



Under ATTACK

by JANE M. SANDERS

Information security battle will require computer users to make tough choices.

Whenever a new virus begins flooding the world's computer networks, individual users rush to download the latest anti-virus updates while network administrators hastily apply the latest patches to vulnerable equipment – then work overtime to repair the inevitable damage and limit the financial costs.

There must be a better way.

Researchers at the Georgia Institute of Technology say solving the world's growing information security problems will demand tough choices involving tradeoffs in cost, convenience and computing performance.

For instance, computer users will have to put a priority on security and be prepared to pay for it. They may have to retain well-tested software rather than install the newest version rushed to market. And they'll have to bear the costs of rebuilding worldwide networks on secure foundations.

"Computers are being used more extensively, more widely and in more critical applications. They are a part of our lives today. They will be even more a part of our lives in the future," says Ralph Merkle,

director of the Georgia Tech Information Security Center (GTISC). "And for the past couple of decades we have put up with buggy code, unreliable computers, insecure computers, and computers that are vulnerable to viruses, worms, spam and other problems. All of this has to change. We need to have reliable computers, systems and networks that we can trust."

From individual users to network administrators to senior government and industry officials, interest in information security is capturing people's attention. GTISC researchers and others are now hopeful that consumer demand will boost efforts to solve myriad issues in the field.

"Information security is not just a technological problem," says Professor of Computing Mustaque Ahamad, the GTISC co-director of technology. "There's a lot more to it. It's a complex problem, and its solutions will require new technology, policy, awareness and education. We're looking at the whole problem."

Though the task is daunting, the world's information security problems can be solved, Merkle confidently predicts. Because these issues have been resolved in special applications, such as aircraft navigation and national defense, researchers know it can be done for computer systems everywhere. Merkle concedes, however, that producing such secure software will be costly in dollars, time and, perhaps, convenience, as well.

Costs in dollars and time will mount as programmers rewrite a lot of computer code, as researchers build new systems with security as a basic component, and then as individuals and

organizations have to update or replace insecure systems, Merkle explains.

"It will take fundamental changes in how we deal with computer software development, which will require fundamental changes in our use of secure systems," Merkle says. "We will have to rethink a lot of the basic approaches that have been used."

Computer users may also have to trade some convenience for security.

"The ideal information security system is transparent to the user, but that's extremely difficult to design," says Georgia Tech Research Institute (GTRI) researcher Jim Cannady, the GTISC co-director of applied research. "Users don't like having to keep up with things like 'smart cards' (used by the U.S. Department of Defense and other organizations for electronic identification). It's better to make a system as secure as possible before you turn it on."

While GTISC and other researchers address the complexity of this design challenge, beleaguered computer users are beginning to favor security and reliability over features and pricing, Merkle says.

"In general, commercially available products face very real marketing and pricing pressures that force companies to write code that is not always perfectly secure," Merkle says. "Customers have voted in favor of this because if you write code with lots of features and it's done quickly, they will buy it even though it's hard to make it reliable. Now the message is changing. Customers would rather have computers that work reliably, and companies are taking that message to heart."

This marketplace change in the understanding of what information security really means may go a long way toward solving the crisis, Cannady says.

"What is the true cost of information security?" he asks. "We may have to sacrifice flexibility, speed and performance to make systems more secure. When people go to Best Buy and want security more than they want a large monitor, things may change."

Another solution may lie in users' willingness to forsake the latest software updates and computer platforms for those that are tested and proven reliable, Cannady adds.

"In the 1980s, NASA wrote the software for the space shuttle, tested it and made it the best they could," he explains. "They continued to fix the bugs in the same software on the same computing platforms. The Hubble space telescope, for exam-

ple, first ran on a 386 processor, and now it operates on a 486. It doesn't have to have the latest Pentium processor. It works. It's been tested so many times. It meets the objective, and it's very reliable and secure. If every year, you upgrade to the next operating system, there will be new problems and vulnerabilities.

"So we must come to a general consensus that information security is important and recognize the costs, or keep the same software and computers that have all the bugs worked out," Cannady summarizes.

As the marketplace debate continues on the tradeoffs between retrofitting old, insecure computer systems versus efforts to design new systems with security built in from the ground up, there will be incremental increases in information security, Merkle predicts.

