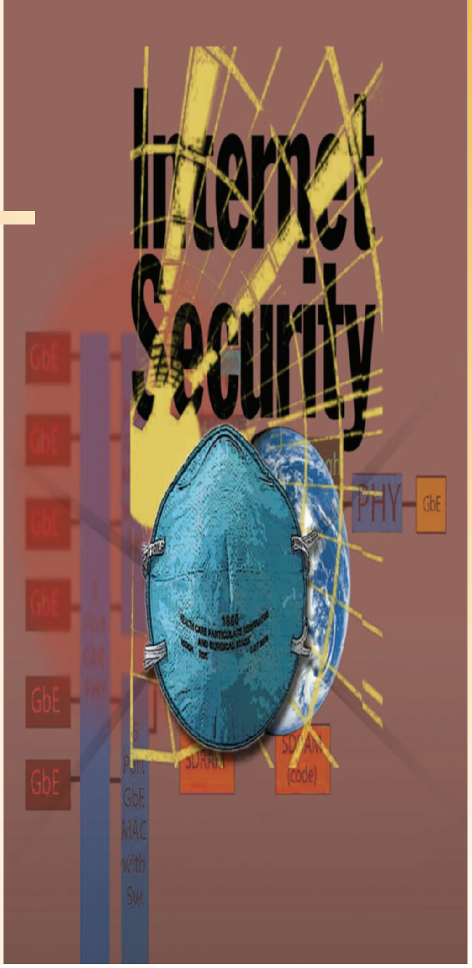
GUEST EDITORS' INTRODUCTION

Securing the High-Speed Internet

As technological advances shift the Internet into high gear, defenses and countermeasures must accelerate to combat viruses that can infect systems at hyperspeed.



Simon S.Y. Shim
San Jose State University

Li Gong
Sun Microsystems China Engineering and Research Institute

Aviel D. Rubin
Johns Hopkins University

Linley Gwennap
The Linley Group

The Internet has brought dramatic changes in the interactions between individuals, businesses, and governments. People and businesses communicate through e-mail messages and engage in e-commerce globally. Global access to the Internet has become ubiquitous. With broadband networks, large amounts of data can be transferred rapidly between parties over the Internet.

Users take these advances for granted until security attacks cripple the global Internet. Attacks spread rapidly through the same broadband networks that made the Internet revolution possible.

The growth of high-speed Internet service has strained the limits of existing network security measures. The CERT Coordination Center of the Software Engineering Institute at Carnegie Mellon University indicates that the number of reported security-breach incidents climbed from 82,094 in 2002 to 137,529 in 2003.

The cost of these attacks to individuals, companies, and governments has increased rapidly as well. According to Trend Micro, virus attacks cost global businesses an estimated $55 billion in damages in 2003, up from about $20 billion in 2002. This Internet security software developer predicts that the trend will continue to climb in 2004.[1]

CURRENT SOLUTIONS

Today, the best security solutions are deployed in layers to protect both the Internet and individual computers. A virus scanner is an essential tool deployed in personal computers, servers, proxies, and gateways to provide protection from many known viruses and remove them from files and e-mail messages. New virus definitions must be updated before deploying the security solution to provide protection. Identifying a new virus requires developing a new definition.

If a known virus exploits vulnerability in an end system, applying a vendor-supplied patch is imperative. However, the huge number of user platforms and their diverse requirements can make using this solution problematic. Thus, some researchers argue that to enforce a uniform security policy, instead of relying on individual users, security solutions must migrate to the network edges or to the Internet service providers at the Internet's core. This requires a security solution that protects networked systems that operate at Internet speed.

Firewalls use *access control lists* to inspect network packets. ACLs perform simple filtering based on port or IP numbers. Stateful firewalls maintain information on each connection and its session states. They perform rigorous checking, especially at the connection setup stages.

Intrusion detection systems identify attempted attacks based on a signature database of common attacks. Although something of a misnomer, active IDSs are often called *intrusion prevention systems*. IPSs understand protocols and provide packet reassembly, scrubbing, and normalization without

0018-9162/04/$20.00 © 2004 IEEE

terminating connections. They also implement protocol conformance and stateful signatures. Firewalls and IPSs probe deeper into network packets, filtering well-known threats against systems. To be useful, these packet inspections must be performed at line speed.

Security solutions must delve much deeper than the network layer and enforce a policy across all application layers.

In industry, firewalls and IPSs are often used in conjunction with *virtual private networks* to allow secure remote access to a corporate network. A VPN provides authentication and encryption for each connection between sites or users. Businesses frequently employ combinations of existing solutions in different security layers.

VPNs typically use ciphers such as the Advanced Encryption Standard to provide encryption; they use constructions such as HMAC—message authentication code using hash functions—to provide authentication. Automated key agreement typically bootstraps off manual keying. Encryption and authentication and decryption and verification must take place before and after transmission, respectively. Although fast hardware often makes this process transparent to applications, the extra load of the security software can create a processing backlog for VPN-enabled machines in very high-speed networks.

SECURITY AT HYPERSPEED

In academia, researchers proposed the Supernet to provide a networking test bed for all US university campuses to use for real-time collaboration at 1,000 times today's performance. Many scientists predict that Internet data network speed will increase from 10 Gbps to the Tbps range. With the explosive growth in Internet e-commerce and the terabit network on the horizon, security experts must reevaluate current security solutions in general, from encryption to trust relationships.

