affect area	Description
Confidentiality	The information could not be reachable by illegal user
Integrity	The information could not be modified
Availability	The service could not be disturbed

Table 3. The VoIP Vulnerabilities Classification

The vulnerabilities affect four layers of the TCP/IP networking model. They are Network Interface Layer, Network Layer, Transport Layer and Application Layer. There are a lot of vulnerabilities in each layer. And the following tables are the sample VoIP vulnerabilities matrix in the paper:

Layer	Vulnerability	Description
Data Link	MAC Spoofing	Media Access Control (MAC) address spoof to impersonating the devices
Internet	IP Spoofing	IP address spoof to impersonating devices
Transport	TCP Interception	To sniff the TCP packet
Application	SIP Call Hijacking	To hijack a SIP call for the voice data

Table 4. Confidentiality VoIP vulnerabilities matrix

Layer	Vulnerability	Description
Data Link	ARP Spoofing	ARP spoofing will corrupt the ARP data
Internet	IP Spoofing	Integrity can be compromised at the network layer by an IP address spoof
Transport	TCP Interception	To sniff the TCP packet and to modify it
Application	RTP Inserting	To insert the Voice data to the RTP stream

Table 5. Integrity VoIP vulnerabilities matrix

Layer	Vulnerability	Description
Data Link	ARP Spoofing	Update the wrong ARP data to ARP table to make the wrong routing
Internet	IP Spoofing	Use wrong IP address to cause the wrong routing
Transport	TCP Flooding	To create many TCP connection to hold the server processing resource.
Application	SIP Call Redirect	Use the “BYE” or “REFER” command to terminate a call illegally

Table 6. Availability VoIP vulnerabilities matrix

“Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors [2]” describes the security issues. Also provide us many useful recommendations for construct the VoIP network. Critical Infrastructure is a term that used by governments. It describes the essential for the functioning of a society and economy. And Critical Infrastructure includes food, water, telecommunication, energy, and transportation. The following table is the summary of threats:

Threats	Description
Protocol Attacks	Most of the VoIP have their own vulnerabilities.
Application Attacks	Java applets might be running on IP phones for supplementary services. Could be hacked.
OS Vulnerability	The overflow might create a backdoor for the hacker to gain full control.
Spoofing on Different Layers	Spoofing can occur on different layers, the complicate identity will increase loading.
Unauthorized Component or User Introduction	Authorization determines what actions can be undertaken with various users.
Unauthorized Access to System Data	The system data, such as configuration files and administrative data should be protected from attackers.
Eavesdropping and Sniffing on Conversations	VoIP can open the doors for eavesdropping or sniffing on both signaling and voice.
Man-in-the-Middle	The rogue proxy could collect the confidential information.
DoS (Denial of Service)	DoS attack to a proxy server could lead to loss the availability of service.
Theft of Service	The ability to make VoIP calls for nefarious purpose.

Table 7. VoIP Security Threats

And all of the vulnerabilities could be address to six security measures. They are Identification and Authentication, Authorization, Confidentiality and Integrity, Access Control, Availability and Security Management. The recommendations remind us the VoIP service providers have to create a secured network, and also care about the compatibility and scalability. In our thesis we will use the Protocol Attacks, Application Attacks and Spoofing on Different Layers to do the interception.

3.1.2 VoIP Security Issues

The signaling protocol is also unsafe in VoIP network. We use SIP as the target signaling protocol in this thesis. A simple spoofed BYE command can easily terminate a call illegally. "A new authentication Mechanism and Key agreement protocol for Sip Using [3]" proposes an identity based cryptography to solve the authentication and key agreement issue in SIP. The Cisco also have the white paper "Security in SIP Based Network [4]" to suggest the user to secure their VoIP network.

The authentication, IPSec and firewall are your countermeasures. "Convert channel for improving VoIP security [5]" provide you a solution to hide the information in your packet in VoIP network. All of these studies are discuss about the SIP protocol securities. We'll also attack the SIP protocol using spoofed SIP redirect command or some other SIP protocol attacks referenced to these studies.

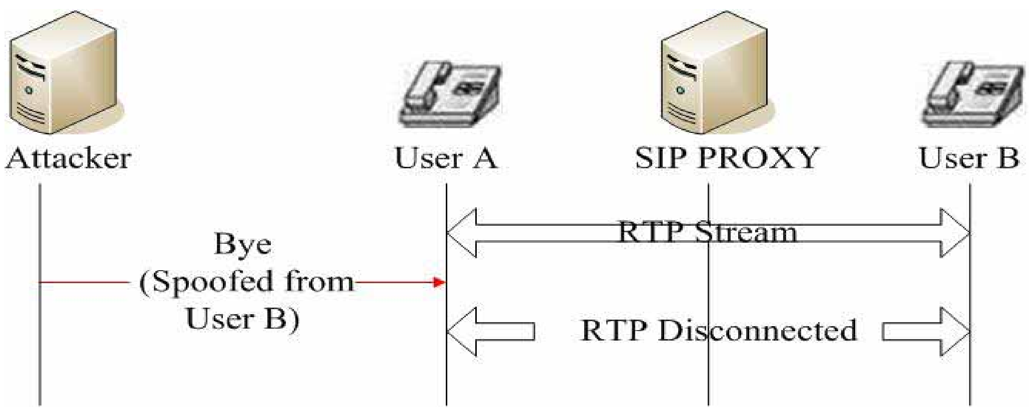


Figure 5. The VoIP attack spoofed "Bye" flow

RTP is an application level protocol to carry audio or video data. In “Real-time Transport Protocol (RTP) Security [6]” discussed the RTP serious confidentiality, integrity and authentication issues. But all of the security features must concern about the performance issue. The complex mechanism may bring up the unacceptable delay and jitter, also serious damage the voice quality. “Study on SRTP and Design Key Exchange for Secure VoIP [7]” discussed how to protect your privacy by Secured RTP. Also provide the measurement the latency of SRTP mechanism. We have been challenged that all of the interception will be useless if the end user uses the SRTP to do protection. Cryptography is not the target of our study. We’ll focus on the interception in the aspects of protocols, networks and telecomm. We do not talk about the cryptography. Our target is to collection the conversation data in the RTP flow. And if the recorded payload is encrypted, government can to use the super computer to do the decrypt.

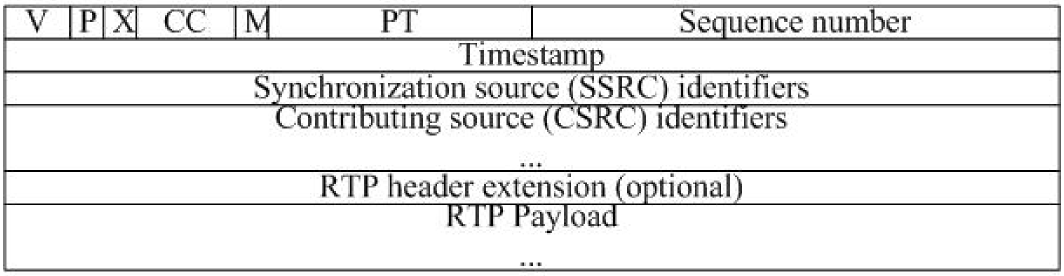


Figure 6. The RTP Content

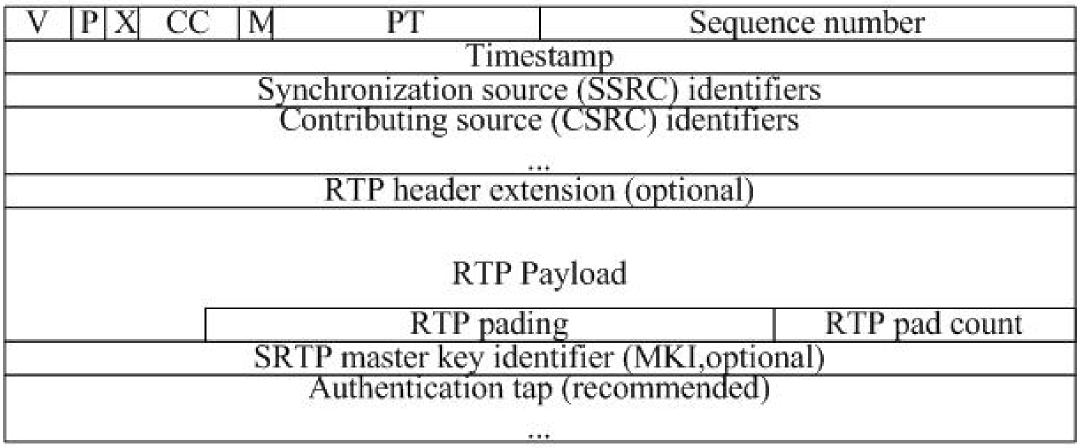


Figure 7. The SRTP Content

"VoIP security in Small Business [8]" reviews several kinds of the VoIP security issues. Not only the vulnerabilities had we discussed before. The infrastructure could be the root cause of the risks. When your data package is traveling through the Internet, it is exposed itself to be an attackable target. The end user will also be the target of denial of service, flooding, eavesdropping and impersonation. The hacker might takeover the control of your computer by the operation system overflow bug. Human vulnerabilities are also a problem. Easy to use and security always be a trade off, and most of the network management engineer will choose the easy one. And we would like to provide a software based VoIP interception without changing the infrastructure. So this thesis provides us the information of infrastructure and management vulnerabilities to do the interception.

3.2 VoIP Interception

A flexible and powerful software based VoIP interception system is the target of this thesis. To reference the VoIP interception related studies is also very important. The released reference materials are not as many as the study of VoIP security issues, but it is still some information for us to reference.

3.2.1 VoIP Interception Model

"Distributed System for Lawful Interception in VOIP network [9]" provide the concept of construct interception architecture. VoIP interception architecture was separate to 4 parts in this thesis: Top-Level Device (TLD), Intermediate-Level Device (ILD), Bottom- Level Device (BLD) and Storage Device (SD). And there are two kinds of interception information in this architecture. The wiretap information is a set of VoIP endpoints that we want to do the interception. The wiretap data includes the time of the call, address of endpoints participating in a call and recorded content of a call. All of the information exchange by using a Wiretap Information Exchange Protocol (WIEP). WIEP defines the communication procedures for the proposed system. And use XML based language to exchange the information. The system also uses authentication and IPSec to protect the information. "Methods for Lawful interception in IP telephony networks based on H.323" is the same writer but focus on the H.323 protocol architecture. The following diagram is a prototype of this system. The Wiretap Controller works as TLD, and implemented as a stand-alone program that can run on PC. The Gatekeeper Wiretap Device works as ILD, and implemented as a software module and incorporated into the OpenH323 Gatekeeper software. The Promiscuous Wiretap Device works as BLD, and implemented as a standalone program. And set the NIC (Network Interface Card) to the promiscuous mode. Intercept the content of the calls and in-band signaling. Reference to this architecture, we'll also provide a distributed environment for the interception.

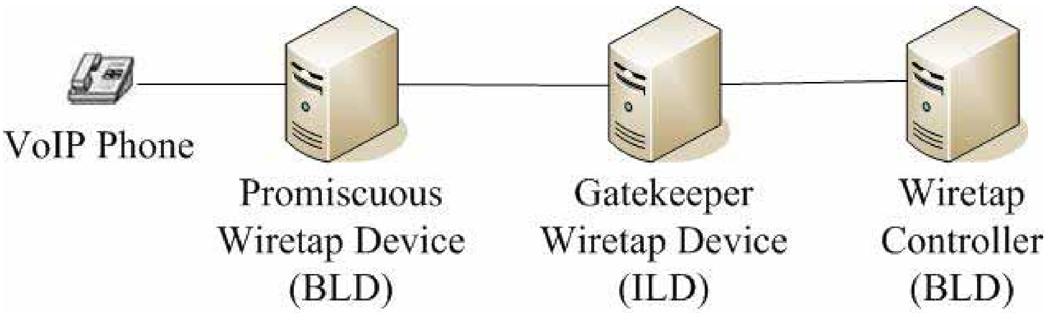


Figure 8. Distributed System for Lawful Interception Diagram

"Legal Call Interception in Next Generation Networks [10]" breaks the electronic surveillance into three categories: communication contents, call identifying information and the store of the transaction records. Only less equipment assist the service provider becoming CALEA (Communication Assistance for Law Enhancement Act) compliant right now. So the thesis also provides the following two solutions for this issue. The MSM (Multi-Service Mediator) can analysis the call information and redirect the data to a lawful interception server. The network architecture could be centralized or distributed. The centralized system will do the interception by a single MSM. And pass the messages to the lawful interception Server. In the distributed MSM environment, each MSM could transmit the interception information to the interception server independently. Our system architecture will similar to the centralized MSM system. We just want to intercept the specific user. Not to monitor all of the users in the network.

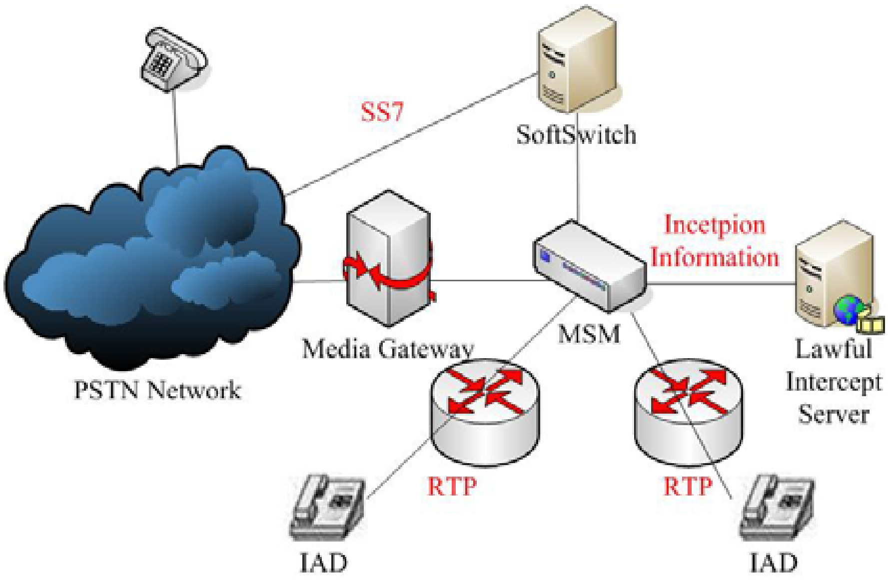


Figure 9. The central MSM system

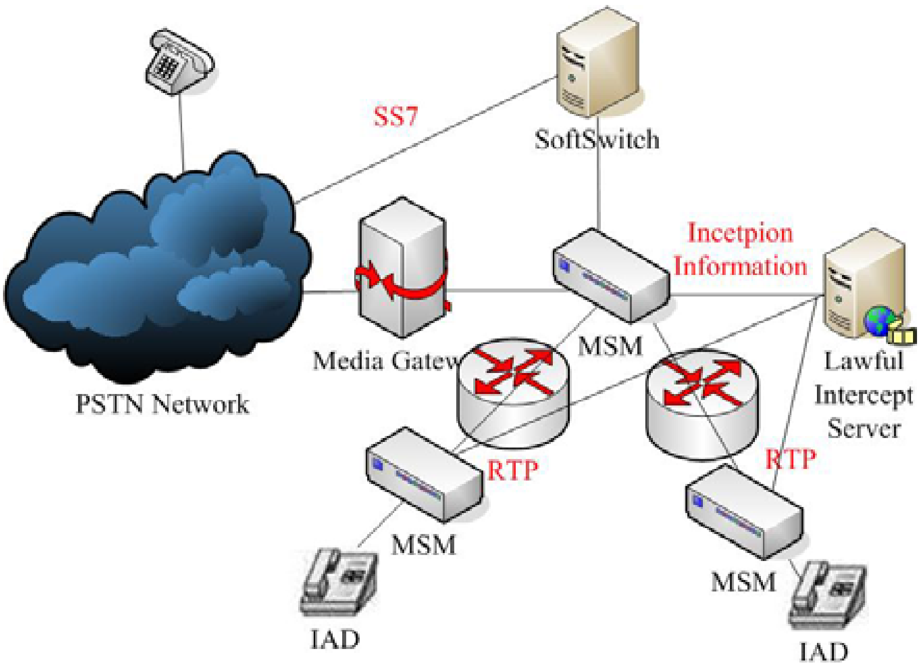


Figure 10. The distributed MSM system

"A Brief Overview of VoIP Security [11]" mentioned many free network analyzers, sniffers and packet capture tools. We can convert the VoIP traffic into wave files. "VOIP HACK: Tips & Tools for Internet Telephony [12]" also introduced some existing program for the VoIP call interception. We can use tcpdump and Vomit (Voice over Misconfigured Internet Telephones) to achieve this goal. We can also use the Cain & Abel to sniff a SIP call. Cain & Abel can corrupt the MAC table to get traffic of other machine. These studies provide us some toolsets for the VoIP network attack and inspection. We'll setup the toolsets and use it to attack the VoIP network, and analysis the behavior. Reference to the behaviors can help us to develop our system.

"HACKING EXPOSED VoIP [13]" is the most important reference book for us. It not only introduced varies skills to break the VoIP network, but also defines various architectures for the VoIP interception. We'll implement some interception models into our system with our own mechanism. The following is the description of the concepts.

The first one is the SIP Proxy Attached. It is running a program in SIP proxy, and the program will trace the signaling and redirect the call. To achieve this goal we can use register hijacking tool to highjack the registration for a key SIP phone user and redirect the phone. The following figure is the topology.

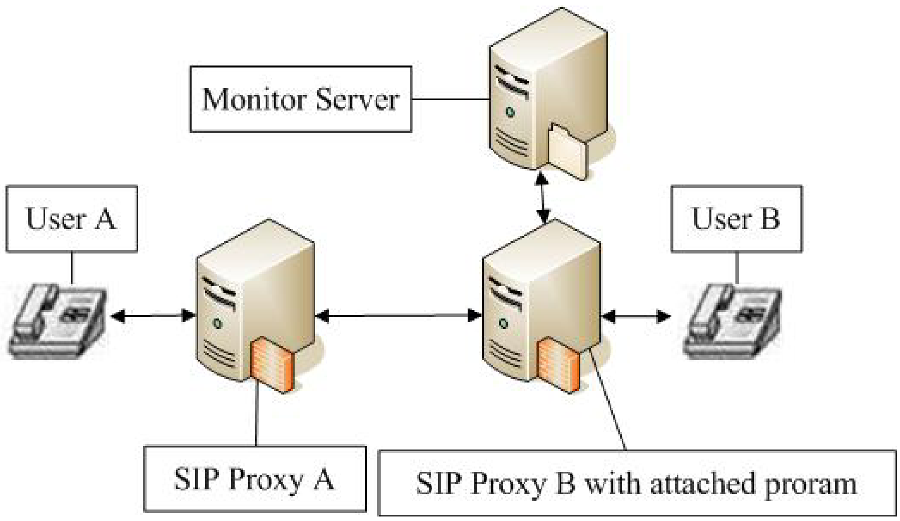


Figure 11. The SIP Proxy Attached Interception

The second architecture is the Rouge Back to Back User Agent. Rogue SIP Back to Back User Agent could be a user agent or a SIP phone. It can be located between SIP proxy and a SIP phone or two SIP phones. The following is the topology.