Some of those incremental increases will result from startup companies' information security products, such as those for spam e-mail management. Others will stem from research at GTISC and elsewhere, Merkle adds.

As they move toward solutions, GTISC researchers are considering how new information security systems would be deployed. Commercially available security solutions must offer good quality and be economical and easy to use, Merkle notes. Policy issues must also be addressed as new threats and technologies emerge.

Merkle believes GTISC researchers will make significant contributions to solving the range of information security problems because of their level of expertise and the cross-disciplinary approach they are taking.

But the pressure is on these researchers and others to deliver solutions.

"We have to make the transition from a world where most computers cannot be trusted with high confidence to a world where we can trust them," Merkle says. "This transition is happening now in large measure because people are finding it very expensive as a society to have unreliable computer systems. We're discovering by experience – the most expensive, but perhaps the most effective teacher – that insecure computers cost time, money and, in some cases, lives." **RH**

■ Contact Ralph Merkle, 404-385-4272 or merkle@cc.gatech.edu.



PHOTO BY GARY MEEK

The world's information security problems can be solved, GTISC director Ralph Merkle confidently predicts, because these issues have been resolved in special applications, such as aircraft navigation and national defense.

"We have to make the transition from a world where most computers cannot be trusted with high confidence to a world where we can trust them."



GTISC Research HIGHLIGHTS

Researchers explore potential solutions to information security problems.

Research at the Georgia Tech Information Security Center (GTISC) is divided into three areas – basic, applied and policy research. Researchers develop and test systems, devices, strategies, policies, practical concepts and techniques. Faculty members in the colleges of Computing and Management, Georgia Tech Research Institute (GTRI), and the School of Electrical and Computer Engineering and School of International Affairs conduct research that covers a gamut of information security issues, including database security, secure networks, cryptography, intrusion detection, quality of information, and policies on unsolicited e-mail, privacy, passive and active defense, and international cooperation to deal with cyber crime and terrorism.

Here are some highlights of GTISC research:



PHOTO BY NICOLE CAPPELLO

Professor of Computing Richard Lipton, right, and Assistant Professor of Computing Wenke Lee realized that most spam e-mail contains a URL or Web address for a Web site for potential customers to visit. So, they have created a filter application based on looking for unwanted URL addresses in e-mails.



Misinformation – the “pushed misinformation” that spam e-mail represents and the “pulled” misinformation from Web searches that yield irrelevant or offensive material is an increasing problem.

“Both techniques for obtaining information can be manipulated with the motive of disrupting service or for profit. So you get information that is poor quality,” explains Professor of Computing Mustaque Ahamad, GTISC co-director of technology. He and Professor of Computing Calton Pu are leading research to understand what sort of attacks can be mounted to degrade the quality of information (QoI) and how researchers can design defenses against those attacks.

Now in the second year of a five-year project funded by the National Science Foundation (NSF), the researchers are building a prototype system that is smart enough to determine which e-mail messages should be tagged as spam and which are useful messages. The interface is similar to currently available spam filters, but the underlying principles are very different, Ahamad says. The prototype also will deliver a trust rating –

similar to the currently available relevance ratings — when Internet surfers submit a search engine query.

Professor of Computing Richard Lipton and Assistant Professor of Computing Wenke Lee are working on a different set of techniques to address spam e-mail. Lee and Lipton realized that most spam e-mail contains a URL or Web address for a Web site for potential customers to visit. So, they have created a filter application based on looking for unwanted URL addresses in e-mails.

“This approach and application is elegant and incredibly computer cheap and fast,” Lipton says. “It seems to work better than the existing commercial products, and the end user can customize it easily.” For more information, see www.gatech.edu/news-room/release.php?id=146.

Ahamad adds: “Spam is a huge problem, and there is no one solution that would take care of it all. We’re working on a variety of different techniques. If we’re going to use e-mail as a medium of communication, clearly we have to find ways to counter the information degradation attacks that spam represents.”



How to store private information securely, while making it easily accessible to authorized users when they need it, is the focus of another NSF-funded research project led by Ahamad.

