Compromising Voice Messaging Systems

Kingpin

@Stake, Inc.
196 Broadway, Cambridge, MA 02139, USA.
http://www.atstake.com
E-mail: kingpin@atstake.com
Revision: 1.0

Abstract. Voice mail systems and answering machines are an important part of the corporate information flow. However, they are frequently left unprotected and are overlooked when performing security assessments. Access to these systems may yield valuable information and may assist attackers to further their attacks on the company's computer infrastructure. This brief introduces the concept and methodologies of compromising voice mail systems and answering machines, provides vendor specific characteristics to aid in voice mail compromise, and lists news reports, advisories, and software tools.

Keywords: voice mail systems, telephony, security, answering machines

1 Importance of Voice Messaging Assessments

Voice mail systems and answering machines have often been overlooked and left unprotected in corporate environments. It is a trivial task to compromise a legitimate user's voice mail box by manual dictionary attack methods or by using automated tools. Voice messaging systems are just as important as other corporate resources and proper security practices should be implemented.

Aside from electronic mail, voice mail is the "life's blood" of communication between corporations and between peers, both internally and externally to the company. Messages left on voice mail boxes can contain critical information or corporate secrets. Gaining access to the entire voice mail system or a particular targeted voice mail box may potentially give attackers valuable information and may assist them to further their attacks on the company's computer infrastructure.

Many times, due to the lack of user education, voice mail box passwords are commonly set to match the voice mail box extension. Even if security measures are in place to force the user to change their password every month, many users keep assigning the same password. Furthermore, users frequently use the same password or PIN number for multiple systems, increasing the chances for an attacker to obtain it. The typical attitude of many voice mail users is "Who would care about me?" and "Why would anyone want to listen to my voice mail messages?". Because of this attitude, voice mail passwords are poorly selected and often easily guessable by a dictionary attack using the most

commonly used passwords (section 2.2, Common Voice Mail Box Passwords). Unbeknownst to these users is the fact that day-to-day information and operations that may seem routine to them might be treasure for an intruder.

Voice mail systems often work in conjunction with a company's private branch exchange (PBX), which serves as a gateway into the telephone network. Access to a PBX, by way of the voice mail system, could give an attacker unlimited usage of company telephone lines. This would allow the intruder to obtain free long-distance phone calls and serve as a launch pad for attacks on other systems.

Voice mail system assessments are a crucial part of a thorough security audit and should be presented as a service and value-add.

2 Methodologies

The process of compromising voice mail systems is simple and follows a logical procedure. It does not require a deep technical knowledge of the particular voice mail system.

2.1 Common Plan of Attack

Identify targets. Using a company directory, automated phone list, or brute-force guessing of extensions, identify the targets for voice mail compromise. Company directories are commonly stored on an internal computer network for easy distribution to employees. Gaining access to such a file is a benefit to the attacker. Other information which may assist in identifying targets can be retrieved from a company's dumpster.

Identify main voice mail access point. In order to attack the voice mail system without dialing an extension directly or going through the company's receptionist, one must identify the main dial-up for the voice mail system. This is the number that is called by employees while they are out of the office in order to access the system. It is easy to attack a number of voice mail boxes using this access point since the attacker is not limited to a single extension. The main access point phone number can be identified on a company directory, obtained by a receptionist, or brute-forced by dialing numbers manually within the same prefix as other company phone numbers. For example, if the main office number is 551-8400, try dialing 551-84*xx*, replacing *xx* with 00, 01, …, 99. The correct number will prompt you with a company greeting or a generic message asking for a voice mail box number and password (section 5, Vendor Specific Characteristics).

Attempt voice mail box access. To attack a specific voice mail box, use the main voice mail access point or dial an extension directly. It might be necessary to enter a 0, 9, #, or * once or twice to be prompted for login. The default and most commonly used passwords should be attempted first (section 2.2, Common Voice Mail Box Passwords). Depending on the feature set of the particular voice

mail system, three incorrect login attempts could lock the box and prevent logins until the system administrator is contacted. Other times, the system will allow unlimited login attempts, but keep a log of those attempts which could be reviewed by the system administrator at a later date. Manual attempts are often faster than using automated tools unless a large number of targets is identified. Programs are available for most computing platforms to aid in the attack (section 9, PC Software Tools). Voice mail systems usually offer online help using voice prompts; after login, the system will list possible commands such as listening to new messages, deleting old messages, or changing the personal greeting.

