8-16-1996

Security Issues Related to Industry's Use of the Internet

Gwynne Larsen
Metropolitian State College of Denver

Charles H. Mawhinney
Metropolitian State College of Denver

Security Issues Related to Industry's Use of the Internet

Gwynne Larsenand Charles H. Mawhinney
Metropolitan State College of Denver

Introduction

With the recent popularity of the Internet and the attendant proliferation of companies using it for all kinds of communication, a serious problem of security has arisen (Anthes, 1995). The Internet has been a major means of data communication for government agencies and universities for many years, with only a limited number of businesses connecting to it. In fact, to do any business on the Internet at all was frowned on. However, that scenario is changing rapidly. Currently, the commercial domain is the fastest growing Internet group with more than 1500 new companies connecting each month (Ellsworth, 1995). In the past the major use of the Internet by business was for email. Now, however, it is becoming an almost essential business tool for communications, research, marketing, and public relations. It seems that connecting to the Internet is almost inevitable for most companies because there are simply too many valid business reasons for these connections and it is virtually impossible to forbid connectivity to the Internet or to the use of dialup and remote connections. (Lipner, 1995).

Literature Review

Advertising on the Internet has become extremely popular recently with the development of the World Wide Web and its browsers. A year ago 15,000 American businesses had Internet addresses; now approximately 50,000 are logging in (Zeiger, 1995).

As with all state-of-the art technologies, there will be nothing forcing companies to climb on the Internet bandwagon; however, there may come a time when certain types of businesses will have to use the Internet if they want to remain competitive.

Briefly some of the advantages of using the Internet for company business are:

World-wide access to people via email virtually instantaneously

World-wide access to information (search document data bases for topics via ftp, telnet, gopher, world wide web)

A relative inexpensive way for global marketing of products and services

A forum for getting product information to customers

A low-cost way to acquire freeware and shareware software

The availability of software fixes for various software programs from companies, such as Novell.

One of the major deterrents to connecting to the Internet is the security issue. Some question whether the cost (possible stealth of confidential information, corruption of files, and damage to systems) is worth the benefits. The paranoia involved with this type of network connection appears to be justified. Thousands of computer passwords have been stolen recently by Internet interlopers, and millions more are at risk (Anthes, 1995). Users generally agree that Internet access brings security risks from viruses and hackers, but few agree on the extent of the risk or what to do about it (Anthes, 1995). Today's Internet is wide open--people put viruses in, steal mailbox IDs, and obtain credit card numbers (Anthes, 1995). The Internet itself does not take precautions for security measures (Green, 1994).

"Look for automated hacking, where entire crimes, including conversion to gain, will be automated. This will require automated detection, mitigation and retaliation to deal with electronic speeds of these crimes" said Parker (Anthes, 1995). There will be LANarchy, where knowledge of equipment and interconnectivity in large organizations is lost. The companies cannot make something secure unless they know it exists (Anthes, 1995). There will also be information anarchy because those who encrypt information in an organization may not be those who have accountability for it. Higher management must control key and device management (Anthes, 1995). Special hacking knowledge is getting encapsulated into computer programs. All hackers have to do to get a password sniffer (a program that detects passwords) is broadcast onto the Internet. "Hackers aren't getting any smarter; their work is just getting easier and easier" said Murray (Anthes, 1995).

Most of the hackers of the 1980s were nuisances; they disrupted the operations of companies and government agencies. However, in the 1990s, computer intruders seem to have experienced a change in character; these hackers are more 'upscale'professional in outlook and motivated by the prospect of financial gain (Lipner, 1995). The potential for sophisticated, wellorchestrated intrusions has become very real, given the expanding use of networked computer systems to process increasingly valuable and sensitive information (Lipner).

At this time virtually the only security team on the Internet is CERT, the Computer Emergency Response Team Coordination Center which is located at Carnegie Mellon University's Software Engineering Institute. CERT serves as a clearinghouse for security issues on the Net and as such receives about 40 informational requests and 500 email messages a week (Fithen and Fraser, 1994). As part of its mission the team "raises awareness of information and computer security and security issues" according to Richard D. Pethia, a center coordinator (Nitowski, 1995).

Systems to Enhance Security

If a company does decide it is essential to connect to the Internet, precautions should be taken. Some of the ways to guard against the intrusion of outsiders into your company's data are as follows:

Passwords. Passwords have not proved an effective deterrent to access; some passwords are easily guessed, others are left carelessly around offices, maybe taped to the bottoms of keyboards, and others are subject to capture on the network (Anthes, 1995). Some solutions are to require specific kinds of hard-to-guess passwords, make users change their passwords frequently, and even use randomly generated passwords that can be used just once.

Encryption. Cryptography can protect confidentiality by encoding data so that no one except the intended recipient can read it; it can insure integrity of communication by permitting a user to detect if data has been tampered with during transmission or during storage; it can promote authenticity by providing a user with a way to verify the identify of the sender (Landau, et al, 1994). Cryptographers apply mathematical algorithms to garble messages and create "digital signatures", the equivalent of fingerprints (Baig, 1994).

Two other types of encryption gaining favor are public-key cryptography and digital signatures, which are similar in design. Public-key cryptography requires every user to have a private key known only to the user and a public key that is universally accessible (Chokhani, 1994). A message encrypted by the private key can be decrypted by the public key; a message encrypted with a public key can be decrypted only by the possessor of the corresponding private key (Greismer and Jesmajian, 1994). In an asymmetric (public key) cryptoalgorithm a pair of distinct, but mathematically related, keys are used for encryption and decryption (Kent, 1993). Probably the most well-known public key cryptosystem is RSA, for its inventors Rivest, Shamir, and Adleman. An important digital signatures system is Digital Signature Standard or DSS. Actually the RSA system can be used for both (Cheswick and Bellovin, 1994).

Privacy Enhanced Mail, a set of Internet standards for email massaging security, includes data origin authentication, content integrity, content confidentiality, and nonrepudiation by the originator (Greismer and Jesmajian, 1994). Privacy Enhanced Mail represents a major effort to provide security for an application that touches a vast number of users with the Internet and beyond (Kent, 1993). The primary focus of the effort to develop and deploy Internet Privacy Enhanced Mail (PEM) is the provision of security for email users in the Internet community. PEM protects the contents of a message against unauthorized disclosure (i.e., disclosure to other than the recipients specified by the message originator). The message is also protected against attacks such as wiretapping during transit and against accidental misdelivery by the message system (Kent, 1993).

Firewalls A firewall is a barrier that restricts the free flow of data between the inside and the outside. A firewall is a collection of components placed between two networks through which all data (in both directions) must pass; only authorized data which passes the local network security policy is allowed; the firewall itself is immune to penetration. Used properly, a firewall can provide a significant increase in computer security (Bellovin and Cheswick, 1994). The most restrictive firewalls allow only email to go in and out of the company; file transfers and remote log-ons are blocked (Ressler, via Anthes, 1994). It is important for companies to put firewalls around sensitive resources--

such as securing a host to prevent remote log-ins (Hickerson et al, 1992). Network firewalls can be used to control access from the Internet and to protect especially sensitive internal systems or networks (Lipner, 1995).

Conclusion

In conclusion, the important point is not so much what type of security devices are used, but that a company has a security policy in place. A security policy is a set of decisions that determines an organization's attitude toward security--the limits of acceptable behavior and what the company's response to violations will be. It is extremely important that every organization have a security policy. If it does not, it has made the default decision to allow almost anything. (Cheswick and Bellovin, 1994).

References available upon request from first author, larseng@mscd.edu.