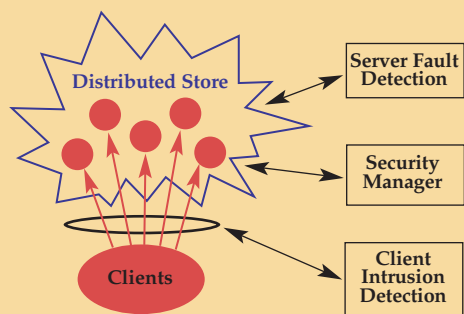
He and colleagues Wenke Lee and H. Venkateswaran in the College of Computing and Doug Blough in the School of Electrical and Computer Engineering are approaching this problem within the context of the Aware Home, an information-aware, sensing- and computing-rich residential laboratory on the Georgia Tech campus. The laboratory is a prototype of future homes.

Researchers have dubbed their new prototype system the Agile Store. In this context, agility means dealing with problems as they arise, rather than making constant demands on computing performance to deal with hacking. Agile systems can detect and then adapt to deal with attacks.

"The Agile Store uses distributed multiple components in case some fail. So its design includes a lot of redundancy," Ahamad explains.

"The Agile Store uses protocols to adapt to change requirements or conditions. When it goes into a defense mode, it may perhaps temporarily degrade performance to deal with the attack."

Ultimately, the researchers will build a system where users can store information and get to it when they need it. "Those who are not authorized will not be able to get the information, even if some of the machines where the information is stored are compromised," Ahamad adds. The Agile Store's protocols don't rely on any one computer for correct operation of the system. Duties are shared and duplicated across a network of computers, such as those that operate in the Aware Home or a much larger network.



GRAPHIC COURTESY OF DOUG BLOUGH

Agile Store is the name of a prototype system that stores private information securely, while making it easily accessible to authorized users when they need it.



PHOTO BY NICOLE CARPELLO

Professor of Computing Mustaque Ahamad is co-director of technology for the Georgia Tech Information Security Center.



A team of researchers led by Professor John Copeland in the School of Electrical and Computer Engineering is developing techniques for tracing information security attackers through the Internet.

Although data packets sent via the Internet carry identification numbers, these IDs can be easily spoofed, Copeland says. His team is studying how data routers can add postmarks that would enable people to determine where electronic attacks are originating — a technique called "statistical packet postmarking."

Using this technique, Internet backbone routers would randomly add a postmark (12 bytes of data to about 2 percent of data packets). Trace-back could be performed even in the case of intentional spoofing because a new postmark will overwrite a previous one. This will keep packet length from building up, but also allow for the determination of actual routes when an adequate number of packets have been received.

"For example, someone could fake a return address on a piece of mail, but its postmark would remain valid," Copeland adds.



PHOTO BY STANLEY LEAR

Seymour Goodman is the GTISC co-director of policy and a professor of computing and international affairs.

“As we move faster, we’re doing the best we can, but the law is still not keeping up with the malicious use of technology....”



Many information security issues include policy components, and researchers led by Seymour Goodman, GTISC co-director of policy and professor of computing and international affairs, are actively examining those and other aspects of the problems.

Goodman’s research – conducted under the auspices of the International Telecommunications Union and the National Academies of Science and Engineering — focuses on policies to address cyberterrorism and cyber crime. These are international legal problems that don’t recognize legal boundaries.

“Mapping malicious behavior where the bad guys think in a borderless way is really hard to do,” Goodman says. “In a physical space, there are clear walls of jurisdiction.”

Cyber crime is also borderless to an extent in the United States as it crosses state boundaries, Goodman explains. “Somebody in one state can commit a crime in another state (via the Internet),” he says. “How to deal with this is not clear. Do you extradite the suspect to the state where the cyber crime victim is located? The law is a strong form of policy, but many issues are not worked out yet.

“Technology is changing faster than the law,” Goodman adds. “In many ways, this is a good thing. But there are dangers in not thinking far enough ahead about how technology can be misused. As we move faster, we’re doing the best we can, but the law is still not keeping up with the malicious use of technology.... This will be a real struggle for some time to come.”

