

Security problems keep

By Bob Felton

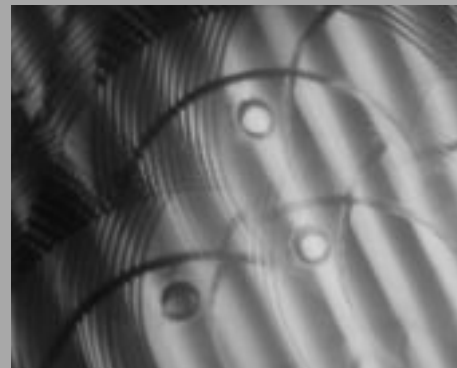
**E-manufacturing
raises the stakes,
makes security
everybody's job.**

"The agency," cryptology historian David Kahn wrote of the National Security Agency in 1967, "may well keep a team examining cryptograms in a given system for two or three years, even though it has had no success, in the hope that one of the cipher clerks may someday blunder and open the way to a solution. For in modern systems, properly used and with frequent key changes, a cryptographer's error is the cryptanalyst's only hope."

Kahn's observation that errors are the cracks attackers exploit to jimmy their way into secret communications is as true today as it was 35 years ago, and some hackers are as tenacious and ingenious as the Bletchley Park eccentrics that wouldn't quit till they'd whipped the Nazi enigma machine. Presently, thanks to instantaneous global communications among millions of desktops via the Internet, representing every possible gradation of user and administrator know-how and conscientiousness, pickings are pretty good for e-thieves.

Today, as enterprisewide networks reach the plant floor and zip data to the far side of the world in a twinkling, and as the number of computers, personal digital assistants, telephones, and pagers communicating with the network increases, there is a corresponding increase in the opportunities for a critical blunder that would allow an attacker to enter your system.

increasing



Science and art

If a computer were given the job of decrypting the monoalphabetic substitution cipher puzzles found in many daily newspapers, and if that computer generated and tested 100 million 26-character solution alphabets per second, it would need about 2.5 trillion years to solve just one puzzle using brute force.

Encrypting a message in such a fashion might prevent another computer from reading your e-mail or your kid from reading your Christmas shopping list, but an amateur cryptanalyst with a pencil and a sheet of paper will read your message in just a few minutes. Security isn't only a science, a matter of developing an impenetrable cipher; it's also an art, and judgment shapes the playing field as much as the niceties of algorithm and key length.

Are you most likely to be attacked from within—betrayed by an employee—or without? Does an attacker have to be locked out for a day, a year, or forever? What resources does the attacker have? It's one thing to foil a vengeful ex-employee possessing only modest computer skills but quite another to hold the National Security Agency at bay. What's the real value of the material you want to protect? How much can you afford to spend before the Law of Diminishing Returns takes over?

Recognizing there's no such thing as perfection, security expert Bruce Schneier (www.counterpane.com) argued that "the historical model of threat avoidance is flawed, and it should be abandoned in favor of a more businesslike risk management model. Traditional security products, largely preventive in nature, embody the threat avoidance paradigm: Either they successfully repel attackers, or they fail. The unfortunate reality is that every security product ever sold has, on occasion, failed.

"A security solution based on risk management encompasses several strategies," he continued. "First, some risk is accepted as a cost of doing business. Second, some risk is reduced through technical and/or procedural means. And third, some risk is transferred through contracts or insurance."

More toys, more danger

Personal digital assistants (PDAs), those handy little electronic organizers, are showing up everywhere, from students' backpacks to the coat pockets of with-it spies.

Robert Hanssen, according to the Federal Bureau of Investigation (FBI) complaint presented at his arraignment, used one to help him carry more than 6,000 pages of documents out of FBI headquarters for delivery to his Russian handlers. At one point, irritated with trudging through muddy woods to deliver material to a dead drop, he asked his contacts to buy him a PDA with wireless capability so he could beam the files to them. They declined, and soon afterward the FBI apprehended Hanssen after he hid documents in a Virginia park for later retrieval by the Russians. In the spy business—as everywhere else, evidently—the value of some perks depends on which side of the transaction you're on.

