An Intrusion Detection System to Mobile Phone Networks

Mirela Sechi Moretti Annoni Notare¹, mirela@lrg.ufsc.br, Azzedine Boukerche², boukerch@siro.csci.unt.edu, Fernando Augusto da Silva Cruz¹, cruz@lrg.ufsc.br, Carlos Becker Westphall¹, westphal@lrg.ufsc.br

¹ Federal University of Santa Catarina, Brazil
² University of North Texas, USA

Abstract: With the increasing popularity of the wireless network, the security issue for mobile users could be even more serious than we expect. In this paper, we discuss several aspects of network security. Then we focus on the intrusion-detection and cloning mobile phones problems, which are currently attracting considerable interest from both research communities and commercial companies.

Keywords: Security Network Management, Intrusion Detection, Telecommunications, CORBA, Web

1. Introduction

Before the mobile phones became widely popular, the greatest threat to the network security in most organizations was dial-up lines. While dial-up lines still merit attention, the risks they pose are minor when compared to wireless and mobile connections. To break the system, one needs only to buy a piece of portable radio equipment, such as a scanner for instance, to program a genuine mobile cloned to debit calls from genuine mobile phone, and register the frequencies where mobile phones operate in a surrounding areas. Then the person committing the fraud may, for example, park his car around a shopping mall, jot down various frequencies, transfer the data to clones, and then pass them to whomever may be interested in these cloned mobiles.

Therefore, rather than ignoring the security concerns of potential users, merchants and telecommunication companies need to acknowledge these concerns and deal with them in a straightforward manner. Indeed, in order to convince the public to use mobile and wireless technology in the next and future generation of wireless systems, telecom companies and all organizations will need to explain how they have addressed the security of their mobile/wireless systems. Manufacturers, service providers and entrepreneurs who can visualize this monumental change and effectively leverage their experiences on both wireless and Internet will stand to benefit from it.

Concerns about network security in general are growing, and so is research to match these growing concerns. Indeed, since the seminal work by D. Denning in 1981 (Denning, 1987), many intrusion-detection prototypes, for instance, have been created. Intrusion-detection systems aim at detecting attacks on computer systems and (mobile) networks, or against information systems in general. Intrusion detection in mobile telecommunication network has received very little attention. It is our belief that this issue will play a major role in future generation of wireless systems. Several telecom carriers are already complaining about the loss due to impostors using cloned phones.
The remainder of this paper is organized as follows. Section 2 discusses current security problems and related works. Section 3 presents some aspects of (wireless) network security. Section 4 presents topics of intrusion detection. Section 5 describes a system proposed for intrusion-detection in mobile telecommunications networks. Section 6 draws conclusions and looks to the future. References follow.

2. Related Works

Despite the fact that there are few intrusion detection systems for networks, automatic cloning detection in mobile telecommunication networks has received very little attention. Many telecommunication companies are losing hundreds of hundreds of dollars due to the use of clones or genuine mobile phones by impostors. One might argue that although it is rather easy to clone an AMPS phone, it is much trickier to clone a D-AMPS, a GSM, or an IS-95 phone. However, the GSM phone was still cloned.

Consequently, there is a great deal of interest in designing mobile phones using new technologies (i.e., enhance the hardware) that will make it much more difficult to clone cellular phones. However, to the best of our knowledge there is very little work being done effectively at the software level. Furthermore, the current software:

(i) does not have an efficient way to verify whether a call is untypical of the normal client pattern, or an automatic process for warning clients that an imposter is using their mobile phone. In most of these systems, human staff are used (only lists of large bills are reviewed to identify cloned phones);

(ii) has no efficient ways to control/identify the impostors; and

(iii) uses an “experimental satisfaction” to prove the correctness of their security framework. Some systems provide the billing process via the Web. However, the identification of a cloned phone is done only at the end of the month. This unfortunately is not quite efficient and leads to a big loss of revenue for the carrier.

While cryptography techniques have been employed satisfactorily in digital mobile systems, it is our belief that neural network techniques could be used to protect both digital and analogue mobile phones and protect against cloning, as well as companies against (future) impostors trying to use cloned phones. Neural networks can be used to learn the behavior of mobile phone users, and could be used as knowledge-based intrusion detection tools to learn imposter traces, and then identify cloned phones and (future) intruders.

In this paper, we present an intrusion detection system in mobile telecommunication networks, and propose adding more security services in order to avoid specific violations, in particular cloning mobile phones.

3. Security Management

An adequate security (Alexander 1998) system management policy has long been an important issue. However, a comprehensive network security plan must also consider the losses of privacy
(Pfleeger and Cooper 1997) when we define authentication and authorization as well as the losses of performance when we define key management and security protocols, for instance.

Therefore, the security plan must encompass all of the elements that make up the network (Dowd and McHenry 1998), and provide important services such as:

(i) access control, i.e., authorization by capability list, wrappers and firewalls;
(ii) confidentiality, i.e., only the authorized party can read a message;
(iii) authentication, i.e., the receiver must be able to confirm that the message is indeed from the right sender;
(iv) non-repudiation, i.e., the sender cannot deny that the message was indeed sent by him/her;
(v) integrity, i.e., message has not been modified in transit; and
(vi) security administration, i.e., checking audit trails, cryptographic and password management, maintenance of security equipment and services, and informing users of their responsibilities.

