Security Technologies

Thomas A. Brooks
Michael M. Kaplan

The growing popularity of such products as wireless telephones, laptop computers, and local area networks has an attendant drawback—the increased threat to privacy and secure communications. End customers are just beginning to become aware of these problems, and are demanding improved security. Encryption technology has evolved to the point at which it is both technically and economically feasible to be employed in public communications products and systems. AT&T, whose work in encryption can be traced back to the turn of the century, is at the forefront in developing products and services that provide encoding capabilities. This issue reviews just a small portion of that work.

Introduction

New technological advances are changing dramatically the manner in which many people conduct their daily business. These changes, to name a few, include:

- The proliferation of wireless and cordless telephones,
- The introduction of a variety of wireless laptop computers,
- The growing use of "paperless" electronic messaging, and
- The expanding use of wireless local area networks.

As customers are just beginning to enjoy the convenience and increased productivity offered by "untethered" wireless communications, they also are just beginning to appreciate the need for protecting their privacy. This, in turn, is creating a need for more stringent, and more ubiquitous, interactive device-based and network-based security measures to protect against illegal eavesdropping and the compromise of information. Alas, it is a never-ending cycle. As new products and services emerge, they often outpace the current security techniques.

Drama of Wartime Security

Historically, our customers—used to the relative security of a wired communications environment—have not truly understood, nor sufficiently appreciated, the vulnerability of their communications. This is often due to the difficulty of pinpointing a security breach when it occurs. After there is an information leak, the cause and results are seldom directly and immediately apparent.

For example, during the World War II air battle over England, the British had to make difficult, often heartbreaking, decisions on how to respond to German air raids without mounting so effective a defense that the Germans would suspect that their codes had been broken. And, because the Allies were successful in hiding their code-breaking successes from the Germans, the consequences for the unsuspecting Germans ultimately were devastating.

The competence of the Allies—both in breaking the Axis codes and in protecting their own information—had a significant impact on the outcome of the war. Stories include volumes written on the Allies' ability to read Japanese diplomatic codes prior to their attack on Pearl Harbor, and of their ability to read Japanese naval codes, which led to victory at the Battle of Midway and the shooting down of Admiral Yamamoto's airplane.

On the 50th anniversary of the invasion of Europe, we should also remember that the Anglo-American successes in the Battle of the Atlantic and the Normandy landing were made possible by the Allies' ability to break the various codes of the German

"*Enigma*" cryptograph machines.

Not that all were success stories, however. General Rommel learned of British intentions in North Africa because the Germans were able to read the communications of the American military attaché.

These are, of course, the intriguing stories of a more turbulent time. Now, we find ourselves moving into an era of communications where security breaches may not threaten people's lives. But such breaches certainly could threaten people's right to privacy, and perhaps even their livelihoods. The stakes are neither as high nor as dramatic as they were during wartime, but they are very important, nonetheless.

Personal and Business Communications

The rapid growth in wireless communications, both voice and data, poses a particular threat to an individual's privacy. News articles appear almost daily pointing out examples of cellular phone conversations being intercepted. Consider the notoriety of press reports highlighting the intercepted telephone conversations of Prince Charles and Princess Diana of Great Britain, and of former Governor Lawrence D. Wilder and Senator Charles S. Robb, both of Virginia. These are some of the most recent cases that have heightened public awareness to the threat of wireless eavesdropping.

But the security of wired communications is also at risk. Not only has privacy become an issue for personal voice communications. The business community is becoming concerned over the security of data, facsimile, and video communications, which have grown exponentially in recent years. Customers also have been exposed to a continual flow of stories concerning large-scale computer fraud, including both scams involving less-than-secure credit cards and hackers breaking into what were supposed to be secure databases. The various emerging forms of electronic commerce, and the much discussed "Information Superhighway," may pose additional threats to privacy and information security than exists today.