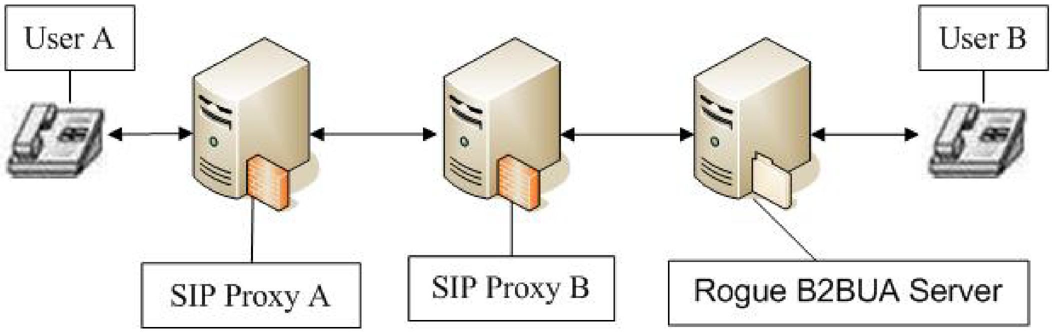


Figure 12. The Rouge Back to Back User Agent Interception

The final architecture is Rogue SIP Proxy. It acts like a SIP proxy. The fake proxy just does the transparent the information and the steal the necessary information. It can be located between SIP proxy and a SIP phone or two SIP phones. The following is the topology.

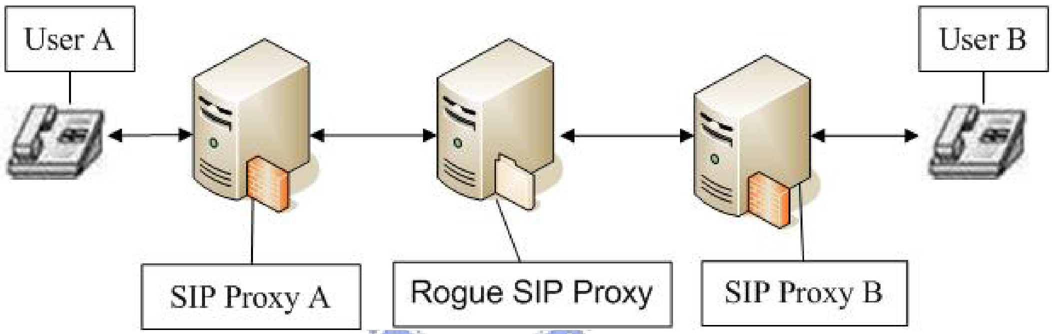


Figure 13. The Rogue SIP Proxy Interception

3.2.2 The VOIP Interception solutions of each vendor

VoIP Interception is a basic requirement of the VoIP network. Government will ask the vendors to provide the solution of this function. So each vendor has their own solutions. Most of the solutions will require the infrastructure change, so government has to buy additional equipments to achieve this goal. The following table is the list of the VOIP interception solutions of each vendor and the patent number and project name. To reference these solutions of the venders is very important, because they have a strict process to release their patents. But most of them will add more equipment in the architecture. So we'll achieve this goal without any new equipment besides the interception server.

Company	Project	Patent
NORTEL	**Method and system for lawful interception of packet switched network services**	**US2004/0255126[14]**
NOKIA	**Method and system allowing lawful interception of connections such a voice-over-internet protocol calls**	**US2004/0157629[15]**
ALCATEL	**Lawful interception gateway**	**US2005/0094651[16]**
Cisco	**Intercepting a communication session in a telecommunication network**	**US2006/0245595[17]**
SIEMENS	**Subscriber status determination and call content interception**	**US2007/0041558[18]**

Table 8. The VOIP interception solutions of each vendor

All of the listed service providers are powerful venders, and can push their solution hardly. Even it the network infrastructure should be changed. But we didn't know the interoperability of each solution, because there might be some conflicts of each solution. And most of the solutions contain a complex call flow or many additional servers in the networks to intercept the messages. Compare to our target, our solution is to keep the original network architecture. Keep the original call flow, and uses software based tools to do the interception. Keep the original architecture of the IP telephony, and try to provide more flexibility for the users. And the software based tool set can also cost down to do the interception. That's the differences between the patents.

Chapter 4 The FIVE System

This chapter is the description of the FIVE system implementation details. We'll introduce the design guideline and the system structure. And also introduce the libraries that we used for network programming. All of the algorithms will be implemented in this system and do the validation. The FIVE system means "Flexible Interception in VoIP Environment". We provide the flexible interception mechanisms to do the lawful VoIP interception. And there will be five different interception models to be described in this chapter. And the software based system will reduce the cost of interception equipment, but still provide the reliable interception quality.

4.1 System Overview

The target of the system is to do the analysis of the VoIP calls and do the interception. We can divide the FIVE system into three functional blocks. And in this section we will describe the design concept. Reference to the following topology that we discussed previous chapter, the red cycles is the access point to do the interception and we provide five different models for the interception.

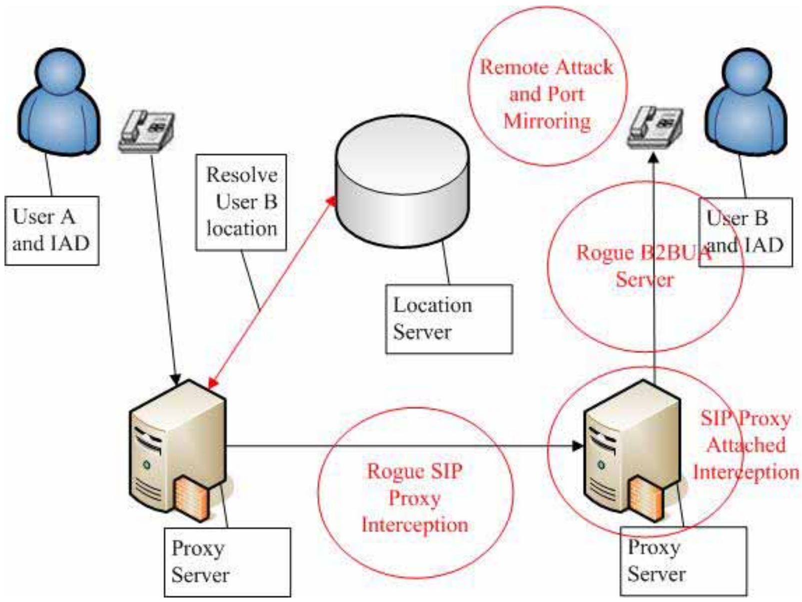


Figure 14. Five System Interception Points

4.1.1 The System Architecture

The target of the thesis is to create a software based VoIP call interception system. We have designed some algorithms and state machines for different interception models. In FIVE system, there will be three major modules in this system. The following is the block diagram of our system. The decision center is the core to do the analysis and make the decision. The packet capture module is the network traffic access module. And the restore to disk module is to save the information to the storage.

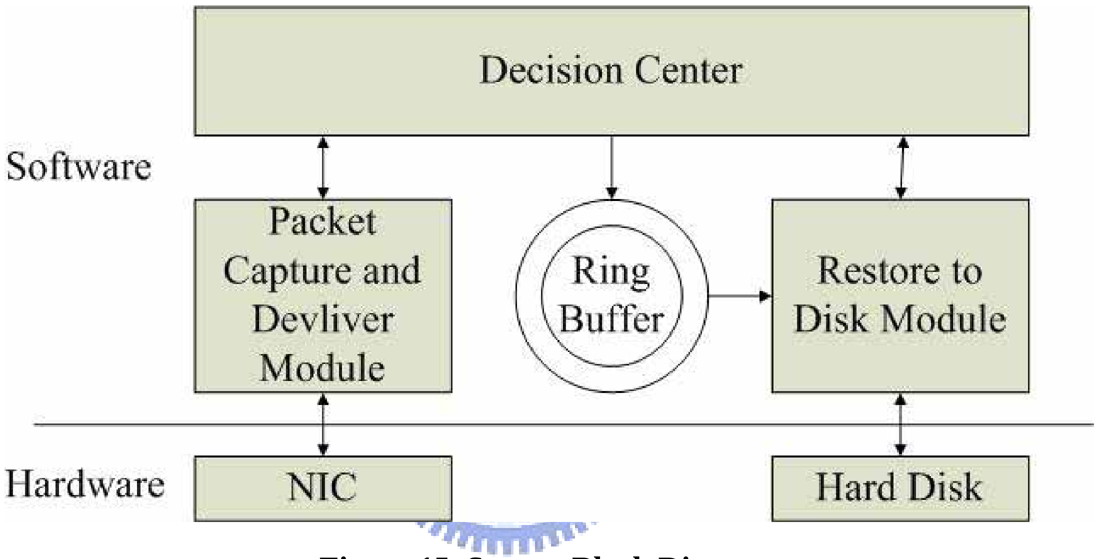


Figure 15. System Block Diagram

The three capabilities is the capability to send and receive a packet, the capability to restore the data to storage and the capability to analysis the packet, and do the reaction. The normal interception procedure is as followed. The packet capture module will keep polling the packet from the network, and send it to the decision center. The decision center will analysis the packet and decides what to do. The decision center will send out a packet to trigger some event or to send the original packet to ring buffer. The restore module will write the RTP payload into the hard disk.

The decision center has different state machines to do the analysis and make the decision. This module will do the protocol analysis and decision making. For performance concern, we would create two tasks to maintain the packet polling and data restore to the hard disk. And the data will pass by a public ring buffer. A public ring buffer is declared by the CRingBuffer data structure. The ring buffer is used to restore the RTP packet payload. And another task will get the raw data and save it to the disk as a media format file. And the save to disk is using normal file I/O function call.

4.1.2 The Programming Environment

We use the Microsoft Visual C++ for the programming environment. It is an integrated development environment (IDE) product provided by Microsoft. The followings are the reason that we choose it for the environment. First is it provides a feasible and powerful environment to implement a system with GUI. It provides many general and reusable modules. The second reason is the WinPCAP provides great library to support the network package processing ability. And last reason is that in the new embedded system like WINCE will support .Net framework program. So we will have the chance to put our FIVE system into some portable devices with the WINCE or Windows Mobile OS. The follow diagram is our develop environment.

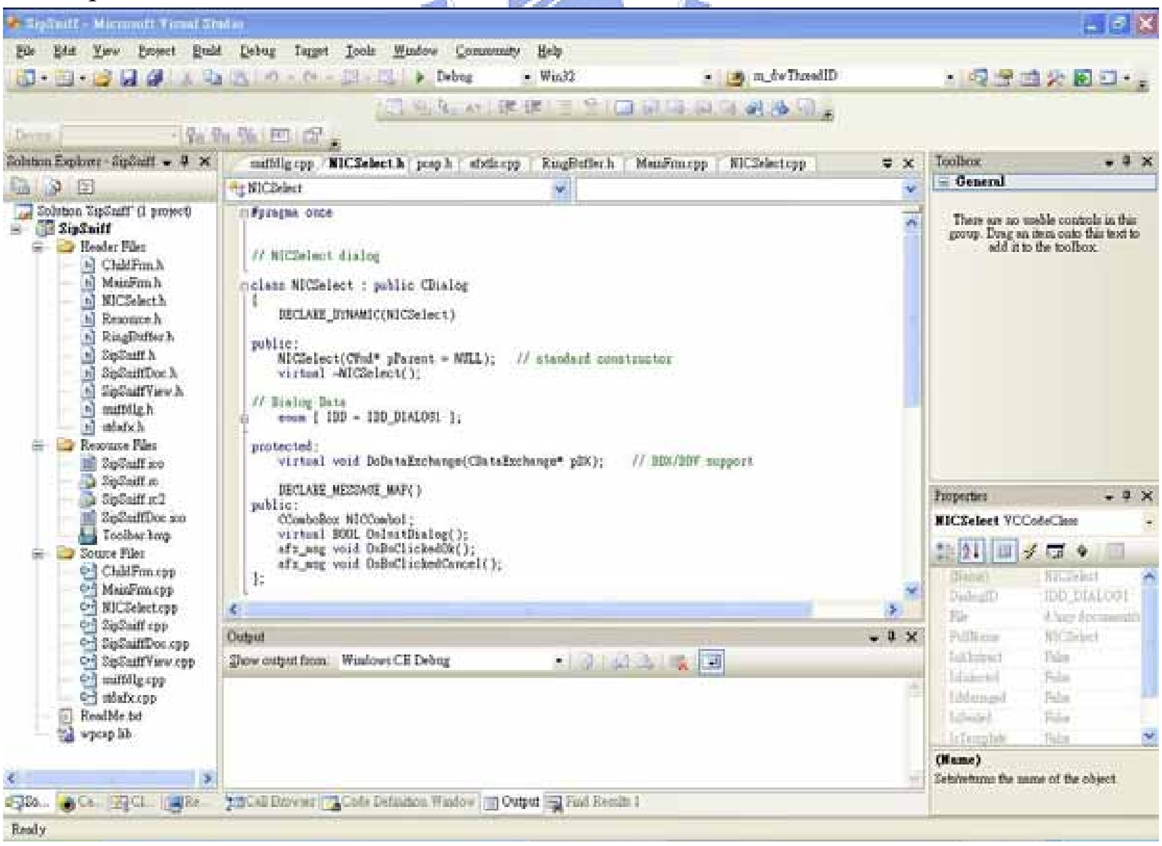


Figure 16. The Microsoft Visual C++ Environment

4.1.3 The Windows Packet Capture Library

The network packet capture function is very common. Most of the programmers will create a raw socket to sniff the packet. And also use the socket to send the packet. This is base on the Winsock2 library. But Winsock2 can only support the function above the IP layer. We need the MAC layer information, so we choose another solution. WinPCAP, the Windows Packet Capture Library is our solution. It allows the network programmer to access the MAC layer information, and create more flexibility for the network programming. The following diagram is the compare of the two architectures:

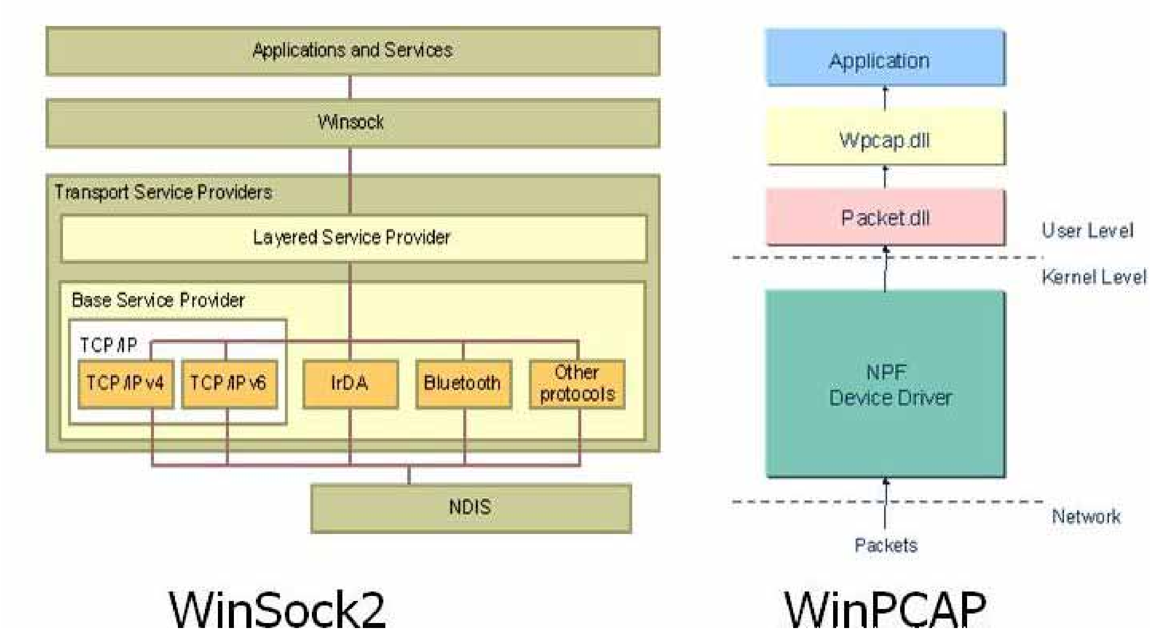


Figure 17. The WinSock2 and WinPCAP architecture

To use the WinPCAP library in Visual C++ programming is also very easy, the programmer just have to include the PCAP library and then to use the library. The WinPCAP provides us the ability to capture the more details about a network packet, and most important of all is that we can change the source and destination IP and MAC to any value we want. The wireshark also use the PCAP library to do the packet capture.

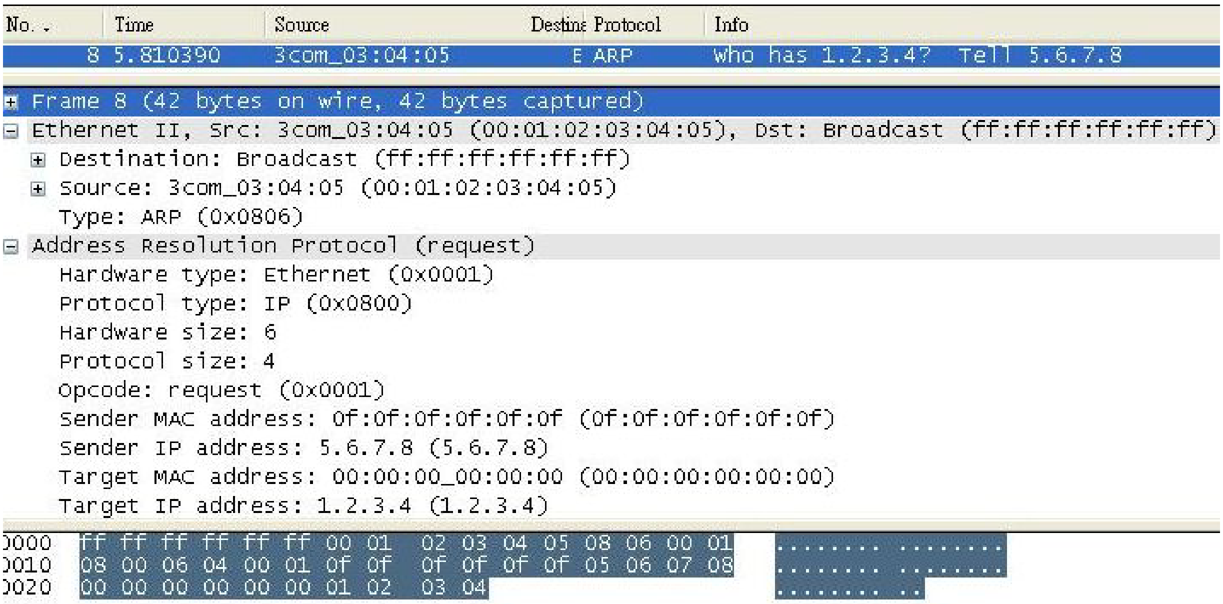


Figure 18. Wireshark Packet Capture Window

In the wireshark log we can see that, it is a spoofed ARP request packet creates by our system. The values of the IP and MAC address could be modify by us instead of real MAC address of our NIC. So we can use the fake ARP or IP packet to corrupt the target machine to control the routing of the packet.

