Global Information Assurance Certification Paper

GCIH PRACTICAL ASSIGNMENT
Version 2.0 - Exploit in action (Option 1)

Phone Phreaking and Social Engineering

Submitted by Richard Tuey
Attended: SANS CDI Conference on 29 Nov 2001

Date Submitted: January 29, 2002

Table of Contents

INTRODUCTION **1**

THE EXPLOIT **2**

NAME 2
CVE 2
VULNERABLE SYSTEMS 2
PROTOCOLS/SERVICES/APPLICATIONS 2
BRIEF DESCRIPTION OF EXPLOIT 2
VARIANTS 3
REFERENCES 3
Exploit *3*
Source Code *3*

THE ATTACK **4**

DESCRIPTION OF THE NETWORK 4
RECONNAISSANCE 5
SCANNING 6
HOW THE EXPLOIT WORKS 6
PROTOCOL DESCRIPTION 7
DESCRIPTION AND DIAGRAM OF THE ATTACK 7
SIGNATURES OF THE ATTACK 9
HOW TO PROTECT YOUR SYSTEMS 10
What Companies Can Do To Protect Themselves *10*
How Vendors Can Prevent This Vulnerability *12*

THE INCIDENT HANDLING PROCESS **13**

PHASE 1: PREPARATION 13
PHASE 2: IDENTIFICATION 15
PHASE 3: CONTAINMENT 15
PHASE 4: ERADICATION 16
PHASE 5: RECOVERY 18
PHASE 6: LESSONS LEARNED/FOLLOW-UP 18

CONCLUSIONS **21**

GLOSSARY **22**

WORKS CITED **24**

Introduction

On 01 through 02 November 2001, X Corporation suffered a series of related toll-fraud incidents that used a combination of Private Branch Exchange (PBX)/Voice Mail System (VMS) vulnerabilities, and social engineering to enable attackers to use X's telephone system to make international calls.

This paper details these incidents in three sections: The Exploit, The Attack, and the Incident Handling Process.

Section One categorizes and defines the exploit used to attack the PBX/VMS vulnerabilities.

Section Two begins with an overview of the attack execution against X Corporation. It then delves into the methods the attackers might have used to prepare for the attack. It further explores alternative exploits attackers might have employed using PBX vulnerabilities, which became evident in the "Recovery" and "Follow Up" phases of incident handling. This section closes by identifying the attack's recognizable signature; and protection measures needed to protect against the attack.

Section Three describes how the six step incident handling process of Preparation; Identification; Containment; Eradication; Recovery; and Lessons Learned was applied to this incident.

Background.

X Corporation is a large, international conglomerate firm that has worldwide clientele. The firm has multiple business sectors, which are broken into business units. Many of the business units are part of X Corporation as a result of mergers and acquisitions. As a result, there are large arrays of offices throughout the United States that do not have a single integrated information technology system, nor are these offices under a single configuration management program. New acquisitions typically operate under the rules of their former corporation until the X Corporation Information Services group has time to work with them and gracefully integrate them into the policies and infrastructure of the overall corporate networks.

X Corporation works feverishly to administratively organize IT management, but frequent change; caps on "overhead" staff personnel; and management reorganization are the order of the day. The subject of this paper is an incident is the home offices of X Corporation's Omega business unit, located in Midwest, USA.

Omega is a manufacturer of goods and supplier of services to worldwide markets. It has facilities located in over 9 countries. The Midwest, USA offices are served by the Northern

Telecom (Nortel) Meridian 1 Option 61C PBX/VMS. The Meridian 1 serves up to 2000 ports. The operating system uses dual Motorola processors.

Nortel claims the Meridian 1 "is currently used by more business people than any other digital communications system" (Northern Telecom, *Meridian 1 Option 51C, 61C or 81C*, p. 1). Unfortunately, it appears to have a default configuration with vulnerabilities that phone phreaks exploit for toll fraud. The downside of having a popular PBX/VMS, is that hacking information is more readily available, and the vulnerabilities better understood by the hackers or phone phreaks who want "free" long distance calls.

Up to this point, the Omega business unit had never experienced a recognized toll-fraud incident.

The Exploit

Name

PBX Toll Fraud and Social Engineering

CVE

None

Vulnerable Systems

Nortel Meridian 1 PBX/VMS
Any PBX/VMS permitting transfers to outside trunk connections

Protocols/Services/Applications

PBX Outside Trunk Access
Direct Outward Dialing (DOD)

Brief Description of Exploit

Unwitting users of a company's PBX/VMS can be manipulated with Social Engineering into transferring external callers (callers not directly connected to the PBX/VMS) to outside trunk lines. Once transferred, the callers initiate operator-assisted local, long distance, and

international long distance calls. The operator-assistance is somewhat a misnomer, since most long distance service is now automated voice prompts.

With further effort, external callers may be able to use voice mailboxes to execute "through dialing" or "call forwarding" to these same surreptitious numbers without operator-assistance.

Variants

PBX Through Dialing
Remote Call Forward

References

In addition to describing how this exploit can be employed, these references describe the vulnerabilities and system information necessary to execute the exploit on a Nortel Meridian 1 system.

Exploit

- http://www.ameritech.com/content/0,3086,92,00.html
  (SBC Consumer Information on Social Engineering Fraud.)
- http://pub56.ezboard.com/fpbxinfofrm18.showMessage?topicID=2.topic
  (Article by D4rkcyde describing method to obtain valid extensions, and how to "out dial".)
- http://home.wi.rr.com/browser/ght/scam90.html
  (Describes extension 9000 scam and provides methods to prevent it.)
- http://pbxinfo.com/maxpages/Meridian_Mail_holes
  (Describes how to identify a Meridian VMS system; password guessing techniques; and describes exploiting the programmed operator assistance number.)
- http://www.infowar.com/iwftp/Phrack/P44-19.txt
  (Phrack article by Iceman that provides a technical overview of the Meridian system; features; and terminal programming.)

Source Code

- http://www.pbxinfo.com/maxpages/Voicemail_Security
  (Description of common voicemail security threats, and how social engineering could be executed to obtain an outside trunk line.)
- http://pbxinfo.com/maxpages/Meridian_Mail_Features
  (Step-by-step guide to using Meridian VMS features. It includes logging in; changing passwords; and through dialing.)
- http://www.pla813.org/texts/An%20Introduction%20to%20Meridian%20Mail.txt
  (Techniques to identify and hack the Meridian PBX/VMS.)

- http://www.phrack.org/show.php?p=47&a=15
  (Techniques to identify a Meridian PBX/VMS; identify valid extensions; guess passwords; and execute out dialing from a mailbox.)

The Attack

While the X Corporation attack at the Omega offices in Midwest, USA could be a simple case of semi-random Social Engineering, for thoroughness I explore how a pre-meditated attack would have been planned and executed. The discussion opens with a network description. It then delves into reconnaissance against the Midwest, USA network; scanning the network; and how the exploit works. The section continues with the PBX/VMS protocols affected by the exploit; a description of the actual attack; and discussion of the attack signatures. Finally, the section concludes with discussion of methods to prevent or mitigate future attacks using the exploit.

