SecurityManagement ONLINE
Security Management Online Archive (1996-2006)

Tech Talk

November 2004

By Peter Piazza

In this issue:

The Buzz Over ZigBee

Focusing on the short range may be bad for business--unless you're talking about remote control technology. The latest short-range wireless option is known as ZigBee, an open standard created by a nonprofit consortium of companies called the ZigBee Alliance.

ZigBee chips require very little power, which means they can be operated for long periods using only a battery. However, because they send and receive data at a low rate, these chips are not right for pushing large amounts of data; rather, the technology is designed to help create wireless sensor networks for close-range remote monitoring, home control, and building automation network applications. While many applications are consumer oriented, some business security uses are foreseen.

RAE Systems, a Sunnyvale, California-based manufacturer of chemical and radiation sensors, has recently rolled out RAEWatch, a wireless sensor bundle that can be used in applications such as monitoring public venues or securing cargo containers.

Bob Durstenfeld, director of corporate marketing for the firm, explains how a shipping container equipped with ZigBee sensors could be monitored: "You'd have a transponder on the dock, on the truck carrying the container to the dock, and on the ship. You'd uplink it and keep track in real time of your containers." The container could thus be tracked from ship to dock to truck to its destination.

Durstenfeld compares the workings of a ZigBee radio network to the Internet, where packets move nonlinearly from server to server until they reach their destination. "The beauty of ZigBee is that it forms an ad hoc network," he says. "It lets you have a cloud of sensors that can talk from sensor to sensor and act as their own repeaters. You can monitor multiple points from one central point or one edge point of the cloud of sensors." Unlike a hub-and-spokes configuration, where if one radio drops, the signal is lost, "ZigBee lets you talk from the closest radio," he says.

Regardé is a new business that plans to sell products with ZigBee technology. Cofounder Jared Richard Brandt says the company is running a beta test with hundreds of homeowners who have installed in their homes some ZigBee-enabled sensors that can detect door openings, smoke, and carbon dioxide, and other sensors that control low-power electric devices such as lights.

The sensors communicate via the ZigBee protocol to a small Linux-based device with a built-in e-mail server that is connected to a homeowner's computer. So, for example, a parent can be notified at work via e-mail when a child has returned from school. Next generation devices will tie into traditional alarm-monitoring services, Brandt says.

One homebuilder, eager to protect homes under construction and high-value tools left on building sites, is working with Regardé to use Zigbee to monitor entry and exit to the work sites using motion detectors activated after working hours. These sensors would transmit data back to a base station that would be housed in one of the model homes, where a broadband connection would allow a project manager to monitor any movement on the site after the construction site was closed for the night. An alert could also be sent to an alarm-monitoring company.

Brandt points out that the transmissions are encrypted; he notes, however, that some security issues are inevitable, because ZigBee devices need to be visible to function. As for security, Chris Lopez, an analyst with market research company ABI Research who forecast high-growth for the ZigBee market, says the specifications have been closely watched to ensure that the technology is secure from attack. But like the Bluetooth protocol before it, problems with ZigBee are not likely to come to light before products are rolled out and security researchers start poking holes in it.

I Spy an End to Spyware

New legislation.

Two bills that would curtail spyware passed the House of Representatives just before members adjourned to campaign for reelection. H.R. 2929, sponsored by Mary Bono (R-CA), criminalizes actions such as the "hijacking" of a browser, modifying bookmarks or a browser's start page, and installing any type of software program that would spy on a user's sessions. It would prohibit keystroke loggers, and make it illegal to use a "zombie" computer to damage another computer.

The bill, known as "Securely Protect Yourself Against Cyber Trespass Act" or the "SPY Act," would take effect next October. It provides for fines that range as high as $3 million per violation, to be enforced by the Federal Trade Commission.

The second bill, introduced by Representatives Bob Goodlatte (R-VA), Zoe Lofgren (D-CA), and Lamar Smith (R-TX), is known as the "Internet Spyware (I-Spy) Prevention Act" (H.R. 4661). It was passed the following day. It differs from Bono's bill particularly in that it imposes not just fines but also prison sentences on offenders, with sentences of up to five years possible.