4.1.4 The Packet Process Mechanism

For the flexible interception, we need to do some modification of the network packet that we have captured. And redirect it to the target machine that we want. We can also modify the register content. We will create a thread to keep polling the network packets and receive all of it to do the processing. After received a packet, FIVE system will parse the packet content, and following the interception state machine to decide the reaction of our FIVE system. Sometimes we have to redirect the packet, or modify the SIP content. After the modification, we still need to correct the IP and UDP checksum. Or the packet will be dropped because of the incorrect checksum. We can take the following Packet Processing Mechanism diagram as example. The FIVE System State Machine will check the content of the packet and make the decision following the state machine. And if the packet is the RTP packet that we want to restore, it will be place into the ring buffer for another thread to handle.

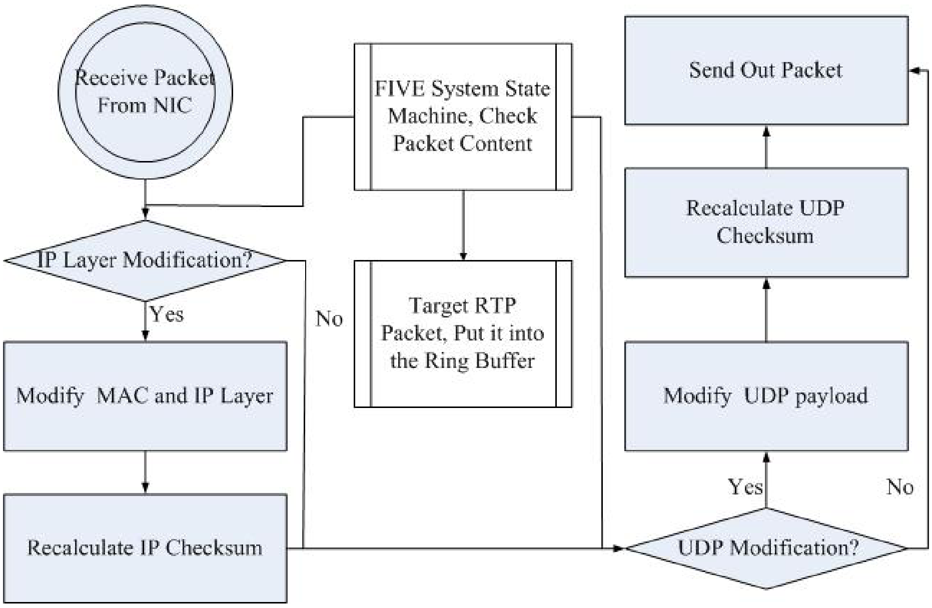


Figure 19. FIVE System Packet Processing Mechanism diagram

4.1.5 The Packet Restore Mechanism

Reference to previous section, the binary raw data of the RTP packet will be put into a ring buffer. At the same time, we use a stack to maintain the packet length information. Every time when we put a packet into the ring buffer, we will also push the length of the packet into the stack. We will create a new thread to write the ring buffer content into the file system as a file. The following diagram is the flow chart of this thread. The thread will push 0 to stack for initial the stack, and do the pop from stack periodically to see if any data needs to write into the file system.

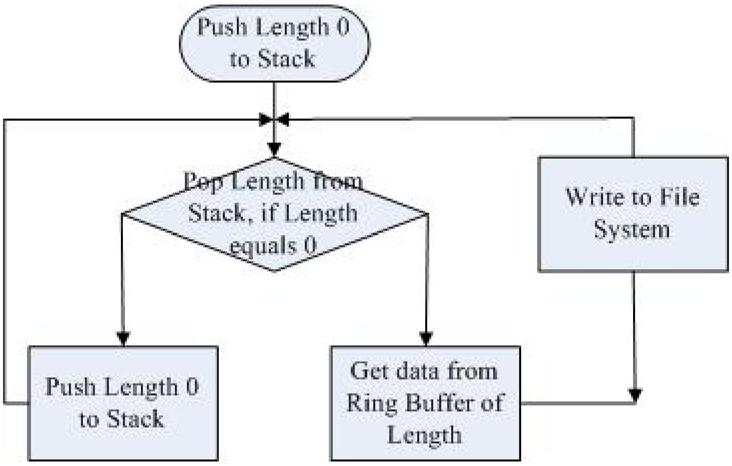


Figure 20. FIVE System Packet Restore Mechanism

4.2 FIVE System Interception Mechanisms

The different interception model is with different intercept mechanism. This section will discuss the mechanisms. The mechanisms will analysis the SIP protocol flow and do the interception. Then we'll maintain different state machine for each different model and to perform the interception.

4.2.1 The Rouge Back to Back User Agent Interception

The system can be configured as different modes to support different interception models. The first model is the Rogue B2BUA Server. The system is running as a SIP proxy server and also a SIP proxy. And the User will be register to the rogue server as the SIP proxy. The B2BUA server will register to the real SIP proxy. The following is the diagram of this model:

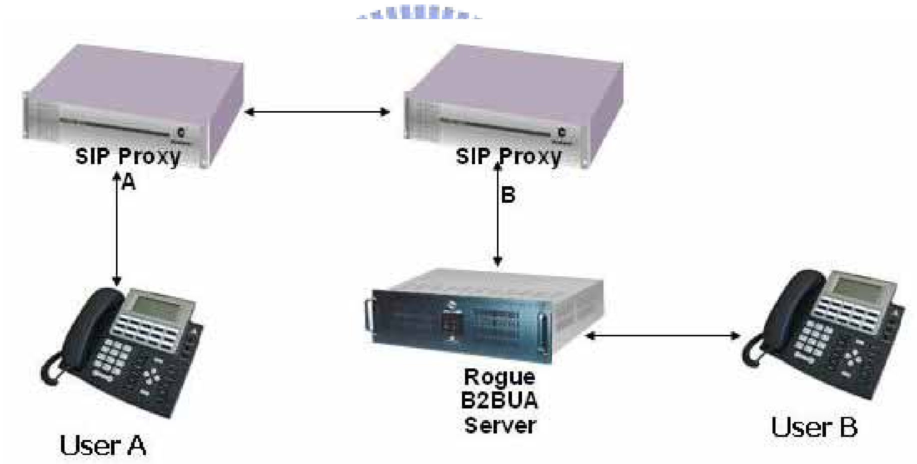


Figure 21. The Rogue B2BUA Server Model

The Rogue B2BUA server is to spoof a proxy server and make the target VoIP phone to register to this server. The following is the flow chart of incoming call and outgoing call interception. In the diagram, the USER B is the target to be intercepted. All of the signaling command to the User B or from the User B will pass through the Rogue B2BUA server. So the Rogue B2BUA server could easily detect the VoIP call and redirect the call by modifies the SDP protocol content.

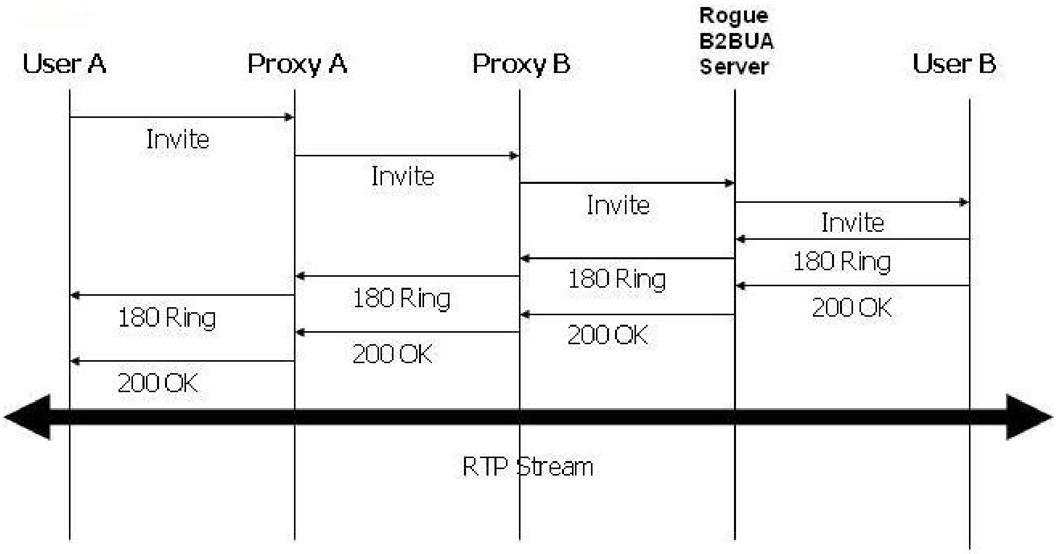


Figure 22. The Rogue B2BUA Server Incoming Call Interception flow

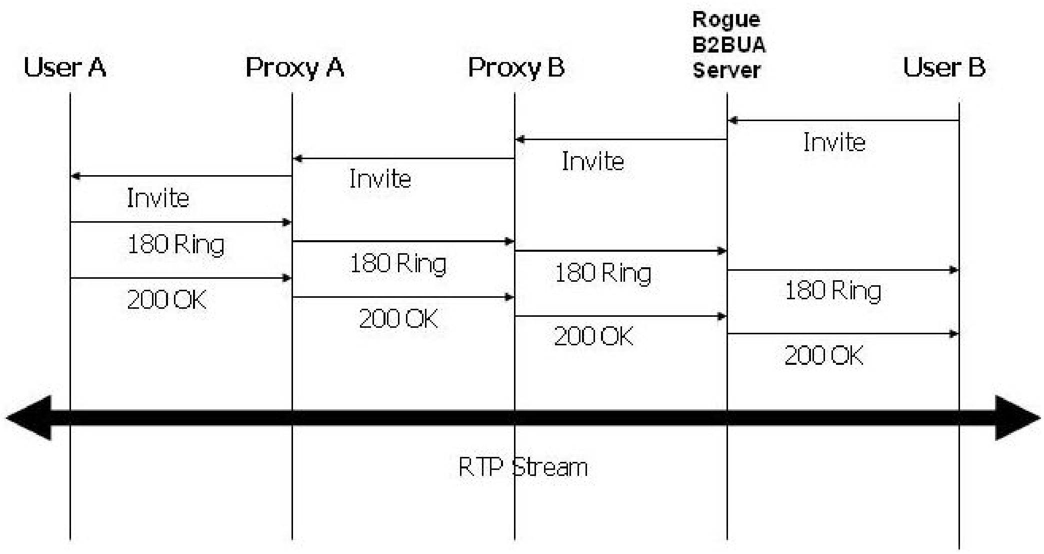


Figure 23. The Rogue B2BUA Server Outgoing Call Interception flow

To achieve this goal, the end user should register to a fake SIP proxy spoofed by our system. The following is the SIP register procedure of the Rouge B2BUA Server architecture system. The end user will send the register command to our Rogue B2BUA Server, and we will modify the register command content to make our Rogue B2BUA Server just like IAD to register to the real SIP proxy. In the SIP proxy point of view, the Rogue B2BUA Server is a IAD, and in the end user point of view, the Rogue B2BUA Server is the SIP proxy. Our Rogue B2BUA server will be the bridge to forward and modify the content of message.

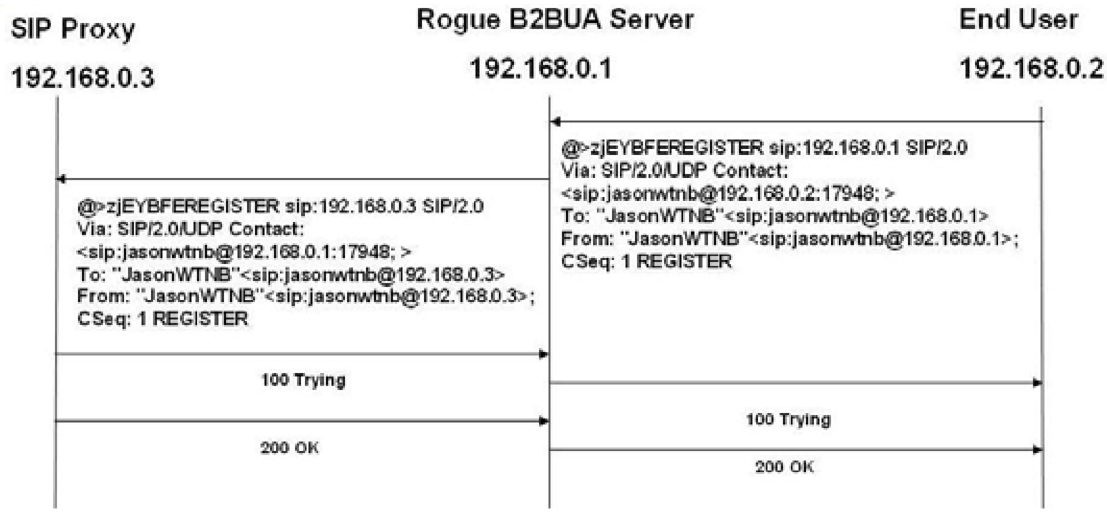


Figure 24. The Rogue B2BUA Server Register flow

And then we can forward the conversation of the end user to our server by modify the SDP information.. The following is the flow of the SDP modification. The SIP call will separate the signaling and voice flow, so we need to redirect the RTP packet to our interception server. The Rouge B2BUA Server will forward it to the end user.

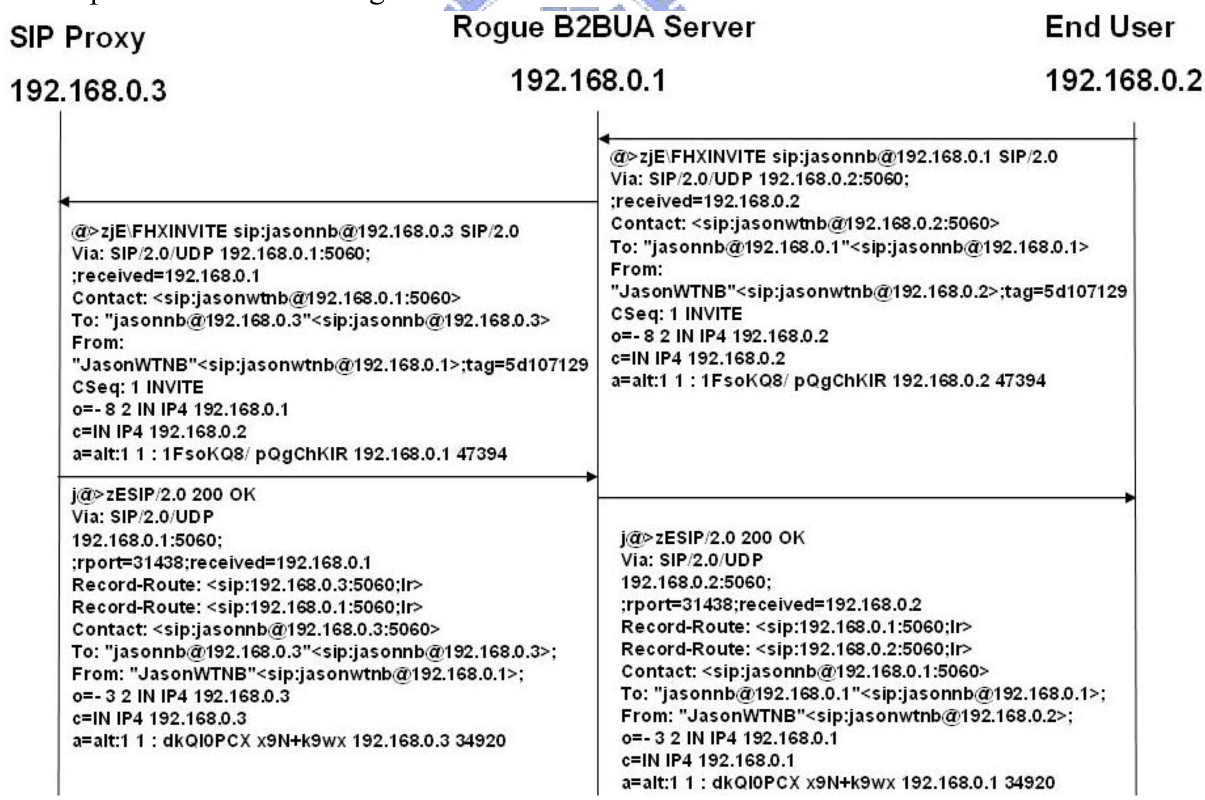


Figure 25. The Rogue B2BUA Server SDP exchange flow

After the modification of the SDP information, all of the RTP will be forward to our Rogue B2BUA Server. And both of the SIP proxy and the end user won't aware they are being intercepted.