The advances in cryptography have provided solutions to many of these network security requirements. Many computer network securities are based on secrets or “keys”. Several policies can be used to enforce the security implementation using cryptography schemes. Each service uses specific schemes as described below:

(i) Access Control – Access Control Matrix, program to access control to another one, and protection wall between two nets, respectively;
(ii) Confidentiality – Checksum and cryptography by key management with a secure key distribution service (the main problem with secret-key crypto-systems is the need to construct elaborated protocols to distribute secret keys securely over an untrusted network; the main problem with public-key crypto-systems in that sophisticated computations are required to produce mathematically related keys, which translates to less efficient and more expensive hardware implementations compared with secret-key systems);
(iii) Authentication – Password by cryptographic-based authentication protocols and message authentication mechanism by checksum (the last, also known as MAC – message authentication code); and
(iv) Non-Repudiation – Proof of origin and proof of delivery by key cryptography (public-key cryptography can be used to enable the originator to sign a message before it is sent by encrypting it using the private key; the use of a private key for this purpose is known as a digital signature).

Readers interested in cryptography schemes might wish to consult (Stalling, 1995) for further details. Digital mobiles use cryptography mechanisms against cloning frauds. Recently (April 1998), the cloning of a digital mobile was announced at the University of California at Berkeley. Thus, we believe there is still much work to be done in the cloning mobile phone area.

4. Intrusion Detection in Telecommunications
Intrusion detection systems are one of the latest security tools in the battle against these attacks. As is well known, it is very difficult to determine exactly which activities provide the best indicators for the established (normal) usage patterns. Thus, researchers have turned to using expert systems or knowledge-based intrusion detection to search for activities known to be indicative of a possible intrusive behavior (Lunt et al 1989). The motivation behind this approach is to seek proper as opposed to normal behaviour.

Knowledge-based intrusion detection schemes apply the knowledge they have accumulated about specific attacks and system vulnerabilities. Using this knowledge database, any action that is not explicitly recognized as an attack is considered acceptable. Otherwise, an alarm is triggered by the system. There are many different characteristics of intrusion systems available in the marketplace (Stillerman and Marceau 1999). Expert systems are based upon knowledge based intrusion detection techniques. Each attack is identified by a set of rules. Rule-based languages (Habra et al 1992) are used for modeling the knowledge that experts have accumulated about attacks/frauds. Information regarding some intruders has also been added to these systems.

A major drawback of knowledge-based intrusion systems is the difficulty in gathering the information on known attacks (which should be updated regularly), and developing a comprehensive set of rules that can be used to identify intrusive behavior.

Some systems use a combination of several approaches to cover both normal and proper behaviour schemes (Lunt, 1988). We refer to them as behavior-based intrusion detection. Their basic idea is that any action that does not match with a previously learned behavior, triggers an alarm. The action is considered as intrusive. The main advantages of these systems are that they can exploit new and unforeseen attacks, and contribute to discovering new attacks automatically. However, the high false alarm rate is generally cited as a main drawback of these systems due basically to the accuracy of the behavior information accumulated during the learning process.

5. An Intrusion Detection System for Mobile Phone Networks

Our main approach to identifying fraud calls is to classify the mobile phone users into a set of groups according to their log files. We assume that all relevant characteristics that identify the users will be stored in these files; i.e., where, at what time, and from where the calls were made, etc. Classifying the users into groups will help our system to identify easily if a specific call does not correspond to a mobile phone owner. Thus, when the call made using a genuine/cloned phone is terminated, the system will check if the characteristics of the call is within the client patterns saved in the file. A warning message could be sent to the client if a fraud was detected. This immediate notification, instead of waiting till the end of the monthly bill cycle, will help to reduce losses to the carrier and to the owner of the mobile phone that has been cloned. In our system, we propose the use of neural network algorithm to partition the users into classes and create the log files which we refer to as baseline files. In this section, we will describe the algorithm, and report on the performance results obtained using real data (real data were obtained from telecommunication carriers).
As illustrated in Figure 1, our framework consists of three main components:

(i) the first part represents the security system against cellular cloning (SSCC);
(ii) the second part presents the security for users on the Web (SETWeb); and finally,
(iii) the third component – a System to Identify Probable Impostors (SIPI) represents the system to avoid future impostors that might try to use the mobile phones improperly, mainly using names of other persons.

Fig.1: Intrusion Detection System Framework.

These three components of the SSTCC (Security System for Telecommunication against Cellular Cloning and Impostors), presented in Fig.1, are described below in the items 5.1 (SSCC – Secu-
Security System against Cellular Cloning), 5.2 (SETWeb – On-Line Phone Bil by Web) and 5.3 (SIPI – System to Identify Probable Impostors).

