GSM Security Architecture to Control Telecom Frauds in ethio telecom

Wondwossen Abebe
HiLCoE, Software Engineering Programme, Ethiopia
Ethio telecom, Ethiopia
sakrumaru@gmail.com

Mesfin Kifle
HiLCoE, Ethiopia
Department of Computer Science, Addis Ababa University, Ethiopia
kiflemestir95@gmail.com

Abstract

Telecommunication fraud is a threat that has grown dramatically over the past decades and becomes a serious global issue for mobile network service providers. It has undoubtedly significant source of revenue losses to operators, carriers and end users at continuing growth. Possibly, fraud is expected with proportional increase. This research is therefore focused on how ethio telecom has to monitor and detect frauds by enhancing the existing GSM Architecture for more effective fraud detections and preventions.

Assessing the network security architecture to control telecom frauds, in identifying fraud types and their causes, threats and risks, proposing possible extended GSM architecture, testing and evaluating the proposed architecture are objectives of this research. We used questionnaire and document reviews for data collection and analysis, in a way to contribute for deploying efficient fraud management. In effect, we addressed possible motivations to perpetrate fraud, prevalent fraud types and occurrence, products and services attacked in GSM network and fraud detection and prevention procedures.

Besides to existing GSM security weaknesses, flaws and opportunities to fraud analysis, architecture improvements and evaluations of solutions on bypass and short message service frauds are proposed.

Keywords: GSM Security Architecture; Telecom Fraud; FMS; Gateway; SMSC

1. Introduction

Global System for Mobile communication (GSM), one of telecommunication services, is a digital mobile telephony system that is widely used in almost all parts of the world [1].

GSM technology has brought key advantages and features such as digital compatibility, new services, international roaming, and open and universal features to the telecommunications industry.

Contrary to the enablers mentioned, providing GSM service has encountered challenges like telecom fraud.

Fraud is as old as humanity [2] and takes unlimited variety of forms, occurs in many areas, and service categories. Telecommunication fraud is a threat to telecom service providers that causes operators huge revenue losses and reputation, and poor quality of service (QoS). Its impact is not only limited to operators but also affects customers with less satisfaction and retention.

In a survey conducted by the Communications Fraud Control Association (CFCA), $72–$80 billion revenue losses were estimated due to telecom fraud worldwide [3]. While many large operators have developed sturdy Fraud Management Systems (FMS) to combat fraud, others have not. It was also concluded that perhaps only about 10% of operators worldwide have put in place sensible and effective fraud strategies [4].

The motivation behind crime is attributed to migration and demographics, penetration of new technology, staff dissatisfaction, operational weaknesses, poor business models, criminal greed, political, and ideological factors [5].

Fraud is a crime in telecom services that is complex and dynamic that can be easily committed by courses of fraud motives, opportunities, capabilities

and rationale. One of the telecommunication services that is most vulnerable to fraud attacks is GSM network which brought numerous impacts on ethio telecom, its customers, vendors, and the country at large.

The general objective of the paper is to assess and propose direction to enhance the GSM security architecture to control telecom frauds in ethio telecom. Towards this end, the existing GSM security architecture, strengths, weaknesses and recommendations of possible improvements to control or reduce telecom frauds in ethio telecom are the main issues to be addressed.

As telecom fraud is widely spread and GSM security architecture attacks are complex, it is difficult to cover all the domains in this paper, It has also limitations due to restrictions to methods of fraud operations as managing fraud in ethio telecom is young (3-6 years) with immature experience.

The research work is carried out through an intensive document review of different literatures that specifically address the research problem and by making use of a questionnaire. The proposed solution has been evaluated using a standard method of testing.

The rest of the paper is organized as follows. Section two deals with literature review. The third section describes summary of identified frauds. The fourth section describes the proposed solution. Finally, the fifth chapter concludes the paper.

2. Literature Review

2.1 GSM Network & Security Architecture

GSM features improved speed for the transfer of data and the ability to operate over data networks like the Internet and encryption was provided primarily by A5/1 encryption with 64-bit stream cipher. The key features of GSM include international roaming, superior speech quality than analog cellular technology, high level of security, user information safety and security, digital convenience, and digital compatibility [6].

