Researchers developing techniques to strengthen the security of information systems

January 5 2010

As computers increasingly transfer patient medical records and other sensitive information, a group of computer scientists at Kansas State University is doing basic research that will help designers keep such information safe.

Complex information systems form foundations in our nation's infrastructure and defense forces, and these systems contain data with different security levels, said John Hatcliff, K-State professor of computing and information sciences. As data are exchanged between various users, there's a danger that information could be released to unauthorized parties.

The ability to guarantee secure information flow is becoming more critical as government and industry push toward increasingly complex information systems in many areas, including health care, the military and in coordinating disaster relief, Hatcliff said. That's why K-State computer scientists are developing high-level policy languages and verification techniques to strengthen the security and integrity of such systems.

"Whether it's health care or military information, what people really want is the ability to push information out rapidly to anyone who needs it," Hatcliff said. "You may have a doctor trying to make a diagnosis or a platoon leader trying to coordinate a maneuver in the context of a larger

battlefield operation. In either case, more information leads to better decision making and better outcomes. However, you have to make sure as you're aggressively pushing information to decision makers that you don't inadvertently leak sensitive information to someone who shouldn't be seeing it."

Hatcliff leads K-State's Specification, Analysis and Transformation of Software laboratory. The other computing and information sciences faculty researchers in the lab are associate professors Turban Amtoft and Robby, and assistant professor Simon Ou. These researchers do work in security, software engineering, programming language semantics and automatic analysis of computer software.

In March 2009, the research group, in collaboration with researchers at Princeton University, received a five-year, $3 million grant from the Air Force Office of Scientific Research. The researchers are developing tools to secure information systems so that when information is transferred across large systems, there is confidence that nothing is accidentally revealed.

"We're doing foundational research on novel forms of mathematical models and logics that enable designers and analysts to precisely state what information is allowed to flow from one point to another and under what conditions," Hatcliff said. "Then we're building tools to help people use those mathematical techniques to verify that their systems are correct."

The researchers also are receiving funding from Rockwell Collins, a company that creates communications and aviation electronics. The work with Rockwell Collins involves applying the K-State research team's verification tools to several systems being developed in U.S. Department of Defense security research projects.

Hatcliff said information leakage is a concern in many domains, like potential integration in the health care system with patients' medical records.

"Millions of dollars are being invested by federal and state governments to set up health information exchanges," Hatcliff said. "The idea of such an exchange is that you have a technology organization that facilitates and mediates the exchange of patient medical information between a variety of parties. The challenge is that the information in patients' records has different levels of sensitivity or security. These exchanges eventually are going to need a way to specify policies describing what information can be released and to whom, and the exchange will need to guarantee that those policies are adhered to."

Hatcliff said K-State's research shows promise for addressing these issues because it involves creating mathematical and logical models that can be used by special computer-based auditing programs to guarantee that an information system conforms to the stated information flow policy.

The researchers' tools also provide graphical visualizations of information flowing through a system so that designers and auditors can more quickly understand a system's information flow behavior. The research focuses on systems where very high levels of assurance are required, and it aims to prove conformance to information flow policies during a certification phase before a system is deployed.

"It's pretty rare in the software engineering and verification research community that you receive a significant amount of money to fund basic research and also have a company that's doing such advanced work fund you to take your basic research and apply it," Hatcliff said.

The collaboration with Princeton University is with Andrew Appel,

professor and chair of Princeton's computer science department.

"We're very good at building tools that help programmers actually apply some of these techniques to real programs, and Andrew's very good at developing the underlying math and logic," Hatcliff said. "We're working together to come up with an even better collection of tools."

Through collaboration stipulations, the universities will provide student visits and exchanges. The grant also funds work for four graduate students and two undergraduates at K-State. K-State's research group has been awarded more than $12 million of research funding the past 10 years. The group's tools have been used in numerous academic research groups and by various industries worldwide.

Provided by Kansas State University