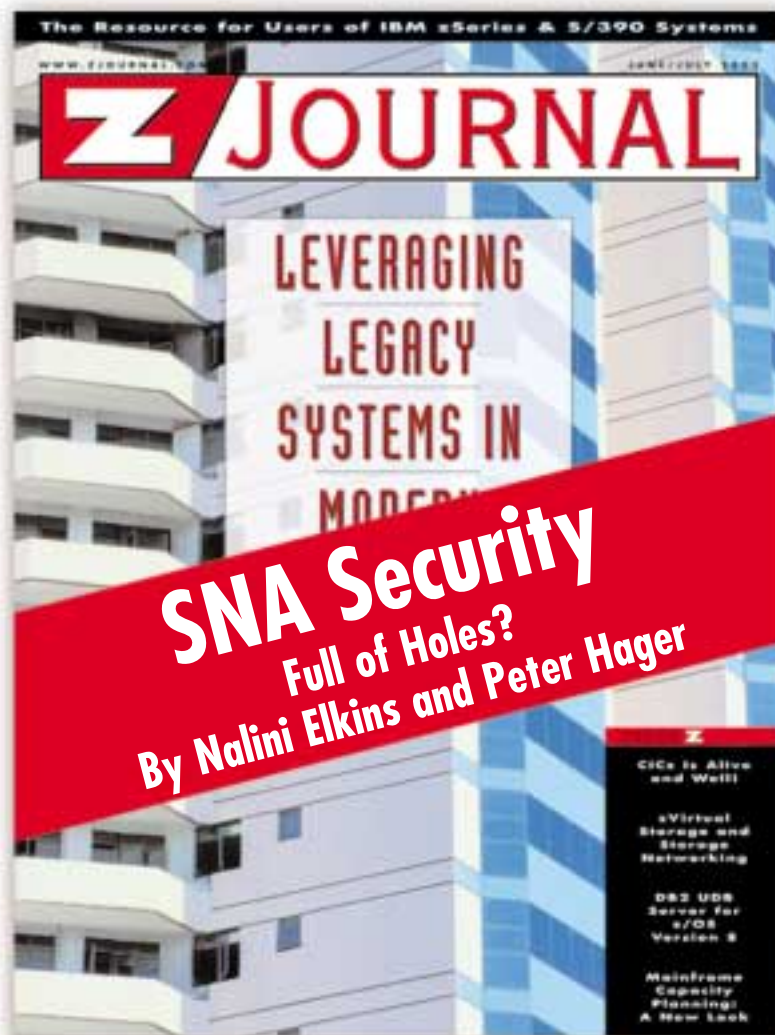


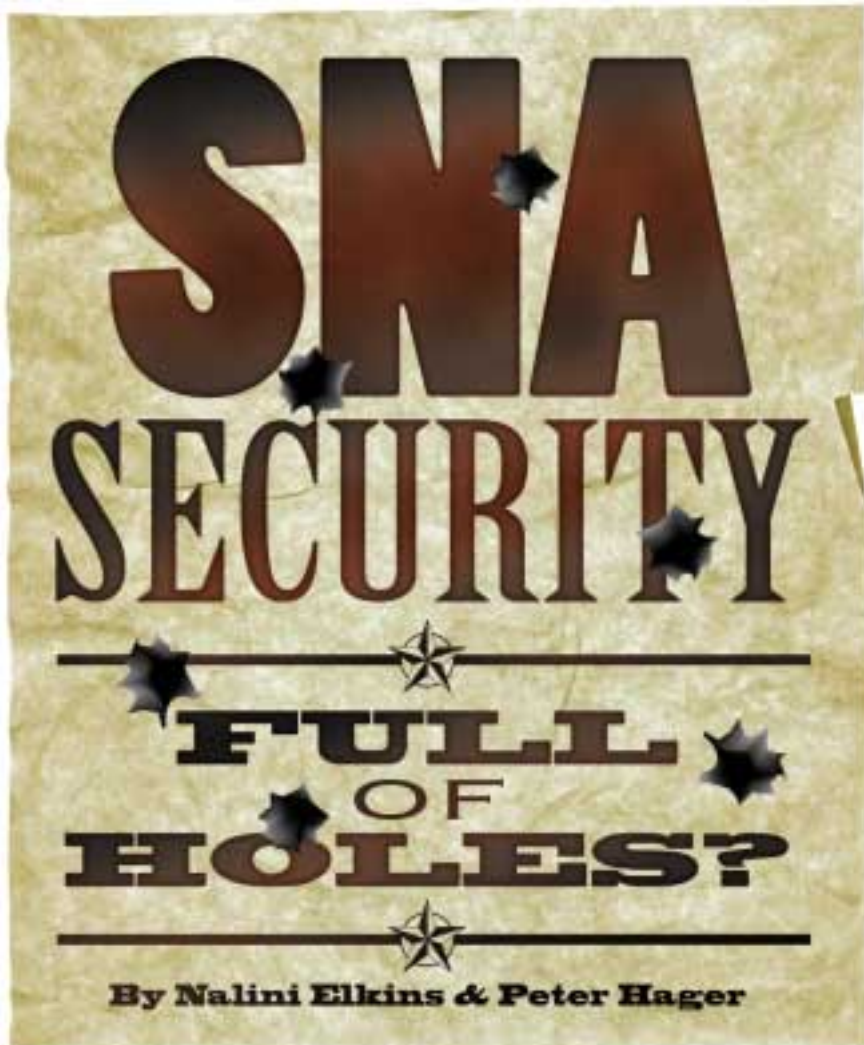
This article appeared in the
June/July 2003 issue of

Z/JOURNAL



Subscribe instantly at
www.zjournal.com

- Free in the U.S. and Canada
- \$36 per year outside of the
U.S. and Canada



Are there security problems with SNA? It is a widely held perception that SNA networks are secure. Despite the rapid adoption of TCP/IP, SNA still lives. The following statistics were taken from the recent Vedacom Corp. article, "SNA and TCP/IP Convergence, a White Paper."

- ▀ **The installed base of SNA-based applications and networks is greater than \$20 trillion worldwide.**
- ▀ **Ninety percent of the world's largest enterprises use mainframes with SNA-based applications. Furthermore, 60 to 70 percent of mission- and business-critical applications in U.S. enterprises are SNA-based.**
- ▀ **More than 50 percent of business data traffic, and more than 70 percent of transactions, are SNA-based.**
- ▀ **SNA supports the majority of Online Transaction Processing applications (OLTPs).**
- ▀ **The cost of using Unix or Windows servers in terms of staffing and software significantly increases when going from 96 to 99.999 percent uptime.**

It seems likely that this will change only slowly over the next five to 10 years. Therefore, it seems imperative to pay attention to security. Let us tell you about some problems at real user sites over the last few years. Then, you can determine for yourself whether or not you should investigate SNA security on your network, and/or what the price may be if you decide to do nothing.

We have found that the tools to implement security are there but often are not used. In many cases, policies for maintaining a secure network are not strictly regulated, and monitoring is non-existent. During a recent presentation at the Online Terror and Technology Conference, speaker Dennis McCallam stated that the number one threat to any information system is from insider attack.

We have developed a proprietary security technology that allows us to check all SNA sessions and BIND parameters. During the course of our installations, we ran into the following incidents, which may interest you. By the way, all of these would fall into the classification of insider attack. We also know of several other incidents that were external attacks.

CASE 1: UNAUTHORIZED VIEWING OF CLIENT DATA

A service bureau data center had two individual banking groups as clients; we will call them Group 1 and Group 2. Because the security algorithms they used for LU6.2 were done incorrectly, Group 2 could view and modify the data from Group 1. The data center did not learn of this problem for a long time. Group 2 kept this information confidential and saw this as a competitive advantage. This changed for Group 1 when they found out that Group 2 was also able to view their information!

Group 2 reacted by complaining to the data center and by requesting compensatory payments against the data center as the service provider. The loss of credibility of the service provider within the community cannot be overstated. To date, their business has not recovered. The provider used RACF on the mainframes, but in this case, the system did not warn anyone nor was the unauthorized group of clients rejected.

