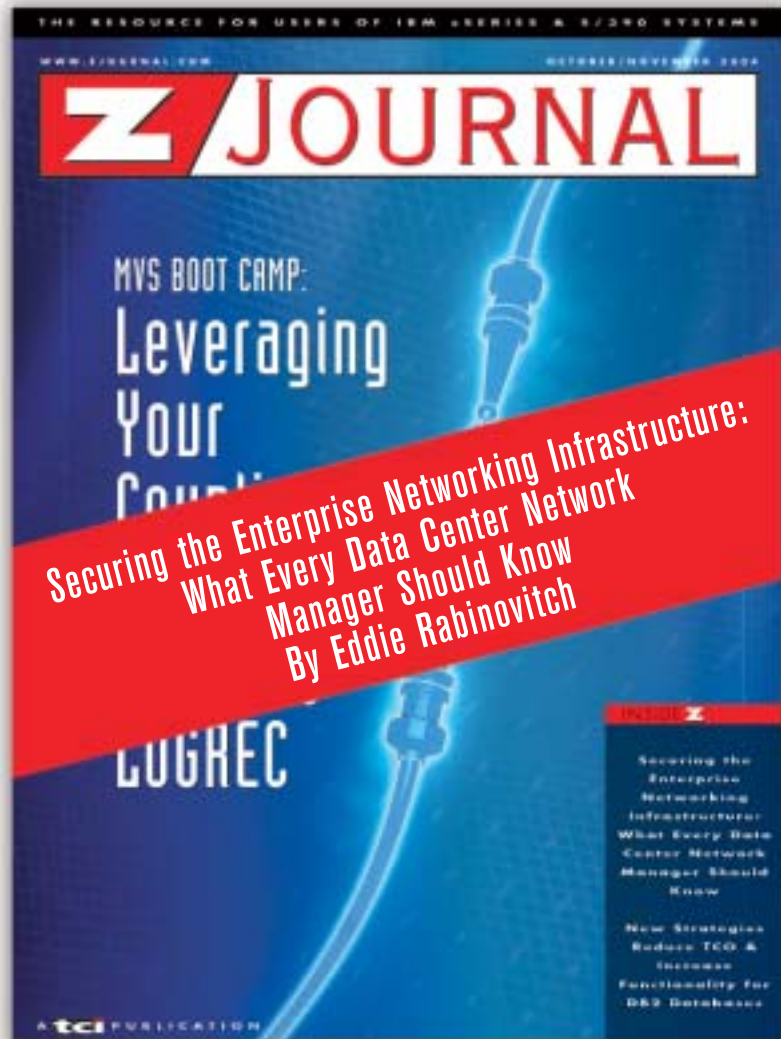



This article appeared in the
October/November 2004 issue of



Subscribe instantly at
www.zjournal.com

- Free in the U.S. and Canada
- \$48 per year outside of the U.S. and Canada



Securing the Enterprise Networking Infrastructure:

What Every Data Center Network Manager Should Know

BY EDDIE RABINOVITCH

What network connectivity options do IBM mainframes support? Several years ago, this used to generate a single answer: SNA, of course! Using either native SNA support or protocol converters or emulators, you could connect any communication device to an IBM mainframe by making the device act as an SNA device. SNA used to be the de facto communications standard of the industry based on market share statistics. This is no longer the case. Today, TCP/IP connectivity for z/OS systems is perhaps the most popular among several mainframe connectivity options.

SNA networks, with their more recent derivatives, such as Advanced Peer-to-Peer Networking (APPN) and High Performance Routing (HPR), are more robust and secure than TCP/IP. But this isn't the first time a better technology lost share to a more mediocre one. Does anyone remember beta video tapes and the OS/2 operat-

ing system? But since TCP/IP communications has become ubiquitous, our goal is making it better by making it more secure and robust.

This article addresses system security and high-availability, which are among the main challenges in modern networking infrastructures.

How do you offer high-availability, connectivity, and accessibility to legitimate users and simultaneously prevent access for illegitimate users and malicious traffic?

SNA networks have been known for resiliency, reliability, and security. When was the last time you heard of an SNA "worm" or Distributed Denial of Service (DDoS) attack that either completely or effectively brought down an SNA network? Unfortunately, TCP/IP networks are not as resilient, reliable, or secure.

The following is from a seven-year-old (but still relevant) book I co-authored in 1997 titled *SNA and*

TCP/IP Enterprise Networking (ISBN 0131271687):

"Securing end-to-end connectivity solutions, utilizing Internet/intranet networks for mainframe-based information access, is becoming more and more popular every day, and for a good reason: Internet's growing popularity promises easy and effective access to information."

