Virginia Tech computer scientist, student design award winning software to combat hacking

November 1 2010

One of the serious threats to a user's computer is a software program that might cause unwanted keystroke sequences to occur in order to hack someone's identity. This form of an attack is increasing, infecting enterprise and personal computers, and caused by "organized malicious botnets," said Daphne Yao, assistant professor of computer science at Virginia Tech.

To combat the "spoofing attacks," Yao and her former student, Deian Stefan, now a graduate student in the computer science department at Stanford University, developed an authentication framework called "Telling Human and Bot Apart" (TUBA), a remote biometrics system based on keystroke-dynamics information.

Their work won a best paper award at CollaborateCom '10, the 6th International Conference on Collaborative Computing, held in Chicago and sponsored by the Institute of Electrical and Electronic Engineers' Computer Society, Create-Net, and the Institute for Computer Sciences (http://www.collaboratecom.org/)

Yao holds a patent on her human-behavior driven malware detection technology, including this keystroke anti-spoofing technique. Her technology for PC security is currently being transferred to a company. The license agreement between the company, Rutgers University (Yao's former institution), and Virginia Tech is expected to be finalized in the

coming weeks.

Internet bots are often described as web robots. They act as software applications that run automated tasks over the internet. Bots usually perform simple and repetitive tasks, but at a much higher rate than would be possible for a human alone. When used for malicious purposes they are described as malware.

"Keystroke dynamics is an inexpensive biometric mechanism that has been proven accurate in distinguishing individuals," Yao explained, and most researchers working with keystroke dynamics have focused previously on an attacker being a person.

The uniqueness of Yao and Stefan's research is they studied how to identify when a computer program designed by a hacker was producing keystroke sequences "in order to spoof others," they said. Then they created TUBA to monitor a user's typing patterns.

Using TUBA, Yao and Stefan tested the keystroke dynamics of 20 individuals, and used the results as a way to authenticate who might be using a computer.

"Our work shows that keystroke dynamics is robust against the synthetic forgery attacks studied, where the attacker draws statistical samples from a pool of available keystroke datasets other than the target," Yao said.

Yao and Stefan also describe in their paper, "Keystroke-Dynamics Authentication Against Synthetic Forgeries," how keystroke dynamics can be used "as a tool to identify anomalous activities on a personal computer including activities that can be due to malicious software."

Provided by Virginia Tech