

Safe at Last?

by John Williamson

Global Telephony, Apr 1, 2001

Threats and Weaknesses Great Walls of Fire

Network security is a huge and expanding business. A common way to give some scale to this is to cite the estimates readily found of the galactic losses caused by denial of service, virus infection and theft of data and network capacity.

In practice, though, however large such figures are, they are likely to err on the modest side. As Nicholas Ellenden, business development manager and security specialist at Espoo, Finland-headquartered Nokia Internet Communications, remarks, not everyone is keen to publicize the fact that their networks have been compromised.

Also, at any one time not everyone is aware that they are being compromised. And in cases of well-publicized network intrusions, notes David Black, security specialist for Accenture (formerly Andersen Consulting), there can be indirect as well as direct damage.

“One of the intangibles is one's reputation,” he says. “It's all very well to say that a one- or two-hour denial-of-service attack, or a Web defacement, is no big deal — and in many cases it isn't. But if you're in the business of presenting yourself on the Web, what's the cost in terms of your reputation?” Black is based in Washington, D.C.

Although it might be difficult to quantify the cost of network security breaches to any exact scale, there's little doubt the opportunity for major mischief is growing mightily.

Part of this has to do with the increased, and generally acknowledged, dependence of societies and economies on the networking of information.

“The main security threat relating to [corporations and telephone companies] is really the growing reliance on information in doing business,” says Chris Gabriel, U.K.-based regional communications director for enterprise networking concern Enterasys Networks. “Which company can really afford to be security breached?”

Allied to this is the remarkable growth in online — and so faceless — commerce. For example, Entegrity Solutions, a San Jose, California-headquartered security enterprise, is now citing a Gartner Group forecast that the business-to-business e-commerce market alone will expand from an already hefty \$145 billion in 1999 to \$7.29 trillion in 2004.

Meantime, use of networks that do not provide direct line-of-sight between correspondents is rapidly increasing. Most famous in this context is the Internet.

“Today's businesses are reliant on Internet technologies,” says John P. Stogoski, Reston, Virginia-based group manager for Sprint ElSolutions. “With that need, and with all those connections established across that open environment, there's a tremendous hacker threat out there.” Sprint ElSolutions provides a suite of managed, assessment and support security services.

Intranets and extranets also have a lack of visibility and control aspects. “When you enter into these kinds of alliances with your partners, suppliers and customers, it becomes harder and harder to define the boundaries of your own system,” says Accenture's Black.

Some observers also perceive that the growth in wireless technologies presents additional network security challenges. Since data travels through the air, in theory anyone with the right equipment can pick it up, says Ivan Vercruysse, director of product development for authentication specialist Keyware Technologies. Keyware is a biometric security vendor co-headquartered in Zaventem, Belgium, and Woburn, Massachusetts.

“On one hand, mobile networks allow user anonymity, mobility and roaming, and thus are more susceptible than fixed,” adds David Ronen, chief technology officer of NetEye Corp., an Internet protocol and next-generation network fraud analysis solutions vendor in Lod, Israel. “On the other hand, fixed IP networks are typically extremely open and unprotected. [Third-generation] mobile networks have included several security mechanisms built into the network protocols and therefore may be better protected than the fixed IP networks.”

Another new technology attracting the attention of the telecom security industry is digital subscriber line (DSL). “This is an always-on connection, but you have a static IP address that just sits there all day and night,” points out Dano Ybarra, vice president and general manager of Efficient Networks' Commercial Access Business Unit, Los Gatos, California. “And when you have a static IP address, it makes it fairly easy for someone to stumble upon it and then start doing things — sometimes malicious, sometimes illegal.” Efficient Networks is a DSL customer premises equipment vendor.

To complicate this volatile security mix further, employee loyalty might not be what it used to be. “The threat used to be from without, but it's increasingly coming from within,” observes Jonathan Cohen, director of Advanced IP Services at AT&T Data and Internet Services.

“There are FBI studies that indicate that the growth in internal breaches is rising at an alarming rate.” AT&T Data and Internet Services, based in Bridgewater, New Jersey, offers a portfolio of managed network-based and customer premises firewall services, the latter of which now work with Checkpoint and Cisco equipment.

A major problem for large corporations with would-be insider miscreants is that, after employees leave, get fired or change position, large numbers of

existing access rights to networked company resources remain in place, but should actually be invalid.

Turning things off might turn out to be more important than turning them on, says Mike New, vice president of marketing at Access360, an access rights management specialist. New says if you've got a valid user ID for access to a resource that you shouldn't have any longer, "... you don't have to do anything weird to get into those accounts." Access360, Irvine, California, provides software to automatically set up and tear down access rights to multiple resources on multiple platforms.

Passive/Aggressive Threats

Networks face a variety of threats, both active and passive, to their security and integrity. Amongst the most damaging are denial of service (DOS), intrusion beyond public/private perimeters, the spoofing of IP addresses, bogus authentication, and the introduction of viruses. Obviously these can appear in combination.

