SECURING THE CALEA ARCHITECTURE AGAINST DENIAL OF SERVICE ATTACKS

By

LIM KONG HUA

A project submitted to the Department of Internet Engineering and Computer Science,
Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Master of Computer Science
August 2011

SECURING THE CALEA ARCHITECTURE AGAINST DENIAL OF SERVICE ATTACKS

LIM KONG HUA

MASTER OF COMPUTER SCIENCE

FACULTY OF ENGINEERING AND SCIENCE
UNIVERSITI TUNKU ABDUL RAHMAN
AUGUST 2011

Table of Contents

ABSTRACT

SECURINT THE CALEA ARACHITECTURE AGAINST DENIAL OF SERVICE ATTACKS

Lim Kong Hua

Law Enforcement Agencies (LEA) around the world utilizes eavesdropping systems that are based on the Communications Assistance for Law Enforcement Act (CALEA) architecture, which provides a platform for transmitting and collecting these data for further analysis. Recent security analysis however has revealed that CALEA is susceptible to Denial-of-Service (DoS) attacks, which could potentially compromise the ability of the system to transmit, analyse and utilize the captured data in real time. The primary reason for this is the limited transfer rate allocated for sending data obtained via eavesdropping. The bandwidth can be easily overwhelmed by dummy messages if the transmission link is hijacked, resulting in subsequent loss of real data being transmitted. This would be analogous to the SYN flood attack observed in web servers.

This project proposes a solution to this issue, which involves splitting the original data to be transmitted into smaller chunks prior to transmission. The motivation is to decrease the probability of packets containing real data being lost when the bandwidth usage increases when a DOS attack is attempted. Subsequently larger amount of real data arrives intact at the receiving end, which can then be gainfully utilized. The process of distinguishing the fake from real messages could be achieved through some

appropriate pattern recognition and classification software, which however would be beyond the scope of this project. The key activities in this project involve the design, implementation and test of the performance aspects of the proposed solution to the DOS attack problem.

A brief overview of the CALEA architecture is provided, along with the various key modules that comprise it. The current solution is proposed after an analysis of various alternatives. The primary research methodology in this project concerns the design of the experimental tests for the proposed solution, its implementation, execution, data gathering and subsequent analysis. The trial runs are repeated for both wireless medium and wired medium in order to compare results. A limited transfer rate link is used to simulate an overwhelmed link and the FTP protocol is used for the file transfer process. A performance analysis is shown to indicate the amount of real data that would have been lost without the use of the solution. A discussion about the strength and weakness of the solution is also provided, along with avenues for future work.

ACKNOWLEDGEMENT

I would like to show my gratitude to my supervisor, Dr. Victor Tan Hock Kim, whose encouragement, guidance and support throughout the phases of the project enabled me to develop a better understanding of the subject.

Lastly, I offer my heartily thankful to all of those other people who supported me in any respect during the completion of the project.

Lim Kong Hua

FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 08 November 2011

PERMISSION SHEET

It is hereby certified that Lim Kong Hua (ID No: 09UEM09065) has completed this final year project entitled "Securing The Calea Architecture Against Denial Of Service Attacks" under the supervision of Dr. Victor Tan Hock Kim (Supervisor) from the Department of Internet Engineering and Computer Science, Faculty of Engineering and Science.

I hereby give permission to the University to upload softcopy of my final year project / ~~dissertation~~ / ~~thesis~~* in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

( )

*delete whichever not applicable

APPROVAL SHEET

This dissertation/thesis entitled "SECURINT THE CALEA ARACHITECTURE AGAINST DENIAL OF SERVICE ATTACKS" was prepared by LIM KONG HUA and submitted as partial fulfillment of the requirements for the degree of Master of Computer Science at Universiti Tunku Abdul Rahman.

Approved by:

_____
(Prof. Dr. VICTOR TAN HOCK KIM)
Date:……..
Professor/Supervisor
Department of Internet Engineering and Computer Science
Faculty of Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

_____
(Prof. Dr.)
Date:……..
Professor/Co-supervisor
Department of _____
Faculty of _____
Universiti Tunku Abdul Rahman

DECLARATION

I hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

Name ____Lim Kong Hua_____

Date ____11 August 2011_____

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS/NOTATION/GLOSSARY OF TERMS

Lawful Intercept (LI)

Law Enforcement Agencies (LEA)

Communications Assistance for Law Enforcement Act (CALEA)

Access Function (AF)

Call Data Channel (CDC)

Call Content Channel (CCC)

Delivery Function (DF)

Collection Function (CF)

Telecommunications Service Provides (TSP)

European Telecommunications Standards Institute (ETSI)

Join Standard (J-STD-025)

Interception Access Points (IAP)

Handover Interface (HI)

Intercept Related Information (IRI)

Mobile Switch Center (MSC)

LIID (Lawful Intercept Identification)

Lawfully Authorized Electronic Surveillance Protocol (LAESP)

Short Message Services (SMS)

Denial of Service (DoS)

CHAPTER 1

INTRODUCTION

We are living in a world where computers are constantly under the threat of being attacked. In January 2010, Google claimed "Like many other well-known organization, we face cyber-attacks of varying degree on a regular basis. In mid-December 2009, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property." [1]. For instance, the Greek Watergate in 2004-2005 was a security breach lesson in history where it happen in one of Greek's largest mobile network service provider involving high ranking officials' mobile numbers been secretly tap. The eavesdropping attack began around August 2004 Olympic Games in Athens and it lasted for about 10 months and the attackers were not caught [2]. It has been estimated that DoS attacks have been launched in the internet was about 12.8K attacks worldwide in the period of 3 weeks [3].

Law enforcement agencies (LEA) around the world in eavesdropping are based on the Communications Assistance for Law Enforcement Act (CALEA) architecture as shown in Figure 1. The specific target numbers from the LEAs can be provisioned into a box which provides the Access Function (AF). When the target makes or receives a call, call data related to the call (CDC) and voice or call content (CCC) will be delivered from the AF to Delivery Function (DF) and then pass down to Collection Function (CF). CF locates in the LEAs domain where the activities can be monitored in real time or/and save into a storage device for later retrieval and evidence presentation. Although J-Standard was defined by US, the European's ETSI architecture is similar.

So basically the architecture of J-Standard CALEA System (The telecommunications service providers (TSP) and Law Enforcement Agency develop the J-STD-025 or J-Standard.) consist of three blocks which are Access Function (AF) or Interception Access Points (IAP), Delivery Function (DF) and collection Functions (CF).

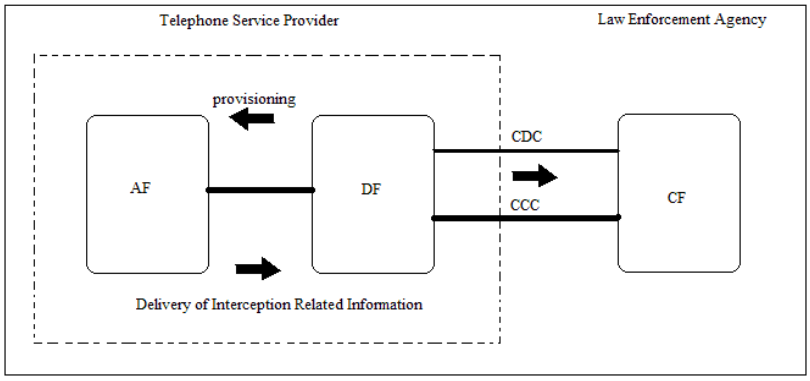

Figure 1: CALEA architecture

As per the ETSI Standard, the Internal Network Interfaces (INIs) between the DF and the AF provided the following functionality:

- INI-1 provisioning suspect identifier into the AF
- INI-2 is for delivering data and signalling information related to the suspect which has been provisioned through INI-1
- INI-3 delivers call content to the DF

Without law enforcement agency spending the resources and time to develop interfaces to all the network elements and protocols, the DF translates the raw target traffic from AF into a standards based interface to the CF. The ETSI standard defines three Handover Interface (HI) :

- HI-1 transports administration information between the LEA and the TSP
- HI-2 delivers Intercept Related Information (IRI) from the DF to CF.
- HI-3 transports the communications content to the CF

AF can be passive probe which is placed in the network to monitor the traffic. These probes need to handle traffic in high bandwidth and it has high processing power to do packet inspection in real time performing string search task or others. Another type of AF can be all the Mobile Switch Center (MSC) in the TSP's mobile network. A second type of AF can be mediation network equipment which can exchange message with all the MSC. Many AF can be connected to a single media where the wiretapping DF component connects to and the media becomes the AF for the DF components. So the DF just need to send a command to the mediation and the mediation will broadcast it to all the MSC behind the mediation device. The is a type of AF which will be described about here.

DF basically can interpret messages from IAP of different vendors which runs in different formats. These messages are then in turn translated into single protocol. CF only needs to understand one protocol from the DF. DF can be a single workstation. In mission critical environment, active and standby or cluster type of configuration solution can be implemented.

CF belongs to Law Enforcement Agency domain. It is where law enforcement official listen or record the communications about the suspect subscriber's identity which has been provisioned in the AF. It consists of six components which are recording workstation, monitor workstation, jukebox archiving system, CD burner, server workstation and CDC gateway.

The works here continues from my paper presented in SPIC 2010. Please refer to the paper in Appendix A.

CHAPTER 2

LITRITURE REVIEW

This chapter is taken from paper in [4]. The CALEA architecture is behind the current and emerging telecommunications services. Call data and call content is not clearly separated. The assumed bandwidth for the call data delivery is not enough to transport the messages across.

Wiretap subject alone is enough to launch an attack. Not only call content cannot be captured, the information itself can be modified without traceability. Call records can be hidden. This section is a summary of the works the researchers in Pennsylvania talks of the vulnerability of the CALEA architecture.

2.1 Call Data Channel (CDC) Resource Exhaustion

The J-standard not adequately address the engineering aspect of call data. Comparatively, more focus has been put on the call content than call data. Problems with bad CDC provisioning are not stated in the standard. Suspect under surveillance can generate non-average traffic which can overwhelm the CDC resources.

The J-Standard is written based on a single ISDN B channel (64kbps) for CCC. Messages are discarded without notice when the CCC is congested. Signalling generated by modern devices at transfer rate exhaust the CCC bandwidth at high rate.

Besides low bandwidth, the CCC is designed based on a single unreliable and heavily multiplexed resource. All the Intercepted Related Information (IRI) from the AF processed by the DF and then sends down to a single CDC through the first-come-first-server fashion. All the targets under surveillance shared this single CDC with the assumption that all or most of the targets does not go online around the same time.

J-standard was developed during the time where the signalling messages going through the network is about the same type. Nowadays there are various types of messages are exchanged between the network equipment. To differentiate between these messages, more information needs to be put into the messages to describe it.

CDC messages can be corrupted beyond recovery. To correlate the CCC with the CDC, both the messages carry an ID. For example, an LIID (Lawful Intercept Identification) is used to correlate the call content with the call data. If the LIID is lost or corrupted, no correlation can be established between the CCC and the CDC. Another example is the CCOpen from AF to signal start of call content and CCClose message from AF is a single to terminate the communication. If the CCClose message is lost, the call content will be un-usable and considered corrupted.

Although high bandwidth between the TSP and the LEA is possible, the TSP is restricted to design their network following J-standard 64kbps upper limit of CCC. The bandwidth is sufficient to handle the traffic when the standard was developed. However, with new service brought online, the rate of signalling is beyond the maximum link capacity.

