Global Information Assurance Certification Paper

Securing A Mobile Telecommunications Network From Internal Fraud

by

Nathan Kurtz

Practical Version 1.3

Summary:

The mobile telecommunications industry faces numerous challenges protecting their networks from internal and external fraud. It has been estimated that the combined financial loss to mobile companies from fraud may be in excess of $25 billion dollars. The largest portion, external fraud, is the easiest to detect because a company's switching systems capture the usage, which can be analyzed to identify the perpetrator. Internal fraud, however, is more difficult to detect because confidential corporate information can be used to alter internal systems and prevent the recognition of fraudulent activity. Protecting against internal fraud will be the focus of this discussion. Starting with the switch, this system's filtering mechanism, VMS (Voicemail System), and HLR (Home Location Registry) can be modified to hide employee fraud. The next system in the process chain, mediation, can also be reconfigured at its filtering mechanism to disguise fraud. Finally, the billing system is explored to show how its consumer rate tables can be changed to affect the pricing scheme of a fraudulent employee's bill. These specific areas of a mobile company's systems constitute the high risk areas for internal mobile fraud.

The first step to secure a mobile network is a well defined, clearly though out security policy. This foundation will provide guidelines for designing and constructing the controls required to mitigate the risks to the switch, mediation, and billing systems. Pervasive controls, such as an employee-signed security policy, can be used to prevent an attack before it is attempted. Specific controls like user account standards or physical access controls prevent an attacker from attempting to access the system. Monitoring controls enable the company to detect attack attempts or quickly identify areas that have been compromised. Each control combined with the security policy form the framework for securing a mobile telecommunications network from internal employee fraud.

Introduction:

The mobile telecommunications industry looses an estimated $25 billion dollars a year due to fraud. While the majority of this activity can be attributed to external exploits of handset weaknesses, a sizable portion of this activity is from internal employees manipulating their company's mobile network vulnerabilities. The purpose of this discussion will be to identify the known internal weaknesses of a mobile network and apply the concepts taught in the SANS Security Essentials Course to mitigate the risk of internal fraud.

I am an accountant by trade with expertise in the financial practices of the mobile telecommunications industry. Throughout my career I have worked with numerous mobile companies and have witnessed the impact that fraud can

have on their financial statements. Most notably is the unanticipated rise in consumer Bad Debt Expense. I firmly believe that this financial indicator only shows the visible "tip of the iceberg", so to speak. Most fraudulent activity, which shows up in this indicator, is from external exploits and can be sourced and corrected because the fraudulent customer account can be identified or the usage activity can be monitored. However, what keeps management up at night is internal employee fraud that can be disguised by altering internal network and system configurations. Only through fundamentally solid security policy and practices can this risk be mitigated.

Background:

A general understanding of a typical mobile network's architecture will be necessary to obtain the maximum benefit from this discussion. The concepts discussed here are derived from Internet research and recent discussions I had with client personnel in the engineering and IT groups. Figure 1 depicts this architecture and should be referenced back to throughout this section.

