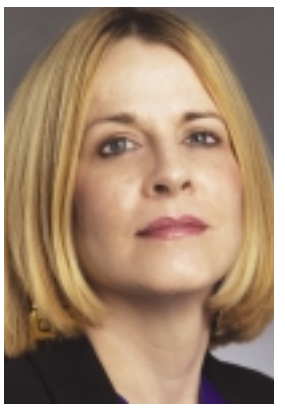
GSN ANNOUNCES:

BPA audit verifies 35,000+ GSN readers
GSN will go bi-weekly in January

GSN. Government Security News

Oracle's Chief Security Officer, Mary Ann Davidson, means business

Page 24



October, 2004 Vol. 2 Issue 8 | *The Newspaper of Record for Government Security* | A Publication of World Business Media, LLC

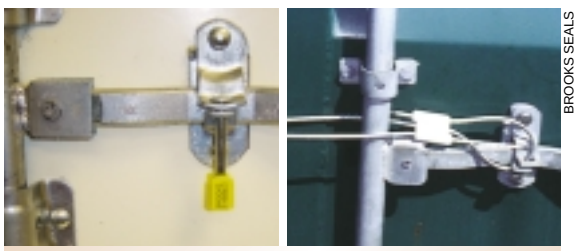
INSIDE

DHS mulls high-security container seal mandate

Under secretary embraces panel's recommendation

By JACOB GOODWIN

Despite a plethora of new *electronic* approaches to sealing and securing maritime shipping containers, an industry advisory committee to the Departments of Homeland Security and Treasury has recommended that DHS take only a partial step by requiring shippers to use high-security *mechanical* seals



BROOKS SEALS

DHS may require shippers to use "high-security seals," such as bolts (left) or cables on inbound containers

More on Page 13

Defense, IT & security firms vie for homeland contracts

By DAVID BATES

The future for systems integrators in the homeland security market appears fairly rosy, according to major players in that market segment. But determining who will be the big homeland security systems integration (SI) contract winners — the defense contractors, the IT sector, or the traditional security firms can be a complicated undertaking.

MARK KAPLAN

Much of the systems integration work during the first 18 months of the Homeland Security Department's existence has focused on traditional security missions, says Tom Simmons,

More on Page 28

U.S. Air Force takes new tack on security training

By STEVEN E. BRIER

When Brig. General James Shamess, director of security forces for the U.S. Air Force, wanted to raise standards for his senior security officers, he could have done things the tried and true way and set up another training school. After all, the military has schools for everything from truck driving to international relations. But that, he says, would not have served the Air Force's needs.

"You can always set something up in the military, but you are always doing the task list," Gen. Shamess said. He was after something more than the typical school curriculum, something that would show mastery of a subject as well as flexibility. "The military pushes directly toward its primary mission and those missions change," he said.

Instead, Gen. Shamess started a program in the fall of 2003 to have up to 1,000 of the Air Force's security personnel strive for Certified

More on Page 29

GSN is on the move...

GSN: Government Security News, an authoritative newspaper covering the government security marketplace, has received its initial circulation audit from BPA Worldwide verifying that it has been distributing more than 35,000 copies each month to government officials and industry executives. Based on the strong support *GSN* has enjoyed from its readers and advertisers since its inception, the publication announced that it will begin publishing bi-weekly, beginning in January 2005, and will produce a total of 22 issues next year.

"We're very proud to be answering the call from our readers and advertisers to double the frequency of our newspaper in 2005," said publisher Ed Tyler. "We'll not only be able to cover more news more quickly, but we'll be able to provide more finely-tuned marketing opportunities for companies trying to reach this market. ■

Heavy IT work load inspires automated network auditing

By RANDY BARRETT

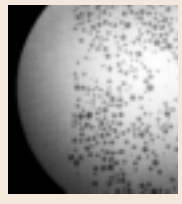
Protecting a network is futile if you don't know which doors and windows sit wide open to the world. Luckily, auditing technology is rapidly improving to give system administrators up-to-the-minute vulnerability information.

What started a few years ago as an obscure craft practiced by a select group of security consultants has blossomed into an industry based primarily on automated scanners capable of

More on Page 15

Covering Physical & IT Homeland Security Solutions www.gsnmagazine.com

MadahCom's emergency notification system safeguards visitors and employees at the Statue of Liberty
Page 8



Glenbrook Technologies makes a high magnification camera that can spot hazardous biological materials in luggage
Page 32

The CardMan 5121 reader from Omnikey can interface with both contact-based and contactless smart cards
Page 32

From Page 1

Automated vulnerability assessments spawn growth industry

quickly sifting through a network's external and internal interfaces to find holes and weak spots. While the evolution is reminiscent of John Henry's epic contest against the steam drill, experts say there is still very much a need for humans in the auditing loop.

"Machines are nice and are getting more intelligent but somebody needs to see what's going on," says Joe Visconti, a security consultant based in Austin, TX.

While scanners can pick up all manner of potential problems, Visconti says a good sysadmin is needed to "filter out the junk" and see which vulnerabilities need quick attention.

So far, network operators are better at tracking and fixing external-facing vulnerabilities than those living inside the system. According to research conducted by Gerhard Eschelbeck, chief technology officer for Redwood Shores, CA-based **Qualys, Inc.**, the time it takes sysadmins to fix external vulnerabilities has dropped to 21 days. But at 62 days, *internal* security problems take almost three times as long to fix.

