

PROTECTING AGAINST DIAL-IN HAZARDS: E-MAIL AND DATA COMMUNICATIONS

Leo A. Wrobel

INSIDE

The Telecommunications Privacy Policy, Tailgating, Dial-Back Modems, Securing the Mainframe, Vendor Solutions, Internet Security, Firewalls, Backup T1s

PROBLEMS ADDRESSED

With the advent of nomadic and home office environments, remote access security is once again taking its place at the forefront of security planning activities. Everyone wants an Internet presence and Internet access. Telecommuting is gaining in popularity. Sales agents armed with laptops roam the countryside.

Opening up systems to casual access by nomadic and home office workers requires the implementation of security procedures before the systems become mission critical and revenue producing. This article presents an overview of considerations to be addressed regarding dial-in and Internet access systems. Tips on how to ensure that standards for both physical equipment and privacy policies for today's mobile data world are also included. For information on protecting against dial-in hazards involving voice systems, see article 5-04-41.

THE TELECOMMUNICATIONS PRIVACY POLICY

What happens if you read someone else's confidential E-mail? Can the company read yours? Does an employee have an absolute right to privacy? Many individuals and companies have no idea how to answer these questions.

PAYOFF IDEA

As more workers use E-mail and data communications, the importance of security grows, and should be firmly established before the systems are used to generate revenue. Beginning with a sound telecommunications privacy policy, organizations should implement protective measures ranging from paging systems, dialback modems, and comprehensive after-market equipment to test firewalls, fully redundant configurations, and backup T1s.

For example, it is a violation of federal law to listen to a telephone conversation without the knowledge of the participants. We all know from television shows that there is a rigid process to secure a wire tap on a phone line. Do similar protections exist for E-mail?

Generally, a company's employee policy on E-mail privacy, usually in a telecommunications privacy document, sets the standard. Unfortunately, many organizations do not have such a document.

Every so often, a story in the paper underscores the vulnerability of E-mail far better than thousands of words by experts. The following is one example.

An office romance was blooming between two employees of a major service company. The company depended heavily on electronic mail in the conduct of daily business, and employees had every reason to believe this E-mail was secure. The young lady involved apparently thought it would be romantic to send a graphic E-mail letter, with an attached photograph, to her suitor. This would have been well and good if she had not clicked on the "All Users" button when sending the message. Suffice it to say this made for good office gossip and sent a clear message to everyone about the use of E-mail systems.

Notwithstanding such human errors, are E-mail systems really secure? Can an employer read E-mail? Do employees have a right to privacy? Article 5-04-41 discussed other forms of communication such as fax transmissions. Is a person breaking the law when he or she receives and reads a fax or E-mail intended for someone else? The answers may surprise you, and could call for a thorough review of security procedures for these systems.

A policy on telecommunications privacy should be broad enough in scope to cover not only E-mail, but voice mail and other mediums. Policies generally fit in between the following two ends of the spectrum:

- "Employees work for the company, and it owns the system. The company will listen to or monitor whatever we feel like monitoring or listening to," or
- "ABC Company is committed to absolute privacy of communications and each employee has the right to not have their communications monitored."

Which approach is right? That depends on your company. We usually opt for the latter, with a caveat, as follows:

- "ABC Company is committed to absolute privacy of communications, and each employee has the right to not have their communications monitored. However, if in the course of normal maintenance activity we inadvertently discover illegal activity, we reserve the right to report this activity to the responsible authorities."
-

Once again, it is wise to contact legal counsel when writing these policies. I was purposely casual in these illustrations to illustrate the range of options, but also because failure to contact legal counsel can leave organizations exposed to risk. An example of this is an employee who ran an illegal bookmaking operation out of a company system. He was fired but then reinstated because the company had no policy on privacy on which to base the dismissal. It is important to contact the corporate legal department, outside counsel, or an internal audit department for further details.