Quoting Reed Hundt, the former chairman of the U.S. Federal Communications Commission (FCC): "We can make the libraries of the world available at the touch of a key to kids in their classrooms. That alone would do more to advance educational equality than anything would since the work of Horace Mann. And such a network would single-handedly change the mass-market, least common-denominator model of the media..."

In our book, I also quoted Frank Dzubeck, president of Communications Network Architects Inc., who eight years

ago predicted that: "By 2003, service providers will have effectively replaced most dedicated private line data networks with virtual network services. This phenomenon is well-founded in history: It will mirror, for data, a similar fate that befell dedicated voice networks."

That was a remarkably accurate prediction. Just one other quote to keep in mind—this one from baseball's Yogi Berra: "Prophecy is really hard—especially about the future."

One of the main reasons service providers haven't replaced most private lines with virtual connections over the Internet is security exposures associated with the public Internet. Or, as Reed Hundt noted, "The economics of the Internet are wacky. We have a hybrid of regulated telephone monopolies and not-for-profit academic institutions where we need to have a competitive market. This hybrid gives us part useful chaos and part pure obstacle."

So, what's so special about Internet security? Why are Internet security concerns many magnitudes higher than those for, say, public circuit, packet, or frame relay switching networks? One of the main differences is the fact that no single body is responsible for the Internet. If, for example, a company were using a certain carrier for public frame relay service, this carrier would have contractual obligations to deliver reliable, secure services. With the Internet, such an approach isn't applicable. Although Virtual Private Network (VPN) offerings present an interesting exception to this notion, this is merely a case of an exception that proves the rule.

Another major reason for security challenges is the ever-growing number of sophisticated users who are surfing the net, sometimes with a clear intention to break into someone's network. Some do it for money, some for demonic reasons, and some even for pleasure. However, don't be fooled by the innocent intentions of the hobbyist amateur hackers. The first computer virus inventors didn't do it for profit either, but caused some significant losses.

People claiming their network is 100 percent secure are probably fooling themselves or their bosses. However, because of the security exposure any business gets by connecting to the Internet, it's the responsibility of network managers to protect their networks to such extent that it would be cost-prohibitive for both professional and amateur hackers to break in.

Security management has recently

gained increased exposure to the general public. Beyond the issues of information integrity, privacy and enterprise reliability, the costs to businesses are enormous. According to statistics published by *z/Journal* in July 2004: "Despite more spending on security technology, attacks by hackers and virus writers are up for the first time in three years and downtime has increased. Research firm Computer Economics calculates that viruses and worms cost \$12.5 billion worldwide in 2003. The U.S. Department of Commerce's National Institute of Standards and Technology says software flaws each year cost the U.S. economy \$59.6 billion, including the cost of attacks on flawed code."

Unless caught and forced to do so, companies rarely disclose compromises to their security. According to statistics published by Carnegie Mellon's CERT Coordination Center, 137,529 security incidents were reported in 2003. This represents almost 43 percent of the 319,992 total incidents reported during the last 16 years. The number of mail messages handled by CERT also grew in geometrical proportion in the last four years: from 56,365 in 2000, to 118,907 in 2001, to 204,841 in 2002, to 542,752(!) in 2003.

The Computer Security Institute (CSI) surveyed about 500 security practitioners, senior managers, and executives (mostly from large corporations and government agencies in the U.S.) and found that:

- The most expensive computer crime over the past year was due to denial of service.
- The percentage of organizations reporting computer intrusions to law enforcement over the last year is on the decline. However, the key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity.
- Most organizations conduct some form of economic evaluation of their security expenditures, with 55 percent using ROI, 28 percent using Internal Rate of Return (IRR), and 25 percent using Net Present Value (NPV).
- More than 80 percent of the surveyed organizations conduct security audits.
- Most organizations don't outsource computer security activities. Among organizations that do outsource some computer security activities, the percentage of security activities outsourced is quite low.
- The Sarbanes-Oxley Act is beginning

to have an impact on information security in some industries.

- Most organizations view security awareness training as important, although respondents from all sectors typically don't believe their organization invests enough in this area.

Security Standards

Extensible Authentication Protocol Over Ethernet (EAPoE - IEEE 802.1X) is a security technology that's getting a lot of attention lately, and rightly so. EAP was originally developed for Point-to-Point Protocol (PPP) and described in the RFC 2284 (www.ietf.org/rfc/rfc2284.txt). The Institute for Electrical and Electronic Engineers (IEEE) extended it to Ethernet LANs. The standard cites several advantages of authentication on the edges of the enterprise network:

- Improved security
- Reduced complexity
- Enhanced scalability
- Superior availability
- Translational bridging
- Multi-cast propagation
- End stations manageability.