2.2 Common Voice Mail Box Passwords

In many cases, the default password assigned to a voice mail box is the same as the voice mail box number. The following most commonly used passwords can be used as a checklist during voice mail system assessments:

- Voice mail box number, for example 1234
- Voice mail box number reversed, 4321
- Voice mail box + 1, 1235
- Voice mail box number with additional digit after, 12340 or 12341
- Voice mail box number with additional digit before, 01234 or 11234
- 0000, 1111, …, 9999
- 1234, 2345, …, 6789
- 9876, 8765, …, 4321
- Telephone keypad up/down, for example 369 or 741
- Telephone keypad diagonal, for example 159 or 753
- Last 4 digits of main voice mail access point number
- Last 4 digits of social security number (which could be retrieved from the company's dumpster)
- Birthday or birthyear (which could be retrieved from the company's dumpster)

2.3 Preventative Measures

In order to keep the voice mail system as secure as possible, user education is the key. Unlike computer networks, which are well protected by various methods of security, voice mail systems are often left open to attack and compromise. The responsibility of security is distributed between all users of the system. System administrators and users should practice the following preventative measures to reduce the risk of voice mail system compromise:

- Configure the voice mail system to prevent logins to a voice mail box after a predetermined number of unsuccessful attempts.
- Ensure that passwords are as long as possible. Some voice mail systems allow passwords up to 15 digits in length.

- Immediately after a new voice mail box has been added to the system, change its default password.
- Ensure that all voice mail box passwords can not be easily found using a dictionary attack and are not one of those commonly used.
- Do not save old messages on the voice mail system.
- Restrict voice mail system features such as "Call Transfer" and other PBX interfacing commands. This will minimize the risk of toll fraud.
- Discussion of confidential company information on a voice mail system should be prohibited. If such discussion is necessary, make sure the message is erased from the box after reception.

There are certain traits that signify a compromised voice mail box. Educate users to identify these traits:

- Old or saved messages have been deleted by someone other than the legitimate user.
- Messages are labeled as "unopened messages" instead of "new messages".
- Personal greeting or password has been changed.

3 Case Study

A security assessment was performed on a large consulting company in Cambridge, Massachusetts while mergers were underway with another company. Permission was granted by the company to assess all nodes of its corporate infrastructure, including voice mail systems, dial-up lines and internet-connected computers.

3.1 Process

The system attacked was a Lucent Technologies Audix Voice Messaging System. The main Audix voice mail dial-up was found by selectively hand dialing phone numbers within the company's main prefix. The system allowed three attempts for a correct login, which consisted of a voice mail extension and password. Each voice mail box was protected by a 4- to 6-digit password.

A target list was created by using the employee directory available from the company's main phone number, as well as from a compromised computer. Among those voice mail systems attacked were finance, human resources, administrative, and employee.

To attack a specific voice mail box, the main number was dialed, the target extension entered, and three passwords were attempted. In many cases, the correct password was obtained within 2 of the 3 tries. Our prime targets were high-ranking officers of the company and managers of specific IT departments.

3.2 Summary

Out of 552 voice mail boxes, 51 of those were attacked with the common passwords (section 2.2, Common Voice Mail Box Passwords). Seven boxes were compromised, yielding a 13.7% success rate.

Although the success rate appears to be low, we compromised the box of a high-ranking executive which contained a goldmine of critical data, some of which was directly related to the merger negotiations.

4 Answering Machines

Answering machines, like voice mail systems, are usually overlooked during security assessments. Many answering machines are protected by a 2- or 3-digit password and rarely contain any type of intrusion detection or logging capabilities. Brute-force methods are extremely simple for answering machines and, depending on the password length, a successful password may be obtained in under 5 minutes. With proper access, the answering machine will allow a remote user to check messages, erase messages, or allow monitoring of a room via a microphone within the device.

Methodologies for compromising answering machines are similar to those of voice mail systems. All that is needed to gain access to the device is the password. Certain answering machines do not require a discrete password entry and are only looking for a specific combination of numbers. An answering machine of this type with a 2-digit password can be accessed with either of the following keystroke combinations:

- 00112233445566778899135790246803692581471593704948382726160517395062840852963007419753186420987654321 0
- 12345678987654321357924686429731474193366994488552277539596372582838491817161511026203040506070809001

5 Vendor Specific Characteristics

5.1 Meridian Mail

- Generic Identification String: "Meridian Mail… Mailbox?"
- Default minimum PIN Length = 4 digits
- Enter "#" after mail box number and password

5.2 Audix Voice Messaging System

- Generic Identification String: "Welcome to Audix. For help at any time, press *H. Please enter extension, and pound sign"
- Default minimum PIN Length = 4 digits

- Enter "#" after mail box number and password
- From outgoing message, enter "*7" to get login prompt

5.3 ASPEN (now Octel Messaging)

- Generic Identification String: "Hello. This is ASPEN, the Automated Speech Exchange Network. Please enter the number of the person you are calling. If you have a mailbox on this system, press pound."