In addition to the establishment of the privacy policy, an evaluation of protective measures for dial-in lines should begin with an overview of their hazards. Any proposed solutions must address the types of intrusion discussed in the following sections if they are to ensure even a minimum level of protection.

HACKERS

Hackers are unauthorized users, often juveniles, who attempt to break into a system for kicks. They may or may not be lethal, but some rudimentary precautions can prevent these break-ins. Because these individuals often use demon dialers, which dial every number in a prefix to find modem lines (e.g., 555-0000, 555-0001, and so on), it is often not difficult for them to find numbers, especially if they are front ended with an identifying script. Therefore, security precautions must be evaluated to prevent this occurrence. These include:

- Modems that dial back the user.
- Modems that screen the CALLER ID of the calling party.
- Modems or equipment that answer initially with silence, rather than with a modem tone.
- Equipment that does not paint an initial screen, such as "Welcome to ABC Widget Company," which can serve to further encourage an unauthorized user.
- Equipment that logs and tracks unsuccessful log-in attempts.
- Equipment that requires a special hardware key to allow access.

Although none of these provides a definitive solution, several or all of these methods can provide a nearly impenetrable defense against unauthorized access.

SABOTEURS

The most unsettling types of attacks come from those who are knowledgeable of the environment. Disgruntled employees, for example, can cause more damage than anyone else, because they know exactly what attack can be the most damaging. Many organizations have a high level of employee trust, and have an established policy of allowing employees

a high degree of system access. This is commendable, but care should be taken because even the most close-knit firms can never be sure when an employee will destroy a critical system because of a personal gripe.

Recommended minimum precautions include:

- A simple process for eliminating log in access when an employee leaves the company.
- A mandatory process for eliminating log in access when any employee is terminated.

TAILGATING

Tailgating is an old ploy used to gain access to a system. It goes like this:

1. A super user or system administrator dials into a remote system.
2. The hacker dials the number (obtained through a demon dialer) and gets a busy signal.
3. The hacker dials 0 and asks the local telephone operator to verify the line.
4. The operator interrupts the line, which usually drops the authorized super user.
5. The hacker is meanwhile dialing out at the same time on another line. If timed perfectly, the modem sees the drop of carrier as a temporary line hit and reestablishes the session with the hacker's modem.
6. The hacker is online with super user access; the super user in turn oftentimes does not even know he has been dropped and instead thinks the system has simply locked up.
7. Working quickly, the hacker grabs the password files and compromises the system for his next attempt later, before the super user realizes anything was amiss. When security logs are checked, only the super user is logged because his session was never terminated.

Sounds rather ingenious? Actually, compared with some of the other tricks, this one is elementary. It underscores that any additional security precautions implemented provide greater peace of mind and protection to organizational assets. Remember, security is a major concern when dozens or hundreds of employees are accessing mission-critical systems through the public telephone network. Careful planning can avoid major difficulties later.

PREVENTIVE MEASURES

Inbound Call Accounting Systems

Each proposed solution should provide an accounting record of all call attempts to make a paper trail of dial-in access. Strength in screening, reporting, and presentation of this information must be a principal selec-

tion criterion in any protective system. A system showing 350 unsuccessful log-in attempts one night is sending a clear signal.

Paging Systems

Some systems that require a high degree of security provide automatic pager notification. When a user logs in, a system administrator's pager goes off. These can be combined with procedures for reporting mysterious login attempts that cannot otherwise be accounted for. They are not terribly expensive considering that a system administrator is instantly notified of anomalies.

Hardware Keys

Hardware devices such as hardware keys should be included in any security recommendations for mission-critical systems. Ease of use, such as plugging into a parallel port, and low cost should be both overriding criteria in the use of these devices.

The keys are a hardware device that usually plugs into a parallel port of a laptop computer. In conjunction with the attendant software, they provide a fairly bulletproof solution because an intruder would have to have both the encryption software, and the hardware key, to get even close to accessing a system.