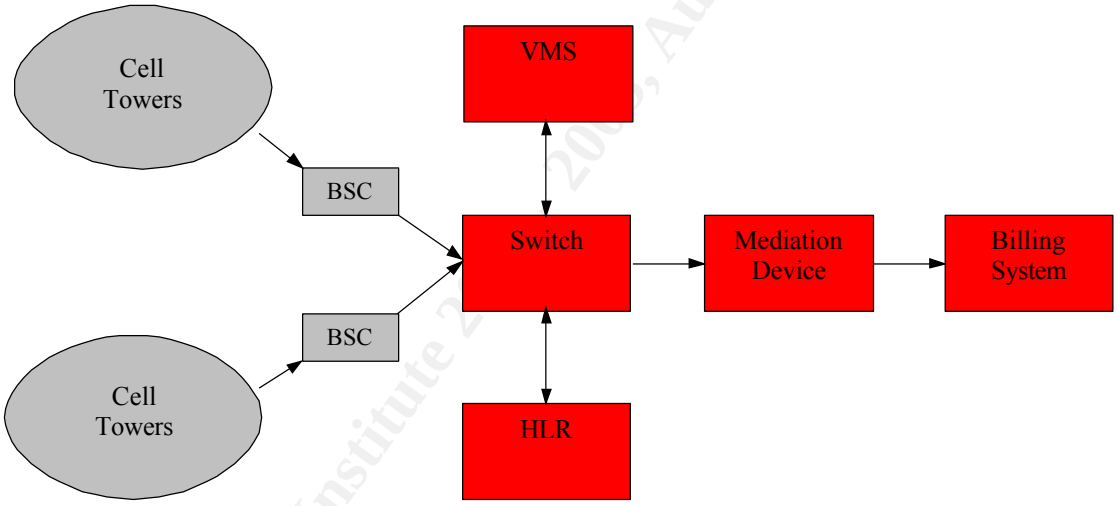

Figure 1

A mobile company's "world" begins with a subscriber making a call and ends with the customer's bill reflecting this usage. In between these two events are three major systems that make this process possible: the switch, mediation device, and billing system. Each of these network elements has an intended purpose and known vulnerabilities that can be exploited to commit internal fraud.

The switch is the most external network element and responsible for routing subscriber calls and generating a digital record of the usage, which is typically referred to as a CDR (Call Detail Record). The switch is connected to multiple BSC (Base Station Controllers), which are connected to multiple cellular towers. The BSC and cellular towers are commonly referred to as the RF (Radio Frequency) network. Therefore, the RF network and switch work in conjunction

to facilitate the delivery of wireless service.

One function of most mobile switching systems is the ability to send and receive voicemails using the carrier's VMS (Voicemail System). Typically, a customer can retrieve a message by calling the VMS and waiting for an automated prompt telling them to enter in their mobile telephone number. Once this information is entered, it is used to authenticate the customer to the system and allows them to retrieve messages and make outgoing calls through their voicemail box.

The final component of the switching system is the HLR (Home Location Registry). The HLR contains a directory of mobile telephone numbers with their corresponding handset identification number. When the customer makes a call attempt, the switch first queries the HLR to authenticate the user as being a valid subscriber. Once this validation is complete the user is allowed to make their call. A CDR is generated documenting the usage and the record is sent to the second network element, mediation.

Since a mobile company's switch and billing system vendor often differ, a device must be placed between this transmission to convert the CDRs into a format that is compatible with the billing system. In near real-time, the mediation device receives the CDRs from all of the company's switches via a frame relay or other type of secured WAN. There is a one mediation device to many switch relationship between these two network elements. At mediation, filtering often occurs where non-billable records (i.e. voicemail) are removed to decrease the processing load on the billing system. After CDR filtering and reprocessing is complete, the CDRs are sent to the company's billing system.

The billing system is the heart of a mobile company's network infrastructure. It is responsible for receiving CDRs from the mediation device via an internal dedicated connection, which cannot be accessed externally. Next, the CDRs are possibly filtered further, depending on the company's business rules, rates are applied to the CDRs depending on the customer's rate plan, and finally compiled into the bill that is sent to the customer. At this point the primary background information of the mobile network infrastructure has been provided. Each of the previous elements will be discussed in-depth with their inherent vulnerabilities and how the fundamentals taught in the SAN Security Essentials Course can be applied to mitigate the risk of internal fraud.

Types Of Fraud:

Fraud comes in many forms and types and each one can severely damage a company. From contractual or procedural fraud to hacking fraud, all types have negative, adverse affects on a company. For the purpose of this discussion, however, the focus will be on technical fraud. The following is a brief description of its characteristics:

> ***"Technical fraud –***
>
> *All frauds in this category involve attacks against weaknesses in the technology of the mobile system. Such frauds typically need some initial technical knowledge and ability, although once a weakness has been discovered this information is often quickly distributed in a form that non-technical people can use… In Technical Internal Fraud, fraudulent employees may alter certain internal information to allow certain users reduced cost access to services. The usage behaviour in these frauds depends on how long the fraud is expected to remain undetected. In the situation where the Fraudster believes that the fraud can be hidden for a long time, then the best approach would be to exhibit normal usage behaviour, as no attention is then drawn to it. However, if the fraud has a short lifetime, then the best approach is to make as much use of the service as possible until it is stopped."*

