Reducing computer viruses in health networks

August 19 2013

The hospital IT networks and medical devices that doctors rely on to treat patients are susceptible to their own maladies—computer viruses and other malware.

Whether a bug accidentally finds its way into a system, or an attacker intentionally injects one, researchers believe such breaches are happening more often with the growth of technology such as cloud

computing.

Two engineering researchers from the University of Michigan are part of a national team that will work to improve the cybersecurity of the nation's health systems.

Associate Professor Kevin Fu and Research Associate Professor Michael Bailey, both in the Department of Electrical Engineering and Computer Science, are involved in the five-year Trustworthy Health and Wellness project that has received $10 million from the National Science Foundation. The project is one of three major cybersecurity awards totaling nearly $20 million announced by NSF.

Fu and Bailey will establish methods to scientifically study the extent of malware in hospital networks. While anecdotal evidence suggests the breadth of the problem, there's a need for high quality, reproducible measurements, the researchers say.

"Malicious software, or malware, can interrupt the function of medical devices, affecting the quality of patient care. By increasing the quality of the science, we seek to create more meaningful discussions about risks and benefits of adapting hospital networks to the threat of malware," said Fu, who directs the Archimedes Research Center for Medical Device Security.

Malware can slow down medical devices and interfere with the integrity of their sensors, but current solutions have drawbacks. A deluge of passwords would interrupt clinical workflow and could increase the chance of human error, for example.

"A challenge is to find approaches that improve the safety and effectiveness of medical devices," Bailey said.

A Dartmouth College professor leads the project, which aims to improve the trustworthiness of health and wellness information systems as they're increasingly pushed into mobile devices and cloud-based services, according to the NSF news release.

"Our research is motivated by the rapid deployment of mobile and cloud information technologies in healthcare, both in clinical settings and at home," said lead investigator David Kotz, the Champion International Professor of Computer Science at Dartmouth. "We aim to help these technologies reach their full potential by ensuring they can protect the integrity of medical data and the privacy of patient information."

The team will work to establish better authentication and privacy tools, trustworthy control of medical devices and effective methods to detect malware, compute trust metrics and audit medical information systems and networks. In the long term, this project will help create health systems that patients can trust to protect their privacy, and that health professionals can rely on to ensure data security, the NSF news release states.

The interdisciplinary team involves experts with backgrounds in computer science, business, behavioral health, health policy and health care information technology. In addition to Dartmouth and U-M, researchers from the University of Illinois and Johns Hopkins University are also participating.

The project is one of three grants NSF announced on Aug. 15 through its Secure and Trustworthy Cyberspace program, supporting collaborative, multi-university research and educational activities that will help protect the nation's vast critical infrastructure and enable a more secure information society.

Provided by University of Michigan