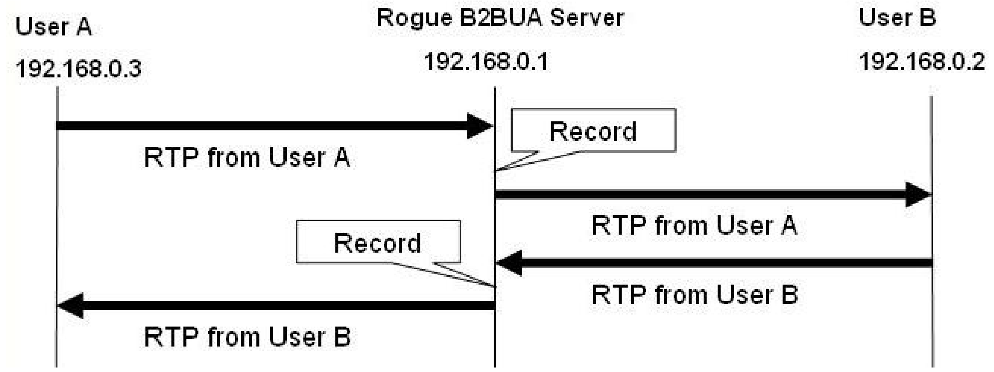


Figure 26. The Rogue B2BUA Server Interception RTP flow

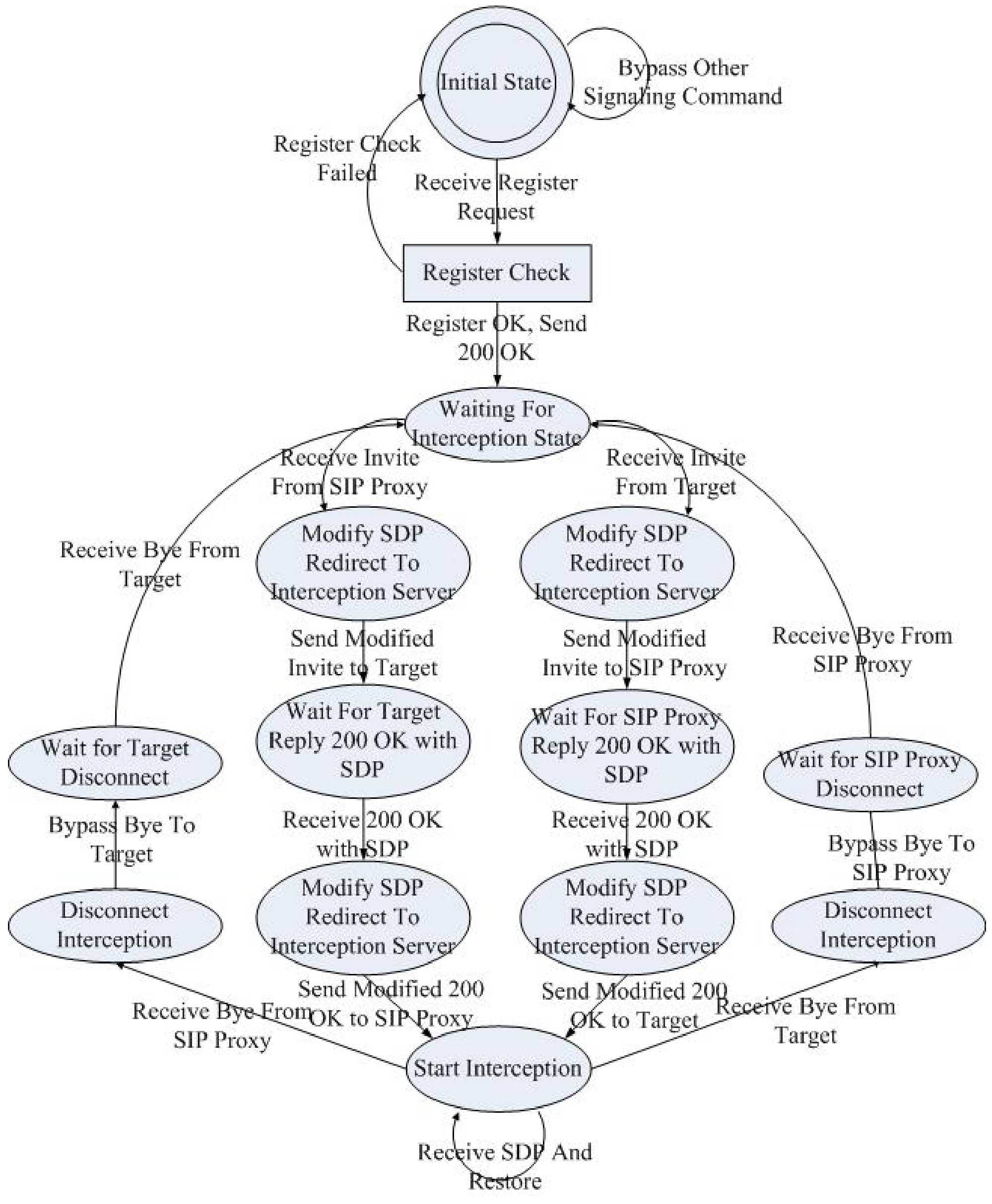


Figure 27. The Rogue B2BUA Server Interception State Machine

The state machine reflects the reaction of the FIVE system in the Rogue B2BUA Server Interception. The upper part of the state machine is the register control. The incoming and outgoing call will have different procedure to do the interception. The key point of the Rogue Server Interception is to redirect the traffic to the Interception Server by modify the content of SDP.

4.2.2 The Rouge SIP Proxy Interception

The second model is the Rogue SIP Proxy mode. The rogue SIP proxy will acts as a normal SIP proxy. The SIP signaling protocol will be exchanged between SIP proxies. The rogue SIP proxy will intercept or modify the message to perform the interception. The following is the diagram of this model:

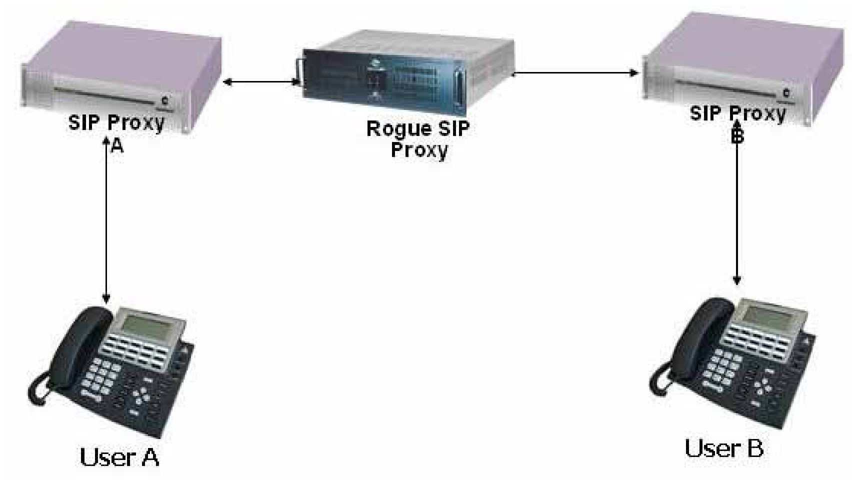


Figure 28. The Rogue SIP Server Model

In the SIP VoIP network, the signaling will pass by the SIP proxy servers. The User B is the target that to be intercepted. In this topology, the Rogue SIP Proxy will play like a normal SIP proxy. But also collect the necessary information or to modify the signaling content to redirect the call information. So the best position of the Rogue SIP Proxy is the next hop of the Proxy B. Because we won’t loss any calls between these two proxies. The following diagrams are the incoming call and outgoing call flow.

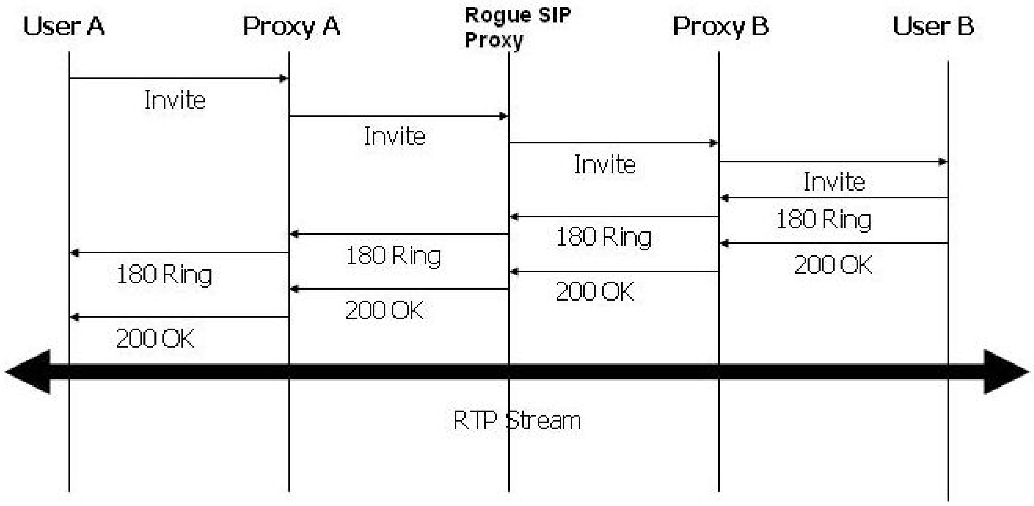


Figure 29. The Rogue SIP Server Incoming Call Interception flow

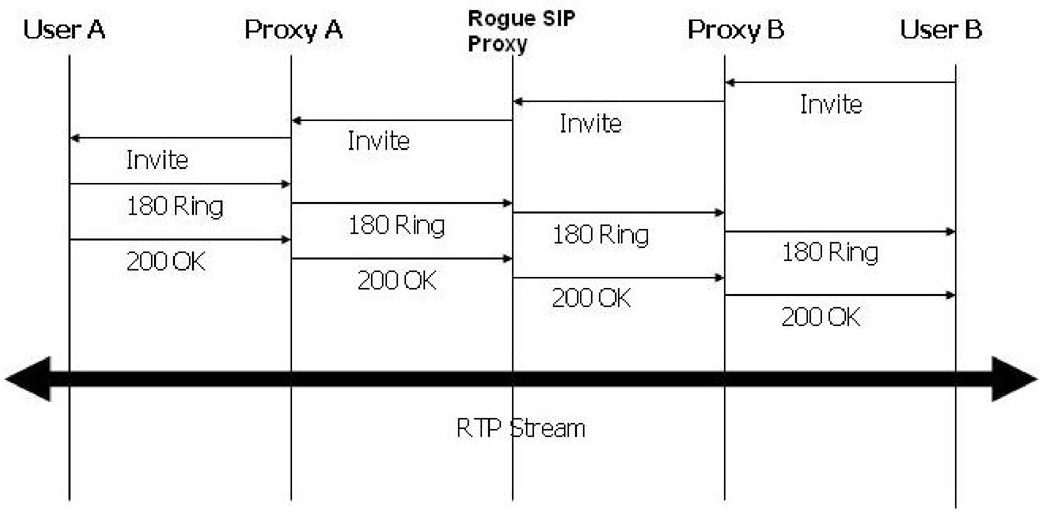


Figure 30. The Rogue SIP Server Outgoing Call Interception flow

The Rogue SIP Server interception has different procedure with the Rogue B2BUA Server. Rogue SIP Server is an SIP proxy that the target user not registers to. So we didn't need to modify the SIP register procedure. But we still need to modify the SDP content to forward the RTP flow to our interception server to record. The following diagram is the SDP modification of the intercepted call.

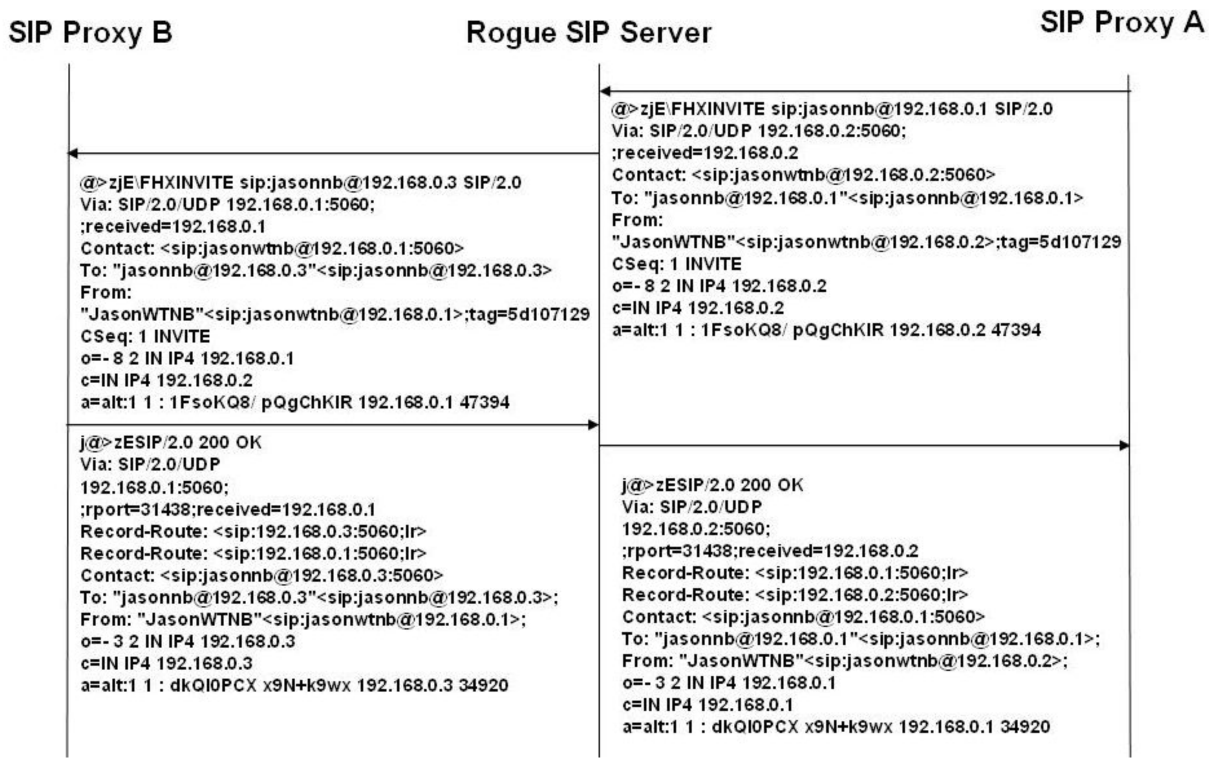


Figure 31. The Rogue SIP Server SDP exchange flow

Because of the SDP information is modified, all of the RTP flow will be redirect to the Rogue SIP Server and being recorded. And in the following diagram we will see that the call was redirected to the interception server.

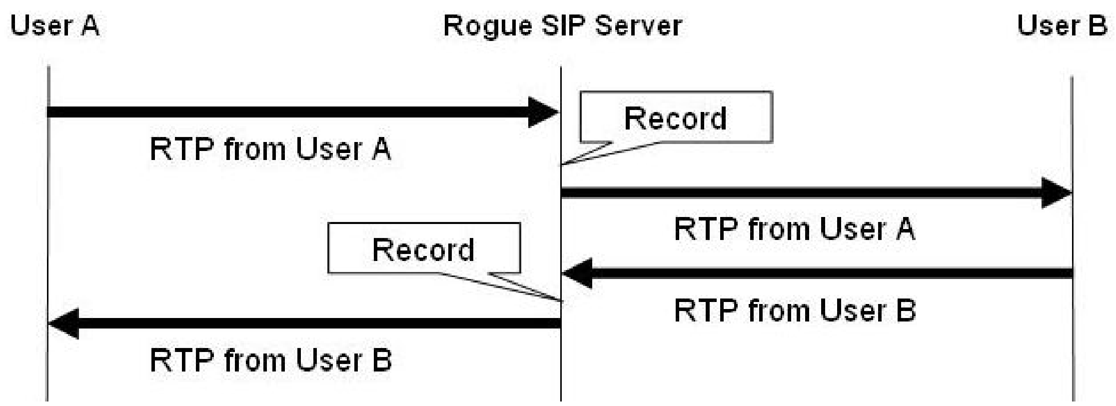


Figure 32. The Rogue SIP Server Outgoing Call Interception flow

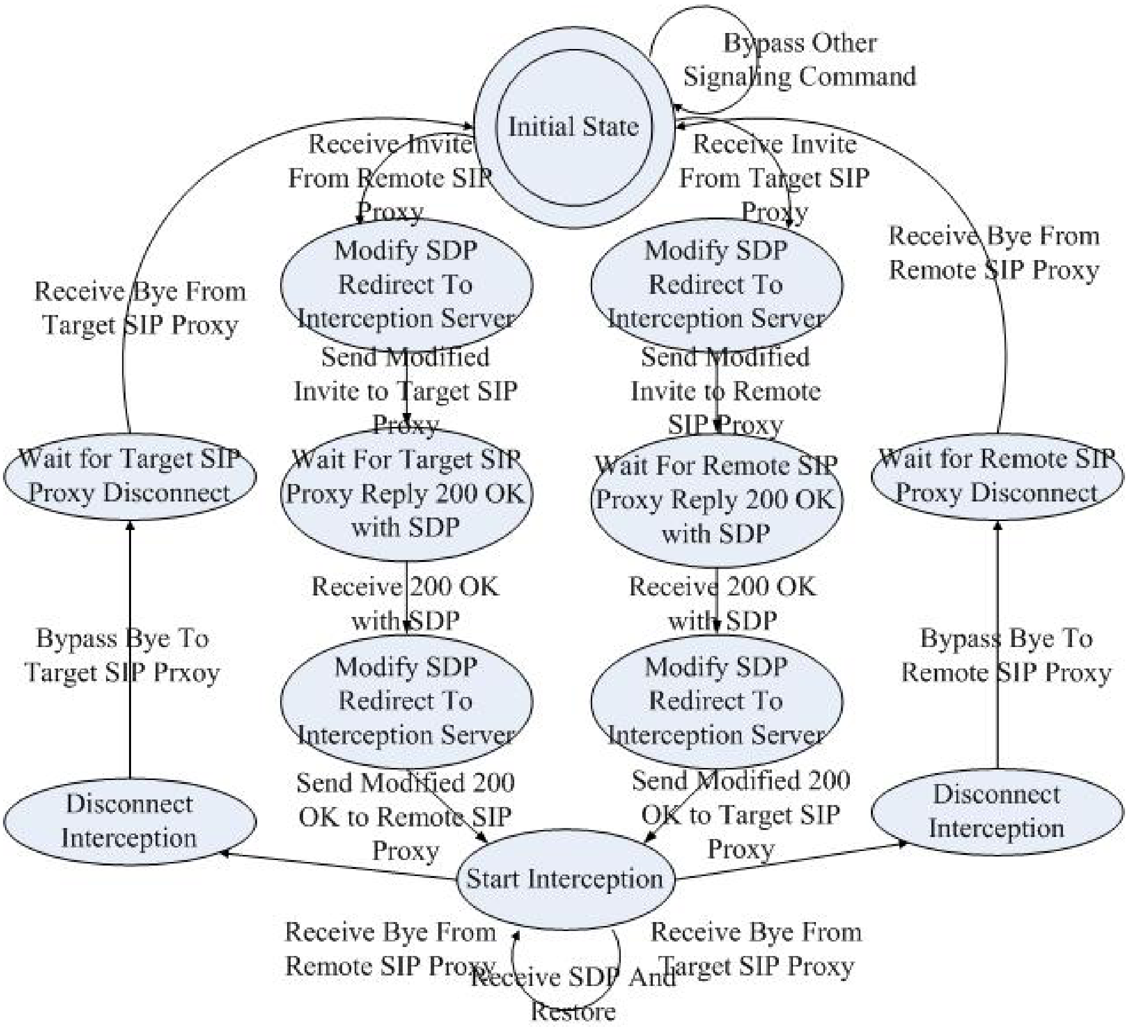


Figure 33. The Rogue SIP Server State Machine

Reference to the Rogue SIP Server state machine, you will see that it looks like the previous state machine. The difference is that the Rogue SIP Server is located between SIP proxies and didn’t connect to the end user. So modify the SDP to redirect the RTP is a simple way to do the interception.