The GSM Security Evolution started with secure conversations and preventing data from interception to prevent fraud and mechanisms are developed to make GSM the most secure mobile communications standard.

Security concerns could be from operator or customer side. Billing the right person, fraud controls, and service protection are known concerns whereas privacy, identity, location and communication, and confidentiality are new concerns. The concerns are measured using principles of authentication of a user, data and signaling cipher, user identity confidentiality and SIM security module [7].

The understanding of security features of a GSM network is crucial to the implementation of security policies and security architectural designs. It addresses the goals of security functions by providing user-related security features for authentication in which secret PIN based validation is required to access SIM, confidentiality in terms of user related data that are encrypted by algorithm A5 and anonymity, meaning that data are encrypted before transmitted.

The length of the cipher keys, 54 bits out of 64 bits, and upgrade of signaling protocols are factors for strength of the encryption algorithm but encryption and authentication mechanisms are very difficult to upgrade.

In addition, individual user authentication keys at the GSM AuC can be accessed and the mobile user can be impersonated. Lack of authentication of VLR/HLR, inter-network location update the triplet (RAND, SRES, Kc) and all unpublished secret algorithms (A3/A5/A8) are GSM weaknesses that cause security vulnerabilities.

2.2 Telecommunications Frauds and Attacks

Fraud is a problem for all businesses, internal, external or a combination with an increased innovation in the telecom industry [8].

In 2013, a survey conducted by CFCA [9] put the following factors leading to fraud.

- How the technology is actually installed, configured, and the default settings,

- How technology, products and services are sold/offered,
- Inherent weaknesses in procedures and working practices,
- Lack of management control, supervision and monitoring, and
- Lack of knowledge and experience of personnel and rush to market - no product or service fraud risk evaluation.

Although fraud is committed by any person, whatever the social status, nationality, or position/role within a business, company management bodies were also named as the biggest perpetrators in a recent fraud survey as they are often not being watched, they are trusted and have access to more information and systems.

Fraud can be committed from external and internal, where external fraudsters can work from anywhere as they often have people working for them whilst they control the fraud activities centrally. Internet access and unlimited opportunities provided by technology are powerful tools for fraud. Internal frauds are committed from inside the company often with outside collusion and influence and are by far easier.

Fraudsters may have different personal reasons. The following are common and known reasons: financial gain for profit or no expense/cost of service by not paying for their own airtime usage including for high value service offerings like roaming, international access, high volume/multiple SIMs on an account and ability to have roaming and international direct dialing activated at the point of sale, and no deposits or restrictions. In this regard, the subscription process and procedure, lack of bad debt management, blacklists, and default account management are also motivational factors [10]. The other reason is Anonymity circumventing detection by network operators and authorities as the 'real' user of the service is unknown. Global fraud losses have risen due to an increase in worldwide terrorism, by illegally gaining access to a network. Lack of legislation and prosecution is also a motivational factor since penalties for telecom related fraud are typically less severe than for other criminal activity.

According to GSMA, fraud types occurring all over the telecom operators worldwide are categorized into 5, namely subscription/payment, technical, business, prepaid, and distribution [11]. Subscription fraud is the oldest type of fraud experienced by all operators. It is airtime related procedural exploitation that is estimated to account to more than 70% of fraud losses. Business fraud (unauthorized service) is the use of a product or service without authority. Technical fraud is more advanced fraud that is based on exploiting loopholes found in the operator network elements or platforms.

The four eyes principle in fraud detection and prevention was used to measure whether the fraud scenario is technical, business, or any other.

Fraudsters attack the weakest link in the operator. The weakest link can be anywhere inside business processes relating to network access, customer activation process, billing, charging process, payment options, revenue share, and value added services, roaming, and PRS [11].

The following are the most prevalent products and services having huge impacts in their respective domains: Mobile services, VoIP services, Satellite services, Roaming service, and Premium Rate Services (PRS).

