PHYS ORG

Computer science researcher hopes to stall malware threat by tracking human use behaviors

January 25 2010

Danfeng Yao, an assistant professor in the computer science department at Virginia Tech's College of Engineering, will use a $530,000 National Science Foundation Faculty Early Career Development (CAREER) grant to develop software that will differentiate human-user computer interaction from that of malware.

The CAREER grant is the National Science Foundation's most prestigious award, given to creative junior faculty likely considered to become academic leaders of the future. The five-year grant will fund Yao's computer science research for building a new malicious software detection system for personal computers that will be able to accurately differentiate network behaviors of a legitimate human user from a malware program.

The new computer program will do this by identifying and enforcing unique properties of human computer usage. Yao's work will focus on identifying characteristic human-user behaviors, developing protocols for fine-grained traffic-input analysis, and preventing forgeries and attacks by malware. She will design and apply a combination of cryptographic techniques, correlation analysis and hardware-based integrity measures to carry out these tasks.

"Existing malware-detection approaches are limited in their ability to identify and discern malicious bots from legitimate and benign ones," Yao said. "The proliferation and sophistication of malware clandestine activities - as well as its growing capacity to do serious harm - requires constant vigilance and upgrading."

Millions of computers worldwide are estimated to be infected annually by malicious software in the form of viruses, worms and Trojan horses, with scores of computers becoming -- unknown to their owners - part of a "bot" army that runs potentially dangerous automated tasks over the Internet. Infected computers can be coordinated and used by cyber criminals to launch illegal and destructive activities such as identity theft, sending reams of spam messages, launching distributed denial of service attacks, and committing click fraud, Yao said.

Greater threats also exist: Some malware, as in the recent case involving hacker sources from China against Internet giant Google, are tools of cyber warfare meant espionage tools or to destroy critical network infrastructure of a major corporation, financial centers or even a nation's defense agency.

"The program will adaptively learn from the user's patterns, to differentiate legitimate network activities and usage from malicious software," Yao said. By example, a malware program could force a "seized" computer to commit thousands of click frauds in a short period of time, or dump a large amount of spam toward one server in seconds, acts that no human user likely would do on their own accord. Hence, the program would not track the actions ever-changing attack methods of malware - which is constantly evolving - but the actions of a user, or multiple users, whose usage patterns remain relatively unchanged.

As part of the educational/outreach component of the CAREER grant, Yao will conduct outreach and educational activities to increase general awareness of cyber security issues in schools and broaden the interdisciplinary participation of undergraduate women and minority students in computer security research.

Yao earned her undergraduate degree in chemistry from Peking University in Beijing, China, in 1998, followed by a master's degree in chemistry from Princeton University in 2000. In the field of computer science, she earned a master's from Indiana University in 2002 and a doctoral degree from Brown University. Before joining the Virginia Tech faculty this past December, Yao was an assistant professor at Rutgers University's computer science department.

Provided by Virginia Tech

Citation: Computer science researcher hopes to stall malware threat by tracking human use behaviors (2010, January 25) retrieved 10 April 2024 from https://phys.org/news/2010-01-science-stall-malware-threat-tracking.html