4.2.3 The SIP Proxy Attached Interception

The SIP Proxy Attached Model is running our FIVE system in the SIP Proxy. FIVE system can intercept the information directly from the proxy server and pass the necessarily information to a remote monitor server. The following is the diagram of this model:

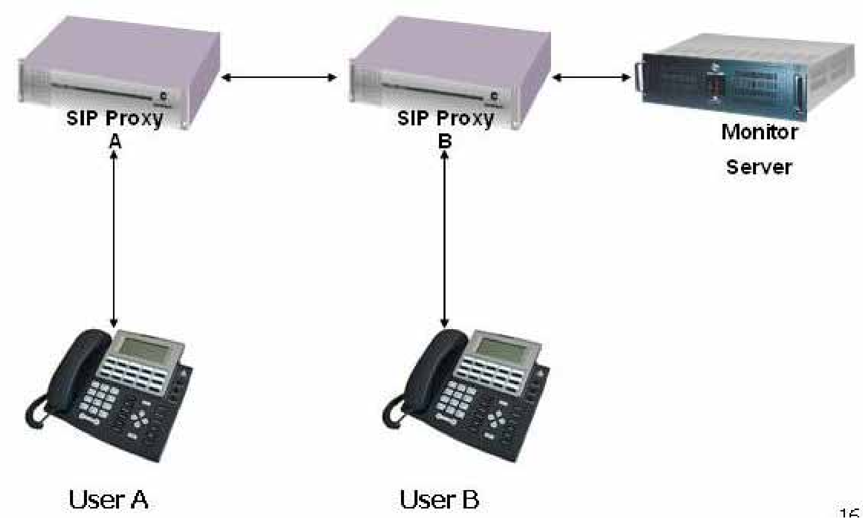


Figure 34. SIP Proxy Attached Model

The SIP Proxy attached mode is to install our FIVE system in the Proxy server. The network module will receive every message to send to this server. In this model we will use a SIP protocol 302 redirect message to make a third-party call. The remote Monitor Server will be the third-party to receive the call. It didn't send out any message but just listen to the conversion. There are several advantages of this interception mode. This is the most directly way to do the interception. And the Proxy B can also do the interception by itself. The following diagram is the flow of the incoming and outgoing calls.

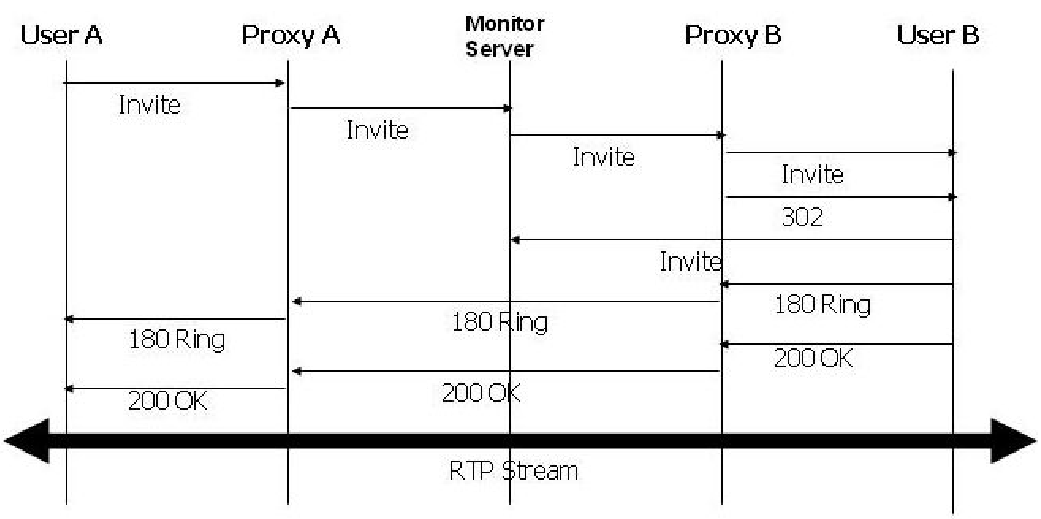


Figure 35. The SIP Proxy Attached Outgoing Call Interception flow

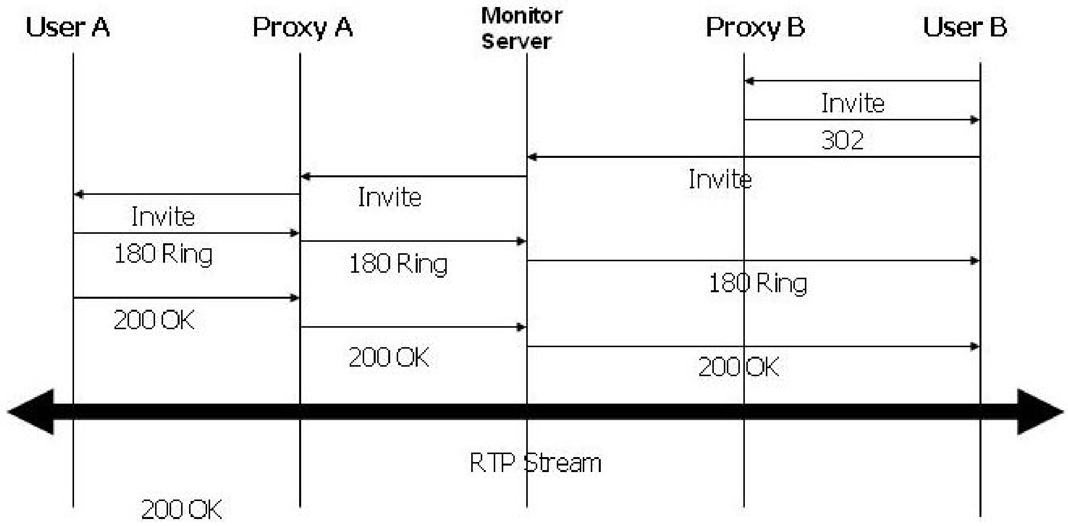


Figure 36. The SIP Proxy Attached Incoming Call Interception flow

In this model, our system is attached to the SIP Proxy server. So we can send the SIP signaling command to make the end user redirect the call. The following diagram is the sample of the redirect VoIP call by SIP 302 Moved Temporarily Response. The Moved Temporarily command often used by the redirection server to inform the user that the user have been moved, and also tell you the correct address. This is also protocol vulnerability for us to use as an interception method. From the following diagram we can see that, a user A wants to call user B. The Redirect Server asks the user A to redirect the call to new address New user B. In our interception scenario, the new user B will be the Monitor Server in the Figure 31 and 32. The Monitor Server will call to the real target that user B. And the voice will be intercepted.

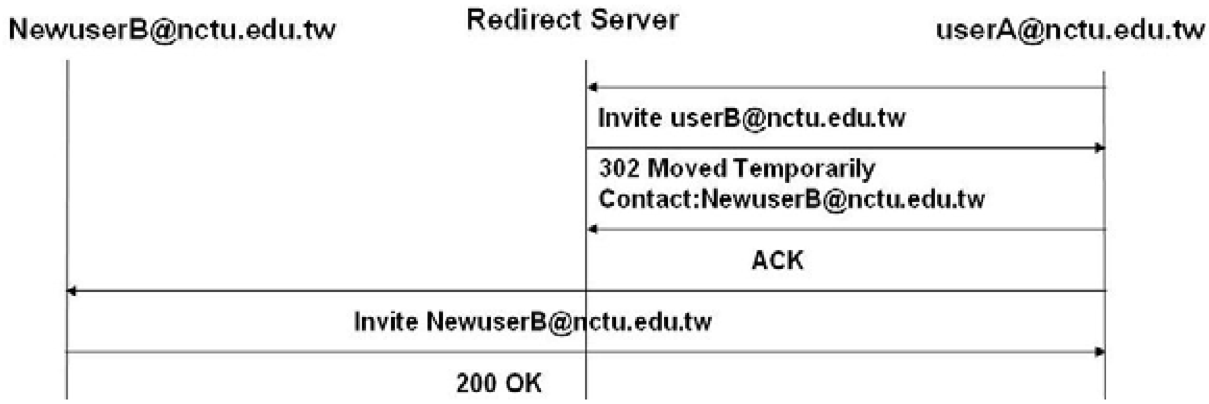


Figure 37. SIP 302 Moved Temporarily Response

To do the SIP Proxy attached interception is different from the previous solution. Our FIVE system is in the SIP proxy. The SIP proxy can receive the entire signaling packet, but the signaling path and the voice path are separated. We still have to redirect the RTP flow to pass to our interception server. Because of the loading of the Proxy Server to being a SIP proxy and an interception server at the same time will be too heavy, so we'll suggest redirecting it to another interception server. The following diagram is the modification of the SIP Proxy attached interception. And the call and interception flow please reference to the Figure.30.

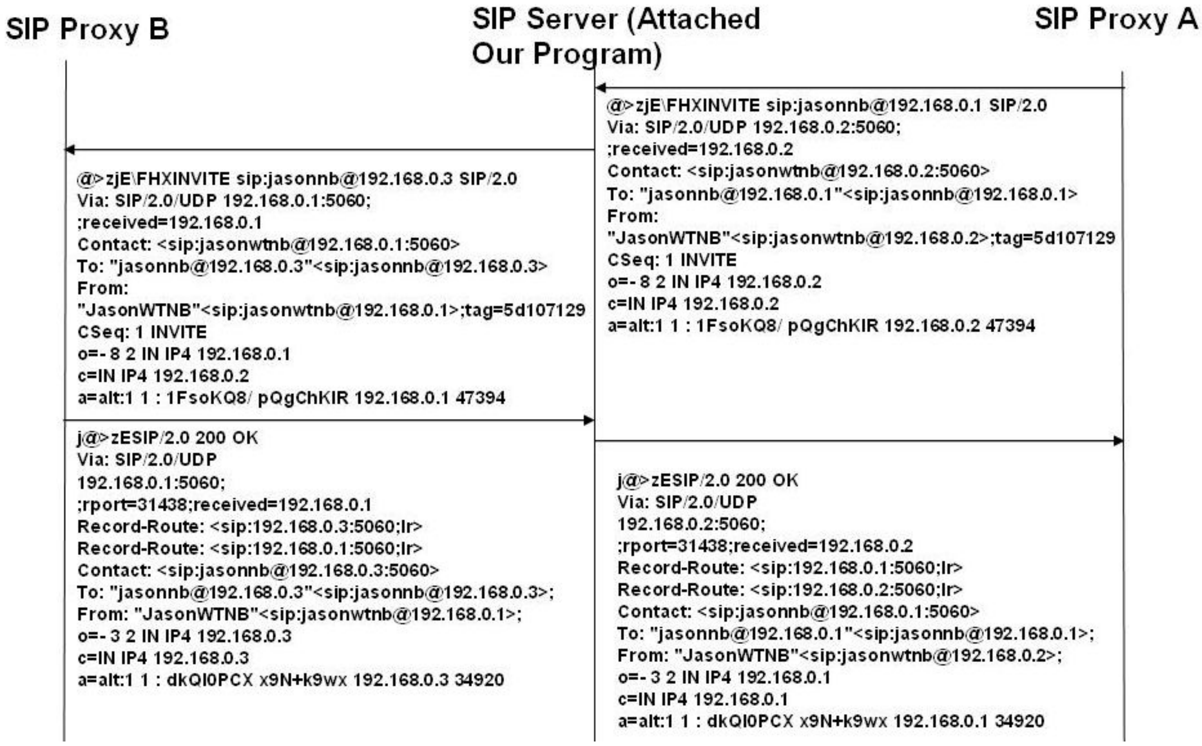


Figure 38. The SIP Proxy Attached SDP exchange flow

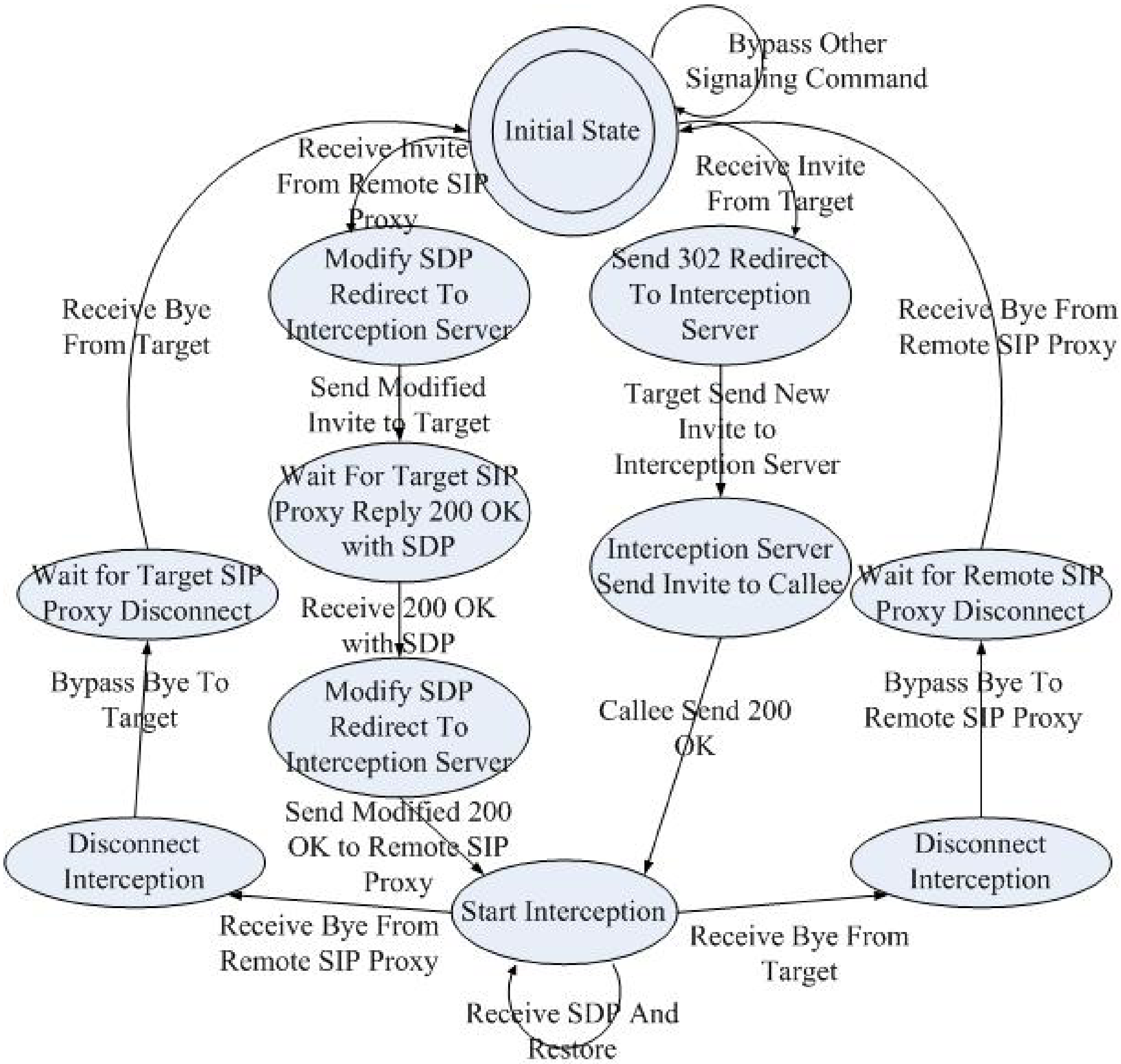


Figure 39. The SIP Proxy Attached Interception State Machine

The SIP Proxy attached Interception is different mechanism of the FIVE system. Because it is already attached in the SIP proxy, so to get the enough information is not the most concern. By the useful PCAP library, we can intercept any network traffic before it be send to the application. We can also send a fake command to any user or cheat the attached SIP Proxy by send a fake command to itself. That's why we will try to use a SIP 302 move temporarily command to redirect the call to our Interception Server. And we will suggest not restoring the traffic in the attached SIP Proxy, because the loading might cause the unstable service of the SIP Proxy. We can easily to off load by redirect the RTP to the Interception Server.

4.2.4 The Remote Attack Interception

The remote attack model is also a different concept. Our system will be a remote Interception Server. The remote attack will attack both SIP Proxy and the end user, and hijack the register of the end user. After all, we can do the interception of end user by spoofing the end user. Reference to the following model, the Interception Server will do the register hijacking to the SIP Proxy, and also do the ARP spoofing to the end user to get the packets that transmit out of the end user.

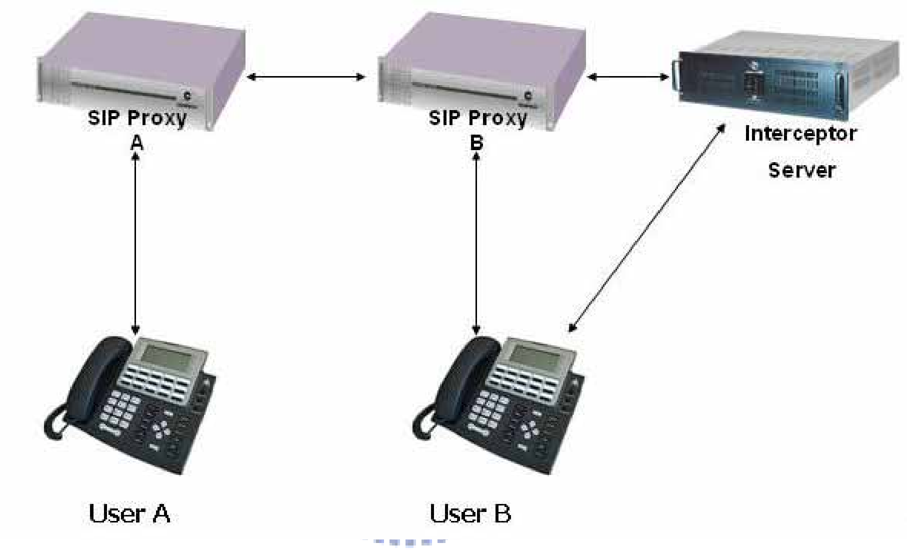


Figure 40. The Remote Attack Model

The Remote Attack is using the network attack skill to cheat the target user to redirect their traffic to our interception server. Our target is to use the ARP spoofing to modify the ARP table of a user, and redirect all of the traffic to our interception server.

