The Coming of Age of Client Security Technology

The Need to Secure the Network's Point of Entry — the Desktop or Notebook Client — Becomes More Visible to Executive Management

Analyst: Roger L. Kay

Although security technology has progressed tremendously over time, awareness of the need for security on the part of people who use computers — both consumers and businesspeople — has not in general kept pace. Essentially, there is plenty of technology on hand, but the understanding of what it does and how to use it has lagged. However, much has changed since the attacks of September 11th. CEOs and IT managers everywhere drew lessons from the differing fates of companies that had backup and restore procedures and those that didn't. Data recovery is, of course, only one piece of the security pie, but as political tensions have increased on the macro level, this and other security concerns have risen in visibility with top managers. **"To what degree is our data — and therefore our business — safe?" CEOs are now asking** in ever greater numbers and with increasing vehemence. "Just where are we with security?" they want to know of their CIOs.

This shift in attitude represents an evolution from the pre-September 11th state, which was characterized by a vague awareness of some subset of security issues, but a misunderstanding of the complete security picture and a widespread lack of adoption and deployment.

Now managers are beginning to assess their vulnerability and to ask what their alternatives are.

In most corporations, the security infrastructure is still inadequate and full of holes. Even the most sophisticated organizations are vulnerable. In one incident, widely reported in the press, that had an impact of major but unknown proportions — the degree of penetration was difficult to assess — a hacker from St. Petersburg, the intellectual seat of the old Soviet Union, broke into Microsoft's network and absconded with a large number of important files, including, purportedly, an unknown quantity of Windows source code files. Naturally, Microsoft never advertised the extent of the damage — if, indeed, it is actually known. And if a company at the epicenter of the information technology business is vulnerable (and by inference should know better), truly, no company is safe from attack.

Lunchtime Attacks

The Microsoft intrusion was a so-called "lunchtime attack," named for the archetypical scenario in which an employee goes out to lunch, leaving his or her computer on, and an intruder simply sits down at the absent worker's desk to feast on whatever privileges that user enjoys, including access to files, programs, and services.

Without having to resort to social engineering, a lunchtime attack can be thwarted quite easily by a variety of authentication methods based on client-level hardware encryption. For example, the operating system can be set to lock out access after a short period of time if it receives no further input and be reactivated only via biometric recognition, a proximity badge, or both, eliminating the need for passwords, which can be forgotten or stolen. If the network had been able to interrogate the remote client to find out whether or not it was authorized, Microsoft would likely have been able to prevent the attack. Had appropriate fail safes been in place, the hack would likely not have been successful.

The security threat is growing in several dimensions at once. The amount of value flowing across the network — in the form of actual money, but also business plans, intellectual property, and strategic documents — is rising by leaps and bounds. And value is at risk in less obvious ways. A reputation can be damaged irreparably by an attack, business can be lost as a result of down time, and the trust on which ebusiness is based can be destroyed permanently. Identity theft, which has become a veritable cottage industry, must be added to the growing list of imaginative crimes. In addition, malicious hackers are getting more sophisticated. Malevolent programmers are not only figuring out more effective ways to harm businesses and individuals, but they are also publishing their tricks on Web sites for other less creative, but perhaps more vindictive, people to find and use.

In this environment, client security can be one of weakest links in the chain. Despite the availability of operating systems with improved security features, desktop and notebook PCs still often have only a Windows password protecting them, and, in older Windows versions, these flimsy mechanisms are easy to crack. Once inside the organization by way of an unprotected node, a malicious hacker has the run of the place to the extent that the legitimate user of the system did. From this position, the intruder can execute transactions as if he were the victim. And worse, in this era of the Internet, the perpetrator does not even have to be physically on site, but can reach the system remotely. And if the hacker is sufficiently sophisticated, he may be able to get at the most sensitive areas of the network, pillaging information, destroying functionality, or even potentially turning computer after computer into a rogue slave that does his bidding. Even if other security measures — such as physical access control, firewalls, network security, software security, database encryption, and server-level intrusion detection — have been instituted, the client node may indeed represent a weak point in the corporation's armor.

Although the mathematics of security are theoretically solid, a secure implementation depends on both the embodiment of the algorithms and the procedures for handling sensitive data and the keys used for encryption and decryption. **Although modern encryption is virtually uncrackable, encryption implemented in software is an open door to hackers.** In software encryption, various ways exist to sniff the most important element — the user's private key. To address this weakness, IBM has embedded the entire process in hardware. An industry group, composed of all the major manufacturers and suppliers and many smaller ones, has agreed to drive the standard into the marketplace. The Trusted Computing Platform Alliance (TCPA to its friends) is now in the second revision of the standard, and this revision is expected to be incorporated into Microsoft's Palladium security infrastructure, due to hit the market in 2004 or 2005. Although IBM acted unilaterally to design and implement its hardware solution, key players in the industry have acknowledged the design point. The TCPA was inaugurated with IBM, Hewlett-Packard, Compaq, Intel, and Microsoft as founding members. Since its inception in October 1999, more than 180 firms have signed up, including Dell. TCPA wants its security technology to be universal in the computing industry, and IBM has committed to making it available via license to anyone who wants one.

IBM itself has moved on from the original embodiment of the TCPA standard, a security chip or cryptographic microprocessor, which was soldered onto the system board of the client and connected to the main processor by a local bus, and now offers an implementation as a modular daughter card. There is no way a Trojan horse can sniff the chip on the card because all private key operations take place within a protected hardware environment. Since its key-management structure is hierarchical, a single private key can be used to secure a large number of certificates (issued, for example, by diverse entities such as a senior citizen's group, a corporate employer, Microsoft Outlook, American Express, and Master Card).

The hardware is designed to work with a suite of other security elements, such as firewalls, antivirus software, security policy software, and Internet Protocol Security (IPSEC), to provide a complete security solution. In addition to being extremely secure, the hardware is simple to use and inexpensive.

In an ebusiness world, trust, protection of privacy, and a secure operating environment are essential. The benefits of hardware-based security are obvious: private keys are truly safe from malicious hackers, multiple secure keys can be generated to facilitate ecommerce with a wide variety of entities, and, combined with a full security suite, hardware encryption enables another layer of security, making ebusiness more viable. **The simple conclusion is this: if your client-level security isn't implemented in hardware, your systems are more vulnerable.**

The need for stronger security is well demonstrated, and effective measures to protect data and users exist in the marketplace today. We're not talking about something two or three years down the road. IT managers should look into these technologies now.

Sponsored by IBM, January 2003