aimpublications LLC

www.aimpublications.com

synthesisseries white paper

1Q2002

Enterprise Security 1

The porous new front line:

defending systems in an unbounded network

After September 11, we're all thinking about how to keep safe what we care about. For organizations and individuals alike, that means finding ways to secure information and network resources. But for systems and networks linked to the Internet, absolute security is pretty much impossible . . .

Unlike earlier times, when most organizations operated closed, internal information systems over which they had complete control, today companies rely on open, unbounded networks. Modeled on and connected to the Internet, these networks engender many kinds of opportunities — commercial, educational, medical, governmental. Similarly, most home-based personal computers no longer stand alone — they're linked, directly or indirectly, to the Internet and its wealth of resources, but now are vulnerable to a Pandora's box of risk.

In our eagerness to benefit from using these open networks, we've overlooked the fact that, in effect, we no longer lock our doors. Controlling access to our information and applications is a hassle: user IDs and passwords to remember, procedures that inflate transaction times, endless administrative interventions. After all, we trust the folks around us; what's the big deal if a password or two gets shared unofficially, or if complex security processes get short-cutted amongst friends?

But the bad guys are out there, invisible maybe, but hard at work trying to break into servers, databases, desktop PCs, even your cell phone.

Threats from the inside, threats from the outside

Security and law enforcement experts believe that computer network break-ins, which have been conducted mostly by students and bored teenagers for 'the fun of it,' are increasingly becoming the work of professional criminals, terrorists, industrial spies, discontented employees and hostile governments. Eventually their efforts will succeed in bankrupting companies, compromising U.S. government security and endangering and even killing citizens.

What's at risk? Just about everything, since just about

everything in our lives — from telecommunications and TV programming to traffic lights and commuter trains to utilities, hospitals and food transport — depends on computers.

In business environments, threats involve loss of money as well as key corporate information like financial and personnel data, R&D information, etc., stashed in corporate servers. This can cost companies plenty: products wrecked or stolen, time and productivity lost, reputations destroyed, customer confidence shattered, confidentiality compromised, revenue and profit as well as business opportunity evaporated.

It's a problem occurring on a spectacularly large scale, though, like an iceberg, much of it remains out of sight. The 2001 survey conducted by the Computer Security Institute and the FBI queried 538 computer security managers. Fully 85% suffered security breaches and most of these suffered financial loss; the average reported loss was around $2 million.

The situation isn't any better in the federal government, where, according to a review by the U.S. General Services Administration, during 2000 outsiders broke into and temporarily controlled at least 155 computer systems at 32 federal agencies.

Yet the bulk of computer crimes — even those involving tens of millions of dollars — go unreported because companies don't want to upset stockholders and customers. The CSI/FBI survey notes that only 36% of the companies that suffered security breaches reported the crimes to law enforcement authorities.

The horror stories

Most of the stories of cyber thuggery, crime and terror that we hear about involve the minority who've actually been caught. Among those:

- A peeved former network administrator at an engineering

company caused the firm $10 million in losses with six lines of well-placed code.

- A Russian cyber-crook robbed Citibank of $10 million, transferring the funds into several accounts before he was tracked down.
- One cyber-gang — dubbed the Phonemasters — tapped into telephone companies all over the U.S. to offer illegal services: a celebrity's address cost $500, FBI records went for $100 a pop and a credit report could be had for $75.
- The social security numbers, birth dates and addresses of 217 of the 400 people listed by *Forbes* magazine as the richest in the U.S. were found in the possession of a convicted swindler who was nabbed after he e-mailed a request to transfer $10 million out of the Merrill Lynch account of one of those 217 people.

More unnerving is the fast-growing list of tales about those who've gotten away:

- A U.S. Bankruptcy Court website running on Microsoft's Internet Information Server (IIS) was hacked by a group that has broken into more than 500 sites in a little more than a year. Yet another hacker group was able to deface almost 700 sites running on a variety of servers — including IIS, Windows NT and Apache on both Unix and Linux — in just 60 seconds.
- Reluctantly, officials at the University of Washington Medical Center last year acknowledged that its computer system had been compromised by an intruder using a sniffer program and thousands of confidential records were stolen.
- The records of 98,000 Amazon.com customers — not just names and addresses but also credit card numbers — were illicitly downloaded from the company's Bibliofind.com book service.
- Last autumn saw several banks cancel and reissue thousands of credit cards after intruders compromised

their, or one of their merchants', databases. By 2005, according to Meridien Research, Internet payment fraud will approach $15.5 billion.