Description of the Network

The Omega Business Unit offices in Midwest, USA use the Nortel Meridian 1 Option 61C PBX/VMS with software release 21. The Option 61C, designed for mid-sized to large businesses, has dual Motorola 68060E processors that uses 250 of the available 2,000 ports using digital or analog telephone handsets.

The system accepts incoming calls to a central switchboard, as well as a number of directly dialed numbers to employee offices. The PBX permits external call forwarding on some stations, but does not permit "through dialing" on any numbers. Because of the firm's worldwide presence, unlimited international calls are permitted on numbers assigned to some stations.

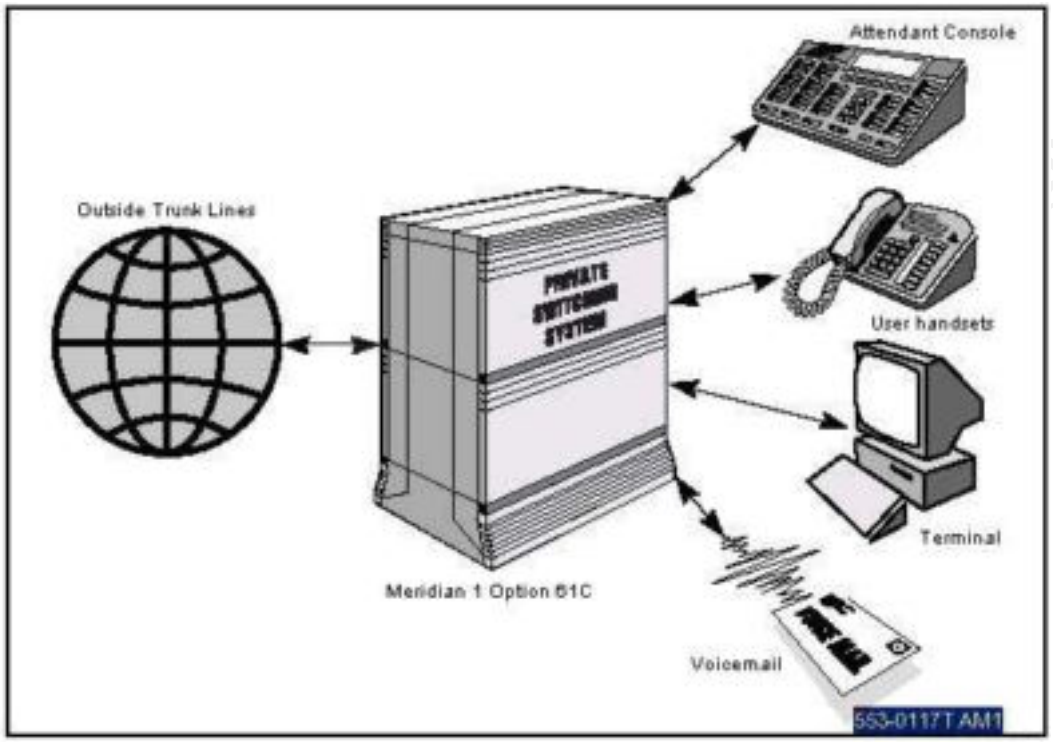
To facilitate business, Omega also maintains a toll-free "800" customer service number. It publishes the toll-free number in its sales literature, and on its web site. The ABC Phone Company provides long distance telephone service to the Midwest, USA offices. SBC is the local carrier.

On weekends and evenings (after 11 p.m. EST), the PBX is programmed to route toll-free and switchboard calls to an attendant console. Contract labor security officers man the attendant console.

Omega out sources configuration and maintenance of its Meridian PBX/VMS to the XYZ Company. XYZ Company remotely accesses the Meridian system via dial-up modem line. To protect the modem from attack, it is on an A/B switch that is left disabled until XYZ Company calls the Omega Midwest Site Telecommunications Manager to request remote access.

The Omega Midwest Site Telecommunications Manager sets both the PBX console password and the VMS password. When needed, the password is provided to XYZ Company personnel to make PBX modem access.

Omega Business Unit PBX/VMS Network at Midwest, USA



(Northern Telecom, *Meridian 1 Option 21C through 81C System Programming Guide*, p. 14)

Reconnaissance

The exploit described will work on most PBX systems where an attacker can reach a person willing transfer a call. However, I will delve into the methods an attacker could have used to identify Midwest, USA site's Nortel Meridian 1 PBX/VMS. This knowledge enables an attacker to pursue other exploits against user mailboxes.

Because the Omega Business Unit has a worldwide customer base, Omega maintains an Internet web site. The web site provides a toll-free customer service number (800-555-5555) to the Midwest, USA offices and a fax number (555-555-5535). The site also lists names and email addresses of corporate officials, many of whom actually have offices at the Midwest, USA site. It is a good assumption that these officials will have extended privileges on the PBX/VMS.

Upon calling the toll-free number, you reach a customer service representative who can forward calls to appropriate technical support or sales representatives. You can also be forwarded to any of the corporate officials on the web page.

On weekdays after 11:00 p.m. EST, weekends, and holidays, the PBX night service engages. Calls on the toll-free line go directly to an attendant console manned by a single contract security person. The security guards work 8-hour shifts that run from 11:00 p.m. to 7:00 a.m. EST; 7:00 a.m. to 3:00 p.m. EST; and 3:00 p.m. to 11:00 p.m. EST. The guard can direct calls to internal extensions, and can make outbound trunk connections. Attackers could acquire

this information by calling the toll-free line a few hours after the working day and requesting transfer to one of the sales representatives listed in the corporation's web page. Additionally, an attacker may request transfer to the customer support mailbox.

The fax number listed is not toll-free, but it does identify the area code (555); the exchange (555); and the dialing block (55xx) that is also used for direct dial lines to employee offices. Directly dialed lines bypass the switchboard and connect to the employee's voice mailbox.

Scanning

Unless trying to locate a modem into the PBX console, "war dialers" are not practical for scanning target numbers into a PBX. Hand dialing and physical monitoring of calls made is required because the attacker needs to hear the VMS response. However, the attacker has a head start into locating valid dialing blocks by using the "55XX" numbers found from the listed fax number.

How the Exploit Works

The default Meridian 1 PBX/VMS configuration does not appear to routinely exclude the following system privileges:

- Direct dialing of "1-900"and "1-976" numbers (toll services often tied to phone sex sites and psychic hotlines)
- Direct dialing of offshore area codes such as the Dominican Republic (1-809), which are frequently tied to toll fraud.
- Internal transfers to extensions such as "9000", which gives a caller access to the operator on an outbound trunk.
- Internal transfers to outbound trunks using incomplete numbers such as "1-(valid area code)".

