NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Winter 2004 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Cyber Cops in Training

It's called electronic crime, or e-crime. The weapon can be a computer, the scene of the investigation can be a hard drive, and the perpetrators and victims can be thousands of miles apart. It can involve identity theft, financial misappropriation, privacy invasion, child pornography, or intellectual property theft. It can render law enforcement agencies helpless.

Since the information technology revolution began, law enforcement has faced the growing problem of cybercrime. But a lack of resources and trained personnel has put many agencies behind the curve. Along with trained personnel to investigate such traditional crimes as murder, arson, theft, and assault, law enforcement needs "cyber cops" to fight electronic crime.

"To meet this growing need for trained personnel, the CyberScience Laboratory (CSL) at the National Institute of Justice's National Law Enforcement and Corrections Technology Center (NLECTC)–Northeast and its e-Crime Intern Program in Rome, New York, are providing college and high school students with a unique opportunity to gain knowledge and hands-on experience in the field of cyberscience in the law enforcement community," says NLECTC–Northeast's Robert DeCarlo, Jr., who is an economic crime specialist with CSL. "The foundation of this program is a joint venture between academia and both the public and private sectors in an effort to expose students to a challenging experience in support of cyberscience developments.

"One of the things that I like to emphasize is that we're trying to help these young people find productive, meaningful jobs," DeCarlo says. "We want to get them involved in the area of e-crime and encourage them to make it their specialty in law enforcement or private industry, as a computer forensics analyst or similar occupation. The goal is to get them involved in the field and have them stay in it."

DeCarlo explains that CSL creates internships in which "students do more than file papers. They perform full-time, productive work, which could include heading up a special project or making a key presentation. Projects vary according to CSL's needs but often include testing and tool assessments."

"For example," DeCarlo says, "one of the interns [Roseanne Comito] who I mentored tested a steganography detection tool . . . . She wrote a detailed assessment for the vendor and the vendor used it to refine the tool." (Steganography is the art of hiding data within a computer graphic or file.) Comito used her knowledge of steganography on another project, working with a group of gifted middle school students who were part of the Discovery Channel's 2002 Young Scientist Challenge competition. [Editor's note: More information about Roseanne Comito's project and the Young Scientist Challenge can be found at http://access.ncsa.uiuc.edu/Stories/Detectives/.]

Comito's project involved middle school students. But another CSL internship program conducted during summer 2003 offered high school students workplace experience and allowed them to create a course about cybercrime for other high school students. "They talked to the staff and got a feel for the workplace," says Andrea Belmont, an electronic crime specialist with CSL. "They chose to create a website to showcase the course," which focuses on information assurance and cybersecurity, or ways to protect network data and systems.

Both the high school and college interns receive wages based on their experience, DeCarlo notes. This experience plays a key role in whether they are selected to participate in the program. He says that he, Belmont, and others review the resumes submitted each semester and select qualified students.

"When we look at resumes," DeCarlo says, "we primarily look for someone who is studying criminal justice, information technology, or computer science; who is interested in cybercrime; and who wants to stay in the field as a career." Belmont adds that although there is no set grade-point standard, students must be in good academic standing and receive a recommendation from an instructor. Many applicants learn about the internship program from their instructors who urge them to apply.

Schools that have participated in the intern program include Utica College, Syracuse University, University of Miami, Florida Atlantic University, George Mason University, Carnegie Mellon University, Dartmouth College, Stanford University, State University of New York Institute of Technology, Hilbert College, Cornell University, Columbia University, and John Jay College of Criminal Justice. DeCarlo points out that interns do not have to relocate to upstate New York for a semester. CSL can place interns with U.S. Secret Service e-crime task forces across the country. DeCarlo says that any college that would like to take part in the program should call him. “We’ll talk and figure out if they have programs we can draw from.”

To find out more about the CyberScience Laboratory e-Crime Intern Program, contact Robert DeCarlo, Jr. at 888–338–0584 or e-mail robert.decarlo@rl.af.mil.

This article was reprinted from the Winter 2004 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

Parlez-Vous Cyber-Speak?

How well do you know the language of e-crime? Try matching the terms on the left with the definitions on the right, then check the answers to see how well you did.

Terms

1. Steganography
2. Firewall
3. Trojan Horse
4. IDS (Intrusion Detection System)
5. Network Sensor
6. Peer-to-Peer (P2P) Network
7. Information Assurance
8. Cybersecurity
9. IP Address
10. E-mail Spoofing
11. Denial of Service (DoS)
12. Social Engineering
13. Packet Sniffing

Definitions

a. A unique string of numbers that identifies a computer or device on the Internet.

b. A malicious program that masquerades as a benevolent one.

c. A type of network in which individual users connect to each other directly, without a centralized server. Can be used to share files (legal or illegal) easily among individuals.

d. The art of hiding data or pictures within a file or files.

e. The act of capturing packets of data flowing across a computer network.

f. An attack that seeks to slow or disable a network by overwhelming it with useless traffic.

g. The protection of data and systems in networks connected to the World Wide Web.

h. A system that scans areas within a computer or network for possible security breaches.

i. The act of deceiving people into divulging information that allows access to computers and network infrastructure.

j. The protection of information systems to ensure their integrity.

k. A set of related programs that protect a private network from users based outside the network.

l. A program that monitors or “sniffs” a system for problems.

m. The act of forging the header information on an e-mail so that it appears to have originated from somewhere other than its true source.

Answer: 1. d; 2. k; 3. b; 4. h; 5. l; 6. c; 7. j; 8. g; 9. a; 10. m; 11. f; 12. i; 13. e