Domestic Risks to Eavesdropping. The market for security solutions has been relatively slow to develop in the United States. The American public, in general, still does not fully appreciate the threat to their proprietary or otherwise sensitive data, particularly when it is transmitted over-the-air both domestically and internationally. The most vulnerable portion of the network today is the customer's premises and the loop plant transmission lines that connect the customer to the central office. Once an eavesdropper gains physical access to a customer's property, an aerial connection on a telephone pole, or an underground connection in a vault, the predominately twisted-pair facilities, and even fiber-optic facilities, are vulnerable to simple physical taps. With the movement toward cordless, wireless, and cellular voice and data communications, customers' communications are becoming even more vulnerable to eavesdropping—since such intercepts require neither physical access to the customer's property, nor physical taps on a line.

In contrast, the digitized public switched telephone network is considered less susceptable to the wide-scale interception of a conversation once the communication reaches the central office switch. This is due, in great measure, to the evolution of the local exchange and interexchange networks from copper wire, such as T1 (1.544 Mbits/s) facilities, and microwave to fiber optics. There still is, however, the possibility of hackers electronically accessing the network, despite the increased vigilance of common carriers against such attacks.

In addition, there are many laws against wiretapping communications from a physical medium, such as a cable, copper wire, or fiber. Although porous in some respects, these laws offer reasonable protection against someone intercepting or listening to someone else's communications, although there is no law that bars monitoring radio conversations on wireless facilities.

Notwithstanding, some businesses are losing vast sums of money annually through various acts of piracy and fraud. As a result, they are demanding even better, more stringent protections, and these demands may run counter to the right-to-privacy interests. To allay the fears of both their residential and business customers, these threats must be met by telecommunications vendors with sound, trustworthy means of providing security that cover all aspects of communications.

International Risks to Eavesdropping. As the world moves to a truly global economy, where multiple gateways to regional and country-specific networks are available through a variety of network vendors, the need to provide sound network security—while still providing full feature transparency—becomes essential.

In the international arena, prudence requires that we remind ourselves that not everyone plays by the same set of rules. Not only do certain overseas companies conduct industrial espionage as a matter of daily operations, some overseas intelligence services routinely try to intercept communications, as well as carry out other espionage activities, specifically against U.S. companies. To many this will sound melodramatic, but there are a significant number of documented cases that establish this to be the case, and it has been confirmed by senior U.S. government officials testifying at Congressional hearings.

Encrypted Communications

One form of security—encryption technology—can not only provide for the confidentiality and the integrity of all forms of data, including voice, but also can ensure that the parties sending the information and the parties receiving the information are, indeed, who they say they are.

Encryption technology also can increase the assurance that electronic transactions, such as check cashing, shifting funds from one account to another, and automatic payments to vendors, are valid and, thus, can not be repudiated later.

And, as mentioned, there is a need for any security technology to provide what is called a "trusted" central authority for the system, that is, a database that is impervious to unauthorized access. For individuals also want the confidence that the expanding amount of information that is stored about them in a growing number of databases will not be used against them at some later time.

Early AT&T Cryptosystems. Secure communications have always been a concern for AT&T. Work on encoding communications goes back to the turn of the century. One of the earliest encoding systems developed by AT&T was the Vernam cypher,[1] a complex encoding algorithm invented in 1917.

During World War II, a secure communications method called the Sig Salley Secrecy System was developed by AT&T Bell Laboratories for the government. More ominously known as Project X, the system, used by the British and Americans during the war, was one of the first successful applications of pulse-code modulation. The system included a voice coder that was developed in the 1930s, and eleven 25-Hz channels (ten spectrum channels and one pitch channel), with a total sampling of 550 times a second (compared to the 8,000 samples a second of current algorithms using pulse-code modulation).

In the mid-1950s, AT&T Bell Laboratories developed the KY-9 system, the forerunner of later encrypted vocoders used for government long distance service.

