2011-03

Research: Projects: RCSEC

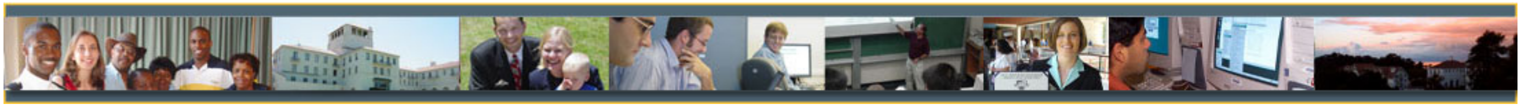
Naval Postgraduate School (U.S.); Center for Information Systems Studies Security and Research (CISR)

http://hdl.handle.net/10945/35371

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Search Site

Centers of Academic Excellence
IA Education & Research



Research: Projects: RCSEC

reconfigurable security

Reconfigurable Security with Reconfigurable Hardware

From Bluetooth transceivers to the NASA Mars Rover, reconfigurable circuits (such as the one pictured below) have become one of the mainstays of embedded design. Combining the high computational performance of specialized circuits with the re-programmability of software, these devices are quickly becoming ubiquitous - unfortunately this hardware malleability can be twisted to disrupt critical operations, snoop on supposedly secure channels, or even to physically melt a device.

The goal of our research is to enable a new class of systems that are both reconfigurable and secure. There are three important areas need to be addressed in order to achieve these goals: enforcing logic-level separation, advanced memory protection, and dynamic policy management.

Dynamic Policy Management

While reconfigurability creates problems as described above, it also creates opportunities: in particular the opportunity for hardware enforcement of adaptive security policies. In an emergency, trusted individuals may need to override the nominal security policy. The reconfigurable component may provide a highly trusted mechanism for secure functionality in changing environments. Thus a key aspect of our work is in establishing a firm foundation for trustworthy dynamic policy enforcement through ontological analysis and formal modeling.

Advanced Memory Protection

Virtual Memory is the mechanism by which many security policies are enforced, it is all but non-existent on embedded systems. While a TLB-like structure could be constructed out of the logic blocks that populate a modern reconfigurable device, instead we need to rethink the way that embedded memory is protected and shared. With reconfigurable hardware we can implement test example enforcement mechanisms and reason formally as to their security.

FPGA
Trustworthy FPGA

Logic Protection and Interface Enforcement

The problem does not stop at memory management. In reconfigurable systems the logic of the hardware can be changed, which opens a host of problems that have no easy analogs in the software domain. For example, configurations can be loaded that cause short circuits or even meltdown. Secret data may need to share the same chip as untrusted intellectual property which has the potential to improperly impede or probe the device. New methods are needed that can statically validate these configurations.

People

This project is a collaborative research effort run jointly between the Naval Postgraduate School in Monterey and the University of California in Santa Barbara. In addition to the research objectives, it is our goal to develop methods and techniques that can be passed to future teachers, researchers and Information Assurance professionals. Initial funding for this research was generously provided by NSF through grant #0524771 for "Adaptive Security and Separation in Reconfigurable Hardware". Pictured below (left to right) are Tim Levin, Thuy Nguyen, Cynthia Irvine, Tim Sherwood, and Ryan Kastner.

Principle Investigators

Cynthia Irvine is a Professor of Computer Science at the Naval Postgraduate School (NPS) where she is the Founder and Director of the Center for Information Systems Security Studies and Research. Dr. Irvine received her B.A. degree from Rice University, Houston, TX and her Ph.D. from Case Western Reserve University in Cleveland, OH. Professor Irvine has published over 70 papers and reports on her research in computer and network security.

Ryan Kastner is currently an Associate Professor in the Department of Computer Science and Engineering University of California, San Diego. He received a PhD in Computer Science at UCLA, a masters degree (MS) in engineering and bachelor degrees (BS) in both electrical engineering and computer engineering, all from Northwestern University. His current research interests lie in the realm of embedded systems, in particular reconfigurable computing, compilers and sensor networks.

Tim Levin

Thuy Nguyen

Tim Sherwood is an Assistant Professor in Computer Science at UC Santa Barbara. Before joining UCSB in 2003 he received his B.S in computer engineering from UC Davis and his M.S. and Ph.D. from UC San Diego where he worked with Professor Brad Calder. His research interests include network and security processors, program phase analysis, and hardware support for embedded software design.

Researchers

Tim Levin
Ted Huffmire

Downloads

RCSec Poster as (PDF) or (PPT)

RCSec Nugget as (PDF) or (Doc)

Visit the official RCSec site at UCSB

This page was last modified: March 2011

Home / Webmaster / Privacy Policy / FOIA / Sitemap / NPS

This U.S. Government Web Site is provided by the Naval Postgraduate School's Center for Information Systems Security Studies and Research for official information regarding CISR's programs and research.