



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

The Overlooked Threat, Phone/Voice Mail System

Robert Cherry

March 11, 2001

Introduction

Second to electronic mail (e-mail) voice mail is the "heart" of communications between corporations and their customers and employees. Have you ever stopped and thought about what information can be obtained from these systems if they were to become compromised? Have you ever considered your company's phone/voice mail system when performing security assessments? This paper will introduce the concept of phone/voice mail system compromises, what information the "bad guys" have, and ways to protect ourselves from this threat.

A typical attack scenario

This section will describe steps that an attacker could use to compromise your phone/voice mail system. These steps were found easily on the Internet and are readily available to anyone.

Attacking a phone/voice mail system is fairly easy, and does not require any technical skills. The first step is to locate a target. The next step involves finding the voice mail's main access point. This is the phone number or extension that an employee will call to receive his or her voice mail when they are out of the office. Many times this can be obtained by listening to the company's phone directory. This is typically available to everyone and is an option from the main greeting prompt. Many times a dedicated phone number will be set aside for message retrieval. If the company's main number is 555-1000, try 555-10xx replacing xx with 01,02,..99. When the main access point is located, you should receive some type of greeting asking for an extension number.

Once you have located the access point to receive messages, attempt to attack a specified mailbox. Depending on the type of system, it may be necessary to enter a 0, 9, #, or * to receive a login prompt. Once the login prompt is given, attempt to brute force the password. Many times the administrator will set up the default password equal to the extension number. If this does not work attempt the most commonly used passwords listed below.

Commonly Used Passwords

- Extension Number
- Extension Number backwards
- 1 + Extension Number
- Extension Number + 1 digit (i.e. 1-9)
- Try 0000 through 9999
- 1234, 2345, 3456, etc.
- Telephone key pad sequences, i.e. 147, 258, 360
- Telephone Key pad sequences, i.e. 159, 357
- Last 4 of Social Security Number
- Birthrates, anniversaries
- Even try a null password

Usually the password needs to be followed by a special character to let the system know the end of the password string. This character is normally and # or an *.

Some systems can be configured to lock the mailbox after x amount of failed login attempts. However many are configured to allow unlimited attempts. Also note that a good system administrator should detect this type of activity.

Once a password has been brute forced, familiarize yourself with the system. Each system has a different look and feel. The following list describes a few characteristics of a few popular voice mail systems.

Popular voice mail systems characteristics.

Meridian Mail

- Generic greeting string "Meridian Mail...Mailbox?"
- Default password length is 4 digits
- # must proceed the password

Audix (very popular)

- Generic Greeting string "Welcome to Audix"
- *H for help information
- Default password length is 4 digits
- # must proceed the password
- *7 to get the login prompt

Aspen

- Generic greeting "Hello, this is ASPEN"
- # will transfer caller to voice mail

How to protect against attack

A voice mail system should be treated as any other Information System. It should be part of the security assessment. Most of the best practices we all use apply to these systems. As with any other Information System, user education is very important. Unlike computer systems, which are generally protected by various methods, firewalls etc., voice mail systems are left "in the open". The following is a list of some security practices the system administrator and end users should practice.

Good Security Practices

- Configure the system to lock the voice box after x number of failed login attempts.
- Force pass words to be as long as possible. Be sure that they are longer than the default.
- When the system administrator creates a new voice box, never use the default password.
- Make sure pass words can't be found using a dictionary attack.
- Don't save old messages on the system.
- Restrict certain features such as Call Transfers.
- Discussion of company secrets **MUST** be prohibited.
- Logs should be reviewed on a regular basis.

Also educate users to identify when their voice mailbox has been tampered with. A few red flags are:

Voice Mail Box Red Flags

- Old or saved messages have been deleted.
- Greeting(s) have been deleted or altered.
- User is unable to access the voice box altogether.

There are a few manufactures of PC based Voice Mail and PBX systems. Many of these are connected to corporate networks and interact with the end users. They can also be connected to other offices via Voice Over IP connections. This can also lead to further compromises into the network. Systems that allow a remote user to initiate call transfers can result in toll fraud by intruders.

An Ottawa business publication stated in a December 1998 article:

"So far this year, Alberta's phone company, Telus has caught cases of toll fraud costing companies between \$18,000 and \$200,000 in a matter of days."

Conclusion

Attacking a voice mail/phone system can be the weakest link that an attacker could use to gain information about your company. The attacker could also gain insight to assist in preparation of a computer system attack.

The number of text documents I located on the Internet surprised me. There are utilities available to assist in cracking the pass word. There are even in depth documents on the technical details of common voice mail systems. I was also able to locate several web pages that detailed the entire process for retrieving a company's voice mail complete with the documentation that the end users are given. Many even indicated the phone number for retrieving messages, password length required, and other information that will assist the attacker.

We must treat our voice mail and phone systems as valid targets of attack. We must include these systems in our threat assessments and perform penetration testing against these systems.

Related Links

<http://www.l0pht.com/~oblivion/blkerwl/telecom.html>
Telephony Utilities

<http://web.mit.edu/is/tel/userguide.html>
Voice Mail users guide for MIT

<http://cns.stanford.edu/voicemail/univ.instr.html>
Stanford University's User Guide

<http://www.geek.org.uk/phila/nd/MERLIN.TXT>
Merlin PBX features and use.

References

"Caveman" The Complete Guide to Hacking and Use of ASpEN Voice Mail Systems.
<http://www.textfiles.com/hacking/aspen.txt> (January 13, 1992)

Atrisoft. Makers of a PC based PBX
<http://www.artisoft.com/products.htm>

"NeonDreamer" Basic Phreaking Skills
<http://www.geek.org.uk/phila/nd/PHREAKIN.TXT> (October 5, 1996)

"Black Knight" Hacking Voice Mail Systems.
<http://www.geek.org.uk/phila/nd/HVMS.TXT>

Securing Your Office Phone System from Voice and Data Network Fraud
<http://www.workingforchange.com/services/business/fraud.cfm>

Ottawa Citizen
<http://www.ottawacitizen.com/business/981211/2093909.html>

© SANS Institute 2000 - 2002, Author retains full rights.