3. Identified Fraud Types

Questionnaire and document review methods are used to assess the existing fraud types and their causes at ethio telecom, where in the questionnaire 38 all rounded questions were hosted online and distributed to 71 participants and among them 57 samples were collected**.**

The respondents' feedbacks have clearly showed that focus must be given against those potential attacks, vulnerabilities, risks and fraudulent behaviors, by assessing the design of the GSM network. From the assessments performed, bypass and SMS frauds are found highly impacting telecom frauds. The flaws

respective to these fraud types in the existing GSM architecture need technical solutions & mitigations

4. The Proposed Solution

In this section, based on the empirical finding, a new solution is proposed targeting the architectural and functional flaw addressing the two serious fraud types. The former is explained using the existing international gateway, where the latter is also explained using existing SMSC. The solution proposed for both fraud types are presented separately and in combined form of global representation. In the end, evaluation is done.

a. The proposed Grey VoIP Traffic Solution

ethio telecom has international links to the rest of the world where traffic comes from and goes to via Italy and France. The VoIP traffic is transmitted via signaling links from/to two destinations/sources each having 25 E1 links, serving more than 40 interconnect traffic carriers and operator partners. Fraudulent traffic might be sent to/from operators via routes, not normal routing paths, called grey routes.

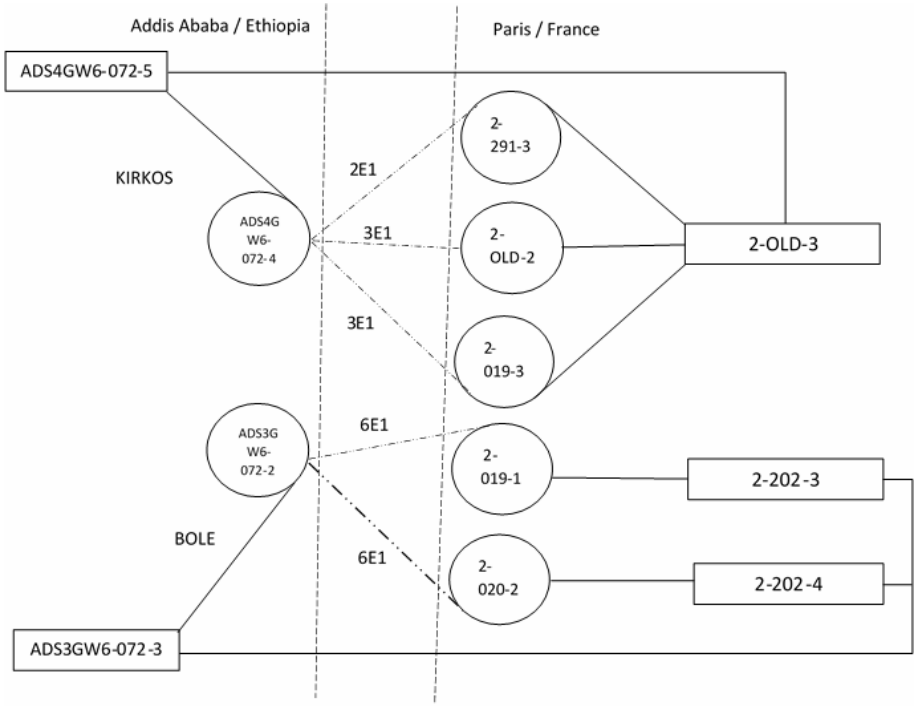

Figure 1: The Existing International Gateway Signaling Link to France

Figure 1 shows one of the existing international gateways - signaling architecture of ethio telecom via France. Solid lines indicate links of signaling traffic connections to France and Italy whereas broken lines are for voice traffic considered normal traffic routes at Bole and Kirkos sites.

One of the most important functions of a national network is international connectivity, which is a major contributor to the carrier's revenue. Thus, it makes sense that the international gateway provides reliable, comprehensive abilities to route, re-route, analyze, and properly bill core revenue-generating international traffic.

This core architecture has limitations in exhaustively analyzing the incoming international traffic and is unable to route whole traffic to normal traffic routes. Its main flaw is that it can't distinguish the source of incoming traffic route, i.e., whether it is white route or grey route.

To mitigate the gap identified, control measures will be set on the existing architecture by adding the proposed solution as shown in Figure 2. The international gateway will analyze the incoming international traffic so that traffic sources will be identified and this will solve the limitation on the existing architecture.

As shown in Figure 2, the signaling traffic links sent to and received from soft switches will be forwarded to 'Grey- incoming VoIP traffic filtering' so that the traffic will be analyzed for its source IP protocols for carrying VoIP traffic.