Also under the GTISC umbrella, Goodman and his colleagues, along with the White House Office of Science and Technology Policy, co-hosted a March 2003 meeting of the President’s National Security Telecommunications Advisory Committee (NSTAC). John Marburger, the President’s science advisor, and Duane Ackerman, CEO of BellSouth and vice chairman of NSTAC, were keynote speakers and participants.

More than 150 prominent researchers and practitioners from the telecommunications industry, government and academia discussed the trustworthiness of national security and emergency preparedness telecommunications systems. Specifically, they examined trustworthiness related to cyber security and software, human factors, physical security and integration of innovative research and development to build trusted tools and systems. The proceedings of the meeting are available at www.ncs.gov/NSTAC/r&d2003.htm.

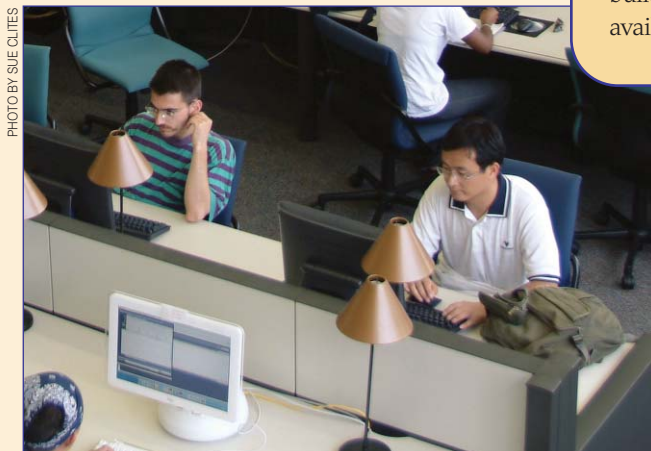


PHOTO BY SUE CLUTES

Computers are used extensively in daily life, despite their vulnerability to viruses and other attacks. GTISC researchers are working to make computers more reliable.



In the Georgia Tech Research Institute, researchers are contributing to the GTISC effort with five major programs. In the Signature Technology Laboratory, the Secure Information Systems Division has two major research and development efforts stressing enterprise-level computer security.

Program manager William Borland leads researchers investigating innovative applications of commercial software tools to instill systematic defense in depth. Database expert Rob Zimmer contributes by hardening his Oracle databases, designing specialized functions for enhanced server security. Working with software architect Ben Lowers, Zimmer weaves an intricate web of layered security design, assembling strong assurances against information leaks and inappropriate access.

“Whenever security is just an after-thought, it has no hope of being robust enough to withstand attack,” Borland says. “With an emphasis on rigorous assurance managed on the server side, these systems present users with a Web-browser experience that feels familiar and comfortable.”

A GTRI project led by Senior Research Scientist John Wandelt assists law enforcement agencies in sharing criminal intelligence information regarding the illegal drug trade in border states of the southwestern United States.

“Now we have an extremely secure network infrastructure to support law enforcement agencies in sharing criminal intelligence and communicating seamlessly,” says GTRI researcher Jim Cannady, the GTISC co-director of applied research. “They don’t have to pick up the phone. We’ve integrated the whole system. Officials can now share information in real time. This effort has been especially successful in light of the emphasis on homeland security.”

In a third effort, GTRI researchers led by Senior Research Scientist George Thurmond and faculty members in the School of Electrical and Computer Engineering are collaborating to help the U.S. Department of Defense identify objective measures of information security. Researchers are quantifying and establishing metrics to define the necessary level of information security.

“In the past, to achieve security requirements, officials used a lot of ad hoc methods,” Cannady says. “They would tape up the system with two or three methods and then go home — based on the available tools and the level of the personnel’s expertise.” This multi-level, long-term research effort is evaluating the military’s information security systems and how they are used. They are testing these systems in large-scale military exercises.

Finally, Cannady leads a consortium of industry groups and universities in an information security study for the U.S. Army Research Lab. He describes it as basic research aimed at developing ways to identify attacks against mobile ad hoc networks (MANET), a collection of wirelessly connected information systems — which, for the Army, operate in a battlefield environment including moving vehicles such as Humvees and aircraft.

