UT Dallas professor to develop framework to protect computers' cores

April 18 2014

UT Dallas cybersecurity expert Dr. Zhiqiang Lin has received funding from the U.S. Air Force to develop a defense framework that burrows deep into a computer system to protect its core.

The Young Investigator Research Program (YIP) award from the Air Force Office of Scientific Research (AFOSR) provides up to $360,000 over three years to support Lin in developing this framework. Lin is an assistant professor of computer science in the Erik Jonsson School of Engineering and Computer Science, and member of the Cyber Security Research and Education Institute (CSI) at UT Dallas.

"We are very pleased with this prestigious award that Dr. Lin received," said Dr. Bhavani Thuraisingham, professor of computer science in the Jonsson School and executive director of CSI.

THE AFOSR awarded 42 grants from more than 230 applicants who submitted proposals for YIP in this round of competition. Lin is one of two current Jonsson School faculty members to receive the award this year.Dr. Majid Minary, an assistant professor of mechanical engineering at UT Dallas, also received the award.

A small but growing percentage of malware, or malicious code, is targeting the central part of a computer operating system known as the kernel, which impacts software and applications.

"The United States Department of Defense networks and information

systems are especially vulnerable to these types of attacks due to their high values to adversaries," Lin said. "While there has been considerable amount of work for kernel malware detection and prevention, all have severe drawbacks and kernel malware still invades. My holistic kernel malware defense framework aims to detect, diagnose and repair the kernel malware attacks and enforce a prevention mechanism to ultimately cut off the kernel malware infection."

Lin will take a fundamental approach to realize this framework, so the solution will be broad enough to be applied to any type of operating system (OS). One of the most difficult aspects will be analyzing binary code and data—sequences of 0s and 1s—to find the unchanging signature (invariants) of both benign code sequences and data behaviors.

"We find OS kernels contain sufficient amounts of invariants that cannot be modified," Lin said. "We enforce these invariants at the hypervisor layer, a layer deeper than most defense techniques now; and, if anything violates the invariants, we will detect them."

Lin will use his experience making defenses for cloud computing to apply his framework to virtual machines as well.

"This award is a great honor and recognition of the edge we have at UT Dallas in pushing the cybersecurity field forward," Lin said.

Thuraisingham, a Louis A. Beecherl Jr. Distinguished Professor, agrees that the UT Dallas cybersecurity team is a leader in the field.

"Our team has received multiple AFOSR YIPs and National Science Foundation CAREER awards, as well as Department of Defense Multidisciplinary University Research Initiatives," she said. "We are building a strong reputation in a number of research areas, including in active malware defense, secure cloud computing, mobile systems

security and data privacy. Dr. Lin is an integral part of our success."

Provided by University of Texas at Dallas