When the Meridian 1 PBX/VMS permits users to transfer external calls to outbound trunks, then transfer to any extension "90xx" results in accessing the outside trunk line with the "9", and dialing the local operator with the "0". The remaining digits of the extension are irrelevant. After reaching an "automated" operator, the attacker just dials the desired number. If a "live" operator is reached, the attacker requests operator assistance in making a toll call to U.S. and international numbers. The call is billed to the company serviced by the PBX.

Alternatively, an attacker could make a call to a user's directly dialed number. If the user does not answer, the voice mailbox engages. At the recorded prompts, the attacker presses the "*" key. This brings up a voice menu. After entering "81", you receive the login prompt. Unfortunately, common weak passwords are often used such as: "1#, bx#, 0000#, 1111#, 2222#, 1234#, 9999# (note: # is the button you press when you finish entering the password)" (The Clone, *An Introduction to Meridian Mail R1s.12*, p. 1)

If the attacker breaks into a voice mailbox with through dialing privileges, the attacker can reach an outside trunk line using the following procedures:

Step 1. Log into (the) Meridian Mailbox.
Step 2. Enter your password
Step 3. While listening to the greeting press #0, then

> immediately dial the number you wish to call, followed
> by the" # " pound key.
> I.e. #0, 9-1-800-555-1212#
> *Remember to include your outside access number whatever it is (9)(8). This feature has to be programmed in your Meridian Voicemail system before it will work. You can set this up to dial internal or external numbers. (PBX Info, *"Meridian Mail – A Beginner's Guide to Meridian Mail Features"; p.1)*

Protocol Description

The Meridian 1 has a feature called the Basic Alternate Route Selection (BARS). This feature controls "the number and type of trunks that are available to each network caller, and a method of controlling the time of day that access to a trunk (or group of trunks) is allowed" (Northern Telecom, *Meridian 1 – Option 11C*, p. 871).

Within BARS, the Meridian 1 defines Network Class of Service (NCOS) groups, which are essentially matrices of privileges and dialing configurations that can be assigned to an extension. "Included as part of each NCOS group is a Facility Restriction Level (FRL) number which ranges from 0 (low-privilege) to 7 (high-privilege). The FRL …determines … the alternate route selection choices available for network call attempts by users within an NCOS group" (Northern Telecom, *Meridian 1 – Option 11C*, p. 875).

Multinational companies, such as X Corporation and its Omega business unit, have many sales and marketing needs that require employees to have ready access to local and international customers. Thus, PBX Outside Trunk Access is critical. Without it, users have only an intercom system. For example, outside trunk access is also needed to establish "conference calls" with multiple external users. For its mobile sales force or telecommuters, a company may configure certain user numbers to allow "through dialing" or "call forwarding" to numbers external to the office.

Because of the previously stated requirements, most user extensions are assigned to an NCOS group that permits outside trunk access. Typically, a PBX user will dial "9" to reach an outside trunk, and then dial the intended phone number. For phones located in public areas, the PBX can be configured to only permit interoffice calls; local calls and/or toll-free calls.

Description and Diagram of the Attack

External callers begin calling the Omega toll-free "Customer Service" number at 2:51 a.m. EST on Saturday, 01 December 2001. The weekend/night service on the PBX routes calls to the attendant console manned by a security guard. Callers request to be transferred to "Steve" at extension 9000. A first series of five calls are made that end by 8:10 a.m. These calls are begun during the 10 p.m. to 6 a.m. guard shift. A second series of four calls begin at 10:59 a.m. and end by 3:39 p.m. EST. The second series are begun during next guard shift of 7 a.m. to 3 p.m. The two series of nine international calls total 1181 minutes and cost approximately $3,560.

At 7:59 p.m. EST on 01 December 2001, nearly 17 hours after the attack begins, the ABC Phone Carrier Corporate Security contacts Bob Smith of X Corporation's network management staff concerning possible a toll fraud incident from offices located in Midwest, USA. Mr. Smith then contacts the corporate Information Assurance (IA) team for assistance. "On-call" IA team member Joe Friday is assigned to the case.

At 8:20 p.m. EST, Mr. Friday contacts ABC Corporate Security. ABC advises that they suspect toll fraud occurring at the Midwest, USA offices of X Corporation. Some nine international calls have been made to a single North African country on a weekend during the early morning. The calls ranged from 23 to 253 minutes. It is nearly 5 hours since the last fraudulent call ended at 3:39 p.m. EST.

Because X Corporation has numerous continental and international locations and subsidiaries; Mr. Friday initially has difficulty locating names or phone numbers of personnel at the Midwest, USA office. He calls Corporate Security Operations Centers on both coasts without success. Finally, he calls the guard at the Midwest, USA site attendant console. The guard provides him the pager number of the site Manager of Telecommunications, Shirley Jones. Mr. Friday explains the situation to Ms. Jones. She agrees that the late night international calls are fraudulent. An employee of over 15 years at Omega, Ms. Jones knows that few employees ever work late in the evening or on weekends, and they would certainly not be making international calls.

At 11:00 p.m. EST, Ms. Jones directs the on-watch security guard at the Midwest, USA site to not transfer any incoming calls to internal company extensions. Most of the security guards at the Midwest, USA site have worked at the site for a long time, and they know Ms. Jones. Ms. Jones feels confident that her instructions are understood and will be carried out.

Unfortunately, the word does not seem to make it to next guard shift from 7 a.m. to 3 p.m. the next day. The regular guard took ill, and a substitute was filling in. On Sunday, 02 December 2001, 11 additional international calls are made from 11:23 a.m. EST to 8:33 p.m. EST. These calls total 852 minutes for approximately $2,634 in charges. The calls begin after the guard shift change. The last call is made at 2:02 p.m., but lasts for 390 minutes.

After having transferred 11 calls to extension “9000”, the substitute security guard is suspicious. He calls Ms. Jones after 2 p.m. He notes that the requests for transfers are unusual. Ms. Jones is surprised that her prior instructions regarding transfers had not reached this guard. She directs that no further transfers be made, and that this be passed on to the succeeding guards.

Meanwhile ABC Phone Company Security recognizes that these calls are similar to the previously detected pattern. Although still to the same North African country, the calls are to different phone numbers. The calls range from 30 seconds to 390 minutes. This time ABC directly contacts Mr. Friday at 7:25 p.m. EST.