[Phil Gosset and Mark Hyland. "Classification, Detection and Prosecution of Fraud on Mobile Networks" http://www.esat.kuleuven.ac.be/cosic/aspect/papers/mobsummit.doc]

An understanding of the type of fraud that the company is attempting to prevent will allow a mobile company to create a detailed security policy and design controls to effectively mitigate the fraud risk.

Pervasive Controls (*Issue Specific Security Policy*):

A comprehensive, well thought out security policy is the foundation of a secure network. Its guidelines must be flexible enough to allow easy access to systems for legitimate business purposes while still being restrictive enough to prevent internal abuse. This trade-off between ease and restrictedness must be weighed when developing a security policy.

A policy that is well designed and takes into account the challenges faced in the environment it was meant to protect will effectively prevent internal fraud. Across every organization, in this case a mobile network, the following key concepts must be integrated into the company's network security policy:

- *What are our risks?* In a mobile network, the highest risk and most financial damage can come from a compromise of the switch, mediation device, or billing system. It is essential that these areas are identified and that the vulnerabilities or risks identified so that the security policy can be designed to protect these areas.

- *Who are our threats to these risks?* In our discussion, the primary culprit would be an employee using internal information of known system vulnerabilities to commit fraud. This threat, weighed against the company's risk enable the company to adequately allocate the proper attention and resources to protect their network. Now the controls can be designed to protect against the specific threat.

- *How do we reduce our risk by defending against the threats?* System controls are used to protect network resources. A control can be classified as being pervasive, specific, or monitoring. A pervasive control prevents an employee from compromising the system before even considering an attack. Examples of pervasive controls would be informing employees on the consequences of deceptive practices or having the employee sign a general security policy before they begin work. A specific control prevents an employee from physically or logically compromising a system. Examples of specific controls would be login passwords, MAC address filtering, or secured data centers. Monitoring controls are the final type of protection. They are used to notify administrators when an attack is in progresss or create a record of a successful compromise so that the weakness can be corrected and the fraudster identified. Each of these controls should be considered and used in conjunction when designing the controls scheme to protect each mobile network element.

- *What is a policy violation?* It may be difficult to reprimand an employee without a clearly defined, measurable list of violations because the violation becomes judgmental or subjective. The information should be present in all security policies.

- *What are the disciplinary actions when policy violations occur?* A security policy without consequences for violation is a dog without teeth. The policy is nice to read but it will offer little protection when someone breaks into the systems because there are no known disciplinary consequences. Without this area clearly defined, the company may be opening themselves to unnecessary litigation from disgruntled employees who felt they were unjustly disciplined.

The above broad concepts must be present in a security policy for it to effectively minimize the risk of internal employee fraud. The policy must also be backed and signed by executive management, so that if a violation does occur swift action will be taken. With the fundamentals of a security policy in place, our discussion will now focus on protecting the individual mobile network elements. While these elements are not the "crown jewels" (a phrase often quoted by SANS instructor Marc Sachs) of a mobile company, they may be considered the rings on the king's fingers or the medallion around his neck.

Specific Controls (*The Switch):*

A switch can be exploited by modifying either its filtering mechanism or the HLR. If an employee tampers with either of these areas, it is extremely difficult for the company to detect the exploit. Typically, a company has limited visibility into the switch. This limitation is partially attributed to the company's engineering department, whose performance is evaluated on throughput and not control over the CDR accuracy or fraud prevention. Therefore, few in-house reporting tools are designed to monitor this system from the perspective of controlling fraud. This fact causes most mobile companies to disable the switch's filtering mechanism and remove the records at mediation or the billing system where monitoring capabilities are more comprehensive. Unfortunately, though, with the proper system knowledge an internal employee could enable the filtering mechanism to remove records only generated by their handset's mobile telephone number. The fraudulent user could utilize the network without a record of the usage ever being sent to the billing system. Therefore, access to this system resource should be extremely restricted. System accounts with access should only be given to the manager of switch operations and should conform to baseline password standards. (Note: password standards will be discussed at the end of this section)