Lawfully Authorized Electronic Surveillance Protocol (LAESP) messages are generated based on the subject's online activities. This feature allows the subject to control the amount and the rate of messages to be generated. With malicious intention, it can be used to overwhelm the CCC capacity. Each of LAESP message contains at least a timestamp, a case identifier, calling/called party identify and may contain the identity of the AF which to facilitate the different cases handling in the LEA end. For example, the one-bit information to tell whether the phone is on-hook or off-hook requires about 100 bytes of a LAESP message represents such condition. There is also messages generated from the higher-level TSP relate to "call released" which further put the attacker in the advantage to launch an attack.

2.1.1 ISDN Feature Keys

ISDN users have direct control of the supplementary feature to generate messages related to call forwarding, call waiting, call holding and others. The feature is specified in the Q.931 signalling protocol which support both stimulus mode and functional mode.

In stimulus mode, the entire subject signal is sent over to the switch whenever a function button is pressed on the handset. When the AF receives such signals, it does not need to interpret or validate the signal and it straight away send it over to the DF. In function mode, it is a computer based communications.

Looking at the byte size of the LAESP message, a Q.931 feature key message is 6 bytes and the corresponding Subject Signal LAESP message size is 82 bytes. Assuming it is a X.25 frame, the subject just need to generated 94.11 signalling messages per second to exhaust the 64kbpds CCC bandwidth. The target signal to the TSP through Basic Rate Interface ISDN is 16kps. So the subject just takes up 4.52 kbps out of 16 kbps of bandwidth. This is much within the subject capability to generate messages and still have much room to exhaust the CCC link capacity.

2.1.2 SMS Messaging

Short Message Services (SMS) is part of the intercepted messages. Whenever there is a SMS originating or terminating message, a corresponding PacketEnvelope LAESP message is generated which contains the calling party, called party, message content and other information. The PacketEnvelope message size comes with about 180 bytes size. The attacker needs to generate about 44 messages per second to overwhelm the 64kbpds CDC. One possible way to send about 44 messages per second is to turn off the destination phone and use another 44 messages from source mobile phone to send 44 messages one by one. Turn on the destination

phone after the 44 messages have been sent. The target will get the messages as these messages are queued in the Short Message Service Center when the destination phone was turned off.

Besides offering service to exchanging SMS between mobile phones, SMSC can also receive messages coming from the internet. It has been shown that such external network connection open doors for DoS attack in cellular networks. Sources in the internet can simultaneously send many SMS to the target phone. To reduce such a risk, TSP has rate limiting and attack detection at the SMSC and the submission interface from the internet. As SMS is gaining popularity, TSP may bring up the SMS rate to bring more services while the CCC bandwidth remains unchanged.

2.1.3 VoIP Signaling

J-Standard is referenced by vendors in the VoIP industry as the standard does not directly address such technology. Evaluation is made on using PacketCable specification.

VoIP signalling data can be generated at broadband rate. In addition, routing policy put priority on VoIP data over non-VoIP IP traffic. Both of these conditions can exhaust the 64kbps CCC bandwidth.

As per the PacketCable specification, a completed VoIP call consist of Origination, CCCOpen, Answer, CCChange, CCClose and Release where the CCCOpen, CCChange and CCClose is delivered for wiretapping. Based on the rate and the size of the messages, the CCC bandwidth again can be easily all used.

If the signalling attacks for rapid hold, transfer, or call forwarding signals are launch, overwhelming the CDC is easily done. Statistical call model used to build the wiretap resources is not applicable in such a scenario.

2.1.4 IP Flow

The J-standard requires the mobile internet activities are to be intercepted. PacketDataEstablishment and PacketDataTermination are generated when the subjects go online and offline in which each message comes with the network connection establishment messages. For TCP, it is the three way handshake and for the case of UDP, it contains source IP, source port, destination IP and destination port. These data comes under the PacketDataFilter message with some other information in there as well. The message must be at least 160 bytes. Only 40 flows of open or close to exhaust the 64 kbps bandwidth. The 40 flows take up only 16kbps bandwidth from the target which the subject can easily generate.

2.2 Inbound Attacks

Attacks can be carried out by other parties other than the target. CCC resources can be overwhelmed by call forwarding service. One CCC is allocated for each call instead of per service. With CCC using up much more bandwidth, a number of call forwarding generated can overwhelmed the CCC bandwidth. The target will be able to evade his or her communications to be monitored.

2.3 Injecting Uncertainty into Packet Traces

Attacks can corrupt the IP flow. The following are the techniques described.

2.3.1 Confusion

False information can be sent out where there are probes in the network doing eavesdropping. This false information causes confusion for analysis of information. There has been suggested future works to counter such an attack by building probes which can learn the pattern of attacks and knows how to filter out such false information. Basically to have some artificial intelligence in the probe [5].

2.3.2 Subject-Oriented cdma2000 Timestamps

Time stamp is taken from the LAESP messages where it payloads is IP packet. This is not required if the application-layer protocol has this timing information. This information can be modified which prevents the correct re-construction of the of the IP flows. The evidence collected for the modified time may be stand as evidence in court.

2.3.3 Loss of cdam2000 Direction Information

Information about the direction of the IP is not there, the source and destination network addresses in the IP header are used. The information can be modified by generating forge IP packet which render it useless or misleading.

2.4 In-band signaling within Service Provider

AF delivers the status of the phone line whether it is in use or ideal to the DF through in-band signalling. For ideal line, the "C-tone" is sent to the DF and DF will then release the CCC and send the CCClose. The CF will stop all recording. The attacker can apply the "C-tone" to send a false message that he or she is ideal but actually the reverse case is true.

2.5 Alternatives Methods to Secure the CALEA Architecture

The following are the possible alternatives methods that can be used to secure the CALEA architecture summarized as following:

- Implement the Defence and Offense Wall architecture in the delivery link between the access function and the collection function
- Integrating Message Queue into the CALEA architecture

The following sections describe these proposed alternative methods in more details.

2.5.1 Passive Provisioning with DOW [method 1]

Remove the DF from method 1 with AF functionality as passive probe and the CF remains. The bandwidth CCC link which is vulnerable to the attack can be removed. The solution comes with the built in intelligence from the works of variant version of DOW (Defence and Offense Wall) [6] to protect against DoS. The following shown the suggested wiretapping architecture:

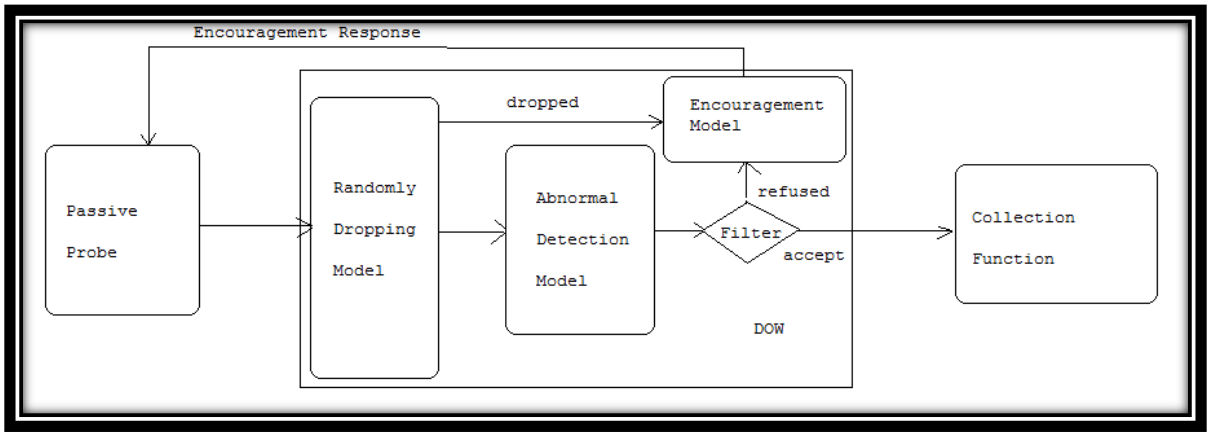

Figure 2 AF + CF with DOW variant

The passive probe can be configured to do traffic inspection to replicate traffic which it has been configure to capture. It can be configured to replicate frames through the DOW to final destination CF. In the field, there can be a number of probes deployed in various location in the network which all goes back to a wiretapping system as shown in the Figure 5 where PP stands for passive probe. The passive probes can be treated as the clients to the DOW.

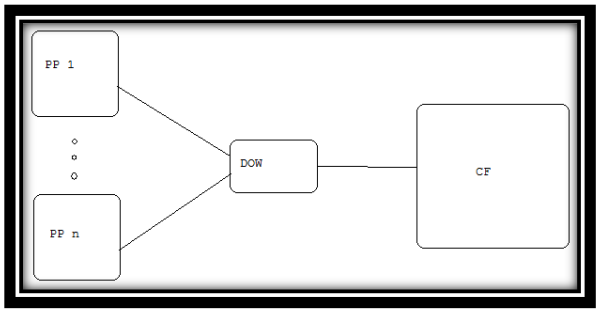

Figure 3 Block diagram view of the multiple probes interception

The DOW will get all the intercepted traffic from the passive probe. It will first goes through Randomly Dropping Model where the selection of dropping traffic is based on probability of overloaded session connection requests. No connection will be dropped if probability is zero which indicates no overload condition. If the calculated probability of overloaded session is high, the link will be dropped. The encouragement model will send feedback message to those clients whose link has been dropped or refused in case those legitimate session actually drop and trying to re-establish connection so that the client attempt to re-establish connection.

The following Figure 4 is the original design of DOW [3].

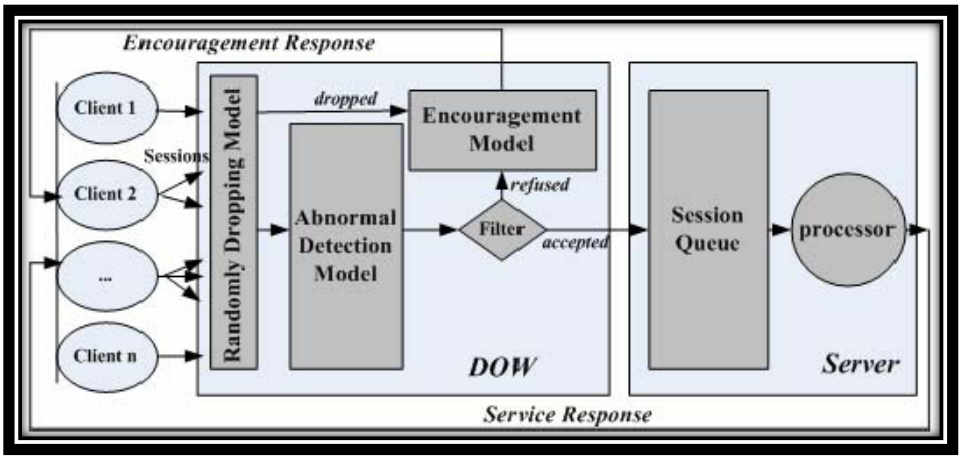

Figure 4 Original Design DOW

As can be seen, the service response part has been removed from the setup in the method here. Since wiretapping system silently listens to the network traffic, the passive probes should not send in any request directed to the wiretapping system and the wiretapping system should not give response. It is integrated into the setup to protect the wiretapping system from session with malicious intend sent at higher than normal rate.

The Collection Function (CF) remains the same as what has been mentioned earlier. It captures all the messages that it received from Passive Probe through the DOW.