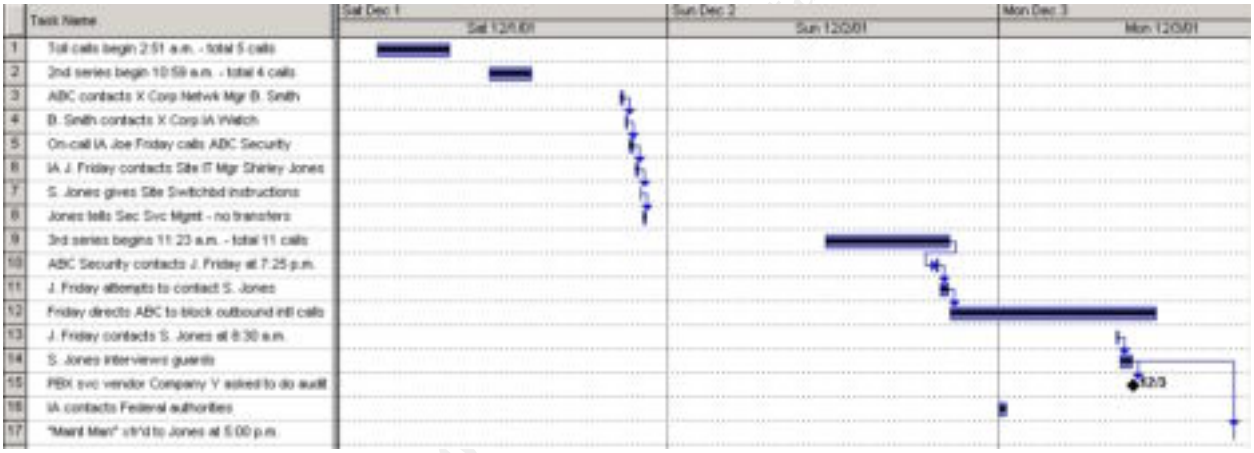
Mr. Friday unsuccessfully attempts to contact Ms. Jones. By 8:20 p.m. EST on Sunday, 02 December 2001, Mr. Friday decides to have ABC Phone Company block all international calls outbound from the Midwest, USA PBX. The last fraudulent call terminates at 8:33 p.m. EST. It is possible that Mr. Friday’s actions shut down this last call. The damage on Sunday was 11 calls totaling 852 minutes for an approximate cost of $2633.

Mr. Friday finally reaches Ms. Jones at 8:30 a.m. EST on Monday, 03 December 2001. Ms. Jones calls the contract security service manager. She learns that her directive to not transfer inbound calls from the attendant console had not been passed to the succeeding shifts. She then learns from the security service manager that the guards had received calls on the attendant console. The callers requested to be transferred to “Steve” at extension “9000”. The guards complied.

As a result of knowledge gained from the interviews, Ms. Jones issued more emphatic instructions to the guard staff and daytime operators that required that any calls to any "90xx" extension be routed to her. She drafted explicit instructions regarding handling of weekend calls. These instructions included orders to not transfer any inbound calls to outside lines, and especially to not transfer to extension "9000".

Alerted to the prior incidences of toll fraud, the contract security officers and daytime operators were instructed to route all new requests for transfers to any "90xx" extension to Ms. Jones. Around 5:00 p.m. EST on Monday, 03 December 2001, a caller claiming to be with the Phone Company indicated he was performing maintenance, and requested transfer to extension 9000 or 9001. The call was transferred to Ms. Jones. When she began to ask him questions to verify his identity, he hung up. This appeared to be the conclusion of the attacks.

The timeline of key events appears below:



Signatures of the Attack

The X Corporation attack reveals several identifying characteristics at different stages. The first and most important signature is the act of Social Engineering. The next signature is the call profile. Finally, there are the unexpectedly high telephone bills.

What are the signs of Social Engineering? First, a definition is in order. In a recent SANS article, Wendy Arthurs describes Social Engineering as follows:

"It can be defined as an outsider tricking legitimate personnel into aiding illicit acts such as supplying proprietary information or allowing inappropriate access. It preys on the weakest link in a security system – the human being. Social engineers are con artists who exploit human vulnerabilities such as ignorance, naiveté and an individual's natural desire to be liked and helpful. . . . It relies on interpersonal relations and deception, using the 'tools' of the trade such as flattery, intimidation, name-dropping, asserting authority and belittling." (Arthurs, p. 1)

Security Focus is more blunt: "social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system." (Granger, p. 1)

With this explanation of what a social engineer does, what are the attack signatures or warning signs? Here are typical ploys:

- Requests for transfers to an operator. . (SBC Ameritech, p. 1)
- Background noise, which indicates that the call is coming from outside of the business (e.g., cars, trucks, street noise that indicates the call is coming from a payphone). (SBC Ameritech, p. 1)
- Requests for outside lines or transfers after hours or on weekends when most supervisory personnel are gone for the day. . (SBC Ameritech, p. 1)
- Unsolicited calls requesting personal or proprietary information. (SBC Ameritech, p. 1)
- Requests for a user to participate in a system test procedure.
- Corporate officials and manager name dropping, and claims of important tasks to be completed that require privileged information or assistance.
- Requests for the name of the supervisor on duty; transferring the call to that individual; and using that person's name and position to invoke familiarity.

"Social engineering usually involves some form of impersonation, of either a particular individual or a role. The person may pretend to be a repairman, a fellow employee, a manager or a person of trust phoning with the authority of an important user." (Arthurs, p. 1) In fact, in the initial X Corporation attack, the attackers impersonated customers wishing to speak to "Steve". At the end, an attacker pretended to be a telephone repairman.

The next signature of PBX toll fraud is the calling pattern. If Social Engineering or another exploit succeeds, the attackers realize that often a small window of time exists before they are detected and the vulnerabilities removed. Thus, they tend to exploit a system for as long, and as frequently as possible. However, the best times to exploit vulnerabilities still remains after hours and on weekends when inexperienced or "contract labor" can be Social Engineered. This results in outbound calls to international and continental U.S. destinations from the PBX, which are unusually long; frequent; and during evening or early morning hours. PBX's such as Meridian 1 have call logging facilities that could record any outbound trunk activity.

Telephone service providers generally have fraud detection programs that identify these unusual calling patterns of call frequency; time of day; call destinations; and length of calls. Once suspicions are raised, the service provider contacts company authorities to indicate potential toll fraud. This was how X Corporation's Information Assurance (IA) Team was notified of the 01 December attack.

If the "through dialing" exploit is being used, then the prior signature of "unusual calling patterns" is still valid. In addition, review of the PBX system audit logs may review series of failed password attempts against voice mailboxes.

A final signature which is usually too late to be of use, occurs when a company receives its monthly phone bill. Accounts Payable personnel will see a spike in long distance charges. They may even notice area codes or numbers not usually associated with corporate business.