Recent Security Developments

AT&T has continued to provide the United States government with a variety of products to safeguard both classified information and sensitive information. One such system, the STU-III secure telephone, is a highly successful product that has allowed the White House, the Pentagon, the Armed Forces, the intelligence community, and a host of other government agencies to communicate securely, effectively, and efficiently. The use of STU-IIIs in the Persian Gulf War protected Allied communications and expedited the operations themselves. Now, the Secure Communications Systems Business Unit is bringing much of that same technology to commercial applications of voice, data, fasimile, and video security.

Of course, an issue as sensitive as privacy brings with it a number of political and social concerns. The recent U. S. Government announcement of its support of the "Clipper Chip" and the associated Escrowed Encryption Standard (EES) have caused a hotly contested debate in the media. The EES would permit law enforcement agencies with a legal wiretap order to access a cryptographic key that can decode conversations, messages, and faxes.

On the one side is the desire of those who want to protect the national and public interests from subversive and criminal elements. On the other side are the American citizens' interests in preserving their right to privacy and their instinctive concern over the specter of "Big Brother," the government, spying on them.

In This Issue...

This issue of the *AT&T Technical Journal* represents just a fraction of the security efforts undertaken by AT&T's research and development community to provide secure communications to our customers.

Information Age Security. The first paper, "Trust in the New Information Age" by Maher,[2] presents some of the reasons for developing information security strategies for such emerging technologies as multimedia teleconferencing, telecollaboration, telecommuting, telepublishing, the "paperless" office, electronic transactions, etc. Many users of these new technologies are often only faintly aware of the new suite of vulnerabilities that these technologies represent.

Maher raises a number of key questions, which also are uppermost in the minds of AT&T customers, over where the new information age and its highly touted "Information Superhighway" are taking us. He provides a valuable background for the other papers in this issue.

Public Key Cryptography. The field of public key cryptography is becoming more popular as the public becomes more aware of the need for security in general communications, using both wired and the increasingly popular wireless networks. Public key cryptography is an economical method for two parties to exchange secret encryption keys without the participation of a third party (commonly called the "key management center").

The paper presented by Odlyzko[1] reviews both the strengths and limitations of public key cryptography, where it can be most valuable in public and private networking, and key management and encoding digital signatures. The paper also discusses several competing technologies to public keys, and the role each can play in the future.

Introduction to Cryptanalysis. Cryptanalysis deals with assessing the strength of cryptographic algorithms and systems. Siil[3] defines cryptanalysis as the process of attempting to find a shortcut, not envisioned by the system designer, for decrypting an enciphered message when the key used to encrypt the message is unknown.

Siil cryptanalyzes a simple substitution cipher, in order to demonstrate the basic principles of cryptanalysis—although he cautions that, because this cipher is no longer secure, it should *not* be used to encrypt messages. His demonstration uses three of the more basic decryption attacks—ciphertext-only, known-plaintext, and chosen-plaintext—on the simple substitution algorithm. As one might expect, all three attacks quickly yield the original message.

The next four papers in this issue cover the very significant and rapidly expanding area of computer and network security.

Trustworthy Systems. The paper on "Issues and Mechanisms for Trustworthy Systems: Creating Transparent Mistrust," by Blaze et al.,[4] presents methods and software that safeguard file systems, communication networks, and distributed services. The authors' concept of "transparent mistrust" assumes that security is an underlying part of a distributed systems' interfaces and services, and not an extra that comes only at the expense of convenience, performance, or functionality.

They describe scalable mistrust mechanisms that can support a wide range of trust models and security policies. These are secured at a sufficiently low level in the distributed system to allow, in many cases, transparent operation—a very important feature for the user.

An Engineering Approach. Amoroso et al.[5] describe an evolving System Security Engineering methodology that is used at AT&T Bell Laboratories to evaluate threats, vulnerabilities, and attacks on computer and network systems. A hierarchical technique, called a "threat tree," has been developed to focus on the types of damage that can occur to a system, and exactly what it is that must be protected. The threat tree yields vital information on the relationship of different threats, ensures that no potential threats are ignored, and indicates where brainstorming sessions should focus their discussion and analysis.