Although IEEE 802.1X is often being associated with security protection for wireless communication, it's much more appropriate for wired protocols, where the physical cabling infrastructure is much more secure. IEEE 802.1X communications begins with an unauthenticated client device attempting to connect with an authenticator. The access point/switch responds by enabling a port for passing only EAP packets from the client to an authentication server (e.g., RADIUS). Once the client device is positively authenticated, the access point/switch opens the client's port for other types of traffic. A variety of networking gear vendors and many client software providers currently support IEEE 802.1X technology.

IEEE 802.1X proved inadequate for securing wireless infrastructure, so IEEE earlier this year finalized a more appropriate security standard for wireless: IEEE 802.11i. The Wi-Fi Alliance (www.wi-fi.org/), a vendor group focused on wireless technology standards compliance, is starting to certify products for IEEE 802.11i compliance. These products will be called Wireless Protected Access (WPA2), not to be confused with the prior version of WPA released by Wi-Fi in 2003 to address some of the shortcomings of Wired Equivalent Privacy (WEP), which was

part of the original IEEE 802.11 standard. It received considerable criticism due to security exposures.

The Center for Internet Security (CIS) (www.cisecurity.org/) is an important source for Internet security standards. The CIS is charged with developing security templates and benchmarks for evaluation of security posture for most popular products on the Internet. Security templates and benchmarks with scoring tools for security rating available free from the CIS include Solaris, different flavors of the Microsoft Windows operating system, HP-UX, Linux, Cisco routers, and the Oracle database.

In September 2004, CIS started development of a new benchmark for one of today's hottest, but least secure technologies: wireless networks. In addition, the CIS offers tips on e-mail and an automated scanning tool for the System Administration, Networking, and Security (SANS) FBI "Top 20" vulnerabilities list.

SANS Institute (www.sans.org/) is a cooperative research and education organization established in 1989 to support security practitioners from industry and academia by providing them with an additional vehicle for sharing information and lessons learned in search of security solutions. Since CIS tools are being developed according to industry best practices based on information contributed by its members, the more organizations that decide to join the CIS and implement benchmark tools, the better and more secure the Internet will become.

Another interesting security standard is the Baseline Operating Systems Security (BOSS) project (<http://boss-wg.org/>) from the IEEE Computer Society. This standard is being developed by the IEEE P2200 Work Group within an emerging IEEE Information Assurance community that aims to realize the full potential of IT to deliver the information it generates, gathers, and stores. In addition, this group helped launch the IEEE P1618 and P1619 standards relating to Public Key Infrastructure (PKI) certificates and architecture for encrypted, shared media, respectively.

Dealing With DDoS

DDoS attacks caused the most financial damage in 2003. Different tools dealing with DDoS attacks are available today. It's fair to assume that anyone trying to implement any security tool into an existing network infrastructure wouldn't want to move it into production without adequate testing. Testing a DDoS protection tool is probably one of the most challenging tasks for a service provider. About two years ago, I had an

work or server, depriving legitimate users of normally available network services and resources. The distributed nature of DDoS attacks, as well as the complexity and volume of such attacks, have so far prevented practical solutions. Most anti-DDoS tools focus on identifying sources of the attacks and then attempting to shut off traffic from the suspected sources or to the victim by manipulating access lists on routers or firewalls. The anti-DDoS tool we were testing uses a different approach. This tool does not reside on a critical path in the network. Once an attack is identified, the appliance will divert the traffic to itself, but instead of shutting off all traffic to the victim, it will simply discard the malicious frames and simultaneously let the legitimate traffic through.

Due to the distributed nature of DDoS, lab tests are inadequate for accurate simulation of these attacks, and therefore cannot sufficiently predict how well a technology will perform in a real-life Internet environment. So, to test a DDoS tool in real-life environment, we decided to simulate DDoS in a coordinated effort from the Internet. This test was successfully performed in coordination with Mercury Interactive, which launched multiple DDoS coordinated and distributed attacks, such as SYN flood, TRINOO, Targa3, Jolt, UDP floods, and IP fragments, via the Internet against our tested devices while concurrently measuring the service levels for legitimate users. The results of this beta test proved in a close-to-real-life situation that sites

How do you offer high-availability, connectivity, and accessibility to legitimate users and simultaneously prevent access for illegitimate users and malicious traffic?

opportunity to beta test an interesting and unique tool dealing with DDoS attacks, which have become critical points of pain, introducing serious problems for many organizations across multiple industries, academia, and government. These attacks have cost businesses billions of dollars in lost revenues.