Escalation *ad infinitum*

Internet security is described by those who know as a mess; it's far less secure than, say, conventional telephone networks. The problems and weak spots are many; here are the most obvious:

Passwords

One the greatest vulnerabilities of computer systems are passwords, which the bad guys have gotten very good at stealing using such tools as automated password-guessing software available on the web. Corporate computer system security is only as good as the weakest password in the company. Countermeasures:

- Software that automatically rejects 'easy' passwords based on names or words and that forces users to change their passwords regularly.
- Security 'tokens' that plug into computing devices and which dynamically generate a new password at each log-in (offered by Symantec, Secure Computing, RSA Security).
- Smartcards with embedded chips containing code that identifies its holder, or containing 'keys' that can read and/or send encrypted data; smartcards can be combined with biometric 'signatures' such as fingerprints and voiceprints (offered by RSA Security, Siemens, Domain Dynamics, Gemplus, Datacard Group).
- The Trusted Computing Platform Alliance, a trade group with 170-plus members (including founders IBM,

Intel, Microsoft and Hewlett-Packard) that is working to build authorization chips into PC and server hardware which can be used with smartcards and other security measures.

Exploited routers

Intruders are finding ways to turn the network infrastructure to their ends by compromising routers, which are frequently less protected by security policy and monitoring efforts than computer systems.

Routers are being used by intruders to do scanning, to launch denial-of-service attacks and as proxy points in order to disguise connections to IRC networks. Intruders reportedly have exploited badly configured and deployed routers with vendor-supplied default passwords to gain unauthorized access and control.

And once in control, even the inexperienced cyber-thug can modify a router's configuration, thanks to any number of publicly-available documents that include the needed advice and executable commands. Once of the scariest prospects: denial-of-service attacks based on compromise of the routing protocols that link the networks which constitute the Internet.

'Leaky' servers

When server let network traffic move too freely, it's easy for intruders to gain access and for malicious code to infect systems. According to a survey of more than 2,500 information security officers conducted last summer by *Information Security* magazine, the number of attacks on web servers doubled from 24% of respondents in 2000 to nearly half in 2001. And buffer-overflow attacks, which often exploit web server bugs, increased by 33%.

Some companies try to plug leaks with software that finds vulnerabilities before hackers do with specially-tagged data packets transmitted within and outside their networks.

Attack of the worms & the Trojans

Virus and worm attacks are becoming ever more sophisticated.

Consider how a virus attack can sneak between well implemented defenses by exploiting the web's Secure Sockets Layer (SSL): As data is SSL-encrypted, proxy servers are unable to scan the downloads for viruses, forcing virus-catching efforts to fall back on desktop antivirus software — but who can ever be sure that all an organization's desktop systems are always up-to-date?

What's more, viruses are being designed to conspire: once a virus infects a particular number of machines, it shares the successful method by posting the relevant code to a newsgroup; from there, other copies of the virus automatically download it and start using it.

Meanwhile, Trojan horses — which generally wait on a compromised machine for incoming connections to deliver instructions — are bypassing the port blocking and intrusion detection systems that typically discover them. Instead, Trojans are using legitimate network traffic to make outbound connections to already compromised machines.

Operating systems

Intruders who get past the front door can often issue commands that grant them privileges reserved for system administrators, whether the operating system in question is Unix, Sun Solaris or Microsoft Windows. Such exploited privileges include access to other servers and an ability to examine files, install 'back doors' that enable easy entry in the future and alter system logs so they can remain undetected.

"Tightening down' operating systems to prevent such breaches requires something like 300 manual programming procedures that many system administrators don't know. Worse, new OS 'holes' are discovered all the time — one can find around 10 new Windows vulnerabilities a month discussed on the web.

Consider the hole discovered in Microsoft's free e-mail and Passport authentication service in Windows 98 and 2000 environments: its 'cross-site scripting' permits a malicious coder to sneak between a website and a user's machine in the interval during which the Passport electronic wallet becomes accessible to the user, exposing personal information to intruders.

Discovery of the hole caused Microsoft to temporarily shut down the service, which has attracted 165 million subscribers, two million of whom maintain electronic wallet accounts. The programmer who discovered the vulnerability has pointed out that cross-site scripting is a vulnerability that impacts the entire Internet, not just Microsoft's services.

Meanwhile, it used to be that virus attacks didn't happen much to Unix and Linux machines. But that's changing, as the recent bug in the Unix log-in command illustrates. Now Unix and Linux machines also will have to be protected with antivirus updates

Wimpy wireless

Running rampant across the Internet are sites to help attackers break into cell phones, PDAs and pagers. Some take up 'war-driving' on roads around corporate and government campuses with gear that intercepts wireless transmissions, enabling them to forego the illicit quest for passwords.