Caller ID

Caller ID is available in many cities. Even in telephone wire centers where it is available, there are limitations. Caller ID is useful for more than just identification of annoying calls during dinnertime. Properly used, it can identify unauthorized users by their telephone number and often by name. Even nicer, caller ID is a built-in feature for many modems and ISDN (integrated services digital network) terminal adapters. The numbers can be logged on a call-by-call basis as part of the dial-in log described earlier.

Owing to the nonavailability of caller ID service in many areas, modems or other equipment that use this service as the sole underlying basis of a protective system may not be considered. Even if caller ID is available, there are still security concerns, namely:

- Caller ID data may not always be passed by interexchange carriers like AT&T, MCI, and Sprint. Your company would in a sense be vulnerable to long distance callers using carriers who do not pass this data. (This is rapidly changing as carriers comply with FCC regulations to pass caller ID data whenever possible.)
 - Even if interexchange carriers were equipped to pass this data, the distant local central office might not be. A company would still be open to intrusion unless other methods were employed.
-

-
- Many local central offices in parts of the country are not caller ID capable for either local or long-distance calls.

Therefore, at least a few calls will still slip through with the “out of area” disclaimer on the modem or display device. Caller ID alternatives should be carefully considered as an exclusive security precaution until the service becomes more ubiquitous. Even after universal deployment, it is recommended that this service is used only to augment existing security measures and not as a solution. Even where caller ID is available, the user can in many cases dial the override code to block it. This demands another level of protection on a modem: rejection of users where the incoming data indicates that the caller ID information was deliberately blocked.

Dial-Back Modems

Many dial-back modems are available on the market today. These devices require that users login, and then hang up and call the incoming caller back at a predetermined number. These are fairly foolproof, but inconvenient. A nomadic user in a hotel will not have an authorized number and will not be able to dial into a call-back modem bank. Nonetheless, special modem banks and numbers can be set up for this purpose with special emphasis and screening for potential intruders.

Securing the Mainframe

Many users are stuck trying to protect legacy mainframe environments where security options for dial-in are marginal at best. While IBM has no graceful and simple solution for the mainframe, it can provide an additional level of security by front ending the protocol converter with a dial-in server. The IBM 8235 dial-in server is one candidate. It provides the necessary accounting, dial-back capability, and with an eight port maximum capacity, it seems sized correctly for any future growth. However, it is somewhat expensive.

More common are solutions where distributed devices are hung off the mainframe through the use of bridges and LAN switches. A PC-based system with appropriate protocol conversion software will often suffice in a pinch as a secure dial-in medium for the mainframe.

Software-Based Solutions

Because transparency for dial-in users is an issue (different departments often use a variety of software packages when dialing in), you may not want to consider a wholesale change of dial-in software emulation packages. This might prove disruptive to your present operating environment.

Software alternatives that augment or enhance the current hardware package in use are most preferable because the need for training on new packages is minimal.

After-Market Equipment

Often, the only way to provide acceptable security across a broad range of installed equipment and large cross-section of users is to adapt some sort of outboard solution. Naturally, the potential exists to black box a company to death by over-broadening the range of installed equipment. It pays to evaluate carefully. Following are several effective alternatives:

- A line of equipment distributed by CDI Incorporated of Clifton, NJ. This equipment seems to most adequately reflect pressing security concerns presented by most users. Although I have not had direct experience with this equipment, on paper it certainly seems to provide a most comprehensive solution to the dial-in security issue and should be carefully considered.
- Another cost-effective solution is brokered by LeeMah Data Comm Security Corp. of Hayward CA. It also appears to meet criteria for transparency and accommodation of diverse remote users.