How to Protect Your Systems

What Companies Can Do To Protect Themselves

Protection comes in two forms:

1) Modifying personnel behavior through policies and training
2) Modifying PBX/VMS configuration

Here are the elements of policies and training required to defeat Social Engineering:

- Well-defined and publicized policy of no transfers to outside lines to anyone, including "telephone company" or "law enforcement" officials.
- No transfers of calls to any "90xx" extensions. Explanation of why makes it easier to remember.
- Employ corporate calling cards for employee access to long distance services.
- Do not provide proprietary or personal information to unsolicited callers.
- Set forth protocols to identify incoming calls from "employees", such as callbacks, employee identification number, employee's supervisor name, etc.
- Reduce the success of dumpster divers by shredding phone lists and organization charts with employee names.
- Stress to employees the need to use non-trivial passwords on VMS mailboxes.
- Remind PBX/VMS administrators to not use trivial or common default passwords when setting up new mailboxes.
- Enforce periodic password changes to the system console.
- Make PBX/VMS security training a part of orientation for new employees, temporary employees, and consultants.
- Provide periodic security reminder training to all employees, temporary employees, and consultants. Inclusion of "real-life" examples of exploits and toll-fraud makes it more interesting, and hopefully more memorable.
- Reminders to PBX/VMS Administration personnel to take care in posting problems to Internet bulletin boards such as http://www.pbxinfo.com. These bulletin boards are a lucrative source of intelligence and even social engineering.
- Review corporate web site pages to ensure that unnecessary personal information is not posted. Organization charts, names, and phone numbers on web sites make "reconnaissance" much easier.

The following steps in PBX/VMS system configuration (if the system has enough programming flexibility) make Social Engineering and "through dialing" exploits more difficult:

- Do not permit "through dialing" on any extensions.
- Do not permit call forwarding to outside trunk lines.
- Require VMS mailbox passwords with 8 numbers or greater.
- Lock VMS mailboxes after greater than 5 failed password attempts.
- Establish blocks on any outbound calls to well known toll fraud area codes such as "900", "976", "809", etc.
- If connections to outside trunks are allowed, do not permit transfers to incomplete numbers such as "9,1-<any area code>".

- Do not permit inbound calls to redirect to other extensions other than the attendant console or other designated number.
- Separate toll-free numbers from access to the corporate address book.

How Vendors Can Prevent This Vulnerability

Many companies do not have the expertise to install, configure, operate and maintain a PBX/VMS. Often, they contract outside vendors to purchase, install, configure and operate their system. Unless otherwise specified, a vendor may presume that a customer wants maximum flexibility from their system. In addition, the vendor usually conducts its work remotely with modem access to the system console. System patches may not be part of the service contract and usually affect the availability of the system.

PBX/VMS manufacturers and system operating vendors can take these steps to reduce their customer's vulnerability to toll fraud:

- Deliver a restrictive default configuration. This includes requiring 8 digit passwords on VMS mailboxes; blocking calls to known toll-fraud area codes; and turning off dangerous privileges such as "through dialing".
- Provide customers with templates for greater privileges that also identify the greater risks involved.
- Using a phone number to the system console that is not within the PBX calling block to make war dialing more difficult.
- Use fax numbers that are not within the PBX calling block.
- Set up system console modem callback, and restrict the modem to calling specific numbers.
- Change default system passwords after system delivery.
- Negotiate a schedule for password changes and system software maintenance with customers.

The Incident Handling Process

This section describes X Corporation's response to the Social Engineering attack using a "Six Phase Approach" of 1) Preparation, 2) Identification, 3) Containment, 4) Eradication, 5) Recovery, and 6) Lessons learned.

Phase 1: Preparation

"The preparation phase is used to ensure that the organization has the resources and skills necessary to respond to an incident. This phase includes countermeasures to deter or detect an attack, creating an incident handling team, establishing procedures, defining policies, disaster recovery and communication plans, and a stock of necessary supplies." (Zago-Swart, p. 19)

The SANS Track 4 segment on Incident Handling Step-by-Step provided a checklist of preparation steps. The following describes the relevant steps and the extent to which X Corporation had covered these steps in relation to the toll-fraud attack:

Policy.
X Corporation has an explicit Incident Response policy document which is held at a corporate proprietary level. A living document that is currently under revision, it delegates responsibilities and provides guidance on measures to be taken at the major steps of the incident handling process. The steps conform to those discussed in SANS training: 1) Identification; 2) Containment; 3) Eradication; 4) Recovery; and 5) Follow-up.

In addition, X Corporation first promulgated a four page policy on "PBX and Voice Mail Security" on 29 October 2001. Of note, the policy strictly prohibits "Direct Inward System Access" (DISA) or "through dialing" privileges on any corporate system. Here are some of the other pertinent policies:

- If possible, restrict international or long distance calling after work hours and weekends.
- Restrict international calling privileges to specified users.
- Prohibit call forwarding to external trunk lines.
- PBX and VMS System passwords must change every 90 days and be at least 8 digits.
- Create classes of service that provide different levels of calling privileges.
- The Corporate Manager of Information Assurance is responsible for policy compliance.
- Prohibit call forwarding to external trunk lines.
- PBX and VMS System passwords must change every 90 days and be at least 8 digits.
- Create and assign classes of service that provide different levels of calling privileges.

People.
X Corporation revised its description of the responsibilities and authority of its Manager of Information Assurance (IA) on 21 June 2001. The IA Manager is charged with providing leadership and management of corporate Information Assurance.

The responsibilities include conduct of technical investigations at the request of the Audit, Legal, Ethics, Security, and Human Resources organizations. As such, the IA Manager is the "Team Lead" for the nine person corporate Incident Handling Team.

This staff is heavily tasked by the many Information Assurance requirements across the large multinational corporation, as well as needing to respond to incidents. Therefore, X Corporation relies on local administrative staff to be the primary responders with guidance from the corporate Incident Handlers. The nine-person team has weekly rotating "watch" coverage for incidents.

When any Information Technology (IT) system problems are encountered, X Corporation employees can contact a 24-hour Call Center/Help Desk. If Help Desk personnel detect or suspect an incident at any site, they page the on-call Incident Handling Coordinator. The Coordinator has these responsibilities:

- Assess the severity and scope of the incident
- Contact appropriate members of the Incident Handling team, and organize a response team
- Maintain a log of all associated activities
- Notify Corporate Security and management
- Generate regular incident handling status reports

The IA Manager remains the overall Team Lead, and is kept apprised of all incidents.

Data.
The incident handling team relies upon information gathering by on-site personnel. In this particular incident, PBX Service vendor XYZ Company was charged with gathering the pertinent log and configuration information. XYZ Company conducts a system audit by outputting the Nortel Meridian 1 system configuration.

A data gathering toolkit is not maintained, since it is corporate policy to have local administrators conduct incident containment, eradication and recovery with remote Incident Handling team assistance. Where incidents involve serious security or legal issues, a team member will travel to the site to maintain the evidential chain of custody. This member will conduct further investigations, as required.

Communications.
Because of the different time zones and locations, communications are usually restricted to pagers; telephone calls; voice mail; and email.

Transportation.
Because X Corporation is a multinational with offices throughout the world; it is not feasible for the corporate Information Assurance staff to personally go to each incident site. Usually, telephone, facsimile (fax), and email contact with local site officials is adequate. When required, X Corporation has 24-hour emergency travel services provided by American Express.