An unlikely area for internal fraud is the switch's VMS. This system can be exploit by adding an invalid mailbox number (i.e. mobile telephone number) to the VMS's registry. When the fraudster dials into the VMS and is asked for their mobile identification number, they simply enter in the false mailbox number. Once authenticated, the employee is able to make outbound calls using the added functions and call back features of the VMS. The CDR from this usage cannot be billed because the switch records the invalid mailbox number as the calling number (i.e. customer account for billing) in the CDR. When the record enters the billing system it would error out because it does not have a corresponding billing account. The VMS is an extremely effective place to hide fraudulent activity because, by its nature, it is viewed by the organization as a low risk area. Access to this system should be restricted to the switch operations manager and conform to the baseline password standards. (Note: password standards will be discussed at the end of this section)

Modification to the HLR is the final primary switch exploit. The user interface tools to this resource are often more user friendly than the switch and in-depth knowledge is not required to access the system. An employee can exploit this resource by adding their personal mobile and handset equipment number to the HLR. When a call attempt is made the switch would record the usage and send the CDR to the billing system where the record would error out because it would not have a corresponding billing account. The magnitude of this risk is large

since an employee has the ability to purchase handsets, provision them into the HLR, and create their own wireless company on their employer's network. Again, access to this resource should be extremely restricted since the financial impact to the company is great. System accounts with access should only be given to the manager of switch operations and should conform to baseline password standards. (Note: password standards will be discussed at the end of this section)

Specific Controls *(The Mediation Device):*

The primary internal threat to the mediation device is tampering with its filtering mechanism. Unlike the switch, though, the mediation device typically filters a high number of CDRs, which can exceed 50% of the network's total traffic. This high volume presents a problem for the mediation administrator because small-scale malicious activity, such as filtering a specific subscriber's CDRs, can be hidden within the legitimately filtered records. This situation is similar to the old adage "draining the alligator swamp". Where the alligator threat (employee fraud) is hidden within the swamp water (legitimately filtered records). Therefore, access to this resource should be extremely restricted. System accounts with access should only be given to the manager of mediation operations and should conform to baseline password standards. (Note: password standards will be discussed at the end of this section)

Specific Controls *(The Billing System):*

After the CDRs are sent to the billing system by mediation they are matched to the customer account and priced according to their rate plan. The database tables that contain a mobile company's various pricing plans are commonly referred to as the rate tables. If there is minimal logical security for the rate tables an employee could commit fraud by adding their own rate plan with a zero pricing scheme. When the employee uses their service, their CDRs would be processed normally except that their bill would have a zero balance due. Another situation where the rate tables could be abuse would be by a disgruntled employee wants to seriously harm a company. The employee could increase the pricing scheme of a common rate plan, thereby harming the reputation of the company by over billing their customers. Each of these situations illustrates the need for restricting access to the billing system's rate tables. Ideally, only a few individuals within the company should have access to these tables. Access to this system resource should be extremely restricted and conform to baseline password standards. (Note: password standards will be discussed at the end of this section)

Specific Controls (*Password Standards):*

A well-designed company-wide password standard will provide a baseline defense against employees accessing resources that they are not authorized to

use. Ideally, these standards should be enforced systematically by each network element and the system administrator, to ensure compliance, should periodically review the access lists. The following password standards should be present in all systems:

- Password Length – At a minimum, passwords should be no less than 8 characters long.
- Password Complexity – Passwords should be a combination of letters, numbers, and symbols. They should not be present in a dictionary.
- Password Change – At a minimum, passwords should be changed every 90 days.
- Unsuccessful Login Attempts – Passwords should be locked after 3 unsuccessful login attempts for 20 minutes to mitigate the threat of password cracking utilities.
- Password History (1) – Passwords should not be reused for 6 consecutive password changes.
- Password History (2) – Passwords can only be changed once every 2 days to prevent users from cycling through 6 password changes to arrive back at their original password.