In DDoS attacks, hackers use potentially thousands of previously compromised computer systems to unleash malicious traffic assaults against a net-

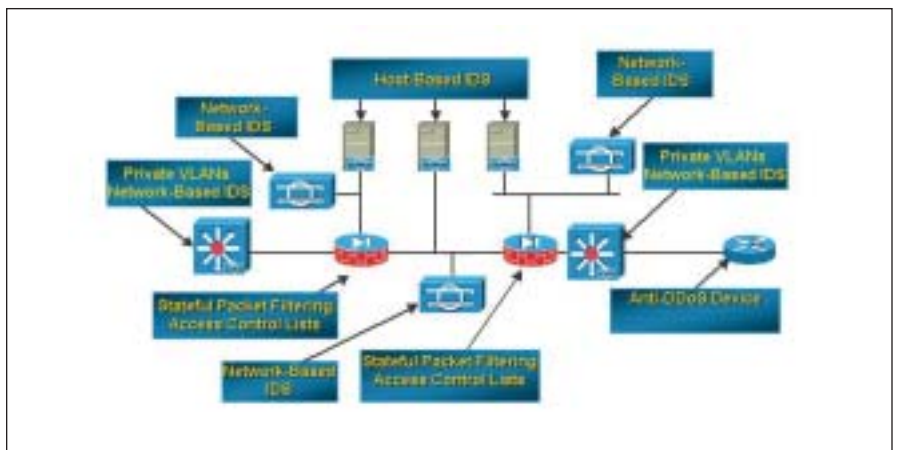


Figure 1: Multi-Level Data Center Security Defense

located within the DDoS-secured environment enjoyed uninterrupted flow of legitimate traffic, even at the peak of the different DDoS attacks.

Summary

Internet security vulnerabilities are never going to disappear. Since z/OS systems are now being connected to the Internet, network managers must be aware that there's no such thing as 100 percent security. Remember, your goal isn't total system security but making it cost-prohibitive for intruders to get through your security defense systems. Technology is certainly getting more sophisticated, but so are security hackers. So, it's even more important to stay on top of the technology and implement the most sophisticated security protection tools available.

Technology is only one element of the security puzzle and enforcement of sound security policies is the most important factor in protection. Assuming such policies are in place, the human factor could be isolated for evaluation when an exposure occurs. It's important for security policies to be accepted and enforced at all levels within an organization, and management must take steps to educate staff about the need for security and how to take appropriate measures to maintain it. In many security-conscious environments, the primary emphasis is placed on blocking external attacks. Too often, organizations fail to recognize the vulnerabilities that exist within their own environments, such as internal attacks from disgruntled employees and industrial espionage.

Network security can be protected through a combination of high-availability network architecture and an integrated set of security access control and monitoring mechanisms. Recent incidents demonstrate the importance of monitoring security and filtering incoming traffic as well as outbound traffic generated within the network. Defining a solid, up-to-date information protection program with associated access control policies and business recovery procedures should be the first priority on the agenda of every networked organization.

There are no magic bullets for security protection and the only way to address security appropriately is to deal with it at multiple levels. Having a well-designed network with secure Virtual LANs (VLANs) and properly configured firewalls with the appropriate Access Control Lists (ACLs) is impor-

tant, but not sufficient. In addition to the firewall, it's important to implement both network- and host-based intrusion detection and intrusion protection tools as well as DDoS protection tools (see Figure 1).

Securing physical and networking layers is critical for building a secure, reliable enterprise infrastructure. Nevertheless, all seven layers of the Open Systems Interconnection (OSI) model play an important role in security infrastructure. Some take it even a layer higher, to the so-called layer 8, or the "political layer." Specifically, a firm's information security posture—an assessment of the strength and effectiveness of the organizational infrastructure in support of technical security controls—must be addressed through the following activities:

- Auditing network monitoring and incident response
- Communications management
- Configurations for critical systems: firewalls, Domain Name Systems (DNSes), policy servers
- Configuration management practices
- External access requirements and dependencies
- Physical security controls
- Risk management practices
- Security awareness and training for all organization levels
- System maintenance
- System operation procedures and documentation
- Application development and controls
- Authentication controls
- Network architecture and access controls
- Network services and operational coordination
- Security technical policies, practices, and documentation.

A properly designed network with comprehensive security policies aimed at high availability, recoverability, and data integrity institutes the necessary infrastructure to conduct activities in a secure, reliable fashion. **Z**

About the Author

Eddie Rabinovitch is an independent consultant with more than 25 years of experience in IT, networking, and security. He is a senior member of the IEEE and an Editorial Review Board member for *z/Journal*. He has authored more than 120 papers, which have appeared in numerous technical and trade publications.
e-Mail: eddie@ieee.org



**Subscriptions to
z/Journal are FREE in
the U.S. and Canada.**

**Subscriptions outside
the U.S. and Canada are
\$36 per year.**

[Click here to subscribe.](#)