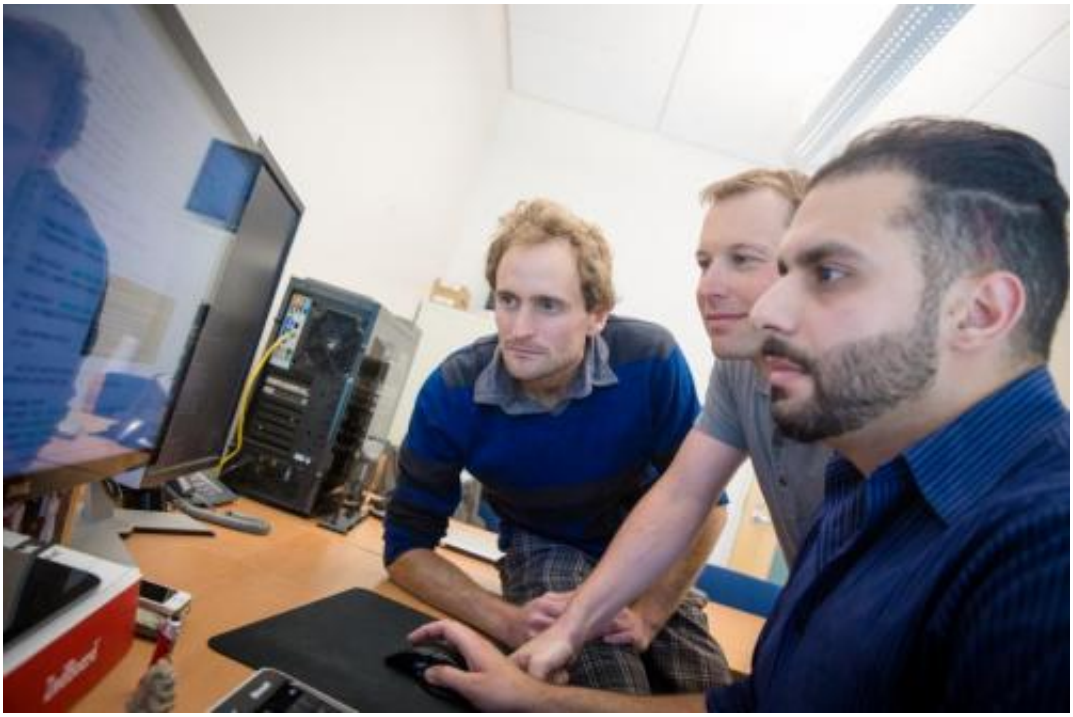
Computer scientists develop tool to make the Internet of Things safer

June 2 2014



From left are: Ph.D. student Jason Oberg, computer science professor Ryan Kastner and postdoctoral research Jonathan Valamehr. Credit: Jacobs School of Engineering/UC San Diego

Computer scientists at the University of California, San Diego, have developed a tool that allows hardware designers and system builders to test security- a first for the field. One of the tool's potential uses is described in the May-June issue of *IEEE Micro* magazine.

"The stakes in hardware security are high", said Ryan Kastner, a professor of computer science at the Jacobs School of Engineering at UC San Diego.

There is a big push to create the so-called Internet of Things, where all devices are connected and communicate with one another. As a result, embedded systems—small computer systems built around microcontrollers—are becoming more common. But they remain vulnerable to security breaches. Some examples of devices that may be hackable: medical devices, cars, cell phones and smart grid technology.

"Engineers traditionally design devices to be fast and use as little power as possible," said Jonathan Valamehr, a postdoctoral researcher in the Department of Computer Science and Engineering at UC San Diego. "Oftentimes, they don't design them with security in mind."

The tool, based on the team's research on Gate-level Information Flow Tracking, or GLIFT, tags critical pieces in a hardware's security system and tracks them. The tool leverages this technology to detect security-specific properties within a hardware system. For example, the tool can make sure that a cryptographic key does not leak outside a chip's cryptographic core.

There are two main threats in hardware security. The first is confidentiality. In some types of hardware, one can determine a device's cryptographic key based on the amount of time it takes to encrypt information. The tool can detect these so-called timing channels that can compromise a device's security. The second threat is integrity, where a critical subsystem within a device can be affected by non-critical ones. For example, a car's brakes can be affected by its CD player. The tool can detect these integrity violations as well.

Valamehr, Kastner, and Ph.D. candidate Jason Oberg started a company

named Tortuga Logic to commercialize this technology. The company is currently working with two of the top semiconductor companies in the world. Their next step is to focus on medical devices, computers in cars, and military applications.

The team recently were awarded a $150,000 grant from the National Science Foundation to grow their business and further their research.

Provided by University of California - San Diego