To do the ARP spoofing, we will use a fake ARP reply command to corrupt a target machine's ARP table. If we can control the ARP table, we can control the routing of the traffic. The following is the evaluation of the ARP spoofing, in the network have a PC IP address is 192.168.1.3 and MAC address is 00-16-41-52-d2-10. Our interception server IP address is 192.168.1.3 and MAC address is 00-0c-6e-43-14-e4. The following is the ARP table in the computer.

```
C:\Documents and Settings\user>arp -a

Interface: 192.168.1.2 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0c-6e-43-14-e4     dynamic
  192.168.1.3           00-16-41-52-d2-10     dynamic

Interface: 172.25.115.24 --- 0x3
  Internet Address      Physical Address      Type
  172.25.115.13         00-12-f0-09-ef-13     dynamic
  172.25.115.254        00-50-bd-ba-9c-00     dynamic

C:\Documents and Settings\user>ipconfig
```

Figure 41. ARP table before ARP spoof attack

And then we perform the ARP spoof attack from the interception server, to send out a fake ARP reply command make the target machine to overwrite the ARP table. The following is the fake ARP reply capture log from the Ethereal.

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	AsustekC_43:14:e4	MitacInt_3e:7a:db	ARP	192.168.1.3 is at 00:0c:6e:43:14:e4
2	3.001441	AsustekC_43:14:e4	MitacInt_3e:7a:db	ARP	192.168.1.3 is at 00:0c:6e:43:14:e4
3	6.003027	AsustekC_43:14:e4	MitacInt_3e:7a:db	ARP	192.168.1.3 is at 00:0c:6e:43:14:e4
4	6.105541	192.168.1.2	192.168.1.3	ICMP	Echo (ping) request

Figure 42. The ARP spoof attack log

And the following figure is the ARP table after the ARP spoofing attack. When the target machine try to send the message to 192.168.1.3, it will send to the MAC address of 192.168.1.1, that is our interception server. By this kind of direction, we can redirect all of the traffics to our interception server.

```
C:\Documents and Settings\user>arp -a

Interface: 192.168.1.2 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0c-6e-43-14-e4     dynamic
  192.168.1.3           00-0c-6e-43-14-e4     dynamic

Interface: 172.25.115.24 --- 0x3
  Internet Address      Physical Address      Type
  172.25.115.254        00-50-bd-ba-9c-00     dynamic
```

Figure 43. ARP table after ARP spoof attack

The register hijacking is also a part of the remote attack model. The register hijacking is to register to the Proxy Server by a spoofed register request. And then we can redirect all of the signaling and voice command to the Interception Server. The following diagram is the sample of the register request from the user agent to the SIP Proxy Server. Please notice that the contact item, the contact address is where the call should be forward to. So the register hijacking is to send a spoofed register request to the SIP Proxy with the modified contact information. For example, we can send a fake request command with contact IP address 192.168.0.4, our Interception Server. If the register is success, all of the incoming call will be redirect to the 192.168.0.4.

```
@>zjEYBFEREGISTER sip:192.168.0.1 SIP/2.0
Via: SIP/2.0/UDP
192.168.0.2:17948;branch=z9hG4bK-d87543-9143986d8b30b640-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:12345678@192.168.0.2:17948;rinstance=311293041eafa42b>
To: "12345678"<sip:12345678@192.168.0.1>
From: "12345678"<sip:12345678@192.168.0.1>;tag=df556f31
Call-ID:
ca67b01b2a520546MWMzM2UyYzg3MTliYmMzNmJlMTg0NWIwMWRhMzJjYWQ.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,
SUBSCRIBE, INFO
User-Agent: X-Lite release 1002tx stamp 29712
Content-Length: 0
```

Figure 44. SIP Register Request

The following diagrams are the remote attack interception model. First the Remote attack Server will do the register hijack to the Proxy B. And then do the ARP spoof attack to the User B to make the Proxy B think the Remote Attack Server is the user B. And also make the User B think the Remote Attack Server is the Proxy B. So the Remote Attack Server can intercept all of the RTP packets during the call.

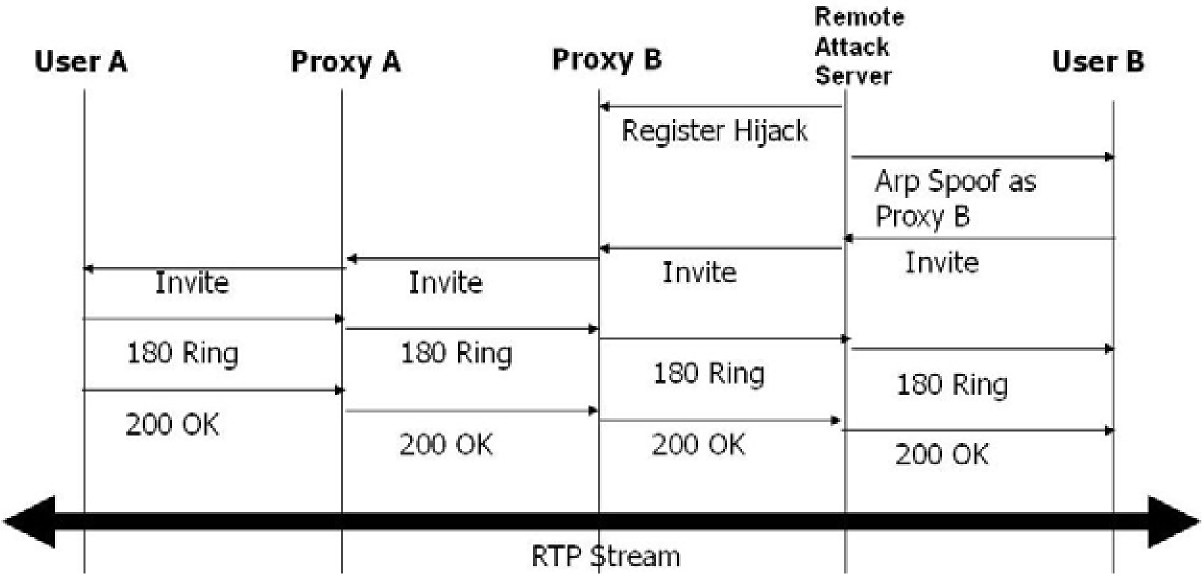


Figure 45. The Remote Attack Outgoing Call Interception flow

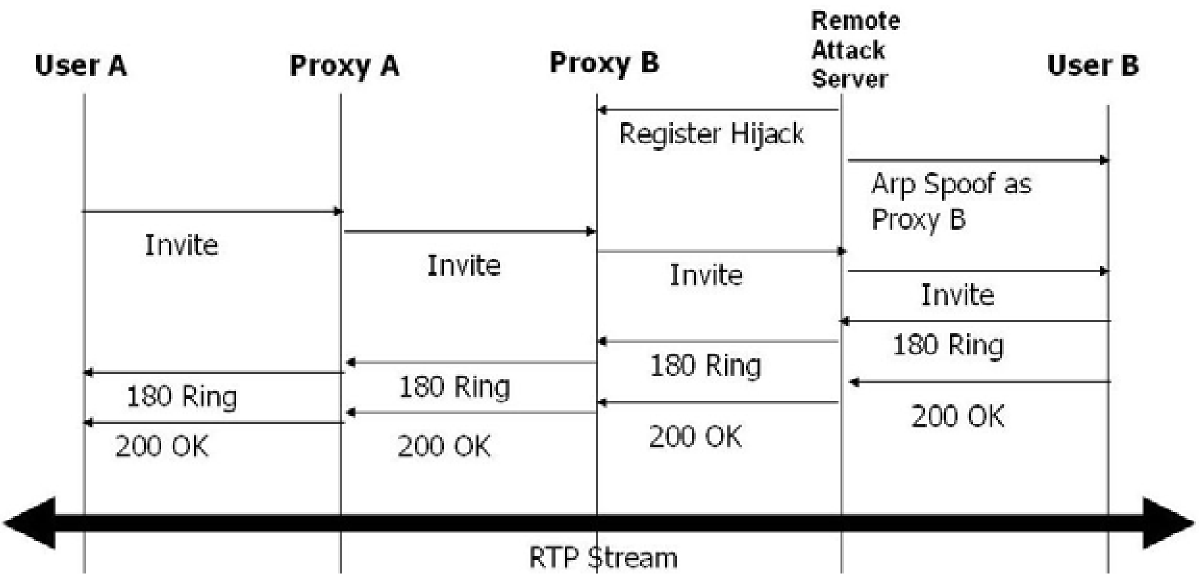


Figure 46. The Remote Attack Incoming Call Interception flow

The first step is to do the register hijacking to the SIP Proxy, and also do the ARP spoofing to make the end user redirect all of the traffic to our Interception Server. And the following steps will be the same as the Rogue B2BUA Server interception. Or another solution is doing the ARP spoofing as the gateway for the end user. And do the register hijacking to the SIP proxy. And then all the incoming call will pass to the Interception Server, the outgoing call setup of end user will send Interception Server. We can modify it as our call setup request.

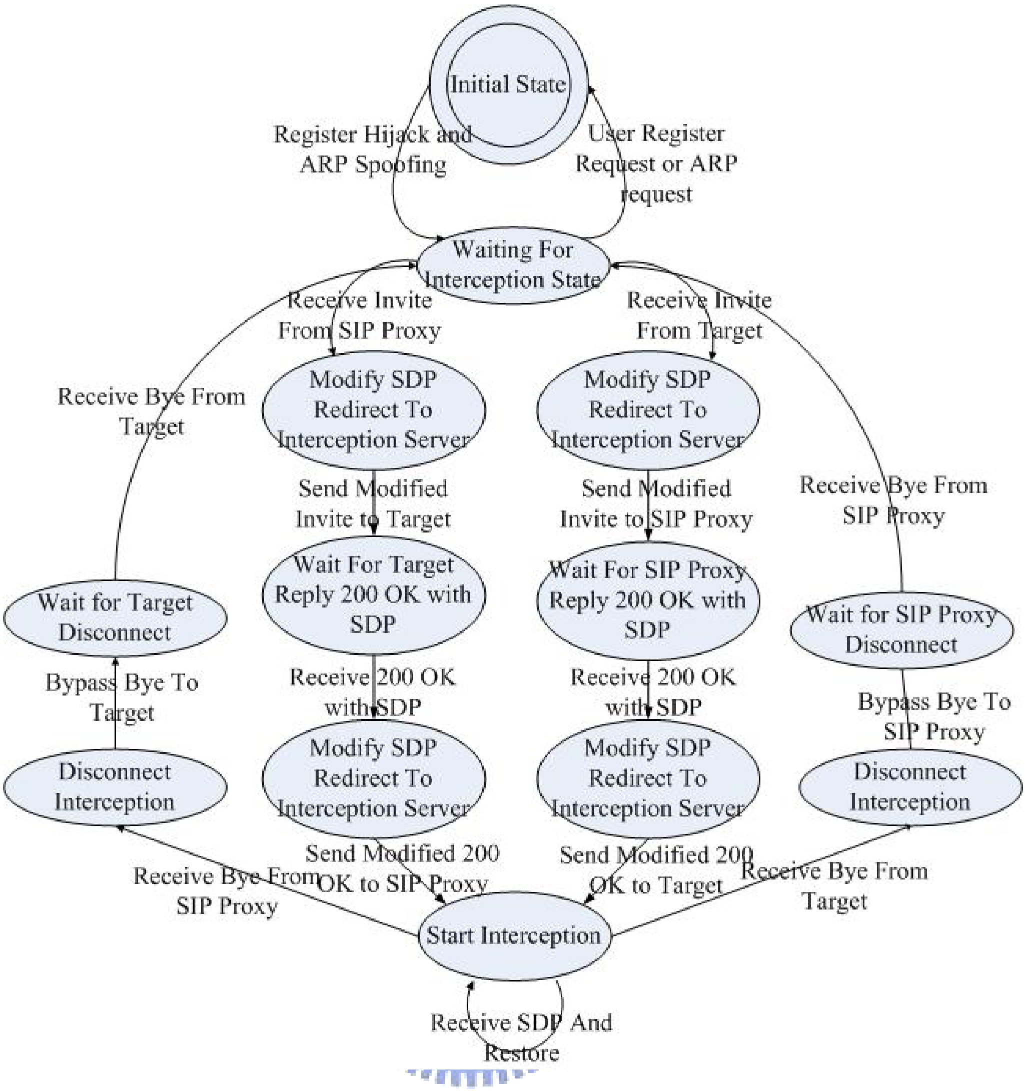


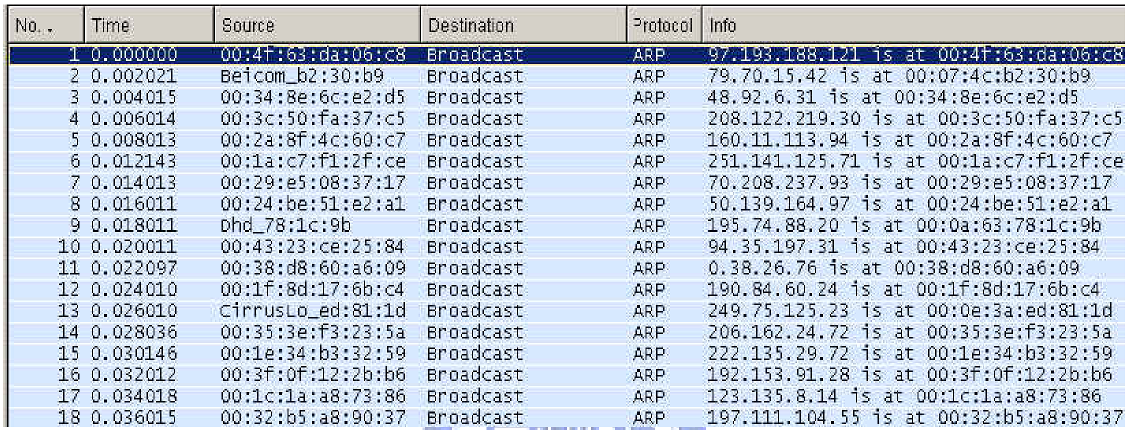
Figure 47. Remote Attack State Machine

4.2.5 The Port Mirroring Interception

The final model is the port mirroring interception model. The concept of the port mirroring interception is very simple. To redirect the traffic of specific user's to a port. A successful interception should make the user not aware the interception is processing. The difference between Remote Attack Interception and Port Mirroring Interception is the Port Mirroring Interception is the pure network interception to the end user. It is not related to the SIP protocol just to get everything to our Interception Server. But Remote Attack Interception is still trying to do the register hijacking by the SIP commands.

To do the port mirroring interception, we should attack the vulnerability of the end user network architecture. And then redirect all of the network packets to our interception server.

If the user is connecting to a switch, our “FIVE” system can do the ARP poisoning attack of switch. A switch can do the packet switching, and it is the major difference from the hub. But the internal ARP table of the switch is always have limitation, so the ARP poisoning is using a lot of random ARP replies to corrupt the ARP table of the switch, and then the switch will just work like a hub. Out interception server can just connect the same switch to sniff the packet and do the analysis and record. The following is the wireshark log of the “FIVE” system is doing the ARP poisoning attack.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	00:4f:63:da:06:c8	Broadcast	ARP	97.193.188.121 is at 00:4f:63:da:06:c8
2	0.002021	Beicom_b2:30:b9	Broadcast	ARP	79.70.15.42 is at 00:07:4c:b2:30:b9
3	0.004015	00:34:8e:6c:e2:d5	Broadcast	ARP	48.92.6.31 is at 00:34:8e:6c:e2:d5
4	0.006014	00:3c:50:fa:37:c5	Broadcast	ARP	208.122.219.30 is at 00:3c:50:fa:37:c5
5	0.008013	00:2a:8f:4c:60:c7	Broadcast	ARP	160.11.113.94 is at 00:2a:8f:4c:60:c7
6	0.012143	00:1a:c7:f1:2f:ce	Broadcast	ARP	251.141.125.71 is at 00:1a:c7:f1:2f:ce
7	0.014013	00:29:e5:08:37:17	Broadcast	ARP	70.208.237.93 is at 00:29:e5:08:37:17
8	0.016011	00:24:be:51:e2:a1	Broadcast	ARP	50.139.164.97 is at 00:24:be:51:e2:a1
9	0.018011	Dhd_78:1c:9b	Broadcast	ARP	195.74.88.20 is at 00:0a:63:78:1c:9b
10	0.020011	00:43:23:ce:25:84	Broadcast	ARP	94.35.197.31 is at 00:43:23:ce:25:84
11	0.022097	00:38:d8:60:a6:09	Broadcast	ARP	0.38.26.76 is at 00:38:d8:60:a6:09
12	0.024010	00:1f:8d:17:6b:c4	Broadcast	ARP	190.84.60.24 is at 00:1f:8d:17:6b:c4
13	0.026010	CirrusLo_ed:81:1d	Broadcast	ARP	249.75.125.23 is at 00:0e:3a:ed:81:1d
14	0.028036	00:35:3e:f3:23:5a	Broadcast	ARP	206.162.24.72 is at 00:35:3e:f3:23:5a
15	0.030146	00:1e:34:b3:32:59	Broadcast	ARP	222.135.29.72 is at 00:1e:34:b3:32:59
16	0.032012	00:3f:0f:12:2b:b6	Broadcast	ARP	192.153.91.28 is at 00:3f:0f:12:2b:b6
17	0.034018	00:1c:1a:a8:73:86	Broadcast	ARP	123.135.8.14 is at 00:1c:1a:a8:73:86
18	0.036015	00:32:b5:a8:90:37	Broadcast	ARP	197.111.104.55 is at 00:32:b5:a8:90:37

Figure 48. ARP poisoning attack

Or we can do the port mirroring interception by the special configuration of the network device. For example the port mirroring functions of the switch. Port mirroring is to copy all of the traffic and send to another port to do the monitor. And the purpose is the intrusion detection or network traffic monitor. If the end user connect to this kind of switch and enabled the port mirroring function, our “FIVE” system can connect to the mirror port and do the call analysis and record. Some of the Cisco switches support this function can name it Switched Port Analyzer (SPAN). The following is a diagram of the port mirroring interception.

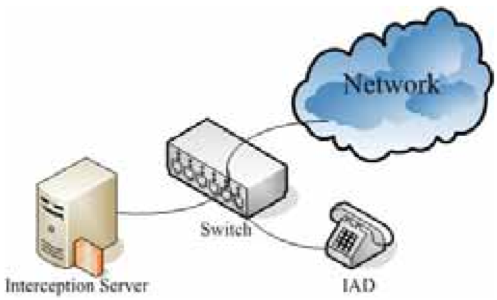


Figure 49. Switch Port Mirroring

After the Interception received all of the packets, we can do the analysis easily by using wireshark or any other SIP call analyzer. The following diagram is the graphical analyze result of the wireshark. We can check the protocol flow of the VoIP calls, and even to replay the voice by player that wireshark provided. It is just like to do the packet collection in the end user's IAD.

