Students to hack hardware, software and data to build security skills

March 19 2014

Come fall, students at Case Western Reserve University and Cleveland State University will begin hacking computers—for credit.

Each university is offering the first of three courses in a new curriculum in which engineering and computer science students will learn how to break into—and then protect—hardware, software and data. The goal is for students to understand how they can then protect their own, or their employer's, computers from viruses, phishing attacks, so-called Trojan horses and other cyber attacks.

"We're doing a lot of computer security research, but we've failed in the need to educate and train students—the future users, developers and controllers of these systems," said Swarup Bhunia, associate professor of electrical engineering and computer science at Case Western Reserve, who will teach the hardware security class here.

Bhunia teamed with Cleveland State colleagues Sanchita Mal-Sarkar, associate lecturer of computer and information science, and Chansu Yu, chair of electrical and computer engineering, to devise a curriculum that is among the first comprehensive cybersecurity education programs in the country offered to undergraduates. The universities plan to offer versions of the courses to graduate students as well.

"The curriculum is comprehensive and uses a hands-on teaching approach to learning software, hardware, network and information security," Mal-Sarkar said. Cyber attacks, she explained, differ in each

arena.

The National Science Foundation awarded a total of $200,000 in grants to the researchers to develop and support the courses.

The scale of the world's cybersecurity problems has become daily news, from the theft of millions of Target customers' personal data to the infiltration of The New York Times computer systems for four months.

The public, businesses and governments are increasingly vulnerable.

Experts estimate that as many as one in 14 downloads from the Internet carry a virus or malicious code. The global electronic piracy market is estimated at more than $1 billion per day, according to the VSI Alliance, which set standards for intellectual property protection in the electronics industry, in 2000.

Hardware was thought to be the safe haven of the digital world, but that was proved wrong when the United States military found more than 1 million counterfeit electronic components, including chips embedded with Trojan circuits, in a review of supply chains in 2009 and 2010.

And Computerworld magazine reported last fall that a team of security researchers from the U.S. and Europe showed that integrated circuits used in computers, military equipment and other critical systems can be compromised during the manufacturing process through virtually undetectable changes made in transistors—the switches used in logic circuits.

"Chips, boards and circuits are often made overseas," Yu said. "The military, government and businesses have expressed concern over their lack of control of the manufacturing process."

The courses will teach students how to analyze, validate and build secure computer hardware and systems.

In all three courses, students will perform about a dozen hands-on experiments that will show them how and where the systems are vulnerable and how they can be protected.

Pairs of students will each be given a circuit board to hack. For example, they may be assigned to hack communications between the memory and processor. If they can hack into the system, they can snoop—see what information is being passed from one to the other. The students may be asked to hack in and introduce a "time bomb" or spy in the hardware, or infect software with malicious code.

If they can hack it, they can figure out how to protect it, Bhunia said. "We agreed this is the best way to learn," he said.

Yu and Mal-Sarkar plan to team-teach the first course in computer science and electrical and computer engineering departments at CSU this fall.

After completing each course, students will finish with a grand project called "Can You Hack It?" in which teams will challenge each other in hacking and protecting a system.

Provided by Case Western Reserve University