2.5.2 CALEA Architecture with middleware Message Queue [method 2]

This method explores Message Queue option to pass all messages through the limited bandwidth in the delivery link from delivery function to the collection function. The following is a block diagram of message queue.

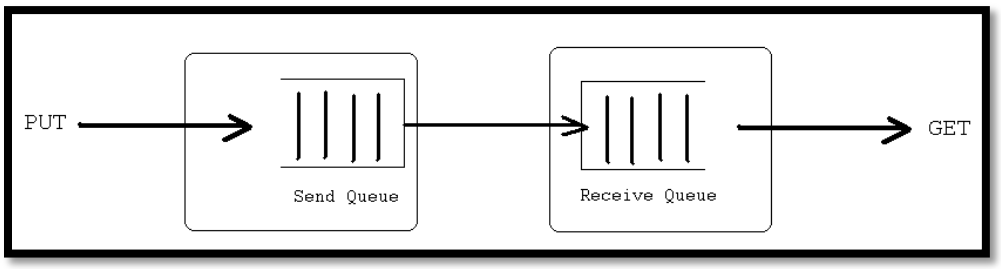

Figure 5 Message Queue [2]

If an the link was overwhelmed whether unintentionally or with malicious intention, the Message Queue takes care of making sure the all intercepted data reach its remote end which is the collection function. It will still deliver the message even if the collection function is unavailable to receive the messages.

The following is a diagram of such an implementation.

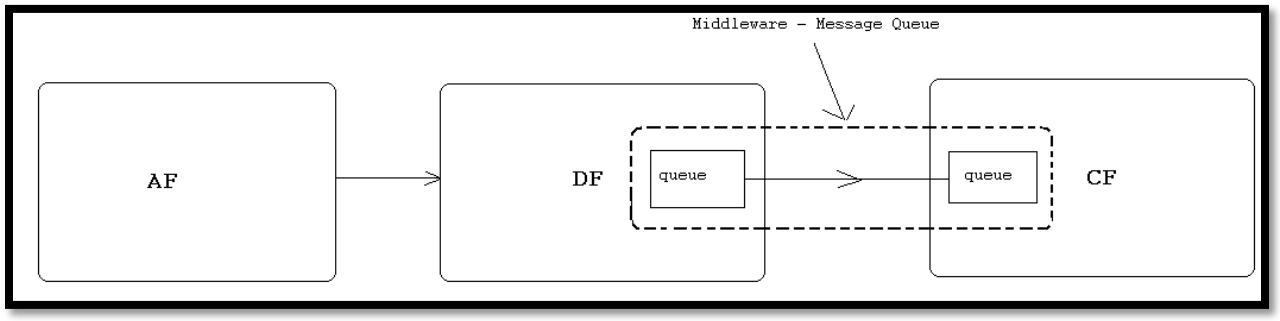

Figure 6 Integrating Message Queue in the CALEA Architecture

The delivery function put all processed messages into the queue through API. The rest of the messages delivery will be taken care by message queue to send it over to collection function.

Once the message reached the collection function's queue, collection function will do a get to take the messages out of the receive queue.

Due to the reliability and performance of message queue, banks have been using it for handling critical accounts transactions without duplication. A few vendors in the market produce message queue software. For example, IBM produces message queue software called MQSeries which is now called WebSphere MQ. Microsoft produces an alternative product called MSMQ.

2.6 Chosen Solution: Split Huge File to Minimize Risk

The contribution here is to divide a large file into smaller files if the original file exceeds a certain boundary of file size during link transfer rate congestion. For designing a production system, the decision of the boundary to divide a file should be about 45.5K bytes to start with and then tuning the value from there. The reason for the selecting this boundary to start with is based on typical target-to-target call file size of 91K bytes taken from test call sample during field implementation test calls. The breaking of the file is at application layer as the boundary to break a file is very application dependent. Congestion control at the lower layer may not work that well it is designed to take care of a more general application. For a single target call, either target origination call or target termination call, the call records should be about half the size of 91K bytes.

2.7 Reasons for Chosen Solution over the Other Two Methods Designs

In view of the following reasons, the chosen method is selected instead of method 1:

- From working experience with the Law Enforcement Agency (LEA) in the field, the end users tend to favour more towards the usage of active provision then the passive provision described in the first method. The cost of implementing the passive provisioning is higher compared to active provisioning. The high number of probes in the

field takes more effort to be managed and to be maintained. Whereas, with active provision, the cost of maintaining the system is shared between the LEA and the Telecommunications Service Provider (TSP). The TSP needs to enable the LI features in the call routing machines (i.e. Mobile Switch Center) and to manage it. The LEA to invest in setting up the structure to connect to the TSP's machines and one monitoring centre. One monitoring centre can be connected to many TSP's machines.

- It is impossible to training the model all the possible attack models. The consequence of losing important messages can have serious implication in assisting LEA investigation should the margin of error in pattern classification is high.
- The risk is higher to set up probes in various locations in the network where only part of the information is captured. Comparatively, the chosen method with one centralized Delivery Function provisioning the switch centres across the regions which have more complete information.

The following are the reasons for not selecting method 2:

- With the data processing sequence of FIFO, the data in the middle of the queue will not be processed if the processes which picks up the first data in the queue hangs.
- There are some proprietary middleware which can be closed system. The flexibility to integrate with multi vendors' environment is limited.
- Networks using MPI (Message Passing Interface) has an effect on long posted received queue which slows down the message delivery. In addition, high CPU resources is been taken up for messages which came from the pre-posted queue. Secondly, network latency increases as unexpected message queue length increases.

There are TCP congestion control features available at the lower layer of the network models. However, the argument here is that the solution here in breaking the file at the

application layer is better for the application here. The reason is that the boundary to break a file is very application dependent. Congestion control at the lower layer may not work that well as it is designed to take care of a more general application.

CHAPTER 3

DESIGN

The system is designed to break large files into smaller files based on the size of the file exceeding certain threshold. This is to minimize the risk of losing information if the link to LEA goes congested. The following diagram is an overview of the process flow in the design:

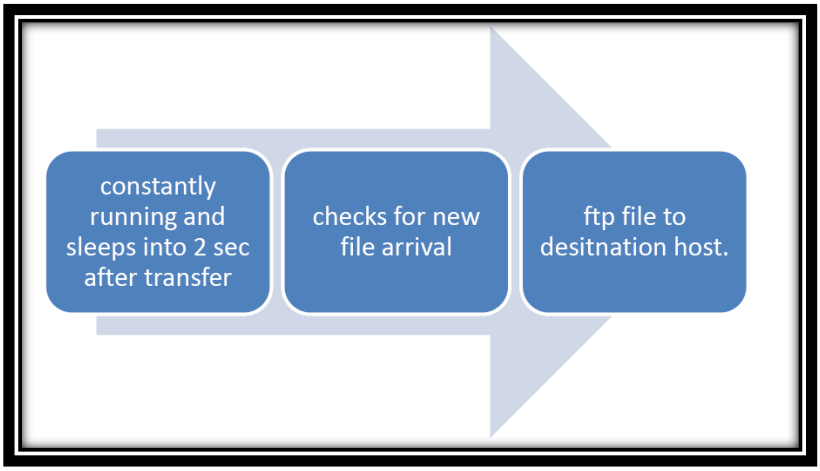

Figure 7 Process Overview

JMeter software is used to simulate AF to generate network traffic to DF. The generated traffic is FTP file over from the simulated AF to the simulated DF. The configuration is described in the IMPLEMENTATION chapter.

Initially, a script starts up with infinite loop to call another script to check for delivery of new file. This part simulate the DF constantly listens for data delivery in the INI2 interface. When new file is being delivered, it will move the file into another location for further processing.

The main innovative part of the project is described as follows. The script in the simulated DF checks whether there is congestion in the delivery link to the FTP server which is a simulated CF. If the ping command time out, the link is categorized as congested. The file will

be broken down in the smaller parts for delivery to remote simulated CF. In addition, the script also checks for the delivered file size. If the file size exceed a certain threshold, the file also be split for delivery. If neither of this two conditions is true, the delivery link is consider being congestion free and delivered as one file. The production solution neither has the feature of check file size nor breaking the files into smaller units to deliver the information. The following Figure 8 is a flow chart of the script

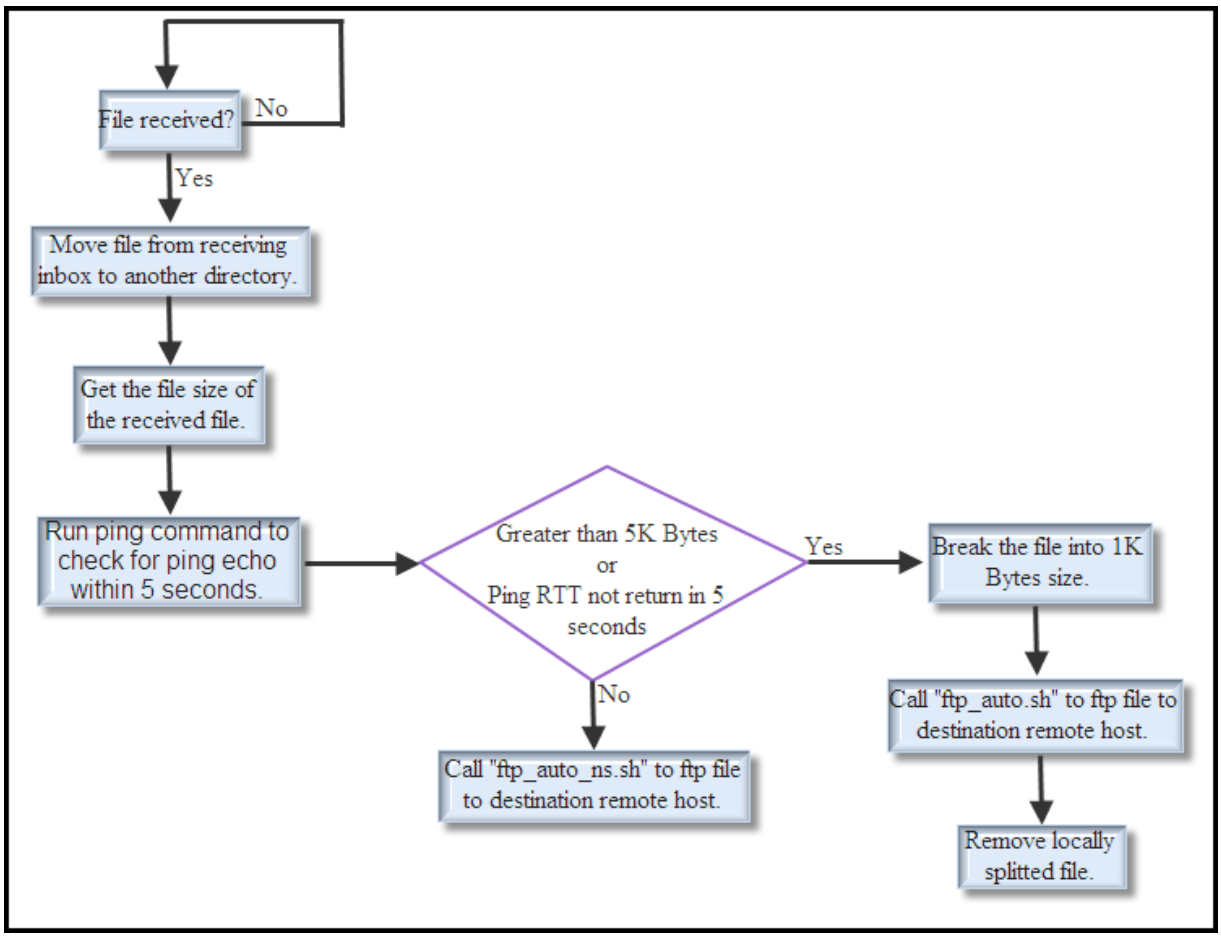

Figure 8 Flow chart of "filet.sh" script

Transfer rate overwhelming simulation is done by using the Linux tc command which stands for traffic control. The actual command used to limit transfer rate is described in the IMPLEMENTATION chapter.