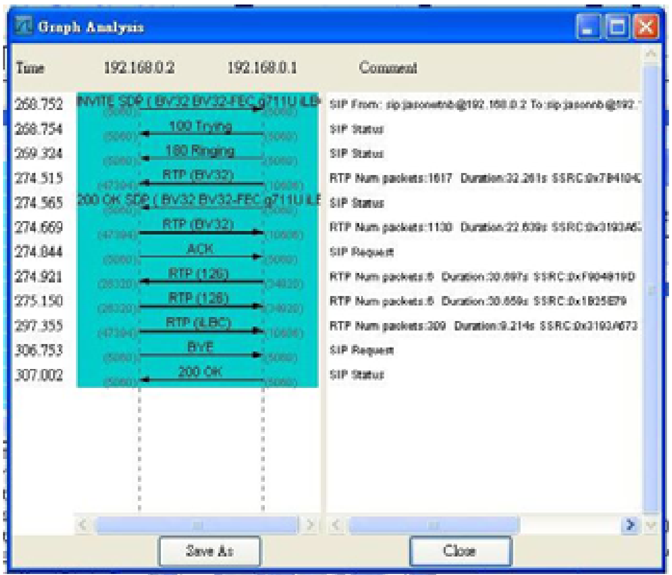


Figure 50. Wireshark VoIP Call Graph Analysis

Chapter 5 Experimental Result

In this chapter we will setup a real experimental environment to evaluate the functionality of our system. And also verify the side effects of our FIVE system. After setup a real VoIP network environment, we tested our interception function, and record the details of the test result and logs. We also finished the analysis of the test result, and try to fine tune our system. At first we will introduce our experimental environment. We have a simple but complete VoIP network test bed and get the test result of each case. After all we will do the analysis of the test result. To evaluate the system performance is very important, because the quality of telecomm service should be very stable. So our interception could not affect the normal service. This is the most challenge. And the details of the test result also could be the reference of the future work for who is interest of this subject.

5.1 Experimental Environment

The following diagram is our test environment diagram. Two PCs simulate the SIP proxies and another two PC simulate the IAD. The Interception Server is the server to perform the interception. The black line is the physical link, and the red line is the logical link. And the Interception Server logical link depends on which interception mode it supports.

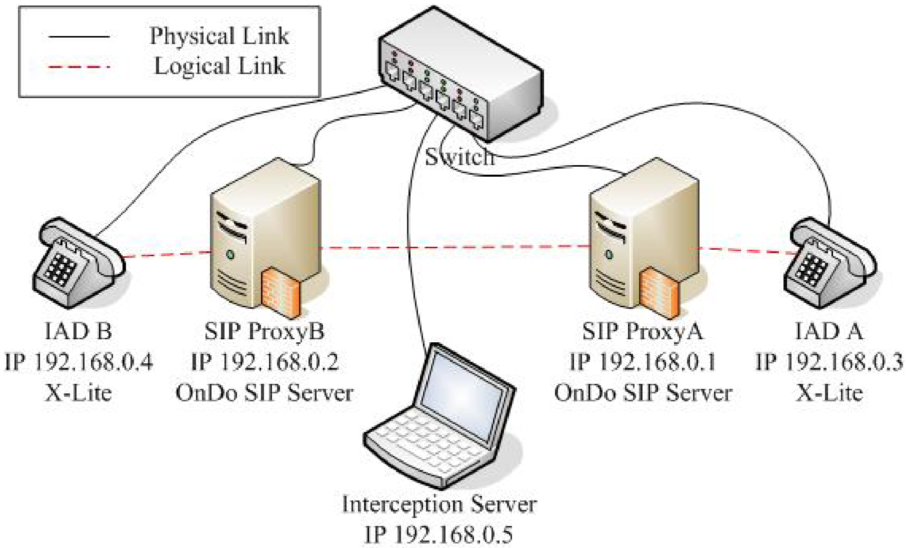


Figure 51. Testing Environment Diagram

The environment is to simulate a small VoIP environment. The Proxy Server is running the OnDo SIP Server application, and the IAD is running the x-lite application to simulate a SIP phone. The following table is the specification of each device.

Device Name	Specification
SIP Proxy A IAD A SIP Proxy B IAD B	IBM T43 CPU: DOTHAN 750(1.86GHz) RAM:DDRII 533 512 MB Harddisk: 80G Interface, 7200 rpm Operation System: Windows XP
Interception Server	Lenovo Thinkpad X60 CPU : CoreDuo T2300(1.66GHz) RAM: DDRII 667 1024 MB Harddisk: 160G SATA Interface, 5400 rpm Operation System: Windows XP
Switch	Marvell 88E6095 Chipset

Table 9. Testing Environment Device Specification

5.1.1 SIP Proxy – OnDO SIP Server

The SIP proxy is a computer running Brekeke OnDo SIP server. The software version is 1.5, and using the OnDo SIP Server with the Evaluation Use license. It is a SIP Proxy and Registrar and the environment needs the JAVA runtime environment 1.4 support. I used it for registers and authenticate users, and routes calls between user agents. And the two SIP proxies to simulate the signaling message transversal between Proxies. The IAD A will configure to register to SIP Proxy A, and IAD B will configure to register to SIP Proxy B. If we want to make a call from IAB A to B, the call setup should be complete by the co-work of the two Proxies. By the different URI, the SIP Proxy will send the request to the remote SIP proxy and try to setup the call. The following diagram is the register list, that a soft SIP phone is register to this server.

Figure 52. OnDo SIP Server Registered List

5.1.2 IAD – X-Light

X-Light is a popular free soft phone using in the VoIP network. We use it to simulate an IAD to make the SIP call. The configuration is also very easy. Just to create an account with username and indicate the target domain. When start up the application, the X-Light will try to register to the target SIP proxy. And then you can make the VoIP call.

Figure 53. X-Lite GUI and configure menu

5.1.3 Interception Server – FIVE System

Our FIVE system will do the packet sniffing and redirect the RTP call by different interception model. The following is the GUI of our FIVE system, it provides basic packet sniff function, and 5 different interception modes. The ARP spoof item will support the network attack method such as the ARP spoofing or ARP flooding. We use the same FIVE system program to do different interception model. When selected an interception mode, the FIVE system will create a thread to do the VoIP interception. Packet sniff will capture all of the packet that the FIVE system received, show up the MAC, IP and UDP header of the packet. This is useful for debug purpose.

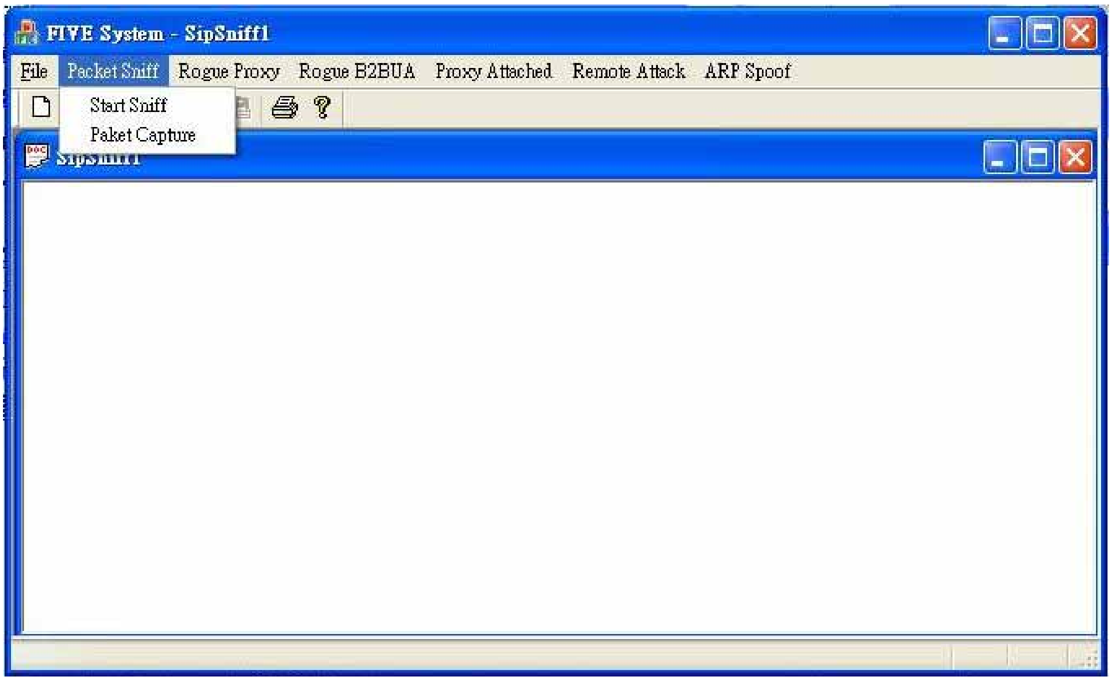


Figure 54. FIVE System GUI

5.2 Experimental Result

The FIVE system could do the interception successfully, it is the major function of it. But the target of this system is not to improve the capability or performance of the VoIP system, so the performance won't be better than the VoIP system that without FIVE system. A successful interception won't create noise and delay to make the interception target aware that they are being intercepted. We'll compare the performance counters to original calls that without interception.

5.2.1 FIVE System performance measurement criteria

We will use the QoS (Quality of Service) to evaluate the performance of our FIVE system. The RTCP will report the result of the QoS for each call, and the following is the QoS material that we will discussed.

Packet Loss is a simple counter for us to check the QoS of VoIP call. The RTP protocol is based on the UDP protocol, so there is no retransmission. The huge packet loss will cause the terrible voice quality. Unsuccessful redirect packet will cause series packet loss problem. The packet loss information will in the RTCP packet receiver report, and we can also compare to the total send packet number to the total receiver received packet number.

Delay will be measured by the timestamp of each packet. The transmission will always have delay, but our man in middle attack will increase the time of delay. The different routing path will also have the different value of delay. Serious delay will damage the quality of voice, and also affect the jitter. The delay will record in the RTCP receiver's report.

Jitter will also cause the serious voice quality issue. Most of the IAD or soft phone will allocate a jitter buffer to avoid the affection of jitter. The root cause of jitter is because the network traffic transmits is not always stable; the different network delay will make the network packet arrive the end user not in order. If our FIVE system make the unstable delay of the network traffic, the jitter will be the big problem.

The following diagram is the example of the RTCP receiver's report, we can see that the packet lose, jitter and delay value will be reported by this packet. And we will analysis our FIVE system by these three items.

```
⊟ SSRC contents
    Fraction lost: 0 / 256
    Cumulative number of packets lost: 0
⊟ Extended highest sequence number received: 3037
    Sequence number cycles count: 0
    Highest sequence number received: 3037
  Interarrival jitter: 0
  Last SR timestamp: 3906756739 (0xe8dc6083)
  Delay since last SR timestamp: 615841 (9396 milliseconds)
```

Figure 55. RTCP Receiver's Report

5.2.2 FIVE System performance measurement benchmark

We setup a simple VoIP environment as benchmark to evaluate the performance of our FIVE system. The environment is two SIP proxies server and two soft phones. The following is the test result of the benchmark. The RTCP packet will report the status every three seconds, so we make each call for half minute to collect the value of the RTCP reported.

First index is the packet loss, in the simple environment we didn't have any packet loss reported. The second index is delay. The delay is the delay time since last SR timestamp. The average delay time of our normal benchmark is 2882.96 milliseconds.

The last index is jitter. The inter-arrival jitter is the variance of the packet inter arrive time. The more complex network environment make this value increased, and the serious jitter may cause the packet loss. The network device will use the jitter buffer to avoid the affection of the jitter. The average jitter value is 66.2 timestamps our test case. The following diagram is the RTCP reported jitter value in half minutes. We can see that the incoming and outgoing RTP packet jitter is almost the same. We do the same test for several times and the following diagram is the average of jitter in different period of time. If the variation was large, it means the network environment is very unstable.

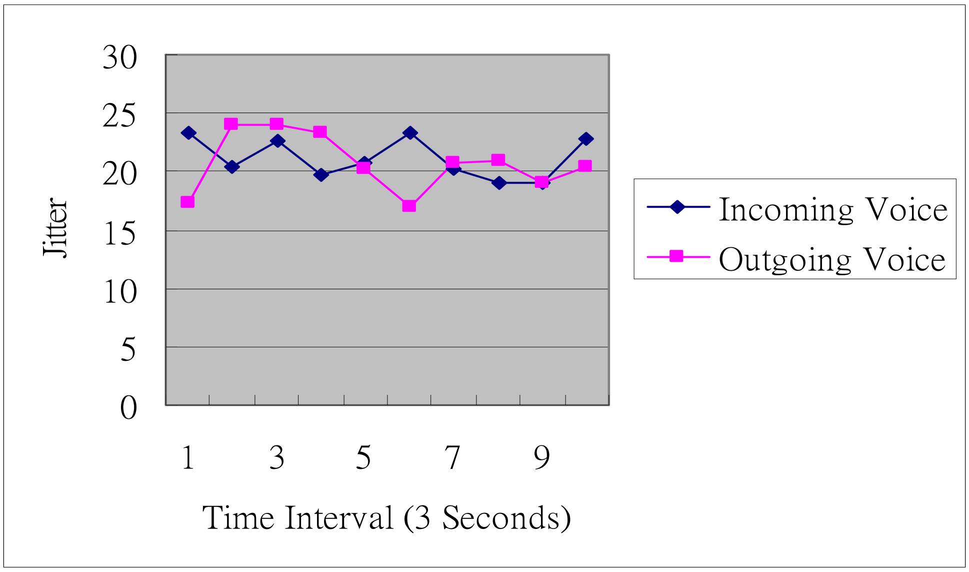


Figure 56. The Jitter variation during a normal call

5.3 Experimental Results

After collected all of the experimental results, we have calculated all of the records and do some analysis. Please notice that the VoIP interception is successful in all of the FIVE system models. And the test result is base on the RTP interception mode. We will use packet loss, delay and jitter to figure out the QoS during the FIVE system do interception. The acceptable QoS value help us to make sure that the user won't aware is being intercepted, or to generate too much traffic to make the network unstable. Only the end port mirroring interception mode is the hardware supported interception function. The port mirroring setting of switch supports to redirect the traffic to another switch port. We also use this to compare with other software based solution. In our test result, we didn't detect any packet loss in our FIVE system.

5.3.1 The Average Delay in FIVE system

The following diagram is the delay of different interception models in FIVE system. The normal call test cases have the lowest delay. The second one is the SIP Proxy interception mode, because the SIP Proxy interception just modify the SDP content and redirect it to the remote interception server, the overhead is low. And other interception models performance are almost the same.

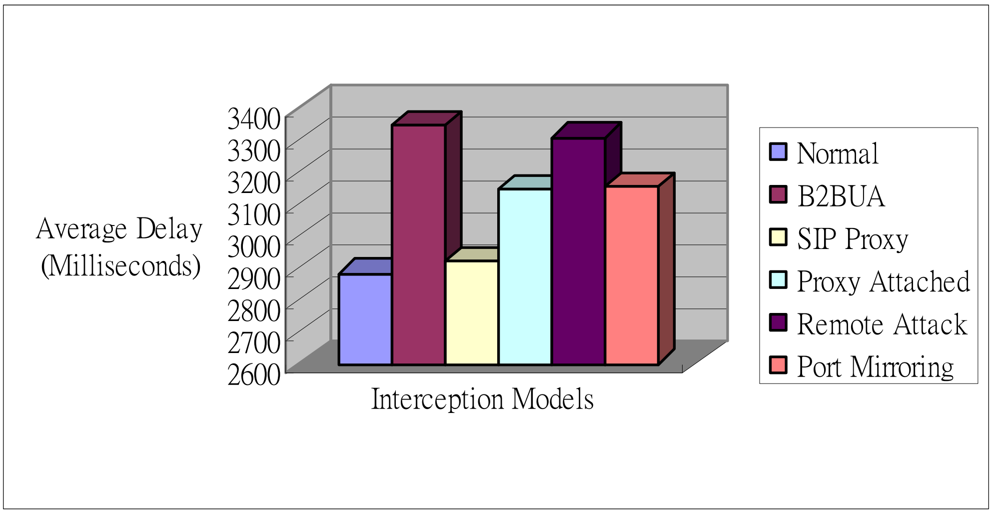


Figure 57. FIVE System Average Delay

Reference to the statistic of the average delay, the complexity of the interception state machine will increase the delay of the system. So the simple SDP modification in SIP Proxy interception mode will bring up less overhead to the system. And another noticeable point is that we didn't have great performance in the Port Mirroring Interception mode, even the hardware supports the packet duplication and forward to another port. But still spend some time to do the port mirroring.

5.3.2 The Jitter in FIVE system

The following diagram is the average jitter of different model. The value is an integer value of the timestamp. We can see that the complex mechanism will bring up the value of jitter. We can notice that the Port Mirroring Interception will increase average delay, but the network complexity is not increased. That's why the jitter is almost the same as the normal mode.

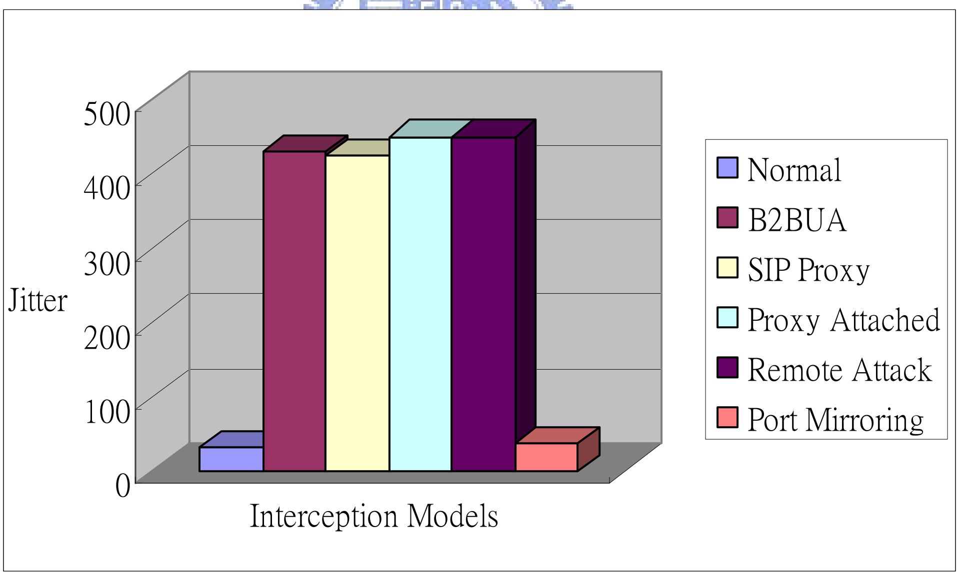


Figure 58. FIVE System Average Jitter

But the timestamp can't show the overhead of our system, so we convert the timestamp into time (millisecond) and minus the overhead of a normal call. So the following diagram is the overhead of our FIVE system. Jitter always happen in the VoIP network, so the jitter buffer is used to avoid the affection of jitter. The root cause of jitter is the routing in the IP network is not always stable. So the packet won't arrive at the destination in sequence.