Clearly, the critical challenge facing the Internet in the future is establishing security and trust. Many researchers argue that automatic detection and protection is the only solution for stopping fast-spreading worms such as the SQL Slammer and Code Red.

E-commerce transaction data must be encrypted for secure transmissions. Data encryption and related protocols often require heavy load and long processing time for Web servers. Thus, security becomes a bottleneck. One solution for removing this bottleneck is to move security functions into specialized hardware. The performance of commercially available hardware accelerators, called *security processors*, has increased by 300 times over the past three years. This trend is enabling the application of encryption even to multigigabit data streams while driving down the cost so that encryption can be installed throughout the network.

Large-scale systems such as Web farms, firewalls, IDSs, and IPSs pose challenges because proxy servers must inspect all incoming and outgoing packets in real time. In the high-speed world, the bandwidth requirements needed to perform the necessary packet inspections overwhelm a generic proxy server. Firewalls and IDSs require load sharing among many proxy servers in this environment. Alternatively, some researchers argue that specialized network packet servers can provide real-time packet inspections at multigigabit speeds. Some companies are already developing silicon to support this function.

Future security solutions must protect systems not only from known attacks but also any new ones. Sophisticated and rapidly spreading new attacks make circumvention by current security solutions less likely. Distributed software systems and e-commerce are moving toward XML as the official language with Web services as the underlying infrastructure.

Given the SQL injection techniques and potential distributed denial-of-service attacks, application-level security becomes a critical issue for securing future applications and the Internet. To protect these high-performance applications, security solutions must examine and understand both application and network protocols. Hence, security solutions must delve much deeper than the network layer and enforce a policy across all application layers.

IN THIS ISSUE

The articles in this special issue analyze several significant Internet security trends.

In "Computer Security in the Real World," Butler W. Lampson observes that most systems in service today remain extremely vulnerable to attack, mainly because security is expensive to set up and a nuisance to run. Thus, people judge from experience how little security they can get away with. However, while the actual harm done by these attacks is limited, their growing numbers make effective security measures increasingly important. In a distributed system like the Internet that has no central management, security requires a clear story about who is trusted for each step in establishing it, and why. According to Lampson, the basic tool for telling this story is the "speaks for" relation between principals that describes how authority is delegated, that is, who trusts whom.

Thomas M. Chen and Jean-Marc Robert observe that recent outbreaks such as the Slammer and Blaster worms have shown that the Internet continues to be a fertile environment for attacks designed to spread through computer networks. In "Worm Epidemics in High-Speed Networks," they examine the role of high-speed networking on the rate of worm epidemics. Although this form of networking possibly may shorten future worm epidemics drastically, it could catalyze future worm epidemics to spread at unprecedented infection rates. Extrapolating from recent worm incidents, future worms could saturate the vulnerable population within seconds. The authors observe that a comprehensive automated defense system is the only possibility for detecting and containing a new worm within this short period.

In "Making the Gigabit IPsec VPN Architecture Secure," Robert Friend notes that while the high-speed connections in virtual private networks offer great accessibility, everyone on the Internet can see all the traffic flowing over these insecure Internet LAN connections between remote offices and corporate headquarters. Friend analyzes the various options used to implement gigabit IPsec security in VPNs, with particular focus on the cost and performance efficiencies of implementations that use software-only, lookaside security processors and flow-through security processors.

"A Quantitative Study of Firewall Configuration Errors" by Avishai Wool provides the first quantitative evaluation of corporate firewall configuration quality based on Check Point FireWall-1 configuration files. The data shows that corporate firewalls often enforce poorly written rule sets. Moreover, many errors obviously violate well-established practices and guidelines that are easily fixed once identified. Further, developers repeat the same mistakes over and over, across different industries, regions, and company sizes. According to Wool, the data shows a clear correlation between a rule set's complexity and the number of configuration errors, forcing him to conclude that, for well-configured firewalls, small is beautiful.

Today, security must be an essential part of any network. As part of the continuing effort to bring high-speed access to all users, security becomes a prerequisite for the high-speed Internet itself. The scalability of existing security solutions, growing widespread use of encrypting and authenticating VPNs, administration of diverse platforms, and application security pose the major challenges to this goal in the near future.

Reference

1. Trend Micro, Inc., "Trend Micro Says 2003 Viruses Caused $55 Billion Damage," 16 Jan. 2004; www.stargeek.com/item/62219.html.

Simon S.Y. Shim *is an associate professor in the Department of Computer Engineering at San Jose State University. His research interests include network security, e-commerce, distributed systems, and multimedia databases. Shim received a PhD in computer science from the University of Minnesota. Contact him at sishim@email.sjsu.edu.*

Li Gong *is the founding general manager of the Sun Microsystems China Engineering and Research Institute. His technical interests include systems, networking, Java, and security. Gong received a PhD in computer science from the University of Cambridge. Contact him at li.gong@sun.com.*

Aviel D. Rubin *is a professor in the Department of Computer Science at Johns Hopkins University. His research interests include network security, applied cryptography, and electronic voting. Rubin received a PhD in computer science from the University of Michigan. Contact him at rubin@jhu.edu.*

Linley Gwennap *is the principal analyst of The Linley Group, a technology analysis firm in Mountain View, Calif. His primary coverage areas are network processors, high-performance CPUs, and security processors. Contact him at linleyg@linleygroup.com.*