“If the network is attacked, how do you know? And what type of attack is it?” Cannady’s team is asking in this study — now in its third of eight years. Since 1995, GTRI researchers have worked to develop methods of network intrusion detection, and researchers at GTRI and elsewhere still haven’t completely solved this problem. “Now, we have new problems because of wireless networks. We need new solutions, such as artificial intelligence techniques,” Cannady says. **RH**



IMAGE COURTESY OF DEA

The U.S. Drug Enforcement Agency confiscated these cocaine bricks from drug trade suspects. GTRI researchers are assisting law enforcement agencies in sharing criminal intelligence information regarding the illegal drug trade in border states of the southwestern United States.



U.S. ARMY PHOTO BY SFC DANIEL ENNST

U.S. Army soldiers wait in the rain by their Humvees as their fellow soldiers search for automatic weapons in a Kosovo town in 1999. GTRI researchers are developing ways to identify electronic attacks against mobile ad hoc networks (MANET), a collection of wirelessly connected information systems — which, for the Army, operate in a battlefield environment including moving vehicles such as Humvees and aircraft.

■ Contact Mustaque Ahamad, 404-894-2593 or mustaq@cc.gatech.edu; Seymour Goodman, 404-385-1461 or goodman@cc.gatech.edu; or Jim Cannady, 404-894-9730 or james.cannady@gtri.gatech.edu.