CASE 2: FREE ACCESS TO DB2 DATA

A data center unknowingly allowed free access to unauthorized users to all data of a core DB2 database. The problem was caused again by invalid security

parameter settings for APPC (LU6.2). Was this done by mistake or with full knowledge of the consequences? The staff at the data center did not know of this security problem for almost a year!

The data center provider could not understand what had happened, as it was using RACF. However, in the end, although RACF protected the system, the provider had to admit that it did not have RACF set correctly to coordinate with the network design!

CASE 3: TAPPING INTO AN APPN NETWORK

A young employee was able to connect into his company's APPN network. Then, he did something really easy – using trace (BUFFER or VIT) he found within the logon requests sent by the central VTAM his own cross domain as well as cross net resources. Then, he wrote a Java program that used the LUNAME of a sensitive IMS application. This program simply sent the welcome panel of that application, "Please Enter User ID and Password." The employee had received the welcome panel by simply cutting and pasting from the original application.

When the end user entered his user ID and password, not knowing to whom this data was going, the false application stored the user ID and password into his laptop and terminated the session. The employee was able to collect many valid user ID and password combinations, which he could then use to logon to the sensitive IMS application. You can imagine the next step! What if he was able to access the payroll application or the application that tells the location of the test wells being drilled for an oil and gas company?

CASE 4: HACKING INTO SNA USING A DIAL-IN FUNCTION

One company has offered dial-in access to its employees for many years. Unfortunately, an unscrupulous employee used this dial-in access to hack into the company network. The company discovered this young man's activities only because after the regular restart of the productive system one weekend, the system could not receive any logons from the network! After several hours of intensive analysis, the staff finally determined that there was a hacker rerouting logons! The result was an unnecessarily long system downtime.

Can you imagine what other ways there are to damage a company or organization? Sometimes the security imple-

Most networks are more often inspected by "hackers" than by "administrators," despite increasing techniques and equipment to detect hackers.

– Computerworld

mented is the weakest element in the chain!

WHAT CAN YOU DO?

The most important thing is to implement LU-LU and CP-CP verification. This will verify for all SNA connections that the LU-LU or CP-CP session is taking place between the appropriate partners. Once implemented, you must check that all sessions are using the verification feature. However, it is impossible to check this without an automated control. We recommend that you use an automated system, which alerts you and

Sometimes the security implemented is the weakest element in the chain!

logs any security problems.

UNUSED DEFINITIONS

Make sure that you have removed all unused definitions from your VTAMLst and other related data sets. This will prevent hackers from using old CPNames or definitions to simulate systems on your network.

ENTERPRISE EXTENDER

Enterprise Extender is a new technology from IBM that is used to integrate SNA applications into TCP/IP networks. It is a set of extensions to the existing APPN High Performance Routing (HPR) protocol. The HPR frames are sent using User Datagram Protocol (UDP) packets. To the HPR network, the IP backbone is a logical link; to the IP network, the SNA traffic is UDP datagrams that are routed without hardware or software changes to the IP backbone.

Unfortunately, the wide adoption of IBM's Enterprise Extender Technology increases the problem of hackers accessing your system because now your data center may be connected to another data center many miles away or many countries away. Now, you have opened your company to hackers from the other end of the Enterprise Extender. You may have adequate physical security at your end of the connection, but what about at the other end?

CONCLUSION

Hackers are getting smarter and more aggressive. Many IT experts don't know that 99 percent of all attacks are a result of already known weak points or wrong configurations. To come directly to the point, that means that 99 percent of all attacks are essentially avoidable. **Z**

About the Authors

Nalini Elkins is the CEO and founder of Inside Products, Inc., which specializes in intelligent network management tools. She has many years of experience in network management and software development.
Voice: 831-659-8360
e-Mail: nalini_elkins@inside-products.com
Website: www.inside-products.com

Peter Hager is the CEO and founder of Net'Q Holding, a recognized tuning expert for large IT networks. The core activity of Net'Q is analysis, optimization, and security audits for TCP/IP and SNA networks.
Voice: +49-89-69969-310
e-Mail: p.hager@net-q.com
Website: www.net-q.com