Goodlatte offered concerns in a written statement that the SPY Act was too broad and sweeping, "and would result in the regulation and penalization of those legitimate software companies that are actually trying to play by the rules."

Studying and Stopping the Insider Threat

While the danger of the "insider threat" has been well cataloged, the details of inside attacks have not been considered in much depth. For example, who are these insiders? And what sorts of

attacks do they launch? A new joint study by the U.S. Secret Service and the CERT Coordination Center helps shed some light on these questions.

Insider Threat Study: Illicit Cyber Activity in the Banking and Financial Sector examines insider incidents "from both the behavioral and technical perspectives." Investigators carried out a thorough review of 23 incidents (from fraud and the theft of intellectual property to sabotage) perpetrated by 26 insiders and found that most incidents--87 percent--were not technically sophisticated. In these cases, "the insiders employed simple, legitimate user commands" to commit their crimes. Seventy-eight percent of the insiders were authorized users, and almost half used their own usernames and passwords in the attack.

In one case, an employee of a vendor of credit card point-of-sale terminals used social engineering to get authentication information that allowed him to add credit to his own credit card. In another case, a fired employee's access account remained open, allowing him to remotely sabotage the system. Fewer than a quarter of the insiders had a technical position such as a system administrator.

The report shows that many of these insiders were caught by persons not responsible for security, particularly customers; additionally, many were caught through nonautomated procedures (for example, customer complaints, manual account audits, and an inability to log in). Three-quarters of the culprits were identified using system logs.

So what can be done to stop insiders, whether technically sophisticated or not? The report concludes that "the detection and assessment...of insider incidents will continue to require manual diagnosis and analysis," as automated anomaly-detection tools tend to be expensive and reactive. @ Read the full *Insider Threat Study* at *Security Management Online*.

New in Plaintext

While the majority of the world's computers run some version of the Microsoft Windows operating system, there's another giant out there as well: the open-source operating system known as Linux. To the uninitiated, the thought of installing the Linux operating system is akin to--and at the same level of complexity as--putting a new engine into a perfectly good car.

While Linux has a reputation as being for only the most technically adept computer users, that's a perception that is going to change, thanks to a new book by Rickford Grant called *Linux for Non-Geeks*. Grant's book is described on the cover as a "hands-on, project-based, take-it-slow" approach to understanding, installing, and using Linux, and the book delivers on this promise, leading readers slowly and without jargon through the world of Linux. The book even comes with a free distribution of Linux known as Fedora that provides an easy-to-use graphical user interface that can compete with Windows. Users can have both Fedora and Windows running on the same machine.

So why bother to install Linux? Grant explains its benefits, including a range of free software that can do anything its Windows counterparts can do, from browsing the Web to creating word-processing documents and spreadsheets that are compatible with Office documents. It's fairly secure even without doing anything additional. And new software is easy to get online.

Linux is not perfect, as Grant points out, in part because some peripheral devices--video and sound cards, for example--still aren't Linux-compatible (though this situation is relatively rare). But if you're interested in an alternative to Windows, and you've been nervous that Linux isn't meant for you, this book may be just what you've been waiting for.

The book is available through online vendors such as Amazon.com for about $24. It comes with a working version of Linux on two CDs.

A Site to See

Worms, rootkits, Trojans. These attacks, along with the rest of their malware friends, represent tremendous risks to any network connected to the Internet. And as with any type of security threat, ignorance isn't an option. The good news is that the Internet Storm Center is out there keeping an eye on these threats in real time. Their graphs show what malware is hitting the 'net the hardest and which ports are being targeted each day, and the daily "Handler's Diary" describes what threats IT security pros from SANS are watching and remediating. The SANS Internet Storm Center is this month's Site to See. Get there via *SM Online*.

Violate HIPAA, Go to Jail

A Seattle man recently pled guilty in the first criminal conviction under the Health Insurance Portability and Accountability Act (HIPAA) that went into effect a year ago.