Such an evaluation should be a "must do" for anyone who installs a system and places significant value on its integrity.

Network Security. Sharp et al.[6] describe issues and methods involved in enhancing the security of networks. They note that, as the administrators of local and wide area networks provide more effective security enhancements for existing networks, some users resist such enhancements.

This paper, tailored to the security novice, discusses these problems. It also defines a process to determine what security mechanisms are required for a network and where they should be placed—without affecting network operation. Several examples are provided using AT&T products.

AT&T Smart Card. The last paper about computer and network security, "Secure Network Access Using Multiple Applications of AT&T's Smart Card" by Sherman et al.,[7] examines a pioneering product: the AT&T Smart Card. The authors discuss the card's technology, including its contactless reader/writer capability, processor, and operating system.

The AT&T Smart Card can secure access to many types of systems and can function in a variety roles, as an identification badge and a credit card. The card supports multiple functions—provided by many vendors—each with its own security capability. Because of this multi-function, multi-vendor capability, the Smart Card could eliminate the nine to 12 credit, debit, and identification cards individuals now carry with them, without losing any of their features and functionality.

Electronic Document Distribution. While the electronic distribution of newspapers and magazines is becoming less expensive and technologically more feasible, the questions of illegal copying and distribution threaten publishers' subscription revenues. Maxemchuk[8] proposes some intriguing security solutions for this new area of information dissemination—electronic document distribution.

The solutions include cryptographic techniques that would make the document difficult and expensive to decrypt, and security techniques that could trace an illegal document back to its original recipient.

Conclusion

This issue presents a representative sample of the work being done within AT&T to provide our customers with secure communications. AT&T recognizes the vulnerabilities that many of the emerging forms of communication present, and is taking steps to minimize or eliminate the adverse consequences. As a result, AT&T will continue to enjoy the trust that its U.S. network has earned among customers, even as the company expands aggressively into the global marketplace.

References

1. A. Odlyzko, "Public Key Cryptography," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 17–23
2. D. P. Maher, "Trust in the New Information Age" *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 9–16
3. K. A. Siil, "An Introduction to Cryptanalysis," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 24–29
4. M. Blaze, J. Lacy, T. London, and M. Reiter, "Issues and Mechanisms for Trustworthy Systems: Creating Transparent Mistrust," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 30–39
5. E. Amoroso, D. Majette, S. Pollak, and W. Kleppinger, "An Engineering Approach to Secure System Analysis, Design, and Integration," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 40–51
6. R. L. Sharp, S. R. Eisen, W. E. Kleppinger, and C. E. Smith, "Network Security in a Heterogeneous Environment," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 52–60
7. S. Sherman, R. Skibo, and R. Murray, "Secure Network Access Using Multiple Applications of AT&T's Smart Card," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 61–72
8. N. F. Maxemchuk, "Electronic Document Distribution," *AT&T Technical Journal,* September/October 1994, Vol. 73, No. 5, pp. 73–80

(Manuscript approved August 1994)

__Thomas A. Brooks__ is a senior vice president of AT&T Paradyne in Greensboro, North Carolina. He is responsible for the Secure Communications Systems Business Unit. He joined the company in 1991, following 33 years in the U.S. Navy, where, as a rear admiral, he was director of all Navy intelligence and cryptographic operations. He has an A.B. degree in Soviet studies from Fordham University in New York City and an M.B.A. degree in finance and accounting from Fairleigh Dickinson University in Teaneck, New Jersey.

__Michael M. Kaplan__ is director of engineering at AT&T Bell Laboratories in the Secure Business Systems Business Unit in Andover, Mass. He is responsible for the design and development of security solutions for voice, data, fax, and video applications in products and services sold to the U.S. government and commercial entities, both domestic and international. He joined the company in 1967. He has a B.A. degree in mathematics from Queens College in New York City, and an M.S. degree in mathematics from Adelphi University in Garden City, New York.