To simulate the CF module, an FTP server application [8] has been downloaded and installed in another laptop. The screen shot of the application is provided in the IMPLEMENTATION chapter of this report.

CHAPTER 4

IMPLEMENTATION

An overview of the lab setup is shown in Figure 9. Starting from JMeter, a file is FTP over to the DF simulator. The DF simulator processes the file and then FTP it over to the CF simulator through a router. The medium of connections between laptop A and laptop B is either air or wired (cable) medium.

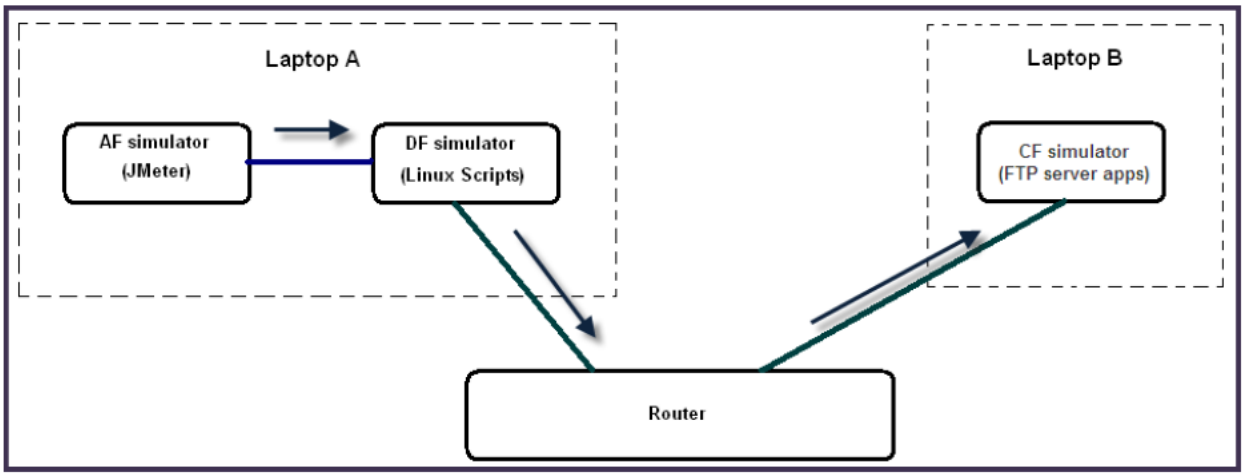

Figure 9 Overview of tools used in the experiment

The following Table 1 list down the tools selected and configured for running the experiment as a proved of concept the proposed solution.

Simulated Modules in the CALEA Architecture	Tools Used in the Experiment
AF (Access Function)	JMeter
DF (Delivery Function)	Scripts running in SuSE Linux
CF (Collection Function)	FTP Server software

Table 1 Tools for Lab Setup

4.1 AF Simulator Setup

JMeter installed in the laptop machine A. It is then configured to FTP a file over to the destination host simulated as DF. The configuration add the elements to setup the profile to do FTP. Next, the destination host or the simulated DF IP address, the text message to be sent, the ftp account user name and password in the simulated DF host are entered. The following is a Figure 10 of the JMeter configuration with labels inserted for illustration. A sample text file used is used for all the experiment run in this work here. The selection of the sample text file has been mentioned in earlier chapter.

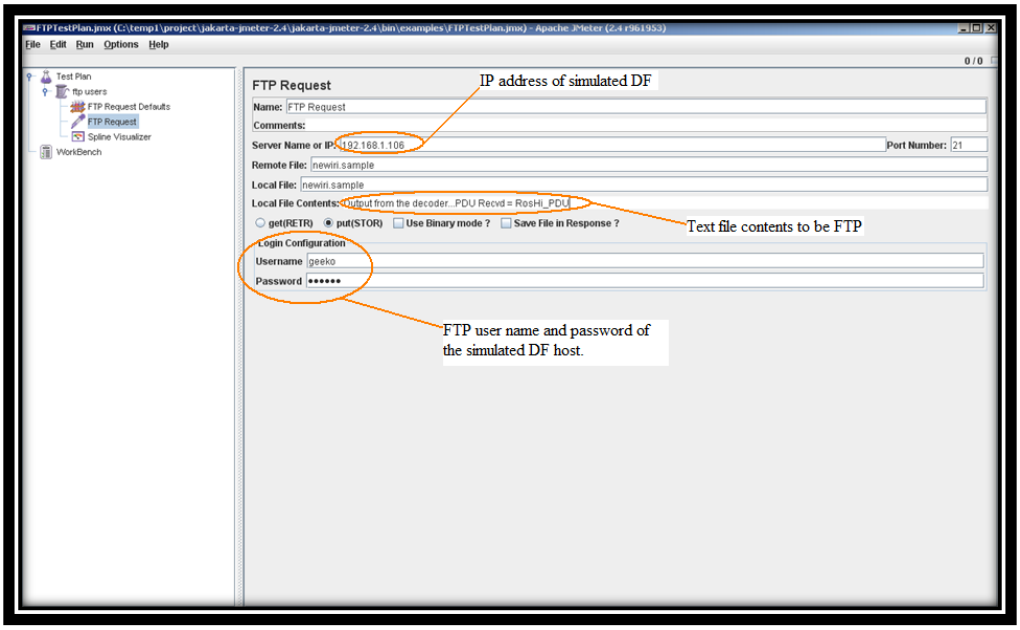

Figure 10 Snap shot of JMeter configuration for FTP request

4.2 DF Simulator Setup

Bash shell script is written to simulate a DF. The script is written to run on a Linux environment in a virtual machine. SuSE SLES 10 is the chosen Linux version which runs in a VMWare player for this virtual machine. The details of the script have been described in the DESIGN chapter. Refer to the Appendix C for the script codes.

To simulate limited transfer rate, Linux tc (traffic control) command is used to limit the bandwidth only to the destination IP address of CF simulator host. Referring to Figure 11, the "Transfer Rate" is the maximum and the mentioned destination IP address.

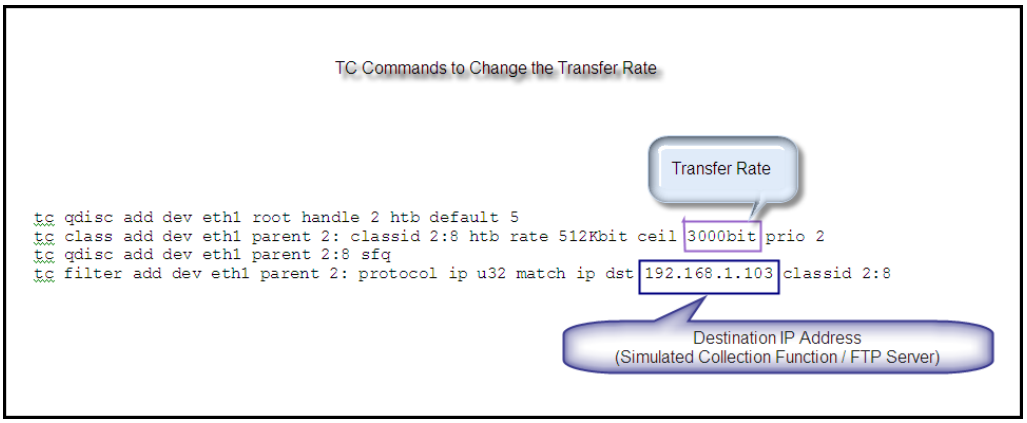

Figure 11 Linux tc command s to Change the Transfer Rate[9]

4.3 CF Simulator Setup

To simulate CF, a FTP software is installed and configured receive and safe the data coming from the DF. It is configured to listen to local IP address as shown in the Figure 12.

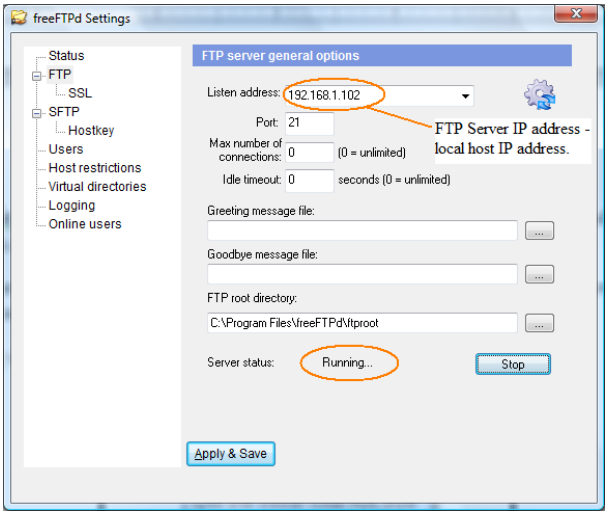

Figure 12 Screen shot of the FTP software

The decision boundary to break a file has been mention in the chapter titled Chosen Solution: Split Huge File to Minimize Risk chapter.

CHAPTER 5

TESTING AND ANALYSIS

The solution is evaluated with lab setup comes with solution versus one without solution under different limited transfer rates of the delivery link. The delivery link is between the simulated DF and simulated CF. File is FTP from the JMeter (simulated AF) through the virtual machine (simulated DF) and finally reached the FTP server application (simulated CF).

The following Table 2 is the experimental result where wireless medium is used:

File Size Received	Transfer Rate [K bps]											
	1			2			3			10		
Bytes	**w/o soln**	**w soln**	**Diff.**	**w/o soln**	**w soln**	**Diff.**	**w/o soln**	**w soln**	**Diff.**	**w/o soln**	**w soln**	**Diff.**
4,992	4,992	4,992	0.0%	4,992	4,992	0.0%	4,992	4,992	0.0%	4,992	4,992	0.0%
12,429	12,429	12,429	0.0%	6,641	12,429	46.6%	10,889	12,429	12.4%	12,429	12,429	0.0%
25,421	19,381	25,421	23.8%	25,017	25,421	1.6%	25,421	25,421	0.0%	25421	25421	0.0%
32,170	17,971	32,170	44.1%	30,720	32,170	4.5%	32,170	32,170	0.0%	32081	32170	0.3%
42,992	34,964	42,992	18.7%	40,625	42,992	5.5%	42,992	42,992	0.0%	42,992	42,992	0.0%
50,194	36,379	50,194	27.5%	46,293	50,194	7.8%	49,125	50,194	2.1%	50,194	50,194	0.0%
56,626	42,026	56,626	25.8%	47,704	56,626	15.8%	56,626	56,626	0.0%	56,626	56,626	0.0%
63,364	49,125	63,364	22.5%	56,207	63,364	11.3%	63,364	63,364	0.0%	63,364	63,364	0.0%
70,002	53,376	70,002	23.8%	64,699	70,002	7.6%	70,002	70,002	0.0%	70,002	70,002	0.0%
76,658	64,684	76,658	15.6%	71,780	76,658	6.4%	76,032	76,658	0.8%	76,658	76,658	0.0%
87,167	73,169	87,167	16.1%	80,276	87,167	7.9%	84,524	87,167	3.0%	87,167	87,167	0.0%

Table 2 Test Result (wireless medium setup)

For comparison purpose, the test setup with 1K bps transfer rate (delivery link) has been run using wired medium setup. Reason for not running the other transfer rate is that wireless and wired medium likely to have similar behaviour based on the observation made in both the wireless medium and wired medium. The following Table 3 is the test result.