Documentation.
X Corporation is comprised of many different operating units and wholly owned subsidiaries. Thus, X Corporation has many different PBX/VMS systems being used at different sites. It is

left to the local site and their Service vendors to maintain adequate system documentation. System backup, and disaster recovery is also left to either the local site, or its PBX service vendor.

Phase 2: Identification

Identifying toll fraud or social engineering incidents requires recognition of the signatures described in Section 1. When employees do not recognize Social Engineering, the next line of defense against toll fraud is recognition of unusual calling patterns in PBX system audits of incoming and outgoing calls. Unfortunately, this is either very time consuming for the site PBX administrator, or very expensive when a site relies upon a 3rd party vendor. The breadth of the 3rd party service contract may also be limited to save money.

In this paper's toll fraud incident, the ABC Telephone Company's fraud detection program detected the unusual calling pattern of multiple international calls very late at night from the Midwest, USA site. The ABC Security Team contacted Bob Smith, a Network Security manager for a business unit within X Corporation. After several phone calls throughout the corporation, Mr. Smith finally reached the on-call Incident Handling Coordinator, Joe Friday.

As previously noted, X Corporation is a large multinational company with sites worldwide. In addition, the business at the Midwest, USA site was acquired by X Corporation in a merger that only concluded within the last 9 months. Although the incident handling team normally has listings of key points of contact at each corporate site, the listings were not current enough to include the Midwest, USA site. To locate someone with IT responsibilities at the Midwest, USA site, Mr. Friday paged a Corporate Security Director who had a current listing of managers for some but not all of the corporate business sectors. Mr. Friday then decided to use the source phone number provided by the ABC Telephone Company Security. This reached the guard manning the Midwest, USA site attendant console. The guard provided Mr. Friday with the home number of the site Manager for Telecommunications, Shirley Jones.

Thus, Mr. Friday called Shirley Jones and apprised her of the situation: ABC Telephone Company Security had detected potentially fraudulent calls being made to a North African country since 2:51 a.m. that morning.

Ms. Jones assumed that actual toll fraud had occurred since Midwest, USA site offices are closed on Saturday, and thus sales or staff personnel would be unlikely to make international calls. However, the incident root cause was undetermined. Mr. Friday and Ms. Jones suspected either social engineering or PBX misconfiguration.

From the first fraudulent call at 2:51 a.m. EST on 01 December to completing discussions with Ms. Jones around 9:45 p.m. EST on 01 December, the incident identification process took nearly 19 hours. By this time, the phone phreakers had made over nine calls totaling 1181 minutes.

Phase 3: Containment

To limit the damage from an incident, X Corporation attempts to take the following containment steps:

- Assess whether the system under attack contains proprietary or sensitive information.

- Determine the nature of the attack – system browsing; system configuration or file changes; or system exploitation for other purposes.
- Decide whether to shut the system down; remove the system from any networks; monitor the system; set traps; or disable specific functions.
- Gather evidence that includes log files with timestamps.
- Damage assessment.

Because of the sensitivity of actions taken at this critical juncture, the IA Manager usually makes the final decisions on the course of action. The decision largely depends upon the nature of information at risk and the extent of damage. The default response is to remove system intruders as soon as possible. This usually means removing the affected system from any networks.

While no sensitive or proprietary information was at risk from the toll fraud, the downside of direct monetary costs from extensive international calls resulted in the decision to restrict inbound calls to the PBX. The cause of the toll fraud was still undetermined. At 11:00 p.m. EST on Saturday, 01 December 2001, Ms. Jones contacted the on-duty watch person who manned the PBX attendant console. The toll fraud incidents occurred on the two previous watches. The guard, with whom she talked, had not experienced any extension "9000" transfer requests. However, Ms. Jones directed that no transfers be made from external calls to any internal extensions.

Unbeknownst to Ms. Jones, her directive was not passed to the succeeding watches. A substitute guard took the place of the regular guard for the 7 a.m. to 3 p.m. shift on Sunday. At 11:23 a.m. EST on Sunday, 02 December 2001, a third series of international calls began. By the time the security guard became suspicious over transferring calls, 11 calls had been made. The last call began at 2:02 p.m. and continued until 8:33 p.m.

Recognizing the same fraudulent pattern, ABC Phone Company had contacted Mr. Friday at 7:25 p.m. EST. As noted in Section 1, Mr. Friday could not reach Ms. Jones. Around 8:20 p.m., he decided to take action to contain further abuse of the Midwest, USA PBX. He directed ABC Phone Company to block all outbound international calls from the Midwest, USA trunk lines until further notice.

This dramatic action was feasible since it was still a weekend and the regular workday did not commence until 7:30 a.m. CST. In addition, employees could use calling cards as a workaround to making directly dialed international calls. This action gave the Incident Handling team breathing room to assess what was happening. Mr. Friday had thought the directives given by Ms. Jones to "not transfer any inbound calls" were sufficient to stop any Social Engineering. It now appeared that the attack might have come through some exploit in the PBX configuration.

Phase 4: Eradication

The eradication phase has multiple goals: 1) Determine the cause and symptoms of the incident; 2) Improve system defenses; 3) Perform a system vulnerability analysis; and most importantly 4) Remove the cause of the incident.

To eradicate or eliminate the cause of the incident, the incident handling team had to identify the root cause of the toll-fraud incidents. After talking with Mr. Friday at 8:30 a.m. on

Monday, 03 December 2001, Ms. Jones recognized the need to fully debrief the current on-duty guards, as well as those who had been working shifts since the incidents began on Saturday at 2:51 a.m. It quickly became evident that the contract security guards were victims of Social Engineering.

The attackers had used the extension "9000" exploit to reach the local operator. Unfortunately, the "local operator" is no longer a person, but automated voice prompts that enabled the attackers to reduce the human interface after they had access to the PBX and an outside trunk line.

Ignorance to the dangers of extension "90xx" transfers, and lack of suspicion to unusual off-hour calls was the incident cause. The most immediate means of eradicating this cause is employee education. By forcefully explaining what had happened to Midwest, USA site employees, Ms. Jones was able to intercept the 5:00 p.m. attack on Monday, 03 December 2001.