5.1. SSCC System

SSCC can be viewed as a black box that interacts with the users via mails or phones; which we refer to as gate-mail, and gate-phone respectively. While the first gate is used by the SSCC to send alarms of possible frauds to the users by “surface” mail, the second gate allows the SSCC to use mobile phone to send the same alarms. The main purpose of sending alarms by phone is for an immediate notification of possible frauds. Although the “surface” mail is more secure, it is still slower than notification by phone.

The most abstract specification of the SSCC system corresponds to a formalization of the user requirements of this system, and it might be used as a basis for future refinements of the project. Furthermore, using this requirement specification, it will be possible to prove – formally – that it is equivalent to the future final and complete specification.

In order to validate our SSCC system, we make use of the CADP tool - Caesar Aldébaran Development Package, (Garavel, 1996) available within the Eucalyptus toolbox. The procedure used to obtain the correction proofs between refinements generates the following two automata: 

SSCC.AUT and SSCC_DET.AUT. These two automata aim at proving correctness of the system in conformity with ISO 8807 (Brinksma, 1988) and US DoD ClassA1 (Simon 1996, Stallings 1995).

Our distributed security system is supported by CORBA that uses on-line telecommunication databases (i.e., CallsFile), as well as database files (i.e., Baseline) created during the training process of the system for the classification of the clients - using neural network/pattern recognition techniques. CORBA and Web/Java security components were added to secure further our system. LOTOS formal specification and validation techniques were embedded in our system to prove the correctness and the validation of our system. Fig. 2 shows a screen of the manager of the system.

![SSCC Manager](image)

Fig. 2: SSCC Manager.
The SSCC manager receives the notifications from the several agents (distributed by CORBA architecture) and sends alarms automatically and immediately to the telecom users. The alarms can be configured as presented in Fig. 2.

5.2. SETWeb System

SETWeb, a system phone bill on-line via Web, has been developed to allow clients to consult their phone bill online via the web, at any time during the day. The client can then observe if a call from a clone has just arrived in his bill – thus, avoiding big losses. See Fig. 3.

![On-Line Phone Bill by Web.](image)

To ensure the security of the carrier site, and protect the privacy of the client, several issues must be maintained, such as access controlling, logging, confidentiality, authentication and administration of the systems resources, just to mention a few. In our design, all these services were implemented using the java.security API with the overall goal of protecting the user’s information from eavesdropping and tampering. To avoid spoofing attacks and ensure that the user is accessing the right phone carrier site, we made use of digital certificates on the server side.

Our system ensures the security and the privacy of the client when he tries to access to his/her file (McGraw and Felten 1997). In our system, the tool policytool creates and manages a text file that
stores security policy definitions, known as mypolicy. Those definitions can give special privileges to users having some forms of authentication, such as a digital signature.

5.3. SIPI System

SIPI, a system to identify probable impostors, has been designed to identify “probable” impostors using cloned phones. There are several types of impostors our SIPI system can identify:

(i) those who changed the mobile phone’s owner call patterns;
(ii) those who bought a mobile phone only for one month (and were determined not to pay); and
(iii) those who bought mobile phones using other names.

To identify these types of impostors as soon as possible and not at the end of the month to avoid more losses for the carrier, we propose classifying them using Gauss’s algorithm (Todesco 1995) according to the call patterns of the owners of the phone and the impostors.

Using Gauss’s classification, we can identify who are the most “probable” impostors as follow: Gauss’s algorithm identifies the impostors and clusters them into several classes. Thus, our distributed security system can identify the most probable impostors using cloned phones. In our system, we propose to use pattern recognition scheme to discover, as soon as possible (and not at the end of the monthly bill cycle) that one client has call patterns almost identical to an (old) impostor.

It is important to highlight that such type of impostors (that buy a mobile with the intention not to pay for the service) can be detected only by software. There is no hardware (i.e., cellular phone) capable of detecting that fraud.

6. Conclusion

Considering the five areas of network management, i.e., configuration, failures, performance, accounting and security, the last area has not received its fair share. With the increasing popularity of mobile and wireless networks, it is about time to acknowledge the security concerns of potential users and deal with them in a straightforward manner. In this paper, we focused upon the network intrusion detection problem and the frauds of cloned mobile phones.

We have identified the major problems in network security, and described the major intrusion detection techniques. We have also presented our security management system that can used to identify frauds, and impostors using cloned mobile phones.

Neural network techniques have been used to classify (mobile) phone users into groups according to their (past/current) profiles. Using this classification it is easy to determine if a call was made by the user or an impostor/intruder. The system might also be used to identify future impostors as well. Consequently, this anti-fraud system will prevent the cloning of mobile phones, and it will
reduce significantly the loss of profit to the telecom carriers and the damage that might be passed to their clients.

As future projects plan to enhance the SSTCC system and its SETWeb module using the next generation of wireless communication systems that will include the web-technology within the cellular phones by the use of WAP – Wireless Application Protocol. In addition, we aim at investigating the use of servlets instead applets in order to increase even more the security of the system.

References