Eschelbeck argues sysadmins are far too busy to conduct manual security audits. Besides, the results usually end up sitting uselessly on the credenza. "Large, book-sized vulnerability reports produced on a periodic basis usually end up on a shelf or in a file drawer. Consultants often use these 'phone books' to justify an audit, but the documents have little or no practical action value for teams working daily emergencies with networks and servers," he says.

His position isn't entirely surprising. Qualys offers an automated vulnerability assessment service costing $1,000 to $150,000 per year depending on the size of the organization. For that retainer, the company will scan both external interfaces and internal systems on a regular basis. To get information from within the network, Qualys places an appliance inside the client's firewall that checks every nook of the organization.

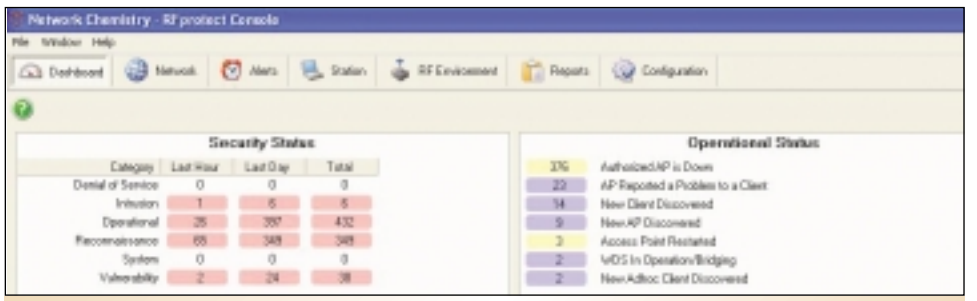
"You do the testing without intruding on the network," Eschelbeck. "You have to make sure the client's systems aren't impacted by the audits."

In the first sweep of an audit, Qualys maps out which devices are on the network. When that's done, the automated system looks deeper into all applications and every device resident in the system. Presently, the platform can detect 3,700 vulnerabilities and 20 more are added each week, Eschelbeck says.

It is becoming common for clients to request weekly audits, says Eschelbeck, and most often those scans turn up forgotten servers, misconfigurations, rogue devices and virtual private network set-up errors.

Archie Alimagno, information security officer for the California Department of Insurance, has been using the Qualys system for a year and chose it because it can find vul-

More on Page 16



Portion of screen from Network Chemistry's "RFprotect" monitors wireless surveillance

From Page 15

Some audits spot weaknesses and prioritize fixes

nerabilities both inside and outside the network. He also likes the vulnerability reports which include detailed information on how to patch security holes in his network of 1,500 workstations and 500 laptops at 18 locations.

"The reports drill down to the specifics of the vulnerability and [suggest] the necessary fix," Alimagno says. "There's no need to know what vulnerabilities you have if you don't know how to fix it."

San Antonio, TX-based **Digital Defense, Inc.** offers a security audit service called Frontline that also requires a server on the customer's premises. "It operates in the same manner as if we deployed an analyst on site full time," says Digital Defense's chief technology officer, Rick Fleming.

The company can run scans at any time of the day, though usually it does so from 2 am to 3 am to avoid slowing down the client's network during working hours, Fleming says. The cost: from $400 to $3,000 per month, depending on the size of the organization.

Another auditing tool is sold by **Tenable Network Security Inc.**, of Columbia, MD. The platform is based on the open-source Nessus sniffer and sells under the name Network Vulnerability Observer, or NeVO. The cost: $10,000 for an unlimited-use license. The company currently has installations at NASA Goddard and numerous large financial firms.

For network owners worried about wireless security holes, **Network Chemistry, Inc.**, of Palo Alto, CA, offers a radio frequency sniffer that can detect devices in spaces up to 80,000 square feet. Unlike some competitors that market hand-held scanners, Network Chemistry permanently places its sensors in clients' office spaces.

"We not only detect these things, more importantly, we tell you what [the rogue devices] are doing," says Network Chemistry CEO Rob Markovich. The cost: $649 per sensor and $2,500 to $5,000 for software.

The two-year-old company has been making steady inroads into the government market and currently has installations at the Air Force and the Marine Corps, as well as in state governments, including the Minnesota Department of Public Health. The company's primary competitor is **Air Defense Inc.**, of Alpharetta, GA.

Once an audit is complete, the automation ends and the very human task of plugging security holes begins. Industry players say the holy grail of network security is to create a program capable of both auditing and repairing security breaches without human intervention.

"Automation tools will get smarter and smarter," says Fleming. "The technology is there to find and fix vulnerabilities."

Not everybody is sold on the idea. Installing patches can be delicate work and an automated fix done improperly could cause havoc, says Visconti: "You would run the risk of bringing down the system."

The situation also raises the conundrum of needing a program to check the automated patches of yet another program. As well, the number of software vulnerabilities is growing exponentially and Visconti doubts even machines could stay ahead of the curve. According to Eschelbeck's research, 50 percent of the most critical vulnerabilities are replaced by new ones on an annual basis.

"Self-correcting robots can't keep up with Microsoft," says Visconti, ruefully. ■