File Size Received	Transfer Rate [K bps]		
	1		
bytes	w/o soln	w soln	Diff.
4,992	4,992	4,992	0.0%
12,429	3,816	12,429	69.3%
25,421	3,816	25,421	85.0%
32,170	17,964	32,170	44.2%
42,992	26,471	42,992	38.4%
50,194	36,379	50,194	27.5%
56,626	50,547	56,626	10.7%
63,364	47,704	63,364	24.7%
70,002	54,796	70,002	21.7%
76,658	61,869	76,658	19.3%
87,167	70,368	87,167	19.3%

Table 3 Test Result (wired medium setup)

The selected sample file is an actual messages delivered to CF taken during on-site testing. Refer to Appendix B to read a partial display of the sample. The messages had been taken from CF after CF has received the intercepted data and converts it into a text messages.

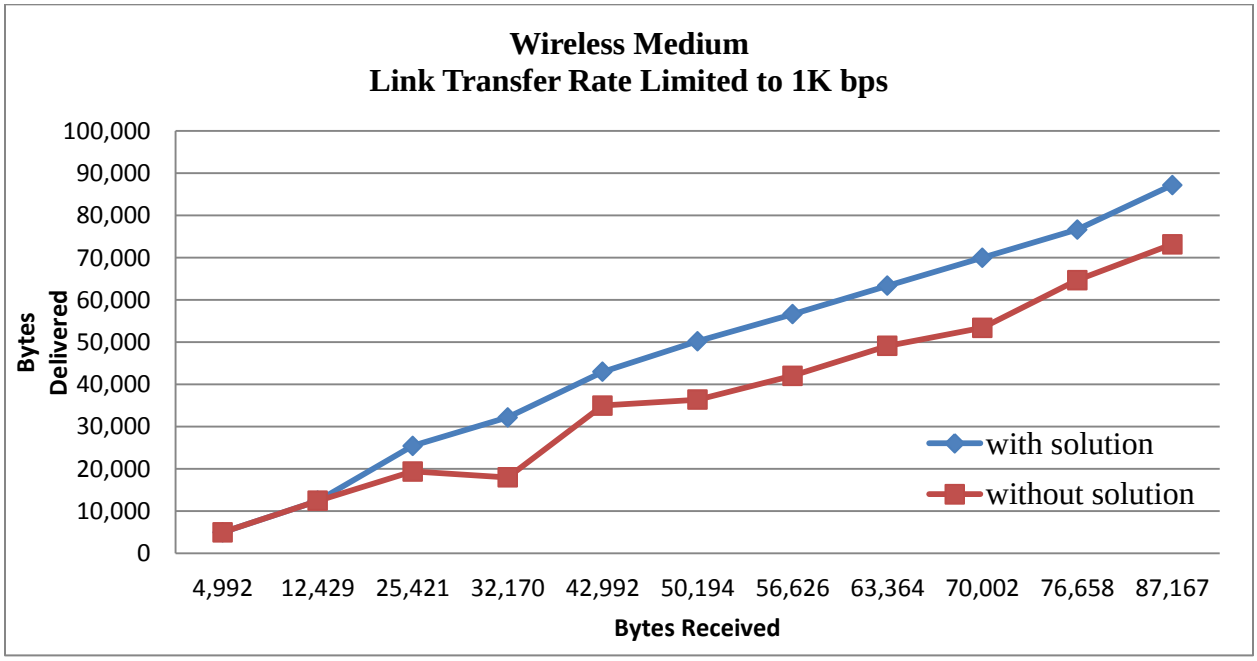

Figure 13 Test Result (wireless medium with delivery link setup at 1K bps)

Through wireless medium, Figure 13 is the test result of a comparison between one with and the other one without solution with a delivery link transfer rate limited to 2K bps. When the received file size is very small, both with and without solution can deliver the file through the congested delivery link. When the received file size increases, the one without solution starts to fail to deliver the whole received file while the one with solution delivers the complete file.

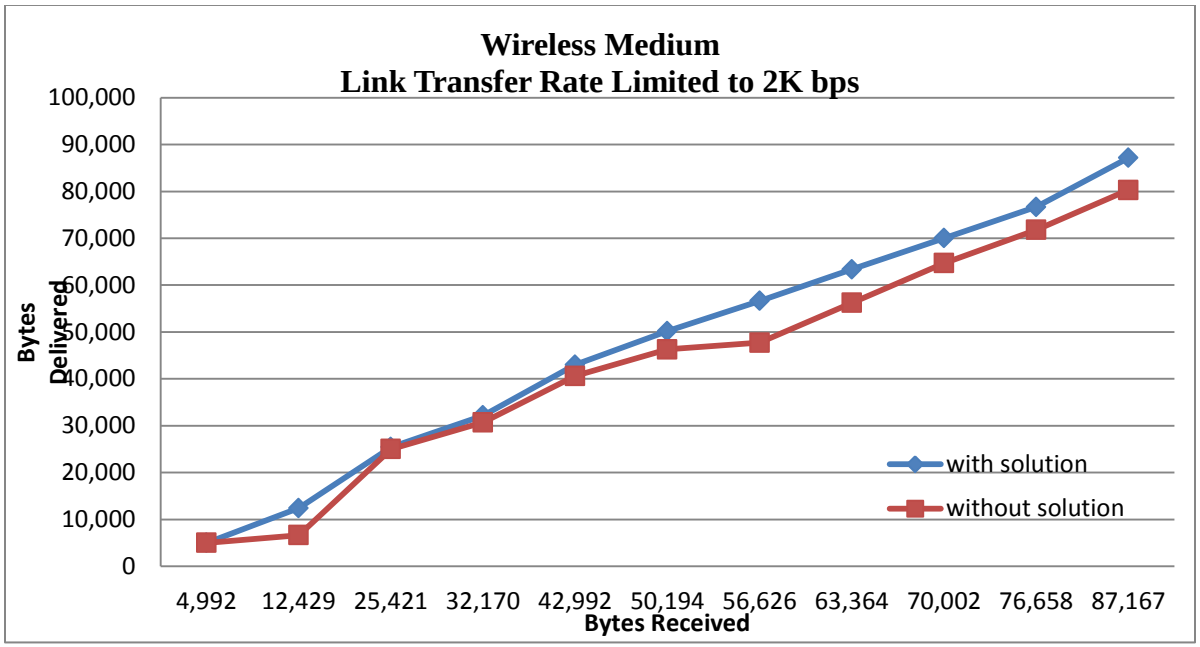

Figure 14 Test Result (wireless medium with delivery link setup at 2K bps)

Similar behaviour has been observed in Figure 14. With the transfer rate of the delivery link increased to 2K bps, the difference in delivering the whole received files to the FTP server is lesser compared to 1K bps transfer rate.

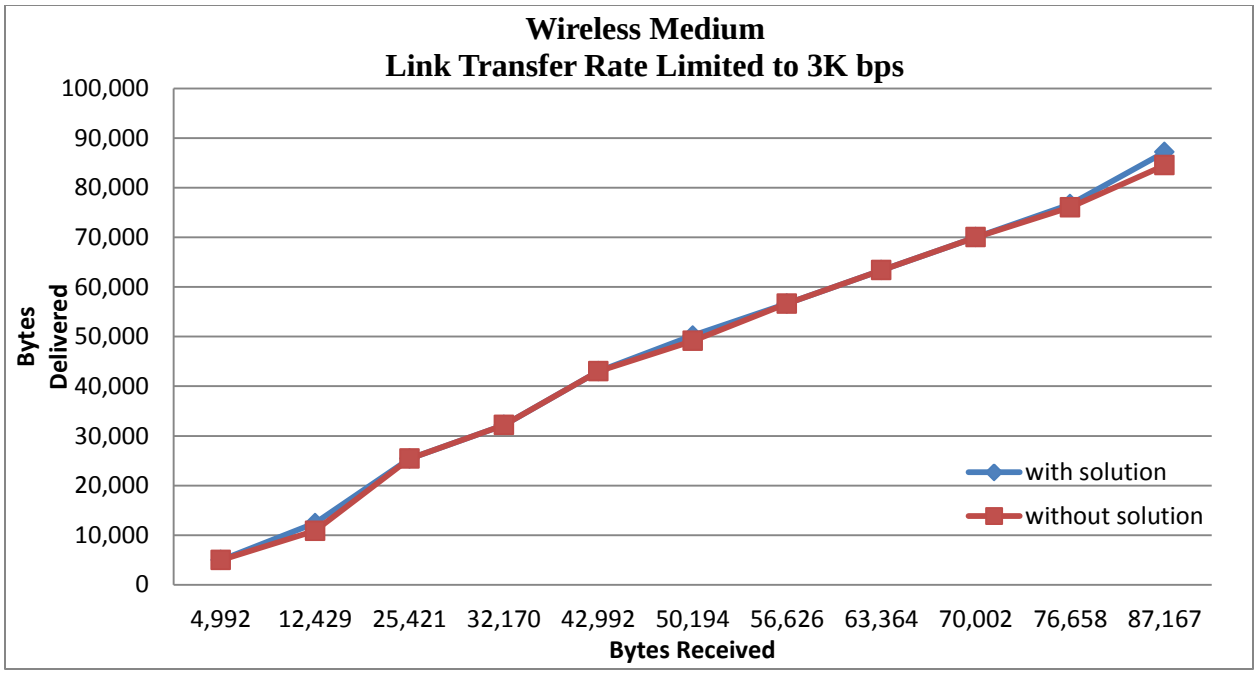

Figure 15 Test Result (wireless medium with delivery link setup at 3K bps)

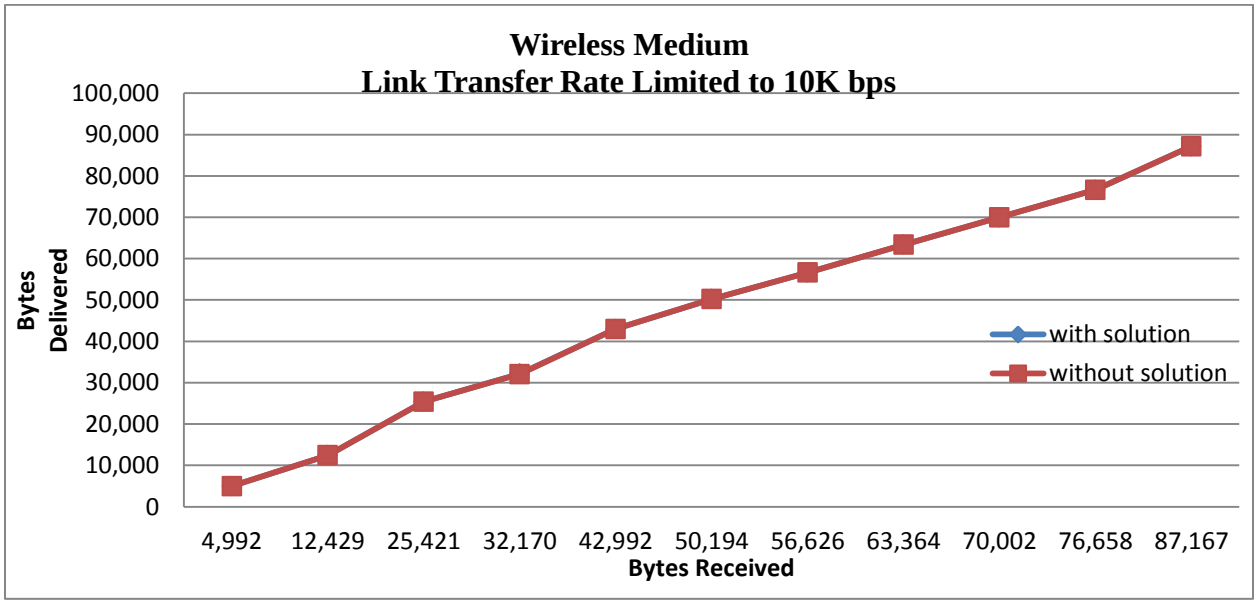

Figure 16 Test Result (wireless medium with delivery link setup at 10K bps)

Reading the Figure 15 and Figure 16, the gap in delivering the received file decreases between the one with solution and the other one without getting smaller. As the transfer rate of the delivery link getting less congested, both the one with and without solution eventually can

deliver the whole file. However, when the transfer rate drops below a certain threshold, the one without solution starts to fail to deliver the complete file to the destination.