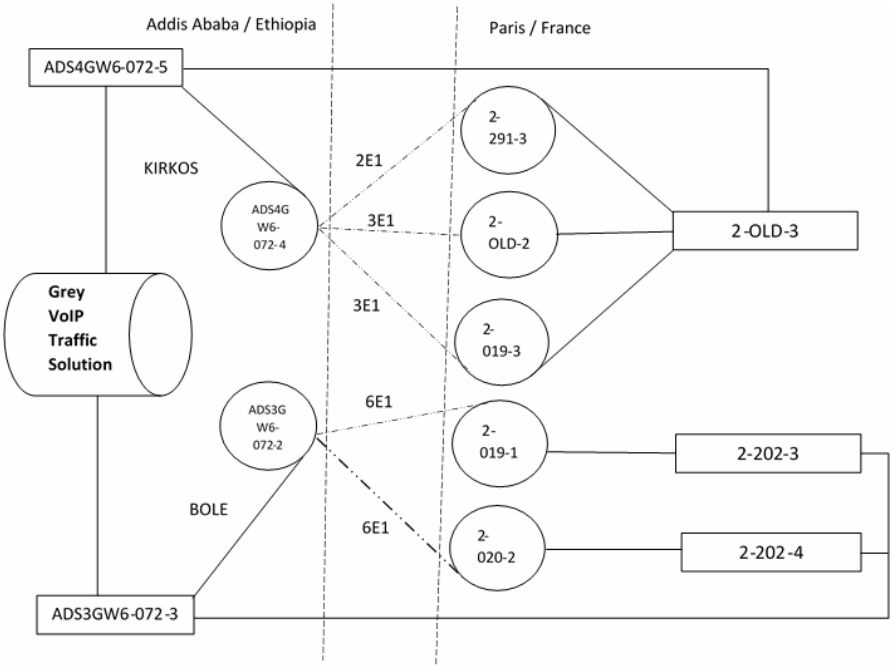

Figure 2: The Proposed Solution for the International Gateway Signaling Link to France

After proper analyses of the captured incoming traffic, actions can be taken including but not limited to rerouting and setting that traffic to proper charging mechanisms. Since the broken lines in Figure 2 connected to France telecom are purely voice traffics, those are considered normal traffic routes.

b. SMS Fraud Solutions

SMS is a popular telecom service due to its features of being convenient, rich in content and comparatively cheaper. When an SMS message is sent from a mobile phone, it will reach an SMSC first, then the SMSC forwards the SMS message towards the destination. It is a store & forward operation. The main duty of an SMSC is to route local and international SMS messages and regulate the process. The above operation can't always be performed free from attacks due to the gap in the existing SMSC architecture.

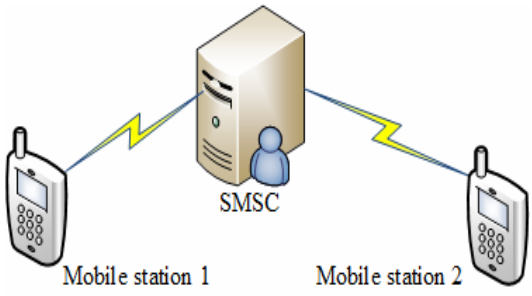

Figure 3: Existing GSM-SMSC Architecture

In Figure 3, short messages are delivered from application to mobile. Consider Mobile Station 1 is malware infected and performs hidden automatic SMS generating operation to Mobile station 2 or it is a smart phone having silent SMS generator installed, and sends to Mobile station 2. Intentionally the SMS generator will have international premium numbers as recipients without any control. Mobile station 1 will surely bring security vulnerabilities and shortcomings including but not limited to SMS faking, SMS

malware, SMS flooding and SMS spamming, while Internet connection is on.

Besides, a user may not be aware of an application's intent beyond providing the superficial services of social messaging and applications.

Existing SMSC has limitations in filtering, capturing and ultimately blocking abnormal SMS messages received from or sent to customers.

To mitigate the gaps identified, control measure is set on the existing SMSC architecture by adding an anti-spamming (SMS firewall) solution that will perform basic services of keyword monitoring, character length monitoring, anti-faking, anti-malware and anti-spoofing, unauthorized and malicious short messages, and others.