When evaluating these or another product, look for the following features:

1. The unit should serve as security device and modem manager. Anyone who has ever repeatedly hit a “ring-no-answer” when dialing a modem pool can appreciate this feature. Make sure the system can automatically busy these lines out, then alert you to the problem.
2. The unit should provide response time information by modem, by phone line, and by port. For example, it should interface to a personal computer for effective performance management. This makes a good source of information to a help desk for when users call in to report trouble connecting.
3. The product should offer effective upgradeability. For additional security, the product should offer token hardware devices that interface to a user’s parallel port. Software token should also be available. DOS or Windows software both should be supported.
4. Software and hardware keys. Because transparency of equipment for users is usually an issue, try not to consider major changes in hardware used by remote users. This might prove too disruptive to the present operating environment. This may cost more later in maintenance and training.

An unbiased opinion makes LeeMah the favorite in terms of flexibility and cost-effectiveness. Some of the features offered provide effective evaluation criteria for whatever system you decide to acquire. These include:

- The unit is a multiple port challenge-response unit.
 - It supports up to 32 modems (Traq-Net 2032).
-

-
- The unit installs between the phone line and modem, allowing for use of present modems.
 - The product allows for use of (optional) proprietary LeeMah Security Modems for additional protection.
 - The product employs either a hardware or software token at user request.
 - It provides a full audit trail.
 - The product meets DES security standard.
 - The product operates transparently, allowing for use of all present emulation software.
 - It offers reasonably priced software (Infodisk).
 - The product supports, for example, Procomm, Qmodem, Crosstalk, PCAnywhere, and Smartcom.

LeeMah DataComm provides a standards-based, virtually impenetrable, flexible, and configurable, security solution for the protection of remote access to telecommunications and data communications network information and resources. LeeMah's remote access security solutions consist of three elements: access control systems, personal authentication devices, and security administration software.

The LeeMah system represents one of the most adaptable and feature-rich solutions to protect dial-in services over a wide variety of equipment types from mainframes to local area networks (LANs). However, it is still wise to evaluate several vendors and base a decision on each unique environment. An Internet search will probably uncover numerous other choices with similar capabilities.

INTERNET SECURITY RESPONSIBILITIES

No discussion of unauthorized data access is complete without mentioning the Internet. The Internet is a relatively new phenomenon for many companies, at least as a revenue generating system, and many companies have unresolved organizational issues about security responsibilities. Who maintains the equipment used for Internet access? Historically, these types of operations often have fallen under a special unit in the IS department, such as midrange computer services. However, today many companies have a separate group of technologists responsible for the actual operation of the Internet firewall and other components. There is not always a clear business unit responsible for Internet security.

Many clients have reported minor snafus (i.e., holes or vulnerabilities left temporarily exposed in the system) due to lack of a clear policy outlining who is responsible for which system and under what circumstances. Although this responsibility will ultimately gravitate to an IT security group (much like the LAN and mainframe services of today), vulnerabilities will

continue in the immediate term, while the technology is in the “tweaking and tinkering” stage.

Another issue includes staffing and resource allocation. Many companies should consider a nominal increase in manpower to avoid creating too small a pool of specialists and provide better depth. When Internet access is established and any possible security breaches or holes are closed, organization changes may be readdressed. If a company has one person who is readily identified as the Internet guru, take note. These folks are in high demand and could leave you holding the bag if they accept other employment. Besides, outgunned and undermanned staffs have little time to probe for security violations.

Installation of Test Firewall

Many companies do not have firewall platform exclusively earmarked for testing and backup. For all intents and purposes, the present technology is single threaded in almost every way. This is not a major concern yet, but will be when the firewall goes into full operation, and the system becomes revenue producing.

Just as in mainframes and local area networks, it is important to establish a protocol and procedure that does not directly introduce new applications into a production environment. This lesson became apparent during 25 years of mainframe operations, and even the most renegade LAN managers have learned to adopt it as a gospel of prudent operation. Like many new technologies, these protocols have yet to catch up in the Internet arena for many firms.

A test firewall also can double as a backup in the event of a major equipment failure in the primary configuration. This will be important again when the system becomes fully revenue generating.

