Research Horizons
Winter 2004

Cover Story

Making Cyberspace SAFER

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

by T.J. BECKER

PDF format

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.

photo by Gary Meek

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. (300-dpi JPEG version - 726k)

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 giga-speeds – 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.

photo by Gary Meek

"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."

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. (300-dpi JPEG version - 684k)

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, 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. "Right now 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."

For more information, contact Tony Antoniades, ATDC, 404-894-5999 or tonya@atdc.org.

Contents Research Horizons GT Research News GTRI Georgia Tech

Send questions and comments regarding these pages to webadmin@edi.gatech.edu

Last updated: March 31, 2004