Especially the RTP is based on the UDP protocol. The jitter buffer can keep the early arrived packet and waiting for the late packet to avoid the voice quality being affected. In normal condition, the jitter buffer will be configured as 120 to 150 milliseconds. So if our over head is over 120 millisecond will make the noise. Reference to the following FIVE system jitter overhead diagram, the maximum jitter is around the 25 milliseconds and the jitter buffer can still handle it easily.

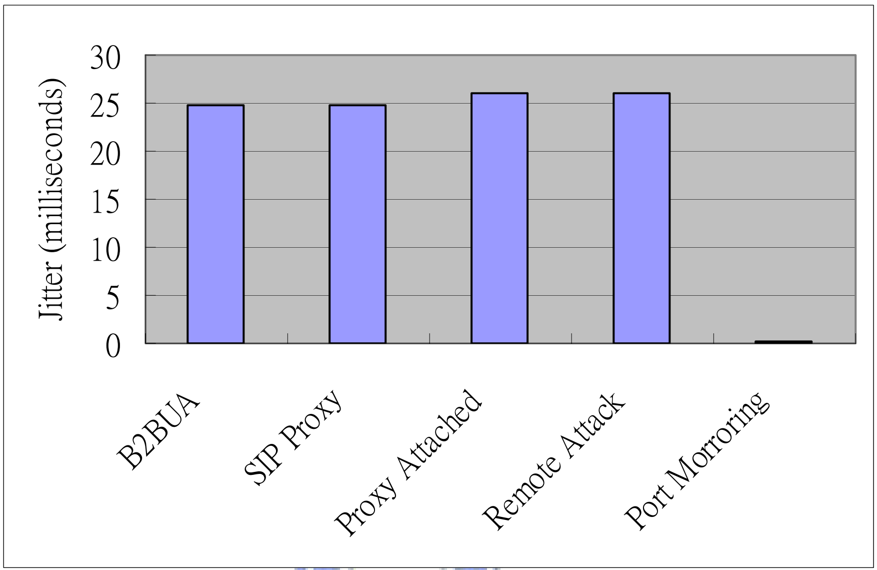


Figure 59. FIVE System Jitter Overhead

5.3.3 The Stability of FIVE system

The stability is also very important in the VoIP system. The QoS always be well discussed in the VoIP telecommunication. Besides we can do the interception well, but we still need to care about the QoS. The bed quality or noise will make the end user aware they are being intercepted. Even we can get a good average delay or jitter. But the burst of error or delay will still serious damage the voice quality. The stability of our FIVE system is very important. The unstable VoIP network environment will cause the VoIP call have very unstable jitter. If the jitter value is greater than the tolerance of jitter buffer, the voice packet will be dropped and the end user will heard the noise during the call. The following diagram will show the changes of jitter during a half minute call. The RTCP will report in every three seconds so we can verify the variance of the jitter to make sure the stability of our FIVE system. Reference to the following diagram we can see that, the B2BUA will have the greatest variance than others. The root cause is the B2BUA interception model has the most state and complex mechanism. The packet processing procedure will increase the jitter. But the normal jitter buffer can still handle our FIVE system overhead as previous we have proofed. The network will be more complex in real world, so we still need long term stability test is necessary to approve the reliability of FIVE system.

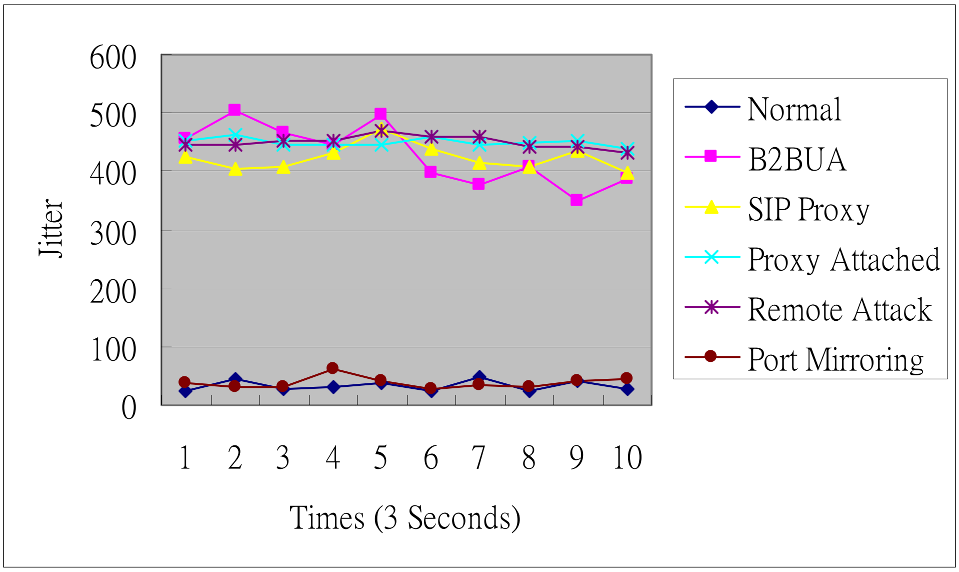


Figure 60. Stability Measurement of FIVE System

5.4 The Problems of the FIVE System

Although we spend much time to improve the capability of the FIVE system, but still have some problems of each interception models. Some mechanism is workable in the aspect of the technique, but not reasonable in the real world. The following will discuss the problems of each model.

First is Rogue B2BUA Server problem, how can we make the target end user to register to our Rogue B2BUA Server? And if the end user trace the network traffic, maybe they will know that they already being intercepted.

The second is the Rogue SIP proxy. The Rogue SIP Proxy is not the SIP Proxy that the end user registers to. So the routing of the network traffic is unpredictable, maybe we will lose some incoming calls because the remote SIP Proxy direct communicate to the Local SIP Proxy not pass through our Rogue SIP Proxy. And if the end user calls the local call that register to the same end user, the local SIP Proxy will directly transfer to the target. We will also miss this call.

The SIP Proxy Attached Interception won't lose call. But the problem is our program is writing by the Microsoft framework, and running in the Microsoft OS. Right now the Linux based VoIP solution is very popular, most of the network device will running the Linux or Vxworks. And the Linux also have the OPENSIP solution free for the users. So if the FIVE system wants to be more flexible, it must support multi-operating systems.

The Remote Attack Interception and Port Mirroring Interception have the same problem. The ARP attack will only work in the LAN, the WAN attack must focus on the traffic routing. There still have other problems such as firewall need to be take care. And most of the end user will connect to WAN by dial up or XDSL technique. The two interception model can still work in the center office site, but if we can access the center office site, we didn't need the remote attack; we can just set the mirror port or bridge the target line to a interception equipment. But we still need to present the possibility of the two interception models, and maybe it will be improved in the future.

Chapter 6 Conclusion and Future Works

We setup the environment to test our FIVE system, and to verify the result of our mechanisms. We can successful intercept the target's call and redirect the content to our interception server. But we still have to take care about the side effects of our FIVE system. The serious side effect will serious damage the voice quality, and make the end user aware that they are being intercepted. And in previous chapter, we already get our test result and analysis. Besides the performance, we also have to discuss other aspects of the VoIP interception. Such as the cost of build up a system; The complexity of implement the system; the practicability of do the interception. After make the conclusion, the government will choose the best way to use the FIVE system to do the interception.

6.1 Conclusion

After collected all of the experimental results, we can do the analysis of the FIVE system, and make the conclusion of it. Successful interception is our basic requirements. Besides the interception, there are many other issues need to be concerned, such as overhead, cost, implementation and practicability. The following table is the conclusion of the experimental results.

	B2BUA	Rogue SIP Proxy	SIP Proxy Attached	Remote Attack	Port Mirroring
Performance	Medium	Medium	Medium	Medium	High
Overhead	Medium	Medium	Medium	Medium	Low
Cost	Low	Low	Low	Low	High
Implementation	Hard	Easy	Medium	Medium	Easy
Practicability	Low	Low	Medium	High	High

Table 10. FIVE System Experimental Results Comparison Table

The five interception models have acceptable performance. We evaluate the performance by the delay and jitter. The overhead of delay is millisecond level. And the overhead of the jitter can also be handled by the jitter buffer. The Port Mirroring Interception has the best performance result, because this is the only one solution implemented by hardware. And in this model, the network complexity will also not to be increased.

The overhead is can be measured by the VoIP network loading. Our software based solution will duplicate the packet and redirect it to our Interception Server. The Port Mirroring Interception mode does only redirect the traffic of the target port to a specific port to the Interception Server. This traffic won't pass to the IP network and increase the network loading.

The cost is the real cost to setup the interception environment. Our software based FIVE system won't take much cost for setup the environment, and also didn't need to buy any new special equipment to do the interception. But the Port Mirroring Interception need the hardware switch supports the port mirroring function, a normal hub or dump switch may not support this function. If you want to set some filters to intercept some specific packets, you will need a management switch, and that will cost you much.

The implementation is the difficulty to implement the solution. The Port Mirroring Interception is easy to implement, because the user only have to configure the port mirroring function of a switch. The Rogue SIP Proxy is also easy to implement, because the related state machine is simple. The B2BUA interception is the most difficult, because the state machine handles a lots of SIP signaling, such as the register of an account or call setup. It's hard to implement a state machine that can cover all of the conditions.

Practicability is also a very serious problem of the interception concept. We can make any assumption and try various cases to do the interception every in the network. But the real interception should not aware by the end user, and is easy for setup. The practicability of End User interception and Remote Attack is high, because the solution is do the remote attack to the user, or redirect traffic by switch. It is very possible and easy to achieve this goal. The SIP

Proxy attached Interception depends on which SIP proxy the end user is register to. To achieve this goal, our FIVE system must can be setup in the SIP proxy. But right now it only supports Microsoft Windows system. The most problem of B2BUA interception is the end user has to register to your Interception Server but not the real SIP proxy server. How can you convince the end user to register to your SIP proxy is a problem. The end user might notice that this is an Interception Server. The problem of Rouge SIP Proxy is that we can't make sure all of the incoming or outgoing call will pass through our Rouge SIP Proxy. We can't full control the routing of the call, that's why we can't make sure that every call will be intercepted.

So we suggest that the hybrid mode should be the best solution. The government unit can choose different kinds of interception model and setup it in the networks to prevent from lost any call. Different interception model with different difficulty and cost, reference to our FIVE system, we can make the decision to choose a good and flexible solution for the lawful VoIP interception.

6.2 Future Works

To make the system getting better, we still need a lot of efforts to make the system more adapt to real world. We need to improve the capability of our system, and also need to increase the practicability in the real interception application. Or we can return to the basis, to modify the SIP protocol for this function.

The experimental environment is base on the LAN, which also means we didn't need to do any network address translation. Although we have confidence our FIVE system will also work in the real world, but we still need to prove it in the real and large VoIP network in the future. The reason is it is more convenient for us to set up the experiment environment. But in the real world, most of the Servers and end users will be located in different networks. The network address translation will be necessary for our FIVE system to work at the real world. Another concern is how the VoIP call registers through the firewall, that's another important topic of VoIP domain, and is not the target of our study.

Right now the FIVE system is implemented base on the Microsoft Visual Studio 2005 frame work. But our concept is also adapted to any embedded system to create an interception equipment. So we can port our FIVE system in the device running WINCE system. The WINCE system can support the Microsoft framework program. We can also base on the Linux IP stack to porting our state machine to make the computer or embedded device become an interception server. We can easily sniff or modify the packets in the Linux IP stack. And both of these two ideas will our FIVE system as a real product for the VoIP interception.

At last, maybe the best solution is to modify the SIP protocol to support this feature. The OPENSIP project have released the source code of the SIP Proxy Server, and we can base on it to development the new protocol to support the VoIP interception, that will be the best way to make sure we won't miss any call that need to be intercepted. The new designed SIP protocol should support the interception by redirect the RTP payload and call information. And also needs to use the security check to protect from the hackers to use this function.

Reference

[1] Jeffrey Albers, Bradley Hahn, Shawn McGann, Seungwoo Park, Rundong Zhu., "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems", University of Colorado.edu master degree thesis. Retrieved April 2005.

[2] Feng Cao, Malik, S., "Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors", Communications Magazine, IEEE Volume:44 Issue:4 Page(s): 138- 145. April 2006.

[3] Jared Ring, Kim-Kwang, Raymond Choo, Ernest Foo, Mark Looi. "A new authentication Mechanism and Key agreement protocol for Sip Using", Information Security Institute Queensland University of Technology. March 20, 2006.

[4] Cisco Systems, Inc. , "Security in SIP Based Network", Whitepaper, 2002.

[5] Zbigniew Kotulski, Wojciech Mazurczyk, "Convert channel for improving VoIP security", Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, 2006.

[6] Ville Hallivuori, "Real-time Transport Protocol (RTP) Security", Tik-110.501 Seminar on Network Security, 2000.

[7] Huei-Wen Ferng, Yung-Ching Chen and Ying-Tsung Chen, "Study on SRTP and Design Key Exchange for Secure VoIP", Department of Computer Science and Information Engineering National Taiwan University of Science and Technology, 2004.

[8] Klaus Steinklauber, "VoIP security in Small Business", SANS Institute 2003,

[9] Andro Milanović, Siniša Srbljić, Ivo Ražnjević*, Darryl Sladden*, Daniel Skrobo, Ivan Matošević, "Distributed System for Lawful Interception in VOIP network", EUROCON 2003.

[10] Naim Maloku, Tomai Aljai, Franc Dolenc, "Legal Call Interception in Next Generation Networks", ConTEL 2003, ISBN: 953-184-052-0, 2003.

[11] John McCarron, "A Brief Overview of VoIP Security", infosecwriters.com, 2006.

[12] Ted Wallingford, "VOIP HACK: Tips & Tools for Internet Telephony", ISBN 978-986-7794-88-8, 2005.

[13] Endler Collier, "HACKING EXPOSED VoIP", ISBN 978-0-07-226364, 2006.

[14] NORTEL, “Method and system for lawful interception of packet switched network services.”, Patent Number US 2004/0255126, 2004.

[15] NOKIA, “Method and system allowing lawful interception of connections such a voice-over-internet protocol calls”, Patent Number US 2004/0157629, 2004.

[16] ALCATEL, “Lawful interception gateway”, Patent Number US 2005/0094651, 2005.

[17] Cisco, “Intercepting a communication session in a telecommunication network”, Patent Number US 2006/0245595, 2006.

[18] SIEMENS, “Subscriber status determination and call”, Patent Number US 2007/0041558 , 2007.

自　　傳

我在民國 67 年於台中縣出生，是家中的長子也是唯一的男生。出生後不久就舉家遷移到台北生活。家中環境小康，父母在做布料批發工作，兩年多前與交往多年的女友結婚，內子亦從事資訊相關產業，目前在南港工業園區擔任測試工程師。

求學歷程：

從國小到高中的求學生涯還算順遂，從大龍國小、百齡國中到成功高中。大學聯招的成績在所就讀的前三志願名校中屬於非常的差。但由於對資訊工程特別有興趣，即使成績差，仍抱定選系不選校的原則，志願卡清一色的填選資訊工程學系，於是到了逢甲大學的資訊工程學系。而在逢甲大學資訊工程系時加入校長 劉安之教授的網路實驗室，也發表了網路拓樸自動發現系統的專題。在這個期間在教授與研究所學長的帶領下，打下我不少未來發展的基礎。在求學的階段，我的專長在於資料庫與網路程式的撰寫。

社團活動：

在求學的生涯算是一個活潑外向的人，也積極的參與種種的課外活動。在成功高中時是康輔社的副社長，在逢甲大學時是資訊工程系的系學生會副會長，並參加系壘球隊轉戰全國各地。

最大的興趣~電腦：

而我從小到大最值得一提的，就是我與電腦那深遠的關係了。因爲從小有許多的長輩在資訊業界服務，所以從我小學起就提供我他們淘汰的機器讓我自己做運用。當然我都是把它當成我的遊樂器，卻也讓我比別人更早接觸這領域。所以在小學時我就有 APPLE 電腦和磁碟機，到國中時則有一台有兩個 Floppy 而無硬碟的電腦，到了高中則有一台陽春的 286。而習慣的作業系統從 MS-DOS、Windows 3.1、95、98、2000 到 XP 都有所經歷。

入伍~任意揮灑專長：

大學畢業後入伍時，很幸運的能夠擔任資訊系統架構與國軍補給保修系統維護工作，由於資訊化的推行，我的專業能力得以在軍中發揮，也因此受到長官的器重。在部隊中鋪設了完善的區域網路，並架起國防部配發的伺服器，最重要的是對於補給保修系統架構的了解，能完善的輔助系統轉換的陣痛期。這工作不止讓我的軍旅生涯因此而豐富多彩，也因爲在工作上的表現，得到長官的肯定，而獲頒國軍前鋒榮譽金質勳章。

工作~永遠邊做邊學：

第一份正職工作是在仲琦科技的新竹分公司擔任研發工程師，主要負責局端通訊設備開發、Embedded 系統和 VoIP 技術開發。而這份工作除了日常的研發計劃外，由於技術門檻高，所以有時候更必須親自到各國協助電信局和客戶解決問題，也給我不少與眾不同的經歷，奠定了我的基礎技術能力。在仲琦科技服務近五年後，因生涯規劃問題，所以選擇到台北文曄科技擔任 FAE 副理一職。工作的內容主要是負責消費電子手持式平台的產品，開發與推展最新的科技。

交通大學資訊學院碩士在職專班：

由於有感於自己的能力與學歷的不足，所以我工作一滿三年就報考交通大學的資訊學院碩士在職專班。很幸運的以第三名的成績考上專班，並且請蔡文能教授擔任指導教授，論文研究題目爲”在 VoIP 環境中的彈性化監聽方案”。在專班的求學過程，深刻的體會到學問與工作相互結合與驗證，並有幸得到書卷獎的鼓勵。

未來：

我是以積極的態度來面對自己的人生，會努力的爭取所有的機會。而最好的投資就是自己。我相信目前的學歷不會是我的學習終點，仍然規劃 MBA 或者是博士的深造機會。我不知道未來我會不會成功，但是我希望在機會來到時，我已經準備好了，這是的我人生目標。