At the beginning of 2002, the U.S. Energy Department's Lawrence Livermore National Laboratory placed a temporary ban on wireless local area networks (LANs), noting that, under testing, the wireless networks' built-in security features were "very insecure." Worse still, breaches of wireless LAN security are tough to detect.

The Wired Equivalent Privacy (WEP) protocol deals with such efforts by scrambling data sent over networks — but last summer the protocol was cracked by researchers at AT&T, making it essentially useless.

Some good news: an IEEE task group has approved a new

wireless security protocol, the Temporal Key Integrity Protocol. TKIP helps defeat passive packet snooping, can help determine whether packets have been modified and addresses the WEP protocol security hole.

The newer Advanced Encryption Standard (AES), which has been adopted by the National Institute of Standards and Technology, has yet to be breached and industry watchers expect AES to be incorporated into silicon in the next year (preferred to software-based AES upgrades, which suffer performance degradation because of more complex algorithms and larger key sizes (at least 128-bit rather than WEP's 40-bit).

Intrusions gone undetected

Meanwhile, software penetration toolkits abound and are easily downloaded from thousands of websites. These automate the processes of intrusion, empowering the inexperienced to join the ranks of cyber-raiders. Intrusion detection software can help by monitoring network traffic for command sequences and data traffic patterns that signal attacks offered by SRI International [Emerald], Cisco Systems [Secure IDS], Network Associates [Cybercop]).

But even legitimate users can trigger alarms, so such intrusion detectors are often ignored or turned off: thus intrusion detection software needs some improvement. Cisco and Network Associates are working with Sandia National Laboratories to develop software that's better at distinguishing between serious attacks and stumbling users and false alarms.

Also under development are systems that will identify extensive, coordinated attacks and will enable entire networks to respond in appropriate ways — by, say, putting certain servers on high alert or shutting them down. Intrusion detection developers are also working on ways to spot 'slow attacks' that are intentionally drawn out over hours or days to avoid detection.

Inadequate law enforcement

One of the reasons companies don't report intrusions to the cops is that the cops aren't very adept at catching the bad guys. The FBI, which marshals the nation's federal response to computer attacks, is widely regarded as ill-equipped to do its job.

New information system architectures

The endless rounds of attack/countermeasure/new-and-scarier attack continues to accelerate. This leads some experts to suggest a rethinking of network architectures. Replace conventional networks that allow users relatively open access to internal databases, they suggest, while restricting access to the rest of the universe with networks that allow open access to the outside and place internal databases and file systems under strong and highly monitored restrictions.

Such ideas are problematic in our increasingly Internet-oriented world where online customers want to know instantly whether product X is in stock, where salesmen need mobile access to key transaction data in real time, where effective supply chain management depends on moment-by-moment access to production databases.

Still, separation of internal (and therefore better-secured) production information systems from externally-oriented customer-, marketing- and sales-oriented systems — as long as they're all integrated across the enterprise and updated in virtual realtime — is architecturally viable and, for many organizations, desirable.

Beware the Internet

Once upon a time, perhaps as long ago as when it was still called the Arpanet, the Internet was a safe and friendly neighborhood, a Disneyworld of well-intentioned academicians and scientists. No longer. Now it's easy to get

mugged and corporations and individuals alike need to watch their backs and hold tight to their wallets.

We also need to plan for a future in which keeping information systems secure is increasingly difficult. Perhaps it's time to design and built information systems based on architectures that emphasize an internal-external duality in which internal systems are highly protected and restricted.

aim*publications* synthesis series
white papers on **ENTERPRISE SECURITY**:

1 The porous new front line:
defending systems in an unbounded network
(www.aimpublications.com/synth-esec1.pdf)

2 Now it's about *survivability*
(www.aimpublications.com/synth-esec2.pdf)

3 Corporate
countermeasures & security tools
(www.aimpublications.com/synth-esec3.pdf)

aim*publications* LLC analyzes and writes about how trends and developments in e-business and IT infrastructures — including security, integration, collaboration, database analytics and implementation of new technologies — affect business competitiveness.

As IT writers and marketing communications professionals, aim*publications'* principals also produce advertising supplement and editorial content for leading business and IT publishing companies — including CXO Media (publishers of *CIO* and *Darwin*), *Forbes*, *Fortune*, *Computerworld*, Ziff-Davis and others.

In addition, aim*publications* has created advertising, marketing and/or editorial content for many IT vendors — among them IBM, Microsoft, Sun Microsystems, Computer Associates, Oracle, NCR, Symantec, Hitachi, Quantum and many others.

For more information about aim*publications* LLC, please visit www.aimpublications.com.