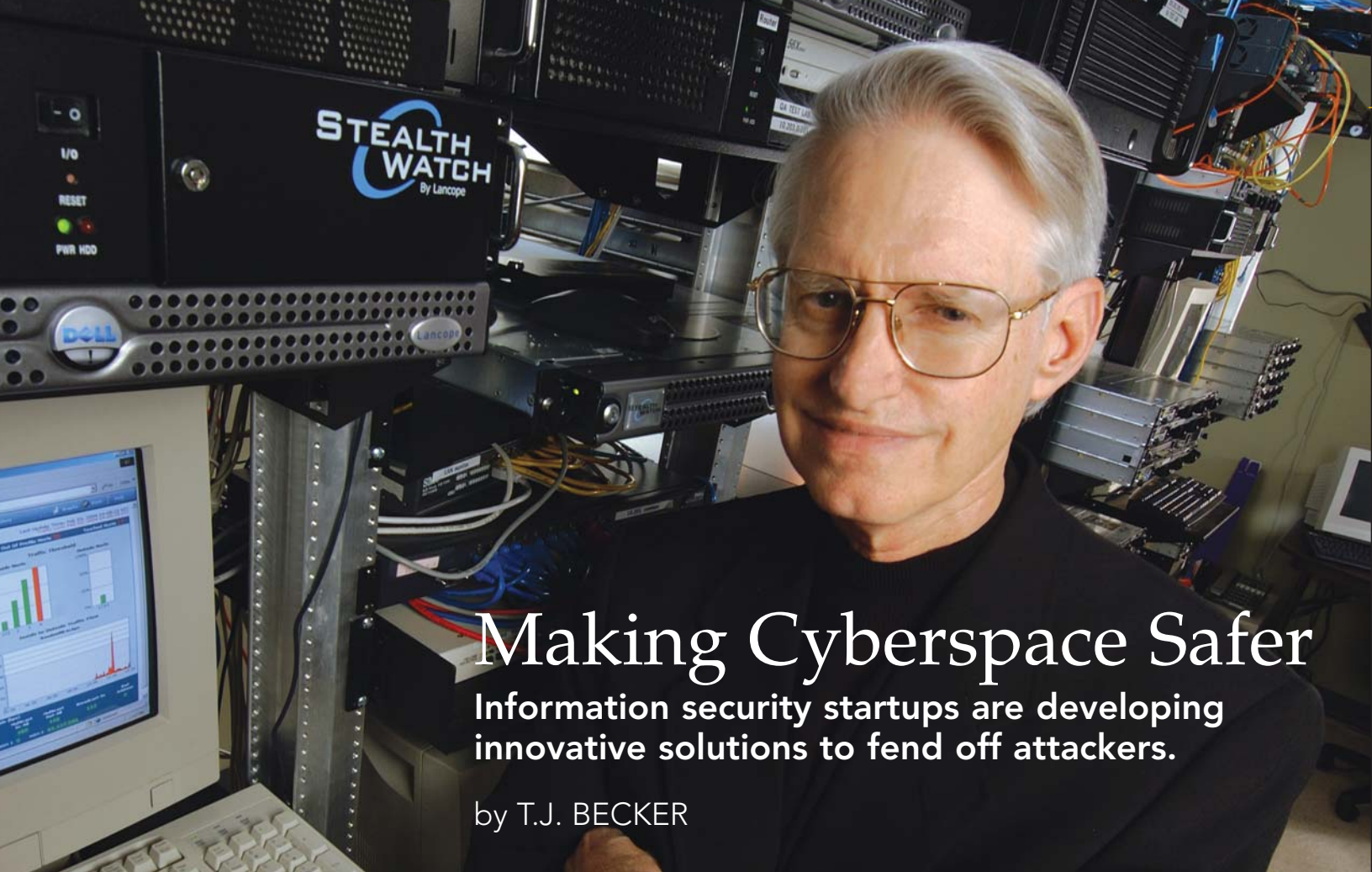


PHOTO BY GARY MEEK

Making Cyberspace Safer

Information security startups are developing innovative solutions to fend off attackers.

by T.J. BECKER

Above: Professor John Copeland is co-founder of Lancope, whose flagship product, StealthWatch™, uses an innovative behavior-based architecture to monitor network traffic and detect suspicious activity.

Atlanta has become a hub for information security companies, and a recent surge of entrepreneurial activity is expanding this market.

The growth is influenced partly by companies such as Internet Security Systems (ISS) Inc. Founded in 1994 by former Georgia Institute of Technology student Christopher Klaus, ISS has already become an industry leader, generating revenue of more than \$243 million in 2002 and sparking several offshoots.

The new wave of information security players is also a response to a growing problem: Hackers have become more sophisticated at wreaking havoc via the Internet. Here are some highlights of how emerging companies affiliated with Georgia Tech's technology incubator, the Advanced Technology Development Center (ATDC), are making cyberspace safer.

Identifying unknown assailants

"A few years ago, you might see someone scan your connection two or three times a day to see if you have the right patches," says John Copeland, co-founder of Lancope. "Today it happens every five to six minutes."

A professor in Georgia Tech's School of Electrical and Computer Engineering and director of its Communications Systems Center, Copeland began working on information security solutions after finding bursts of data on his home computer that he recognized as the work of hackers.

Incorporated in 2000, Lancope introduced its flagship product, StealthWatch™, in May 2001. StealthWatch uses an innovative behavior-based architecture to monitor network traffic and detect suspicious activity. Unlike signature-based and protocol-anomaly products, it can identify unknown assailants.

Because StealthWatch doesn't need to look inside individual data packages, it operates at gigaspeeds – up to six times faster than other intrusion detection system (IDS) solutions. It also quickly traces the source of attacks, which is crucial in responding to hackers.

"That's become even more important as we've seen worms spread around the world in hours or even minutes before there was time to detect and distribute the signature," Copeland observes.

Last summer, Lancope graduated from ATDC, and the company now has more than 50 employees. Another milestone is Lancope's new product

release: StealthWatch+Therminator, which includes government-licensed visualization technology that graphically highlights unusual network behavior.

Detecting vulnerabilities faster

Recently admitted to ATDC, Intrusec enables companies to continuously monitor their networks for changes to determine if they may be susceptible to an attack.

In contrast, traditional vulnerability-assessment tools require so much bandwidth that they're used on a weekly or monthly basis — which may be too late.

"Hackers are constantly scanning your network and the Internet with automated tools, which can give them an upper hand," says Marc Winn, Intrusec's CEO. "We take that advantage away by detecting holes before they can be exploited. The idea is to shut the door before anyone can get in."

Launched in 2002 by ISS alumnus David Meltzer, Intrusec introduced Exposé, a network change-detection system, in July 2003. Because Exposé works at the network level, it's easier to install and more flexible than host-based solutions that must be installed on every computer.

Exposé complements existing vulnerability-assessment and patch-management solutions by enabling them to function as real-time tools. It also provides information to reduce false alarms that can occur with IDS solutions. "The problem with audit-based tools is that they typically aren't there at the right time," Winn says. "And with reactive solutions, you can't possibly stop everything — and you may be stopping something that looks like an attack but is legitimate network traffic."