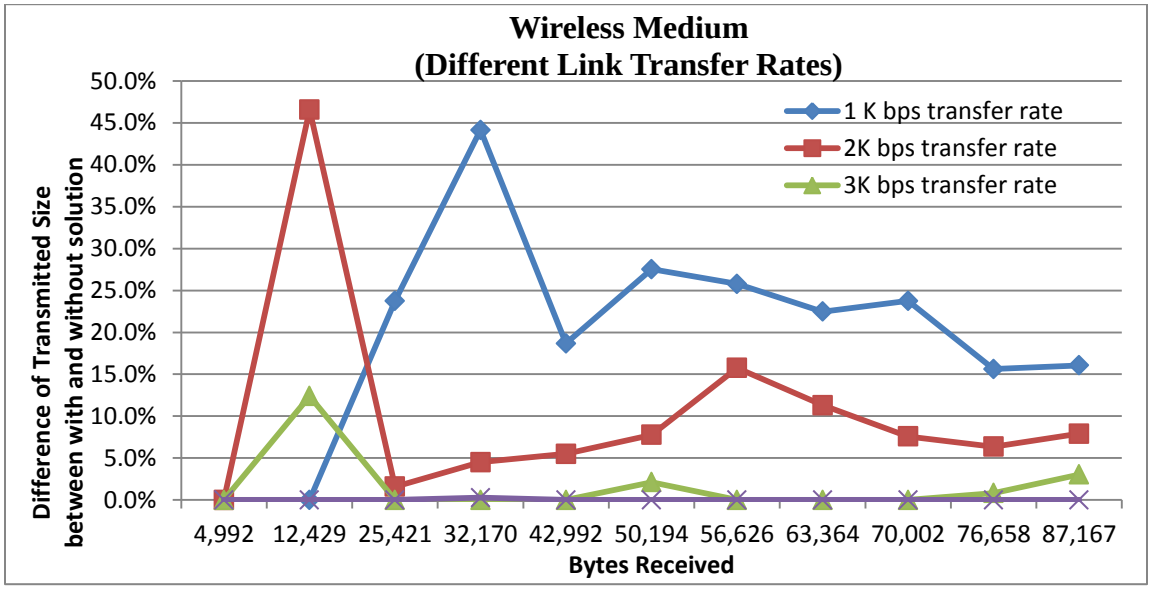

Figure 17 Difference between with and without solution in delivered file size

Referring to Figure 17, the difference of delivered file size of the one with solution and the one without solution decreases. A test run of sending 114K bytes size file at 1K bps link rate shows that the gap between the two setups remains with a percentage difference of about 12%. So it is likely there will be lost of data when sending even larger file. It seems that during low transfer rate of the delivery link, the frames place into the network is too slow to consume the data already placed inside the TCP transmit buffer. Note that no testing beyond the 45K bytes file size is carried out as this is about the file size for a single call.

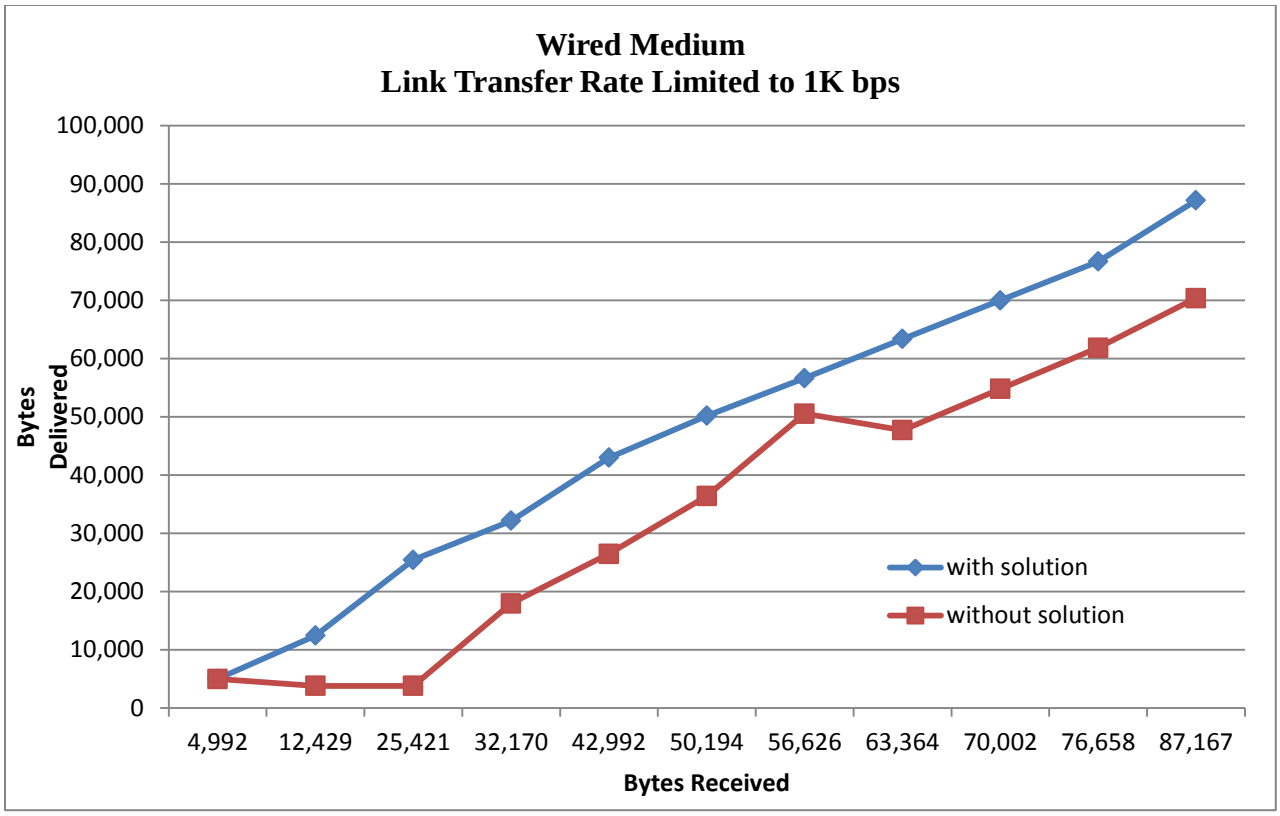

Figure 18 Test Result (wired medium with delivery link setup at 1K bps)

Figure 18 and Figure 19 are the test results to see to how the solution behaves through a wired medium. From Figure 18, the difference curves of the wired and wireless solution showing signs converging to about 20%. Difference between the two is not much. One uses electro-magnetic wave through air medium to transmit data while the other using copper medium to transmit electrical signals to transmit data.

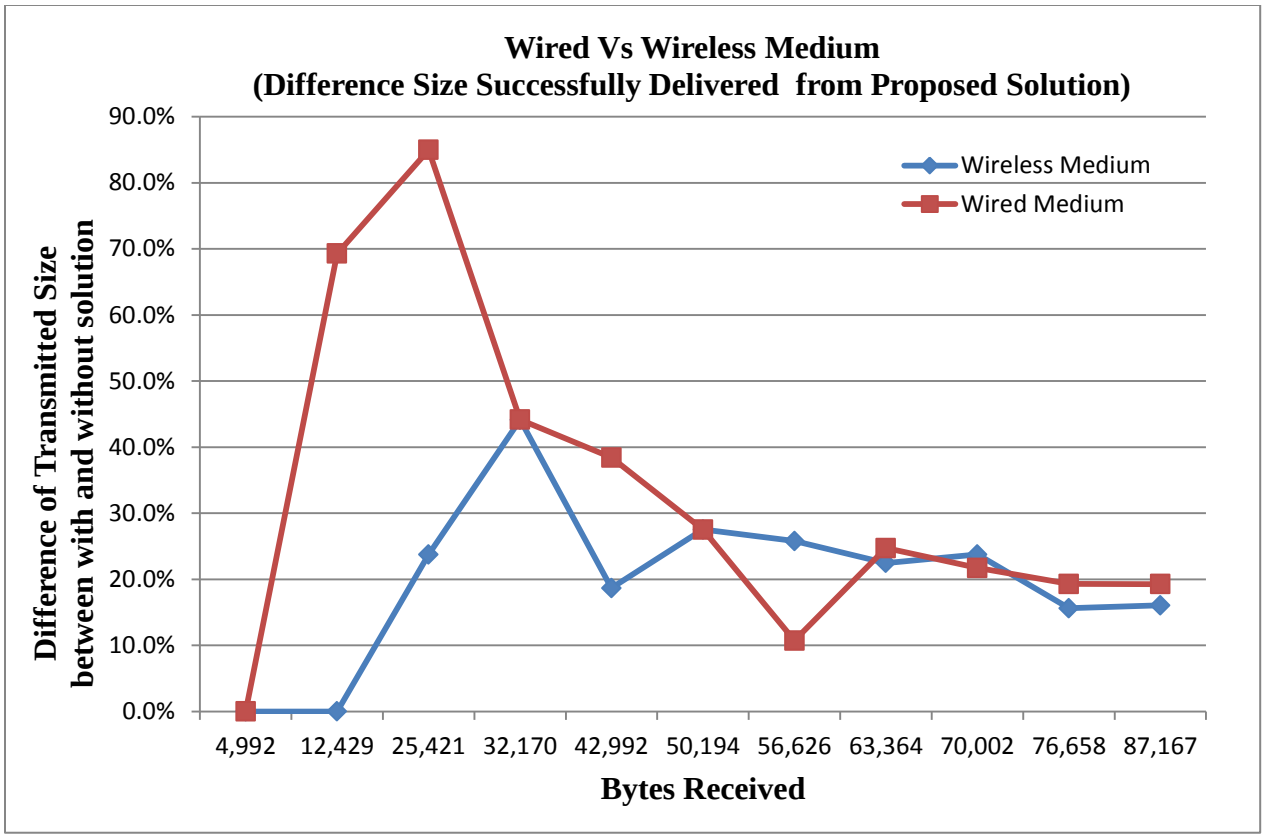

Figure 19 Difference between with and without solution in delivered file size Wireless and Wired Mediums

Despite that the proposed solution has been giving positive result in functionality, it does not do well in performance. By breaking files into smaller parts, it incurred some overhead in transferring the file. In addition, the Linux utility tools to simulate a constant congestion environment. A life system likely to have a random congested link environment. Also, the VMWare player running virtual machine as a simulated DF is not a real machine. There are room for improvement here and for future works. There is still room to improve the performance of the system and other aspects of it.