In the case, an employee of a Seattle cancer center, Richard W. Gibson, stole information about a cancer patient. Gibson used the patient's name, date of birth, and Social Security number--all identifiable health information as defined by HIPAA--to obtain four credit cards with which he spent more than $9,000.

According to the plea bargain entered into the United States District Court in Seattle, Gibson's offense violated HIPAA by meeting four conditions. Gibson "disclosed to another person individually identifiable health information." He made the disclosure knowingly, and for a purpose other than that permitted by the law. And he disclosed the information with the intent to use this information for personal gain.

Under the terms of the plea agreement, Gibson faces up to 10 years in prison (the prosecutors recommended 10 to 16 months) and a fine of up to $250,000. He also must pay restitution to the victim and repay the credit card companies.

Benjamin T. Butler, counsel with the Washington, D.C., law firm Crowell & Moring LLP's Health Care Group, says that he finds this case particularly interesting because it shows that prosecutors are eager to remind businesses that HIPAA has teeth. "It appears that this person could have been prosecuted under a number of other statutes," Butler says, but prosecutors chose HIPAA. They wanted "to send a message that this authority is out there, and people shouldn't forget about it."

The case had another interesting wrinkle, Butler says. "The information that was provided [by Gibson] was name and Social Security number, not what you would typically think of as the paradigm case under HIPAA, which would be disclosing somebody's diagnosis or something to that effect."

While the type of information disclosed by Gibson is covered under the statute, Butler points out that it could have been just as easily stolen if Gibson worked at a bank or insurance company. The fact that he worked for a hospital "just made it more aggravating because the [victim] was suffering from cancer and added to the deal for the prosecution."

Defining Moments

Test your knowledge of tech terms by guessing the following.

This acronym has been attributed to Gene Amdahl, who spent decades creating mainframes for IBM. The three-letter acronym refers to what companies would try to spread to discredit their competitors' products. It was intended to fuel concerns about potential flaws that could cause major problems. Hint: Bugs Bunny had trouble with a fellow with a similar name.

For answer, see below

Quick Bytes

- **PDA forensics guide.**
  PDAs are more popular than ever, with 2.75 million hand-held devices shipped in the second quarter of 2004 alone. Because criminals are among the loyal users of the devices, those who are tasked with performing forensic examinations of computers must also know how to get data off a PDA in a way that preserves evidence for a court case. A Special Publication of the National Institute of Standards and Technology (NIST) has been developed to help organizations create policies and procedures for dealing with PDA forensics. The document includes information on forensic tools and proper procedures. @ *Guidelines on PDA Forensics* is available through *SM Online*.
- **Shutting down spammers.**
  A U.K. group of Internet service providers (ISPs) has taken steps to stop spammers with a new "get tough" antispam policy. The 150 members of the London Internet Exchange (LINX)--which also includes major ISPs from Europe, the United States, and Asia--agreed to target and shut down the sites of "spammers who host their e-commerce Web sites with a reputable ISP while sending spam from another network," according to a release from the group. LINX is also calling on ISPs to shut down Web sites that sell spamming tools including CDs "containing millions of illegally collected e-mail addresses."
- **Michigan IT has the blues.**
  Michigan's Department of State runs several large IT systems to manage driver and vehicle information, and it collects nearly $2 billion annually in revenue from vehicle violations and fee collections. However, a recent audit of the IT infrastructure of the department by Michigan's Office of the Auditor General found that the "general controls over security, access, program and data changes, segregation of duties, and service continuity that support mainframe information systems were not effective." As a result, the report concluded that there was "significant risk" that unauthorized access to the systems could compromise the data on these systems. @ The *Performance Audit of the Automated Information Systems* is at *SM Online*.

Defining Moments Answer: FUD (fear, uncertainty, doubt)

Back to SM Online

Magazine Highlights| Marketplace | Library/Links | Events | Beyond Print| Today's News | Forums | Feedback|Subscribe | Advertise | Reader Service | Writer's Guidelines | Contact Us | Security Industry Buyers Guide|ASIS Online