Hackers also can coordinate attacks from multiple PCs to increase their firepower — notably in distributed denial of service (DDOS) attacks. "In a DDOS attack, the coordinated intruder attack uses multiple PCs or workstations to instruct and control many other PCs or workstations, called Zombies or Daemons, for the DDOS attack against the specified target," says Ben A. Bittle, senior vice president of product development at VHB Technologies Inc., a high-speed network content-monitoring concern in Richardson, Texas.

"DDOS attacks are more damaging and crippling to networks vs. the more mature one-on-one DOS attacks. Once the coordinated attack has begun, the boundary devices located at the victim's site are quickly consumed with a barrage of TCP [transmission control protocol] or UDP [user datagram protocol] packets, consuming all processing capabilities."

In a similar vein, the networking of PCs can increase the hackers' cryptanalysis power. "If I can distribute a screen saver which comes on during an unused cycle, and I can embed a capability in that screen saver to do a chunk of cryptanalysis, and I can distribute that capability to a thousand machines, then conceivably I could bring a considerable amount of computing power to bear on a particular problem," calculates Black.

Various technologies have been drafted to combat these threats, although traditionally there has been a trade-off between improved security and reduced network speed and processing capabilities. Nokia, however, doesn't think the trade-off is still a stumbling block. "That's how it's perceived. But with a well-crafted solution you don't need to have that anymore," says Ellenden.

Reasonable Protection

Well-crafted solutions could involve combinations of public key information (PKI) systems, more robust encryption techniques, stronger and more numerous firewalls, better authentication technologies, more pervasive intrusion detection technologies, and the use of smart cards.

Of these, it's generally agreed PKI is a highly useful and, in some applications, indispensable technology. PKI uses two different keys, binary numbers used by an encryption algorithm to encode and then decode the transmitted data. One key is private and known only to the end user, the other public and known to the opposite party in any communication.

A well-known analogy is that there is general availability of a dictionary to translate from one language to another, but the mechanism for the reverse translation is only available to a particular individual.

There's some debate, though, whether the common PKI Rivest, Shamir and Adleman (RSA) algorithm key length of 1,024 bits (or more) is too long and cumbersome for some applications.

"If implemented appropriately, PKI is never too slow or cumbersome for applications," asserts Greg Meffert, chief technology officer and founder of extended PKI solutions provider Certia, Herndon, Virginia. "The additional effort goes into creating a symmetric key encryption for the content being secured online by the public/private key pair."

The adequacy of the performance of PKI has been questioned in the context of applications such as mobile commerce. However, Marconi SecurTrust achieved what it claimed was the world's first successful full RSA implementation on a mobile device.

"We've shown that it is possible to provide the same strong level of encryption using PKI technology for a mobile device as for a PC, when everyone has been saying that this required more information than could be stored," claims John Dale, chief operations officer of Marconi SecurTrust, Camberley, England.

Although the length of the PKI key certainly has an effect on performance, most users would never notice the difference between a 1,024- and a 2,048-bit key, says Robert Lendvai, vice president of marketing for PKI software house Kyberpass Corp., Ottawa.

"The issue more directly impacts the server," he argues. "Processing hundreds of keys per second places a heavy burden on most servers, which is why the market for crypto accelerator boards and products is exploding."

Kyberpass also says many PKI-enabled applications are not operating at their maximum capacity due to flaws in the complex underlying code. "This problem can be easily overcome by using PKI middleware," claims Lendvai. The circumstance that different vendors' PKI solutions are not yet interoperable also will drive the PKI middleware market, the company says.

Other necessary components of PKI systems are digital signatures and digital certificates issued by digital certificate authorities. Put simply, the first — contained in the PKI private key — are electronic equivalents of written signatures, while the second provide the framework for verifying the digital signature belongs to the digital signatory.

However, if the private key of an individual becomes known to others, how does the digital certificate authority actually verify that the person using the signature is the rightful owner?

The smart card industry reckons it has the answer. To get into the loop in this case, you must not only have the key, but be in possession of an actual card. According to smart card specialist Gemplus, a digital certificate by itself is as useful as a passport without a photograph.

Not everyone has unfettered enthusiasm for smart cards, though. "The problem with smart cards is the complexity of managing them, and the operational and procedural requirements," reasons Sprint's Stogoski. "It's a very costly and challenging proposition."

An alternative PKI authentication adjunct could be biometric technology, where identity is assured by the unique characteristics of individual fingerprints, retinas or voice.

"Biometric measures clearly provide a higher level of security in authentication of the user. It is a simple matter to guess most user names and passwords, and tokens can be stolen. Biometrics is the next logical level," says Paul Henry, director of Asian operations at CyberGuard Corp., a Ft. Lauderdale, Florida-based security solutions provider.

If it can be made foolproof, voice authentication has attractions in its immediacy and convenience. "Voice verification offers maximum security and is more efficient in remote service access than other types of biometric verification such as fingerprint or retinal scans," says Ran Keren, vice president of sales and marketing at Tel Aviv-based speaker identification concern Persay Ltd. "Voice is natural and is easily employed in all mediums of remote access: mobile and fixed phones, PCs and laptops."

Taking the Offensive

In its rather short history, the science of protecting pervasive electronic communication networks has been largely passive and defensive in nature. That might now change.