CHAPTER 6

CONCLUSION

The works here started with an introduction about CALEA architecture and a literature review of various attacks which can be launch against it. A proposed solution is provided, its design and its implementation is described. Next, tests are run to evaluate the proposed solution with the analysis of the result provided. It is hope that the concept behind the works here can be used to improve the security of LI system and make our world a safer place to live in.

Reference

[1] Craig Silverman, “A Hacker’s Tale”, Discovery Channel Magazine, August 2010.

[2] Steven M. Bellovin, Matt Blaze, Whitfield, Diffie, Susan Landau, Peter G. Neumann, Jennifer Rexford, “Risking Communications Security: Potential Hazards of the Protect America Act”, IEEE, 2007

[3] David Moore, Geoffrey M. Voelker and Stefan Savage, “Inferring Internet Denial-of-Service Activity”, USENIX, 200"

[4] Micah Sherr, Gaurav Shah, Eric Cronin, Sandy Clark, and Matt Blaze, “Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps”, ACM, November 2009

[5] E. Cronin, M. Sherr, and M. Blaze. “On the (un)reliability of eavesdropping”, International Journal of Security and Networks (IJSN), 3(2):103-113, 2008.

[6] Jie Yu 1, Zhoujun Li, Huowang Chen 1 , Xiaoming Chen, “A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks”, IEEE, 2007

[7] Keith D. Underwood, Ron Brightwell, “The Impact of MPI Queue Usage on Message Latency”, Sandia National Laboratories, 2004

[8] http://www.freesshd.com/?ctt=download

[9] http://pupa.da.ru/tc/

Appendix A

SECURING THE CALEA ARCHITECTURE AGAINST DENIAL OF SERVICE ATTACKS

LipEng Yong[1], *KongHua Lim*[2]

[1] University Tunku Abdul Rahman, Malaysia
[2] Nokia Siemens Networks Sdn. Bhd.
yongle@utar.edu.my , konghua.lim@gmail.com

ABSTRACT

Law enforcement agencies (LEA) around the world in eavesdropping are based on the Communications Assistance for Law Enforcement Act (CALEA) architecture. Unfortunately the system is vulnerable to all kinds of attacks especially to Denial-of-Service (DoS); whence, the importance of having a secured system to be used by the LEA to do surveillance work is imperative. This paper starts with describing the functions of the components and the delivery interfaces in the CALEA architecture. Next, the vulnerability of the system in general is been examined, and particularly in DoS attack. Finally, an architectural improvement of the security is provided against such attack by removing the Call Data Channel (CDC) interface and combining part of the collection function (CF) with Delivery Function (DF).

Index Terms— Telephone Interceptions, Eavesdropping, Greek Watergate, Greek Tapping, CALEA.

1. INTRODUCTION

Since the Watergate scandal in the 1970s, interception of information has subsequently tighten up, but then at that time technology was not that advance and not easily be accessed by the public and hence there were not many hackers around. Today things change not only in the technologies that are easily available for the public but also the number of people involve in the area of interception of information, and many are just for the self satisfaction of it.

The Greek Watergate in 2004-2005 was a security breach lesson in history where it happen in one of Greek's largest mobile network service provider involving high ranking officials' mobile numbers been secretly tap. The eavesdropping attack began around August 2004 Olympic Games in Athens and it lasted for about 10 months and the attackers were not caught [1].

ATM (Automatic Teller Machine) is one of the earliest distributed systems in business, and it security is paramount to all who use it. Yet on the 29th July 2010, an Australia News [2, 3] has this title"Computer hacker makes ATM spit cash" the vulnerability of it has been exposed. It has raised public concerned with ATM security.

Another recent case was from Las Vegas News reported in Malaysia's The Star newspaper on 02 August 2010 [4] that a snooping kit for mobile phones, which is in an unsecured mobile network, cost less than five thousand ringgits said Chris Paget. All these incidences have brought up the importance of having a secured system.

The architecture of J-Standard CALEA System (The telecommunications service provides (TSP) and Law Enforcement Agency develop the J-STD-025 or J-Standard.) basically consist of three blocks which are Access Function (AF) or Interception Access Points (IAP), Delivery Function (DF) and collection Functions (CF). Figure 1 shows the CALEA architecture [5].

The specific target numbers from the LEAs can be provisioned into the IAP. When the target makes or receives a call, call data related to the call (CDC) and voice or call content (CCC) will be delivered from the IAP to DF and then pass down to CF. CF locates in the LEAs domain where the activities can be monitored in real time or/and save into a storage device for later retrieval and evidence presentation. Although J-Standard was defined by US, the European's ETSI architecture is similar.

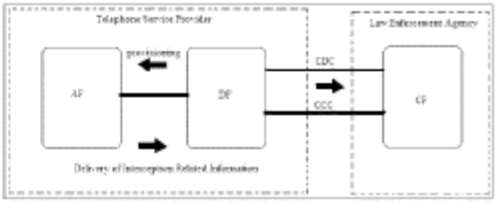

Figure 1: CALEA architecture

To illustrate the application for the CALEA architecture, the following Figure 2 [6] shows how CALEA model integrates into the VoIP system shown in an entity relationship diagram.

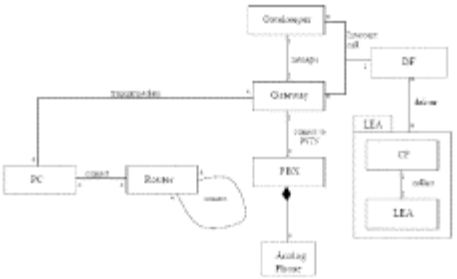

Figure 2: Entity Relationship Diagram for CALEA Model

The Figure 2 to show how the wiretapping system integrates into the VoIP. The vulnerability of the deliver channel limited bandwidth to transmit call data and call content is there for the attacker to exploit.

Pennsylvania researchers have found that in the J-Standard where the highest bandwidth in CDC configuration is a single ISDN B channel running at 64 kbps and the channel bandwidth can be easily used up by the messages generated by the suspect under surveillance [7]. The CDC messages include Answer Message, Close Message, Open Message, Network Signal Message and other messages. Since these messages come with overhead and payloads which incurred a bigger message size, it is easier for the hacker to deplete the CCC link capacity by sending the messages at lower transfer rate.

The architectural change proposed in this paper was to distribute the CF where some receiving processes in CF resides in the DF and the other CF processes remains in the Law Enforcement Agency. No more CDC channel in between the DF and the CF and hence eliminates the bottle neck. The following give some back of the wiretapping systems and elaborate the proposed changed.

2. MODULES IN THE SYSTEM

2.1. Access Function module

AF can be passive probe which is placed in the network to monitor the traffic. These probes need to handle traffic in high bandwidth and it has high processing power to do packet inspection in real time performing string search task or others.

Another type of AF can be all the Mobile Switch Center (MSC) in the TSP's mobile network. A second type of AF can be mediation network equipment which can exchange message with all the MSC. Many AF can be connected to a single media where the wiretapping DF component connects to and the media becomes the AF for the DF components. So the DF just need to send a command to the mediation and the mediation will broadcast it to all the MSC behind the mediation device. This is the type of AF which will be discussed in this paper.

2.2. Delivery Function module

DF basically can interpret messages from IAP of different vendors which runs in different formats. These messages are then in turn translated into single protocol. CF only needs to understand one protocol from the DF.

DF can be a single workstation. In mission critical environment, active and standby or cluster type of configuration solution can be implemented.

2.3. Collection Function module

CF belongs to Law Enforcement Agency domain. It is where law enforcement official listen or record the communications about the suspect subscriber's identity which has been provisioned in the AF. It consists of six components which are recording workstation, monitor workstation, jukebox archiving system, CD burner, server workstation and CDC gateway.

3. INTERNAL NETWORK INTERFACES AND HANDOVER INTERFACES

3.1. Internal Network Interfaces

As per the ETSI Standard, the Internal Network Interfaces (INIs) between the DF and the AF provided the following functionality:

- INI-1 provisioning suspect identifier into the AF
- INI-2 is for delivering data and signaling information related to the suspect which has been provisioned through INI-1
- INI-3 deliver call content to the DF

3.2. Handover Interfaces

Without law enforcement agency spending the resources and time to develop interfaces to all the network elements and protocols, the DF translates the raw target traffic from AF into a standards based interface to the CF. The ETSI standard defines three Handover Interface (HI) :

- HI-1 transports administration information between the LEA and the TSP
- HI-2 deliver Intercept Related Information (IRI) from the DF to CF.

- HI-3 transports the communications content to the CF

4. DENIAL OF SERVICE ATTACKS ON CALEA WIRETAP

It has been estimated that DoS attacks have been launched in the internet was about 12.8K attacks worldwide in the period of 3 weeks [8]. DoS attacks comes with a goal to deny legitimate users to information, applications, system or/and communications [9]. This paper is going to focus on DoS attacks against communications exploiting the CCC's limited bandwidth in the CALEA architecture.

Under provisioned CCC capacity, it can be easily overwhelmed by subjected generating high event rate while the subject still can make or receive calls [7]. If the CDC channel is busy when AF needs to send intercepted related information to DF, the messages will be drop without retry or notification. In addition, traffic in the modern day network can load the CDC with call-identifying information for voice calls, IP data and SMS messaging which load the CDC with many overheads. If the CDC channel is busy when AF needs to send intercepted related information to DF, the messages will be drop without retry. For example, either lost of CCOpen or CCClose message will cause the call content data to be incomplete and lost.

Confusion can be introduced in different layers of the TCP/IP model [10]. For VoIP lawful interception, the confusion can easily overwhelm the CDC.

5. PROPOSED CHANGE

The proposed changed is to split the CF into two portions where the part of the CF processes resides in the DF. The rest of the CF processes resides in the LEA domain. Figure 3 is a solution overview:

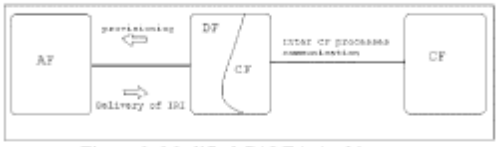

Figure 3: Modified CALEA Architecture

The AF acts as a client while the DF listens to the messages coming from the AF. Information about target's online activities is sent through these messages. On the other side, the DF is acting as a client role while the CF plays a server role in their respective components. With the proposed changed, instead of listening to a port in the CF component, this CF role is copied into the DF component and register itself on top of the same TCP/IP stack DF is registered on. The Figure 4 provides some illustration about the points just described.

Figure 4: DF and CF Components solution

When the DF received the intercepted messages, it will save the messages into a local storage device. DF opens a new file, records the signaling messages and then closes the file with completed messages. Message which starts with CCOpen and ends with CCClose are considered to be completed message. The local CF routinely checks the storage area for completed/closed files. CF will reads the file and sends it over to CF in the remote LEA's CF. While the previous solution drops the messages in congested CCC, the CF checks the network and resend it. It first tries to establish a connection, TCP/IP connection for example. If the network is busy due to depleted bandwidth due to attacks, the call method write( ) on the TCP socket will be blocked until it is cleared [11]. The connection process on client side goes to sleep. It wakes up later for another attempt to establish the connection until it is successful. The attempt should not be indefinite where it can be programmed a fix number of re-tries until it stops and an exception is thrown. The thread will release the lock to the local resources once the writing to the remote CF is completed.