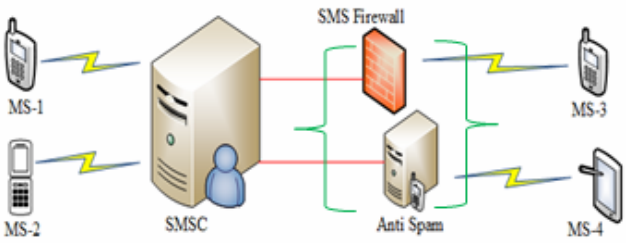

Figure 4: SMS anti-Spamming (SMS Firewall)

As shown in Figure 4, assume MS-1 and MS-2 will generate text messages to recipients MS-3 and MS-4. If the content that is sent to MS-3 is found to violate criteria like "keyword" then the anti-spam/SMS firewall will filter and block, raise alarm, or the SMSC is notified to return it to the sender.

Grey VoIP traffic filtering and anti-spamming/SMS firewall respectively will monitor, detect and prevent/block any identified potential risks, if deployed successfully.

c. Evaluation of Extended Architecture

The evaluation of the proposed solution of identifying international incoming VoIP traffic at international gateway is planned to be conducted in Intranet network environment using call manager. The call manager will support all the necessary functions at the international gateway (soft switch) which is required to perform the intended evaluation.

Grey routes will be analyzed and mitigation action will be set to control those routes before converted or terminated into local calls.

5. Conclusion and Future Work

This paper addressed the need of fraud detection, investigation and analysis. All the monitoring, detection and investigative analysis processes of telecom frauds is very helpful in identifying the root causes of fraud.

Clear understanding of the whole state of GSM network security to control frauds was properly stated including two proposed solutions of identifying grey traffic & Content Based SMS Spamming.

The following points are drawn based on the findings.

- Fraud policies and practices are not visible to most of the employees and customers which means that it fails to produce and work to standard operating procedures. On the other hand, bypass fraud suspects and/or fraudsters claimed innocent in front of courts for ambiguity and clarity of terms stated in proclamations.
- Telecom services could not be free from vulnerability. It is better for ethio telecom to target marketing new services and other vulnerable business areas before the fraudster target it, by making awareness to customers by doing electronic and paper based surveys.
- ethio telecom needs to think strategically to expertise knowledge in fighting telecom fraud and encourage researchers so that professionals and researchers can conduct detailed studies in the area. This research provides solutions on two most prevalent fraud types in the context of ethio telecom only, while there are more than 120 fraud types in the network, distribution, business, and prepaid categories.

The basic principles for better fraud management are to ensure that detection and prevention of fraud requires an understanding of the actual threat, know

what is the fraud incident, what is the motive for committing the fraud, what are the periods for the fraud attacks, time frame, persons involved, is it externally or internally, and finally the way it is perpetrated.

References

[1] M. Rouse, "GSM (Global System for Mobile communication)," Techtarget, May 2007. Available at http://searchmobilecomputing. techtarget.com/definition/GSM, Accessed on 08, October 2013.

[2] Richard J. Bolton David J. Hand, "Statistical Fraud Detection: A Review," Statistical Science, Vol. 17, No. 3, pp. 235–255, 2002.

[3] Communications Fraud Control Association, " Worldwide Telecom Fraud Survey," CFCA, Roseland, NJ, 2009.

[4] R. Shelton, "The Global Battle Against Telecom Fraud," Cerebrus Solutions Ltd, 2003.

[5] S. Brown, "Telecommunication Fraud Management," Waveroad SecuriT, Montreal, 2005.

[6] SANS Institute InfoSec Reading Room, "The GSM Standard-SANS Institute, The GSM Standard (An overview of its security)," SANS Institute, 2010.

[7] Jeremy Quirke, “Security in the GSM system". AusMobile, Available at http://ausmobile.com, [Accessed 15 Sept. 2013]. 2004.

[8] J. Hollmen, "User profiling and classification for fraud detection in mobile communication networks", Helsinki University of Technology, 2000.

[9] KPMG, "India fraud survey report", Fraud Survey New, India, 2006.

[10] R. Robert, D. Dabija, "Telecom Fraud Management Training ", Presidium, Qtel, 2009.

[11] GSMA, "Fraud Manual Version 9.0", Official Document Fraud Forum 21 - Fraud Manual, 2014.