"There is very good reason to believe that the next step in the data protection evolution will be to 'go-on-the-attack,' " says VHB Technologies' Bittle.

Integrating anti-virus, intrusion detection, multiple distributed firewalls, network address translation, anti-spoofing, PKI, biometrics, and smart card technologies, among others, will be the springboard for new network protection offensives. This integration looks complicated, and it is. But its benefits could go beyond simply stemming current financial and credibility losses, however gargantuan they are.

"A high level of security increases flexibility rather than limits it," points out Lynda Colman, managing director EMEA (Europe, Middle East, Africa) of the U.K. arm of VPNet Technologies, a virtual private network specialist.

"By offering secure access, organizations and enterprises of all levels can open up to a wider audience. Picture the freedom and expanded range of use rather than locks and chains."

John Williamson at 101741.2671@compuserve.com is Global Telephony's Senior Technology Editor based in Chelmsford, England.

Threats and Weaknesses

Here's what some industry experts believe now are the main threats to, and weaknesses of, network security:

Defenses often are just not up to the job in 2001, reckons Jeff Meyers, managing principal of Crescendo Technologies Group, an information technology solutions concern based in Alpharetta, Georgia. "While most organizations have put in place security solutions such as firewalls and vulnerability assessment systems to protect their computer networks, many of these systems were not built for the level of information sharing that occurs," he says.

Paul Henry, director of Asian operations at Ft. Lauderdale, Florida-based security solutions provider CyberGuard Corp., lists three main security weaknesses. First is the failure to implement, for verification purposes, the TCP [transmission control protocol] three-way handshake. In this situation, the destination receives a synchronize/start packet from the source, sends back an acknowledgment, and then receives back an acknowledgement of the original synchronize packet. Without this interactivity, Henry maintains, it's simple to fool systems into thinking you are someone you are not.

Second up are covert channel attacks that are made easier by the maintenance of traditional client/server architectures, allowing the remote hacker a direct connection to the protected server and the ability to hide data in the communications stream. Third is over-reliance on stateful packet filtering (SPF). This technology is popular because it is fast and flexible, but, according to Henry, mostly concerned with verifying source and destination addresses, offers little protection against spoofed communications.

Greg Meffert suggests that "currently, viruses and lack of authentication are the main threats; however, security from outside interception is always a major issue."

Ben A. Bittle reckons a major weakness resides in the corporate access pipe. "The only way to ensure your access links are not flooded with DOS/DDOS [denial of service/distributed DOS] flood traffic is to provide filtering at the Internet service provider or intranet level," he says. Filtering is usually at the corporate front door, but under a concerted attack an optical carrier/synchronous transport module (OC/SGTM) pipe becomes vulnerable to transmission control protocol/user datagram protocol (TCP/UDP) "flood" traffic.

"Have you ever tried to drink water from a fire hydrant?" asks Bittle. "Yes, you can get some water, but it's rushing at you so fast you're likely to drown first."

[RETURN TO TOP](#)

Great Walls of Fire

There's a wide range of industry views on what to watch out for in firewalls of the future. Here are some of the views:

-

“Increasingly complex security scenarios, incorrect configurations, and ever-growing security threats all contribute to the firewall's inability to be a total security solution. A firewall, if configured properly, will keep out 95 percent of the troublemakers, so added defenses are needed. Some corporations' strategy is to start with firewalls as a primary defense mechanism, then add network intrusion detection on the more critical junctions in the network, and host-based intrusion detection on critical application servers and database servers. Robust virus screening, e-mail virus screening, and malicious code screening products might round out the solution.” — **Jeff Meyers, managing principal of Crescendo Technologies Group.**

•

“The trend is integration — firewall technology moving down into the LAN switch port and router port. Moving the firewall technology down into the switch means a much greater level of control, and it also distributes the firewall's power and performance around as many points of entry as possible. And that can only be a good thing.” — **Chris Gabriel, regional communications director, Enterasys Networks.**

•

“[There will be] virtual firewalls in which specific rules for a group or user are only entered into the rule base after a member of the group properly authenticates. This allows ports to be only opened when necessary and effectively hides them when they are not in use. You can't hack a rule and resultant filtered port if it does not exist.” — **Paul Henry, director of Asian operations at CyberGuard Corp.**

•

“I believe we're going to see much faster performance. We're going to see many more firewalls appearing on the inside of customer networks. There's going to be a vast increase in the use of intrusion detection technologies too.” — **Nicholas Ellenden, business development and security specialist, Nokia Internet Communications.**

•

“Future firewalls will grant access based on validation of identity and origin of the transmission (for example, digital signature and/or key matching).” — **Greg Meffert, chief technology officer and founder of Certia.**

•

“They'll be easier to install, configure and manage for a casual user.” — **Dano Ybarra, vice president and general manager of Efficient Networks' Commercial Access Business Unit.**

[RETURN TO TOP](#)

© 2001, IndustryClick Corp., a PRIMEDIA company. All rights reserved. This article is protected by United States copyright and other intellectual property laws and may not be reproduced, rewritten, distributed, disseminated, transmitted, displayed, published or broadcast, directly or indirectly, in any medium without the prior written permission of IndustryClick Corp.