6 News Reports

1. "Hacking: Not just a 'phone problem'", *Lan Times*, February 8, 1993, http://www.geocities.com/SiliconValley/Byte/9951/hacktips.html.
2. S. Ranger, "Sun Sacks Employees For Modem Security Breaches", *Network Week*, May 1998, http://www.techweb.com/wire/story/TWB19980318S0012.
3. D. Spurgeon, "A cautionary message on voicemail: Chiquita story shows vulnerability of the popular systems.", *The Washington Post*, July 7, 1998, http://sand.loper.org/~george/trends/1998/Jul/98.html.
4. Associated Press, "Former Chiquita Lawyer is Charged in Thefts of Company Voice Mail", September 20, 1998, http://www.sltrib.com/1998/sep/09201998/nation_w/53327.htm.

7 Advisories and Whitepapers

1. T. Wozniak, Jr., "Passwords", April 30, 1999, http://www.geocities.com/SiliconValley/Byte/9951/password.html.
2. C. Palo, "An Overview of Toll Fraud Today", http://www.riscnet.com/protect/individuals/toll.html.
3. Kingpin, L0pht Heavy Industries Security Advisory, "AT&T Model 1320 and various other answering machines", http://www.L0pht.com/advisories/ansmach.txt.

8 Computer Underground Textfiles

1. Caveman, "A Complete Guide To Hacking and Use of Aspen Voice Mail Systems", http://www.textfiles.com/hacking/aspen.txt.
2. Black Knight, "Hacking Voice Mail Systems", *Phrack Magazine #11*, http://www.phrack.com/search.phtml?view&article=p11-4.
3. Night Ranger, "Hacking Voice Mail Systems", *Phrack Magazine #34*, http://www.phrack.com/search.phtml?view&article=p34-6.
4. Anonymous, "Centigram Voice Mail System Consoles", *Phrack Magazine #39*, http://www.phrack.com/search.phtml?view&article=p39-6.
5. Scott Simpson, "A Brief Guide to Definity G Series Systems", *Phrack Magazine #41*, http://www.phrack.com/search.phtml?view&article=p41-6.
6. The Red Skull, "StarTalk Voice Mail Systems", *Phrack Magazine #46*, http://www.phrack.com/search.phtml?view&article=p46-18.

7. Erudite, "AT&T Definity System 75/85 Communications System Description & Configuration", *Phrack Magazine #46*, http://www.phrack.com/search.phtml?view&article=p46-25.
8. Substance, "Complete Guide To Hacking Meridian Mail Systems", *Phrack Magazine #47*, http://www.phrack.com/search.phtml?view&article=p47-15.
9. Predat0r, "Hacking Answering Machines 1990", http://www.textfiles.com/hacking/amhack.txt.

9 Vendors

1. Lucent Technologies Voice Messaging Solutions: AUDIX®, Octel®, MERLIN®, PARTNER MAIL®, http://www.lucent.com/enterprise/who/docs/product3.html.
2. Lucent Technologies Octel Messaging, http://www.octel.com.
3. Lucent Technologies Octel Messaging Quick Reference Guide, http://www.anu.edu.au/facilities/need_help/aria-guidev2.pdf.
4. Nortel Networks Advanced Messaging Solutions: Meridian Mail, Norstar Voice Mail, StarTalk, http://www.nortelnetworks.com/solutions/messaging/.
5. Plexus Systems and Voice Mail User's Guide, http://www.plexus-pbx.com/document.htm.

10 PC Software Tools

1. "VrACK 1.0a Voice Mail Box Hacker", http://www.L0pht.com/pub/blackcrwl/hack/vrack051.zip.
2. The Hacker's Choice, "THC-Scan 2.0", http://www.infowar.co.uk/thc/files/thc/thc-ts20.zip.
3. L0pht Heavy Industries, "Telephony Files Index", *Black Crawling Systems Archives*, http://www.L0pht.com/~oblivion/blkcrwl/telecom.html.