The following is a Figure 5 showing conceptually how the components of DF application logic and CF application logic can co-exist together in the same host or the DF/CF center component. As mention earlier, the DF can pass down the messages and write it into the storage. CF read it and sends it over to the remote CF.

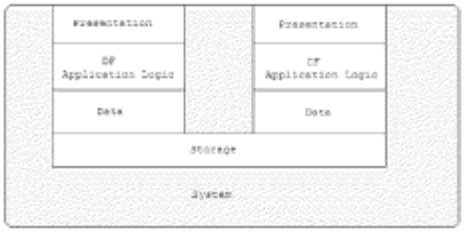

Figure 5: Middle Component: DF + CF

The presentation layer is the user interface for DF and CF respectively. The DF application logic relates to the DF function described above. The CF application logics represent to the local CF described above. Data shows the memory of the system which the application caches information for processing

.

6. TEST SETUP

The test to be setup under a simulated environment is as follow:

A traffic injector to be setup to simulate AF by sending traffic to DF at the high rate to overwhelmed the CDC link between DF and CF.

To simulate the DF, a machine with two network ports or a single port with two virtual IP addresses where one IP address connects to the simulated AF and the other connects to the simulated CF. The port connects to the CF remote end has been configured with significantly low bandwidth to simulate low capacity CCC link.

To simulate the CF, snooping application to be used to snoop all IP traffic. The Figure 6 provides illustrate the setup.

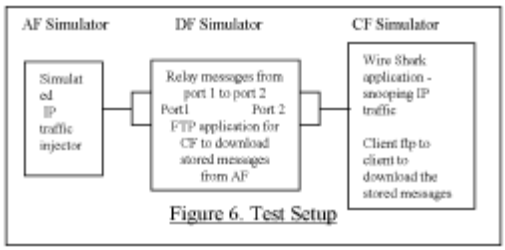

Figure 6. Test Setup

For the tools to run the test, DF can be simulated in a SUN machine with a network card with two ports. The network interface card can be configured as a router to relay messages from AF to CF. The AF sends the traffic with a destination to CF with DF in between to route the AF messages.

To simulate the overwhelm CCC link, the port which connects to the CF can be configured with significantly low transmit and receive rate.

Application which can generate IP traffic at an adjustable rate can be setup and configured to simulate the AF. Low transmit rate to simulate normal traffic condition and high rate to overwhelm the CCC link.

Wire Shark application can be used to simulate the CF component. It can be configured to operate under promiscuous mode to eavesdrop on a specific network interface where all captured frames can be saved into a file. A windows machine running this application will be sufficient to do the job.

To implement the solution, DF component need to be changed. An application can be setup to capture all frame in the interface connects to the AF. A Java program can be develop to send the saved frames to write it on the remote CF through output stream using socket based communication. The data as bring up from the hard disk into the memory and then send out to the remote CF byte by byte through output stream. The remote CF runs another Java programs as a server to receive the messages byte by byte and then serialized it into the hard disk. The CF runs multi-threading, blocks the write method until the traffic is no more overwhelm.

7. TEST CASES

Four test cases have been defined here to test the proposed changed. First test case (Case Number 1.1, Table 1) is to send IP traffic to simulate the signal messages from AF to DF at a traffic transfer rate where after relayed by DF to CF not overwhelming the link between DF and CF. The local CF instance in DF is turned off. The expected test result is that the CF can receive the frames originated from DF.

In the second test case (Case Number 1.2, Table 1), to simulate attack, the AF sends out traffic at a rate to deplete the link capacity. CF is expected not to receive any or minimal traffic from AF.

For the third test case (Case Number 2.1, table 1), the AF will remain the same sending rate. DF configured to save all messages from AF and the local CF instance is turned on. The expected outcome is that CF will receive the AF traffic.

Finally, the AF traffic transfer rate will be reverted back to test case one. No change in the DF+CF and remote CF configuration. The expected result is the CF remains able to receive the traffic coming from AF. This will falls under test case number 2.2 in Table 1.

The test cases illustrated above are summarized in the following Table 1.

Case Number	AF Traffic Transfer Rate	Local CF in middle component [On/Off]
1.1	Low	Off
1.2	High	Off
2.1	High	On
2.2	Low	On

Table 1: Test Cases

The test cases are designed to test the functionality of the proposed changed. The condition where the AF is

sending the traffic at low or high transfer rate, with the local CF turned off and then with the CF turned on. The proposed change should works under either low or high traffic sending out from AF.

To improve other security aspect, the following are the common recommendations:

- Messages are exchanged between TSP and LEA through site-to-site VPN.
- Periodic auditing and system logs analyzed.
- Firewalls installed and Intruder detection systems installed
- Latest updates for operating system related to security.
- Latest virus definition.

8. OTHER ASPECTS

The tools need to be identified to setup and run the test to gather the result for further analysis of the effectiveness of the solution. Various traffic models from AF to simulate attack is can be included to run more tests.

The performance aspect of the system is not discussed here. When the target is online, delivery of intercepted information will be delayed during the CCC link is busy. The solution does not work well under critical situation.

In the event of one host goes down, there is no backup or standby host to stand in to restore the service. In the event the middle component goes down, for example, the suspect's online activities will be lost.

The system's scalability should also be taken care of. There number of end users of the system can increase to cover more branches and different areas of law enforcement agencies. For example, law enforcement agencies include police, customs and immigrations.

The cost incurred to implement such a solution should be taken into account. The cost to have back up system, overhead to run the operations, license purchase of various applications, application and hardware yearly support and maintenance and others.

The manageability and the maintainability aspects also need to be looked at. For example, the police officers are not technically orientated. They need to be trained to manage and maintain the system.

9. CONCLUSION

Background of the lawful interception has been provided and the vulnerability has been shown with suggested change and limitations came with it. Although the Greek Watergate
incident has brought up questions related public's privacy and security at risk [12], the usage of the information interception is to serve a good cause to keep our world a safer place to live in.

10. REFERENCES

[1] Steven M. Bellovin, Matt Blaze, Whitfield, Diffie, Susan Landau, Peter G. Neumann, Jennifer Rexford, "Risking Communications Security: Potential Hazards of the Protect America Act", IEEE, 2007

[2] http://www.vcstar.com/news/2010/jul/28/hacker-hijacks-atm-computers-to-demonstrate/

[3] The Star, Monday 2 August 2010, pp w34, world section.

[4] http://www.pcmag.com/article2/0,2817,2367247,00.asp

[5] CALEA standards

[6] Juan C. Pelaez, Eduardo B. Fernandez, M. M. Larrondo-Petrie, Christian Wieser, "Misuse Patterns in VoIP", ACM, 2007

[7] Micah Sherr, Gaurav Shah, Eric Cronin, Sandy Clark, and Matt Blaze, "Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps", *ACM*, November 2009

[8] Whitfield Diffie, Susan Landau, "Communications Surveillance: Privacy and Security at Risk", ACM, 2009

[9] Douglas C, Sicker, Tom Lookabaugh, "VoIP Security: Not an Afterthought", ACM, 2004

[10] E. Cronin; M. Sherr; and M. Blaze. "On the (un)reliability of eavesdropping", *International Journal of Security and Networks (IJSN)*, 3(2):103-113, 2008.

[11] Kenneth L. Calvert, Michael J. Donahoo, "TCP/IP Sockets in Java. Practical Guide for Programmers", Morgan Kaufmann Publishers, 2nd edition

[12] David Moore, Geoffrey M. Voelker and Stefan Savage, "Inferring Internet Denial-of-Service Activity", USENIX, 2001

Appendix B

Collection Function Messages

The following is sample of target-to-target call messages sent from DF after been decoded by a CF Simulator using ETSI Rose standard. This two targets phone numbers are test phone collected during on-site customer test run.

```
The ASN for 201671 is being used.
------------------ ETSI ROSE CF Simulator ---------------------
Starting CF Simulator...
CF Simulator running as Server....
Server address (192.168.209.196:10001)
Simulator Listening the port ...
Waiting for incoming connection...
Connection established with (192.168.209.196:62734)

Received  26 bytes
RosHi CHOICE
  invoke SEQUENCE: tag = [1] constructed; length = 24
    invokeId InvokeId CHOICE
      present INTEGER: tag = [UNIVERSAL 2] primitive; length = 1
        1
    opcode Code CHOICE
      global OBJECT IDENTIFIER: tag = [UNIVERSAL 6] primitive; length = 7
        { 0 4 0 2 2 3 1 1 }
    argument OpenType
      0x300a81033132338203313233
Message Successfully Decoded...
Output from the decoder...PDU Recvd = RosHi_PDU

---------------------------------- Message #   1 -------------------------------------
Printing RosHi Message...
ROSHI INVOKE chosen
InvokeID:
  InvokeId_present = 1
OpCode:
  global :
    { 0, 4, 0, 2, 2, 3, 1, 1 }
argument : present
Operation Received = " sending_of_Password "
Password-Name SEQUENCE: tag = [UNIVERSAL 16] constructed; length = 10
  password OCTET STRING: tag = [1] primitive; length = 3
    0x313233
  name OCTET STRING: tag = [2] primitive; length = 3
    0x313233
Message Successfully Decoded...
Output from the decoder...PDU Recvd = Password_Name_PDU
  Printing Password_Name Message...
  Password length = 3, value = 123 (Hex Format : 313233)
  Name length = 3, value = 123 (Hex Format : 313233)

<The message continues from here.>
```

Appendix C

```
#!/bin/sh

elc=1
until [ $elc -gt 1 ]
do
 sh ./filet.sh
 sleep 2
done
```

endFile

```
#!/bin/sh

# checks if the file exist
while [ ! -f /home/geeko/newiri.sample ]
do
 echo "."
done

echo "File Exist!"

mv /home/geeko/newiri.sample /home/geeko/20110406/solution

# check file size
FileSizeChk=`ls -l ./newiri.sample | awk '{print $5}'`
echo "file size = $FileSizeChk"

#ping to check for echo. Link congestion check.
ping -q -c 1 -W 5 -s 5000 192.168.1.103 2>&1 >/dev/null
ls=`echo $?`

# Condition to check whether congested link or file size over boundary
if [ $FileSizeChk -gt 5000 ] || [ $ls -ne 0 ]
 then
   split -b 1000 /home/geeko/20110406/solution/newiri.sample SPLIT
   echo "Link congested or file size exceed 5KB threshold. File Splitted!"
   /home/geeko/20110406/solution/ftp_auto.sh
   rm SPLIT*
 else
    /home/geeko/20110406/solution/ftp_auto_ns.sh
 fi
```

filet.sh

```
#!/bin/sh
#HOST='192.168.1.103'
HOST='192.168.0.196'
USER='khlim'
PASSWD='khlim'
FILE='SPLIT*'

ftp -n $HOST <<END_SCRIPT
quote USER $USER
quote PASS $PASSWD
prompt
mput $FILE
quit
END_SCRIPT
exit 0
```

ftp_auto.sh

```
#!/bin/sh
#HOST='192.168.1.103'
HOST='192.168.0.196'
USER='khlim'
PASSWD='khlim'
FILE='newiri.sample'

#echo "iri counter is " $iriCounter " .\n"
#iriCounter=`expr $iriCounter + 1`
#echo "increamented ic "$iriCounter"\n"
#export iriCounter

ftp -n $HOST <<END_SCRIPT
quote USER $USER
quote PASS $PASSWD
put $FILE
quit
END_SCRIPT
exit 0
```

ftp_auto_ns.sh