Rather than rely only upon employee awareness, Ms. Jones contacted its PBX/VMS service provider XYZ Company on Monday, 03 December 2001 to conduct a thorough security audit of the Midwest, USA Nortel Meridian 1 system. This audit was completed on 20 December 2001. Together with Joe Friday and another member of the IA team, Ms. Jones reviewed the security audit and proposed several PBX/VMS configuration changes to enhance overall security and close the extension "90xx" vulnerability. Key audit results and changes were as follows:

- 98 of the 250 stations permit call forwarding to external numbers. This resulted from the XYZ Company using a default template when new phone extensions were set up for the Midwest, USA offices. Ms. Jones asked to have this permission removed from the 98 stations. She further requested that care be taken to ensure that a secure configuration be used in future phone extension setups.
- PBX and VMS password lengths were 6 digits. This was increased to at least 8 digits. Passwords had not been changed regularly. Ms. Jones agreed that corporate policy of password changes every 90 days would be executed.
- Direct Inward System Access (DISA) was not being employed.
- VMS system and menu items were programmed to block outbound calls through the voice mail system.
- The VMS is already programmed to allow only 2 password attempts before the voice mailbox is locked. Only Ms. Jones can unlock the account.
- Audit logs already record both incoming and outbound calls. However, the Nortel Meridian 1 Release 21 software does not provide sufficient details. Ms. Jones is working with XYZ Company to upgrade the PBX/VMS software to a later release that provides greater call detail. However, time limitations and other commitments have slowed this process down.
- Many stations have unlimited access to international dialing. This is still required because of Omega's international customer base.
- Ms. Jones asked that transfers to any "90xx" extension be blocked.

Phase 5: Recovery

"In the Recovery phase, systems are put back into production. To make sure that the vulnerability has been eradicated, the system is tested and monitored." (Zago-Swart, p. 27)

In this incident, the PBX/VMS were never completely off-line. Local and continental U.S. calls were still permitted. After approximately one week, outbound international calls were again permitted due to economic necessity. While senior staff members had calling cards, the more junior employees did not. In addition, sending faxes became extremely cumbersome.

Ms. Jones plans on upgrading the Nortel Meridian 1 PBX/VMS software release. This should enable generating more detailed incoming and outgoing call detail logs. Once this is in place, she will be able to make periodic reviews of audit logs.

Phase 6: Lessons Learned/Follow-up

The Lessons Learned and Follow-up phase is where the incident handling participants assess the timeliness, and effectiveness of actions taken during the incident. The participants also study the status quo to determine if policy changes or countermeasures are required to remove inherent vulnerabilities or poor practices.

The overall handling of this Social Engineering incident appears to have been ultimately successful. There were information glitches that delayed the initial response; and missteps that permitted additional attacks after believed containment. However, the attack was detected the same day; an Incident Handling Team quickly assigned; the root cause identified; training implemented to help prevent future Social Engineering; and the PBX/VMS re-programmed to remove the "90xx" vulnerability.

In retrospect, the following weaknesses become evident, as well as possible mitigating steps:

- Reliance upon 3rd party vendors to configure and administer site PBX and VMS systems adds a layer of complexity in understanding if the system meets desired corporate policies. The vendors must be provided copies of pertinent corporate policies. Then, the vendor should provide written feedback on whether these policies can be met. Ideally, all sites should fall under a single or a limited number of corporate vendors. This results in better understanding of vendor responsibilities; economies of scale; and more direct interface between the Corporate Information Assurance personnel and the vendors.
- It can be difficult to obtain timely and comprehensive PBX security audit logs when a 3rd party vendor administers the system. Initial audit information provided by XYZ Company, the PBX service vendor, was simply a partial dump of the PBX configuration. It was not clearly annotated and did not contain information such as what area codes were blocked. Incoming and outgoing call detail logs were not provided by XYZ. In addition, the PBX software release would not provide much more than summary information on the incoming and outgoing calls. "Caller ID" type information on the incoming calls is only available from the local service provider, SBC. It has been difficult obtaining the call logs from SBC.
- However, the ABC Phone Company did provide explicit detail on call destinations and times. Questions of what is needed from the vendor in toll-fraud incidents can be solved by creating a form with a list of desired call audit information and PBX/VMS configuration.

- Reliance upon an outside vendor to man the PBX attendant console during off-hours creates accountability issues when timely policy directives are given. Care must be taken to provide clear and forceful instructions to vendor personnel. Requesting that a person log and "read back" directives can help prevent misunderstandings and "forgotten" requests. Relying upon the known guards to pass the information did not work because a substitute guard filled in for the sick, regular guard.
- The acquisition of new subsidiaries and businesses makes dissemination of corporate IT policy difficult. It is unlikely that the Midwest, USA site ever saw a copy of the 29 October 2001 PBX/VMS Security Policy. While the PBX/VMS policy can be found on the Corporate intranet website, a proactive approach of sending periodic copies to personnel responsible for site facilities might get the information out. Furthermore, abstracts or bulletized versions of the policy highlights would make it easier for busy inundated managers to browse the material.
- Maintaining accurate points of contacts across a large multinational corporation that includes many new subsidiaries is very difficult. Although the timeline indicates no great damage was done, the delay in finding key contacts at the Midwest, USA site was very frustrating to the Incident Handler Mr. Friday. In future incidents, that delay may prove costly. There is probably no way around the time and effort necessary to update and maintain the lists. It just has to be done.
- Employees and contract labor need periodic training and education to combat Social Engineering. Publicizing sanitized case histories of incidents through corporate emails might prove an entertaining and memorable means of educating personnel to the signs and consequences of Social Engineering.
- Detection of toll-fraud usually relies upon time-late notice from the telephone service provider. Available manpower and costs preclude active PBX/VMS security audits.
- Newly acquired subsidiaries and businesses need to have their systems brought into configuration management. Unfortunately Corporate staff is spread thin. New acquisitions make the problem snowball.
- Once in configuration management, a system of periodic security audits of the PBX/VMS system may be necessary. Again, tight corporate staffing and budgets make this very difficult.

Exhaustive reviews of each incident are a time and personnel luxury. After suggested changes were made by XYZ Company, member of Corporate IA Team reviewed the Midwest, USA site PBX/VMS configuration. The review indicated that the site met corporate guidelines. The incident is considered closed.

As was mentioned previously, the Midwest, USA site had never experienced a known toll-fraud incident. Little thought or instruction was given to guards about telephone transfer policies on weekends and off-hours. The guards and day staff operators did not realize it was even possible to reach outside operators through a "9000" transfer. To prevent future Social Engineering incidents, Ms. Jones disseminated clear instructions on telephone policies. She is working with XYZ Company to obtain additional user training for the Midwest, USA employees.

Conclusions

Good security depends upon better recognition of the threat and contingency planning. The original PBX/VMS configuration was reasonably secure. Voice mailboxes would only permit two attempts before lock down; the PBX console modem was disconnected without prior authorized permission for use; through dialing was not permitted; and only 98 of 250 extensions had the capability to execute the extension "9000" transfer. The system failed at the human interface. Never "bitten" before, the site did not prepare its people for a Social Engineering attack in either training or procedures.

Most phases of the incident handling response were hindered by communication problems. Key personnel could not be reached because lists of corporate sites were incomplete, and points of contact unknown. Greater effort needs to be paid to IT security during transition after mergers and acquisitions. The incident was not initially contained because the security guard did not successfully pass down the instructions at watch turnover. Analysis of the incident was difficult because the PBX/VMS service vendor provided incomplete configuration data, and the local telephone service provider did not provide timely incoming call records. Better employee training; written procedures for contingencies; and "canned" data request forms to obtain information from vendors would significantly improve communications.