Because the Internet is a relatively new technology for many firms, staff should be encouraged to dabble. Although it is not prudent to experiment on a production platform, the backup firewall configuration can provide a practical option. The backup can be justified further by encouraging the staff to experiment, improve, and refine without jeopardizing operation of the enterprise. In summary, the extra expense of a backup firewall capability can be justified for the resiliency it provides the network and because it shortens the educational curve when principal technologists are encouraged to try new processes.

Upgrading to a Fully Redundant Configuration

The issue of redundant physical componentry of the Internet firewall raises several items of concern. Again, these will not be major concerns until the Internet and firewalls go into full production and become revenue-generating systems, but they will demand increased attention in the

future. The first is in the area of general fault tolerance on the physical components.

Many routers in use, such as the CISCO 4000 series, have no redundancy. The CISCO 5000 series has redundant power and a redundant CPU, which will be required later. Every other component in other systems generally has a redundant backplane, power supply, CPU, and other common logic. As usual in the world of technology, the newer systems play catch-up for a couple of years with regard to redundancy. CISCO appears to have responded commendably to user demands for such backup systems, as have other vendors. Organizations should explore these options and use them as soon as Internet access is about to become revenue generating or otherwise mission critical.

Backup T1s

Another issue to consider is that most large users install only one T1 to the Internet Service Provider (ISP), which creates a point of vulnerability. A wiser approach is to consider adding a second T1 along with "Round Robin DNS" for greater resiliency on the wide area network connectivity to the ISP. Many local telephone companies offer services designed to diversify T1 access as well. In Southwestern Bell territory, the service is called SecureNet™, which offers a completely diverse T1 circuit at a significantly reduced rate. Other components, such as CSUs and DSUs, are single threaded without redundancy. Spares should be kept or depot arrangements should be made with vendors to ensure that failed components can be replaced quickly, minimizing the impact on the business.

As the Internet becomes more and more of an integral part of a company's operations (as defined by impact on revenue or other valid measurement), storing of spare components, including hard drives, redundant controller cards, spare tape drives, and power supplies should be considered.

In summary, to ensure a system up to par with revenue-generating applications, companies should upgrade to series 5000 or 6000 routers (or equivalent), combined with dual connections to the ISP and "Round Robin DNS" at the same juncture. Depot arrangements should be established for spare parts, and services such as Southwestern Bell SecureNet and other methods for diversifying T1 access should be considered. Such precautions will provide cheap insurance for what will fast become a revenue-producing system.

RECOMMENDED COURSE OF ACTION

Although revenue-generating dial-in systems may seem to be far away for many companies, experience shows that systems like these have a way of catching on. Insurance companies love the idea of roving claims adjusters with dial-in laptop computers. Everyone wants to work at home.

Commerce is blossoming on the Internet. Waiting until there is a revenue impact after a failure resigns an organization to be almost perpetually in the reactive mode of trying to keep up with the protection of a potentially business debilitating system. The alternative is to start now, while these systems are still relatively immature and design the protective systems in before the Internet becomes a fully functional business system.

Leo A. Wrobel is president and CEO of Premiere Network Services, Inc., in DeSoto, TX. An active author, national and international lecturer, and technical futurist, he has published 10 books and over 100 trade articles on a variety of technical subjects, including *Writing Disaster Recovery Plans for Telecommunications and LANS* (Artech House, 1993) and *Business Resumption Planning* (Auerbach Publications, 1997). His experience of nearly two decades includes assignments at AT&T, a major mortgage banking company, and a host of other firms engaged in banking, brokerage, heavy manufacturing, telecommunications services and government, as well as the design and regulatory approval of a LATA-wide OC-12/ATM network for a \$10 billion manufacturing giant, the first of its kind. A three-term city councilman and previous mayor, Leo Wrobel is a knowledgeable and effective communicator known for his entertaining presentation style on a wide variety of technical topics. For more information, contact his web site at <http://www.dallas.net/~premiere> or phone at (972) 228-8881.