Computer Science Grad Student Wins Symantec Fellowship

February 27, 2007

Daniel Kane

A third-year Ph.D. student in the Computer Science and Engineering (CSE) department of the UCSD Jacobs School of Engineering has won one of three Graduate Fellowships from Symantec Research Labs for the 2007-2008 academic year. Justin Ma will spend this summer in a Symantec research lab in Santa Monica, California, working elbow to elbow with senior security researchers on real-world problems. Symantec will also pay Ma's tuition and fees and provide a stipend for the 2007-2008 academic year.

The Symantec fellowship organizers look for outstanding Ph.D. and M.S. students who are working on research projects likely to have real-world practical value in information security, availability and integrity.

At UCSD, as a part of the CSE Systems and Networking group, Ma has worked on various real-world problems including worms, remote code injection and automated protocol inference. His Ph.D. advisors - Stefan Savage and Geoff Voelker - are both CSE professors in the Jacobs School.

Working with professors Savage and Voelker is "a lot of fun," said Ma.

Savage and Voelker, along with Ma, and other CSE faculty and graduate students are involved in the multi-institution Collaborative Center for Internet Epidemiology and Defenses (CCIED, pronounced "seaside"). Savage is one of two principal investigators (PIs) and Voelker is a co-PI. CCIED projects address critical challenges posed by large-scale Internet-based pathogens, such as worms and viruses.

In October 2006, Ma traveled to Rio de Janeiro, Brazil to attend the Internet Measurement Conference. Ma is the first author on two CCIED-related papers published in the conference proceedings.

One of the papers covered efforts to identify the diversity within a class of malware responsible for "remote code injection." In these malicious network-based exploits, inputs are "injected" into running programs and executed. Slammer and Blaster are two well-known examples. The exploit payload may download additional software, join a centralized botnet, or reconfigure the operating system to evade detection. Remote code injection exploits inflict a significant societal cost, and an active underground economy has grown up around these continually evolving attacks.

Ma, Savage, Voelker and collaborators at Microsoft research developed a semi-automated way to identify how different remote code injection exploits are related, based on shared computer code.

From network samples in which active network code injection attacks had occurred, the researchers came up with a way of emulating exploits in order to decrypt and analyze them. "We measured their similarities and clustered them to infer their phylogenies," said Ma. This kind of work should be useful for gaining a better understanding of how remote code injection exploits evolve.

The second paper was presented at the conference by co-author Kirill Levchenko, also a UCSD Ph.D. candidate from the CSE department. The paper described efforts to automate the process of identifying traffic in

a network using the same application-layer protocol, relying solely on flow content. "From a security perspective, you need to know what's running on your network," said Ma.

Ma and Levchenko returned to San Diego with lots of ideas about Internet measurement - and with the hope of stocking the CSE biometric vending machine with cans of Brazil's carbonated, caffeinated Guaraná Antarctica.

Media Contact: Daniel Kane, 858-534-3262