Glossary

Basic Alternate Route Selection (BARS) - BARS … functions to direct a call from a switch in one geographical location to a switch in any other geographical location in a cost-efficient and easy-to-use manner by:
— eliminating long, complex dialing plans and replacing them with an abbreviated Uniform dialing plan (UDP) common to all switches which are part of the network
— providing a means of controlling the number and type of trunks that are available to each network caller, and a method of controlling the time of day that access to a trunk (or group of trunks) is allowed
— selecting automatically the least-cost trunk route available to complete a call between network switches
— providing uniform network access to stations served directly at a Meridian 1 node … and stations served at SL-1 mains or conventional mains … connected to a Meridian 1 node by Tie trunks (Northern Telecom, *Meridian 1 – Option 11C*, p. 871)

Direct Inward Dialing (DID) – "Allows an incoming call from the exchange network to reach a station without attendant assistance. The DN for each station will normally be the last 2,3 or 4 digits of the 7 digit exchange network number." (Iceman, p. 1)

Direct Inward System Access (DISA) – Allows an incoming call to obtain an outbound trunk dial tone through the PBX using an access code. It is often used to provide mobile employees long distance service through the PBX in lieu of using a credit card.

Direct Outward Dialing (DOD) - "Allows a station to gain access to the exchange network without attendant assistance and receives a second dial tone." (Iceman, p.1)

Facility Restriction Level (FRL) – a number which ranges from 0 (low-privilege) to 7 (high-privilege). The Meridian 1 software uses the FRL to determine which route selections are available to an extension assigned a specific Network Class of Service (NCOS).

IA – Information Assurance

PBX – Private Branch Exchange

Meridian 1 Option 61C – "The Meridian 1 product line consists of system types referred to as system Options. A system option is made up of Universal Equipment Modules (UEMs) stacked one on top of another to form a column. Each column contains a pedestal, a top cap, and up to four modules. A system can have one column or multiple columns. Each UEM is a self-contained unit that, when equipped, houses a card cage and backplane, power and ground cabling, power units, I/O panels, circuit cards, and cables. . . . Option 61C is a dual-CPU system with standby processing capability, fully redundant memory, and a full-network group." (Northern Telecom, *Meridian 1 System Overview*, p. 10, 14-15)

Network Class of Service (NCOS) - the means to control:
— which trunk routes are eligible to be accessed to attempt call completion
— whether or not queuing is offered to a call originator

— whether or not the call originator receives a warning tone when an expensive trunk is selected to complete a call
— whether or not the user is allowed to access the Network Speed Call feature trunks (Northern Telecom, *Meridian 1 – Option 11C*, p. 874)

Nortel – Northern Telecom

Overlays/Non-resident programs – "Non-resident programs (overlays) are loaded into an overlay area of the system memory to perform specific tasks. Overlays refer to non-resident administration and maintenance programs. Overlays are identified by the letters LD and numbers, for example LD 17. Administration overlays allow data entry to customize Meridian 1 system features, telephones, trunk groups, hardware, and data devices. Maintenance overlays diagnose Meridian 1 system operation and faults." (Northern Telecom*, Meridian 1 Options 51C, 61C, 81C System Programming Guide*, p. 16)

Phone phreak – a person who exploits, explores or "phreaks" a PBX or voicemail system

Phreaking – "Using different "boxes" and "tricks" to manipulate the phone companies and their phones, you can gain many things. The most important of these things are: knowledge about telephones and how they work, and free local and long distance phone calls." (Revelation, p. 1)

Remote Call Forward – a PBX function that permits a remote user (located outside of the PBX) to direct calls to any telephone (including those outside the PBX).

Through Dialing – "Extension or tie-line users may request access to a number which requires use of a trunk which they are not allowed to access. Access the trunk for the user. Then the user can then dial out (except onto fully restricted trunks)." (Northern Telecom, Meridian 1 Attendant PC Software User Guide, p. 154)

VMS – Voice Messaging System

Works Cited

Arthurs, Wendy; "A Proactive Defence to Social Engineering"; *SANS Institute Information Security Reading Room*. August 2, 2001. 28 Dec 2001; http://www.sans.org/infosecFAQ/social/defence.htm .

Granger, Sarah; "Social Engineering Fundamentals, Part I: Hacker Tactics"; *SecurityFocus InFocus*; December 18, 2001. 28 Dec 2001; http://www.securityfocus.com/infocus/1527.

Iceman; "Northern Telecom Meridian SL-1", *Phrack Magazine*, Vol 4, Issue 44, File 19 of 27; 26 Dec 2001; http://www.infowar.com/iwftp/Phrack/P44-19.txt.

Northern Telecom; *Meridian 1 Attendant PC Software User Guide*, 1999. 09 Dec 2001. http://www142.nortelnetworks.com:8081/bvdoc/meridian1/m1253x/p0891256.pdf.

Northern Telecom; *Meridian 1 System Overview, April 2000*; 24 Dec 2001. http://47.249.32.115:8081/docs/M1242x/5300100.PDF.

Northern Telecom; *Meridian 1 Option 11C 1.5BMb DTI/PRI Administration and Maintenance Guide,* Oct 2000. 24 Dec 2001. http://www142.nortelnetworks.com:8081/bvdoc/meridian1/m1253x/5301310.pdf.

Northern Telecom; *Meridian 1 Option 51C, 61C or 81C System Programming Guide*, May 1999. 24 Dec 2001. http://47.249.32.115:8081/docs/M1242x/T_SPG.PDF .

Northern Telecom; *Meridian 1 Option 51C, 61C or 81C*, 24 Dec 2001. http://www.nortelnetworks.com/products/01/meridian/mer1/options/option51c.html.

PBX Info; *"Meridian Mail – A Beginner's Guide to Meridian Mail Features";* 26 Dec 2001; http://pbxinfo.com/maxpages/Meridian_Mail_Features.

SBC Ameritech; "Social Engineering Fraud", *Consumer Information*. 28 Dec 2001; http://www.ameritech.com/content/0,3086,92,00.html

Revelation; "The Ultimate Beginner's Guide to Hacking and Phreaking" 01 Apr 1997; *Securitywire.com*, 09 Dec 2001; http://securitywire.com/fileview.php?file=starthak2.txt

The Clone; *An Introduction to Meridian Mail Rls.12,* 14 Dec 2001; http://www.pla813.org/texts/An%20Introduction%20to%20Meridian%20Mail.txt

Verizon; "PBX Social Engineering Scam", *Phone Fraud*; 28 Dec 2001; http://www.bellatlantic.com/security/fraud/pbx_scam.htm

Zago-Swart, Adrienne; *Advanced Incident Handling and Hacker Exploits Practical Assignment*, 05 November 2001; 18 January 2002; http://www.giac.org/GCIH.php.