The previous password configuration standards were derived from content taught in the SANS Security Essentials Course and the following Internet resource:

[Tom Perrine. "SDSC User Password Selection Standard" (10 January 2000) http://security.sdsc.edu/help/Standards.Guidelines/password-selection_Standard.shtml]

The previously mentioned password guidelines are exactly that, guidelines. Depending on the nature of the environment that they are intended to protect the standards may need to be strengthened for high-risk areas.

Monitoring Controls (*System logs):*

Even with a detailed security policy and adequate logical access controls the risk of internal fraud can never be assured. The final piece that must be in place to provide maximum protection is system access logs for each of the previously mentioned network elements. The administrators for each of these systems should generate logs for the following two types of activity:

- *Log access attempts into sensitive areas* – This log should be used to identify all users who attempt or successfully access these areas. When an unauthorized attempt is made, the employee can be quickly identified and dealt with according to the company's security policy before any damage can occur.

- *Log each change made by the user* – This log should be used to keep a historical record of all changes made by all users. If a fraudulent act has occurred, the compromised area can be located quickly and corrected before the unauthorized modification can severely impact the company.

Each of these logs should be created and reviewed daily by the system's administrator. When a violation has occurred, the administrator should escalate the occurrence to upper management personnel, who could discipline the employee in question. A comprehensive set of access logs will also provide evidence to defend the company if the reprimanded employee intends to pursue legal recourse because they felt wrongly accused of the violation.

Conclusion:

Throughout this discussion the topic of securing a mobile telecommunications network from internal fraud has been discussed in-depth. A company must begin to protect against fraudulent activity by first determining the type of fraud they are attempting to prevent. Next they must create an issue specific security policy statement that outlines the measures that will be taken to protect the network elements. Once executive management signs the policy and incorporates it into the company's standards, the individual system administrators can design the appropriate pervasive, specific, and monitoring controls to mitigate the risk of internal employee fraud. If these various controls are used sporadically or only in certain situations they will provide little protection against the company's risks. Vulnerable areas will be quickly identified by the insider and exploited for fraudulent purposes. However, when these concepts are used in conjunction with one another a security framework is created. The framework will enable the company to adequately prevent unauthorized activity or, in the event of successful fraudulent attack, will enable the company to quickly source and contain the problem before it affects their customer base. Thus, the company has successfully secured their mobile telecommunications network from internal fraud.

References:

Phil Gosset and Mark Hyland. “Classification, Detection and Prosecution of Fraud on Mobile Networks” (No Date Was Given)
http://www.esat.kuleuven.ac.be/cosic/aspect/papers/mobsummit.doc

Tom Perrine. “SDSC User Password Selection Standard” (10 January 2000)
http://security.sdsc.edu/help/Standards.Guidelines/password-selection_Standard.shtml

John Scourias. “Overview of the Global System for Mobile Communications” (14 October 1997) http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

Robert Williams. “Chapter 9. Sharing Without Sacrificing: Securing Wireless Networks” (26 April 1999)
http://www.tsl.state.tx.us/ld/pubs/wireless/chapter9.html

Renendra Bhattacharyya, Jandria Alexander, Robert Williamson. “Telecommunications Switch-Protection Profile” (1 November 1999)
http://niap.nist.gov/drafts/Switch_PP_Update.pdf

Jeff Crollick, Dick Gove, Ed Hall, Bob Montgomery, Art Priest. “Reliability Issues-Changing Technologies Focus Group - Wireless/PCS Subteam Final Report” (22 February 1996)
http://www.nric.org/pubs/nric2/fg3/6wrlspcs.pdf

Patrick Richardson (Mediation and Billing System Administrator)
North American Wireless Company

Dale Weaver (Switch Administrator) North American Wireless Company

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event