# CHAPTER 1: THE PROBLEM

First thing need to do before developing secure call log/CDR files in PT. Telkom International (TELIN) is understand the problem that occurs within company. This chapter describes the problem occur in the company.

## 1.1 Rationale

The study conducted by InformationWeek Researchshows that there are280 companies are planning to use VoIP [4], because VoIP technology has some advantages as shown in the table below:

| Reason | Percentage |
|---|---|
| Lowering telecommunications costs | 66% |
| Desiring to merge voice and data networks | 43% |
| Obtaining a platform for one-stop communications in two or more areas | 41% |
| Increase collaboration benefits in two or more areas | 36% |
| Ease of management | 31% |
| Scalability | 24% |

**Table 1-1 The advantages of useVoIP technology [4]**

Besides having advantages above, VoIP technology also has weaknesses which can be used by hackers where An attacker can login to the server, Modify, or delete the call log files.

According to Margaret Rouse, Call log/CDR in VoIP is a file containing information about recent system usage such as the identities of sources (point of origin), on destinations (end points), the duration of each call, the amount billed of each call, the total usage time in the billing period, the total free time remaining in the billing period, and the running total charged during the billing period. When call is made it will be recorded in the Call manager database (or SIP proxy in case SIP is used). At some points the call Details Record (CDRs) may be transmitted to another server for further processing, for example for billing purposes. There are some reasons why call log or CDR files need to be secured. Some of the reasons are below:

1. Call log or CDR can be used to resolve dispute problems between operator or operator with customers
2. Call log or CDR can be used as the bases for every transaction or billing process in VoIP network.

There are many risks related with the call log or CDR, e.g. revenue lost, settlement dispute, expense not clear, if Call log or CDR file is corrupted then revenue recording or expenses will

give an error, settlement process with partner also will dispute. And also if this case happened to telecom operator which has retail user, then billing process to the users will error, raise complains etc.

PT. Telkom International (TELIN) is one of the biggest Telecom company which has been implementing VoIP technology. There are Some security standards for server which have been implemented by Telkom International for the severs which store call log or CDR files are below:

- Limited physical access to the Call log servers
- limited logical access to the call log servers
- limited access to the application or node which handle call record
- Implements SOA to the processing, collecting call log

More details about Telkom International security system and problems faced concerning withsecure call log or CDR files in the servers can be shown in the Table below:

| No | Date | person in Charge | Location of the visit | Purpose of the visit | Security VoIP issues | problems | Remarks |
|---|---|---|---|---|---|---|---|
| 1 | july, 4 2011 | Mr. Hadi (VoIP Expert-Telecom International) (TELIN)-Jakarta | Telekom International Head Office-Jakarta address: Menara Jamsostek Lt.24. Jln. Gatot Subroto Kav.38 Jakarta | Site survey and collecting data. | 1. Currently Telkom International (TELIN) use VoIP server or another words Call Details Recorded (CDR) for billing system.<br>2. VoIP server (CDR) security system being implemented:<br>▪ physically, Limited access to the server Call log<br>▪ limited access to the server call log<br>▪ limited access to the application or node which handle call record<br>▪ SOA to processing, collecting log call<br>3. tape drive as backup media for call log and after one year will deleted. | According to Mr. Hadi:<br>1. No serious problem have been found since implementing VoIP system<br>2. Transmission sometimes caused delay etc,<br>3. No use encryption-Decryption system for VoIP server | Complete Network diagram and some important data which related with the topic will send via email by Mr. Hadi |

**Table 1-2Result of site survey in Telkom International -Jakarta**

From the security point of view without using encryption and decryption in the server site, there will be vulnerability to the server call log server itself, because unknown users can login to the server and modify or delete the contents of call log or CDR files. That is why by developing new method which is a combination between AES and MD5 algorithm the server will be more then without using it.

## 1.2 Theoretical Framework

There are 3 main goals of data Security in VoIP network, these 3 main goals sometimes called CIA (Confidentiality, Integrity and Availability)

### 1.2.1 Data Confidentiality

Data confidentiality means data that has not been seen or read by any individuals who do not have any right to access it. According toClaudio LoCicero [18] confidentiality is ensuring that the information is accessible only to authorized individuals, regardless where the information is stored or how it is accessed.

### 1.2.2 Data integrity

Data Integrity means data that has not been modified byany individuals who do not have any right to access it. According to Claudio LoCicero [18] integrity of data can be compromised by malicious users, hackers, software errors, computer virus infections, hardware component failures, and by human error in entering or tranferring data.

### 1.2.3 Data Availability

Availability is a simple idea that when a user or system attempts to access something, it is available to be accessed. This is extremely important for mission critical systems. Availability for these systems are so critical that most companies have business continuity plans (BCP's) in order for the systems to have redundancy. Considering previous explanation about VoIP billing system which has implemented by Telkom International (TELIN) it is found that TELIN VoIP Network has vulnerabilities to the hacker to login, delete or modify the call log or CDR files. Therefore, to solve the problem it is needed a new method which is called combination between Advanced Encryption Standard (AES) and MD5 algorithm.

## 1.3 Conceptual Framework/Paradigm

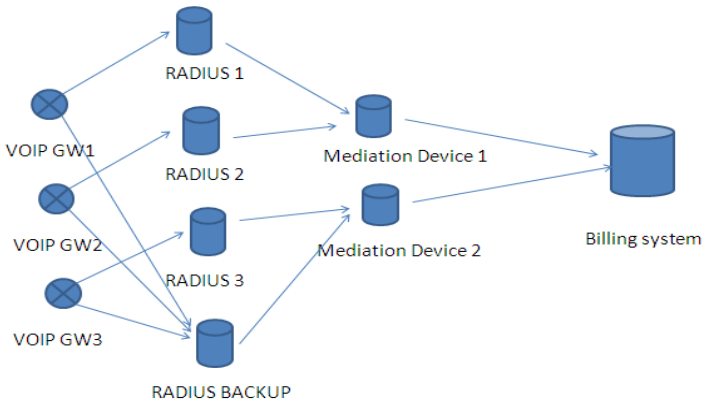


**Figure 1-1TELIN VoIP for billing system**

Each VoIP gateway (GW) at Telkom International (TELIN) Network uses two RADIUS servers to backup each others, then each radius server sends call log or CDR file which is scheduled daily to the mediation device, TELIN VoIP network system also uses two mediation device which can backup each other, after that these mediation device will send CDR file to the Billing machine which is scheduled daily. Billing machine always received two duplicate (same) CDR data from this process, and billing machine will be able to do Sorting. Based on figure 1-1 above it is indicated that unknown users (attackers) have possibility to login, modify, or delete call log or CDR files.

## 1.4 Statement of the Problem

The problem in this thesis is:

- Hacker has the possibility to login, modify or delete file call log/CDR files because the server itself connected to the network.
- Data is easily corrupted so there are a lot of errors in the billing process that create a lot of complaints from the users.

## 1.5 Hypothesis

By applying these three methods, User privilege, AES and MD5 algorithms, the call log/CDR files in the server will be more secure without worrying about losing data. Besides AES also suitable to secure call log or CDR files in term of security, size of the files, and data processing speed.

## 1.6 Scope and Delimitation

This thesis will focus on the security of call log or CDR files in the server and no transmission issue will be discussed in this thesis.

## 1.7 Importance of the Study

This thesis is expected to contribute the security Call log or CDR in the VoIP server. The combination between AES and MD5 Algorithm willprevent unknown users to login, modify or delete the call log/CDR files.