"Something big is happening," the Motorola Web site proclaims. "Houses are talking to computers. Magazines are talking to wireless phones. Cars are talking to the Internet. It's already begun. . . . We are entering the era in which things don't just think but share what they know with each other."

Indeed we are, and whether all that extra chatter is a good thing remains to be decided. Telephone cloning has been a big and growing problem for years, and there are now viruses designed to specifically attack Web-enabled telephones. It won't be long before PDAs and two-way pagers come under similar attack.

Every remote device represents yet another potential security breach, and attackers don't have to be especially sophisticated. A Federal Reserve governor inadvertently left his PDA in a taxicab a few months ago, and in the hands of the wrong person that's a first-class ticket to ride; fortunately, as far as anyone knows, it was returned to its rightful owner without incident. And that's the rub: Misfits United might boast about successfully defacing a Web site, but somebody who's figured out how to divert a penny of every credit-card transaction to an off-shore bank will probably keep mum. Not hearing about problems doesn't mean you haven't any; it might mean your security is truly awful.

The consequences could be ruinous. According to a recent survey by the Computer Security Institute, the cumulative loss of 186 companies that quantified their losses in 2000 reached \$378 million, or about \$2 million each. Roughly \$151 million of that loss was theft of proprietary information—information your competitors want.

One of the best places for plant engineers to learn about network security, besides brown bagging with a peer in information technology (IT), is at the Computer Security Resource Center, a Web site (csrc.nist.gov) established by the National Institute of Standards and Technology (NIST). There you'll find primers that explain security issues and technologies, news about current problems and security initiatives, and downloadable copies of the standards that govern electronic communication with Uncle Sam.

One of the most useful items at the site is the March 2001 draft of the "Self-Assessment Guide for Information Technology Systems," a comprehensive questionnaire that assesses data security from every possible perspective, from cooling fans at the chip to physical security and labeling of backup disks. Originally developed for the use of U.S. government IT personnel, the questions

can teach plant engineers a lot about security and the problems confronting network managers:

- Does building plumbing endanger the system?
- Have you performed a consequence assessment that estimates the degree of harm or loss that could occur?
- Do your emergency exit and reentry procedures ensure that only authorized personnel reenter after fire drills, etc.?
- Do you sanitize media before reuse?
- Do you share incident information and common vulnerabilities with interconnected systems?
- Do you maintain a current list of authorized users and their access?
- Do your security controls detect unauthorized access attempts?

The draft is available at csrc.nist.gov/publications/drafts.html. Careful reading and consideration of the questions make it clear that the electronic ganglia tying together the extremities of the modern manufacturing plant are susceptible to attack across many fronts and that security is everyone's business. More than ever, it's vital that plant engineers work effectively with IT to identify potential breaches, shore them up, and train everybody to be security conscious.

Nor is it only NIST that's getting into the act. The National Infrastructure Protection Center (www.nipcc.gov) was created by Congress to defend the nation's computer networks by serving as the national focal point for gathering information on threats to critical infrastructures. It is the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. The center issues updates about new viruses, Internet frauds, and disruption attempts almost daily. It is located in the FBI's Washington headquarters and maintains its own investigative staff.

Cybersecurity isn't an exclusively local matter, however: A complaint filed by the U.S. Attorney for the Southern District of New York provides an instructive example of the reach of today's e-thieves. The complaint alleged that Oleg Zezov and Igor Yarimaka, residents of Kazakhstan, penetrated the computers of Bloomberg.com, in New York, and demanded \$200,000 from the company to tell how they had done it. Bloomberg agreed to pay but only following a face-to-face meeting in London. There, accompanied by undercover London police officers, Bloomberg met with Zezov and Yarimaka. They repeated their demands, and police arrested them the next day. The U.S. is now seeking their extradition. ■