msn
MSNBC News

MSNBC HOME

Technology & Science
HACKS, VIRUSES & SCAMS

News
Business
Sports
Tech • Science
Living
Travel
Health
TV News
Opinions
Weather • Local
Shop@MSNBC
MSN.com

Profiling the hackers

Software aims to nab computer intruders in real time

"Hackers are a step ahead of you always," says chief researcher Shambhu Upadhyaya, sitting in one of the computer labs at SUNY Buffalo.

David Duprey / AP

ASSOCIATED PRESS

BUFFALO, N.Y., Jan. 20 — A suspected crooked insider at a New York software company sells consumer-credit reports to identity thieves, at roughly $30 a pop, in a high-tech scam that prosecutors say victimizes thousands. An unemployed British computer administrator fights extradition to face federal charges in Virginia and New Jersey that he hacked into 92 separate U.S. military and government networks, often getting past easy-to-guess passwords to download sensitive data. These and other recent data intrusions, whose authors are typically intent on theft, sabotage or cyberterrorism, have given rise to a promising profiling strategy aimed at preventing online break-ins as they happen.

E-MAIL THIS
COMPLETE STORY

I'M FREE!
GET A FREE NOKIA 1260
Exclusively with new service from attwireless.com
*with select plans and recurring billing online.
AT&T Wireless

'The ultimate goal is to detect intrusions or violations occurring on the fly. There are systems that try to do this in real time but the problem is it results in too many false alarms.'
— **SHAMBHU UPADHYAYA**
computer science professor, SUNY Buffalo

JUST AS AUTHORITIES USE profiling to guard against criminals at ports and borders, researchers at the State University of New York at Buffalo are developing software that can generate highly personalized profiles of network users by analyzing the sequences of commands entered at each computer terminal.

The system — a prototype is likely to be ready for intensive testing this summer — could provide a high-grade layer of protection for military installations and government agencies as well as banking or other commercial networks that require especially tight monitoring.

The software draws up regularly updated profiles by closely tracking over time how each person performs an array of routine tasks, such as opening files, sending e-mail or searching archives.

Designed to tell if someone has strayed into an unauthorized zone or is masquerading as an employee using a stolen password, the program keeps watch for even subtle deviations in behavior.

Alerted to anomalies, network administrators then begin monitoring more aggressively to assess whether pilferage is in progress.

"The ultimate goal is to detect intrusions or violations occurring on the fly," said chief researcher Shambhu Upadhyaya, a SUNY Buffalo computer science professor. "There are systems that try to do this in real time but the problem is it results in too many false alarms."

Keeping false alarms to a manageable minimum is

AT&T Wireless
GET A FREE NOKIA 1260
WITH PLANS STARTING AT $19.99
with select plans and recurring billing online

key, but extremely difficult to achieve, said Bruce Schneier, a network security and cryptography expert and author of “Secrets & Lies, Digital Security in a Networked World.”

“These systems live and die on false alarms,” said Schneier. “You see this problem in facial recognition, trying to catch terrorists by recognizing faces in airports. All those trials failed miserably.”

The Buffalo school is one of 36 research and teaching centers designated by the National Security Agency since 1998 to help safeguard America’s information technology systems.

Aided by doctoral student Ramkumar Chinchani and Kevin Kwiat of the Air Force Research Laboratory in Rome, N.Y., Upadhyaya began examining in 1999 whether monitoring simple user commands instead of network traffic might produce faster, more effective monitoring.

Some computer-security products that feature user-profiling seek out deviations on the basis of huge amounts of data flowing through entire networks. They’re typically 60 percent to 80 percent reliable, whereas simulation tests indicated the new software would be up to 94 percent reliable, Upadhyaya said.

Hacks, Viruses & Scams

- Identity-theft complaints double
- British virus writer gets 2 years
- Norway appeals in DVD code case
- Legendary hacker to get unleashed

The software borrows from risk-analysis economic models. And even if it proves successful, the software would be just one tool of the many needed to defend computer security, Upadhyaya said.

“Hackers are a step ahead of you always,” he explained, noting that the military “is especially worried about the insider who’s been there a long time and learned all the loopholes.”

Mike Kurdziel, an information security specialist at Harris Corp., which makes tactical military radios, thinks Upadhyaya has come up with a solid way to curtail false alarms.

“Other intrusion techniques require something like looking at audit logs after the damage has already occurred,” Kurdziel said. “The advantages offered by this approach is an intruder with malicious intent can be identified very early and a system operator can contain the damage, repair it in real time and shut out the intruder.

“This really is an advance,” he said. “This means that systems that have been attacked by an intruder maliciously might not necessarily be brought down.”

TECHNOLOGY & SCIENCE TOP STORIES

STORY Identity-theft complaints double
STORY Satellite videophones go to war
STORY Another delay for Lara Croft game
STORY Microsoft seeks EU antitrust deal
STORY ISP ordered to identify Kazaa user
HOME MSNBC Cover Page

MSNBC READERS' TOP 10

Would you recommend this story to other readers?
not at all 1 - 2 - 3 - 4 - 5 - 6 - 7 highly

● BACK TO TOP

Cover | News | Business | Sports | Local News | Health | Technology & Science | Living | Travel
TV News | Opinions | Weather | Comics

InfoCenter | Newsletters | Search | Help | News Tools | Jobs | Write Us | Terms & Conditions | Privacy