Solving the password problem

WiKID Systems, another ATDC member, is making authentication easier, safer and less expensive. Traditional passwords are expensive — and don't necessarily provide adequate protection. Because of the number of passwords they must remember, people choose weak ones and use the same codes on multiple accounts. When companies try to enforce stronger passwords, people typically forget them and call the help desk. "It costs \$15 to \$30 to reset a password, and with people forgetting several times a year, those costs add up quickly," says Nick Owen, WiKID's founder and CEO.

WiKID's patent-pending system helps remote users access their corporate networks safely with two-factor authentication: a personal identification number (PIN) and a wireless device with public-key cryptography (also known as asymmetric encryption). People only need to remember their

PIN. Using asymmetric encryption, the PIN is transmitted via a wireless device, such as an RIM Blackberry or Java-enabled phone, and WiKID's authentication server then sends a one-time pass code to remote users.

Hackers can't access WiKID's PINs because they aren't stored on users' computers. WiKID's technology is also cheaper and more convenient than existing solutions. Smart cards and biometrics are expensive and difficult to deploy because they require readers. Hard tokens, another alternative to passwords, are cumbersome and frequently lost.

Launched in October 2001, WiKID is concluding beta testing and plans to introduce a commercial product early in 2004. "Granted, we're a point solution, but it's a huge market," Owen says, noting that recent federal legislation has put more pressure on companies to increase information security.

What's more, economic demands require companies to integrate with suppliers and vendors for just-in-time initiatives. "That stretches out your security-supply chain," Owen observes. "If you're passing customer records to a vendor, you need to make sure that vendor's system is secure — and we make that very easy."

Fighting internal threats

Taking a different tack on information security, Oversight Technologies focuses on what's going on inside an organization.

Oversight continuously monitors a company's financial transactions, looking for insider misuse and fraud — from simple invoice errors to deliberate crimes, such as an employee writing checks to a fake vendor account. The idea is to reduce loss and increase operational efficiencies.

"People tend to have more risk than they recognize," says Patrick Taylor, Oversight's CEO and another ISS veteran.

The company's patented software combines cutting-edge analytic technologies and audit techniques to monitor business transactions in real-time. An automated detective of sorts, the software searches for clues or events that appear to be suspicious and then digs deeper to determine the reason behind irregularities.

Admitted into ATDC last year, Oversight expects to begin initial deliveries early in 2004.

"We bring a new dimension to the market," Taylor says. "Most information security companies are focusing on network activity or server access, intent on keeping out unauthorized users. We want to see what legitimate users are doing." **RH**

■ Contact Tony Antoniadis, ATDC, 404-894-5999 or tonya@atdc.org.

"Hackers are constantly scanning your network and the Internet with automated tools, which can give them an upper hand."

Intrusec technology enables companies to continuously monitor their networks for changes to determine if they may be susceptible to an attack, says Marc Winn, the company's CEO.

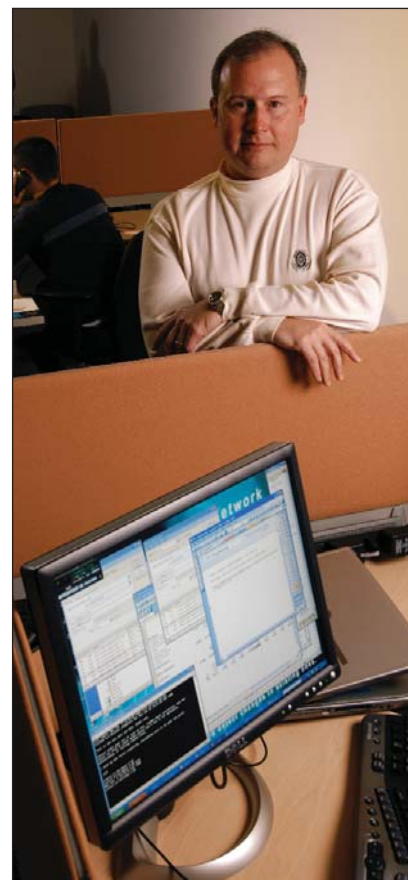


PHOTO BY GARY MEEK