New computer architecture aids emergency response

October 31 2007

Princeton researchers have invented a computer architecture that enables the secure transmission of crucial rescue information to first responders during events such as natural disasters, fires or terrorist attacks.

Electrical engineering professor Ruby Lee said the new architecture allows for what she describes as “transient trust” – the ability to transmit sensitive information to parties on an as-needed basis so that it cannot be intercepted by others and so that access stops as soon as the recipient no longer has a legitimate need for it.

A paper describing the new architecture by Lee and her graduate student Jeffrey Dwoskin will be presented Wed., Oct. 31, at the ACM Computer and Communications Security conference in Alexandria, Va. [1].

Data provided on a transient-trust basis might include floor plans of a building, medical information about occupants, or satellite maps of a given area.

The paper describes SP (Secret Protection) computer architecture, which relies on two new elements that are embedded in the hardware of an electronic device: a “device root key” and a “storage root hash.”

A trusted authority such as a municipal Fire Department would initialize a device -- for example, a PDA used by a firefighter – with these features so that during an emergency a firefighter could be given access to relevant floor plans, security codes or other essential information.

Once the emergency was over, the access to this sensitive information would end.

This new research emerged from the Princeton Architecture Lab for Multimedia and Security (PALMS) led by Lee, the Forrest G. Hamrick Professor of Engineering. The lab's major focus is "clean-slate" computer architecture design. As chief computer architect at Hewlett-Packard, Lee was a key figure in a revolution in computer architecture that swept through the industry in the 1980s. Since coming to Princeton, Lee has been working to revolutionize computer architecture again.

"Computers were not originally designed with security as a goal," said Lee. "I'm trying to rethink the design of computers so they can be trustworthy while at the same time retain all their original design goals, such as high performance, low cost and energy efficiency."

Lee aims to build fundamental security features directly into the hardware of a device, whether it is a personal computer, cell phone or PDA. Her researchers are working to build "trust anchors" into computer hardware to which different software can be tethered, to provide important security coverage.

Lee said that many researchers do not think it is possible to build security features into computer hardware without slowing the computer down or causing it to consume lots of power. However, research done by her lab demonstrates that this is not the case.

"Our research shows that these hardware 'roots of trust' are actually quite deployable on consumer devices like desktop computers or PDAs, and also in sensor networks and larger servers," said Lee. The work is part of the SecureCore multi-university research project, funded by the NSF Cybertrust program and DARPA, which aims to integrate essential security into the hardware, software and networking at the core of commodity computing and communications devices.

In addition to trust anchors for software, Lee is also researching hardware “safety nets” to defend against software vulnerabilities that remote attackers exploit to gain entry into a computer. The ultimate goal is to inoculate individual computers and electronic devices such as cell phones against threats like viruses, worms and bots so that they cannot infect, or be used to attack, other machines.

Lee’s students study all aspects of building more secure microprocessors and hardware. In June, at the IEEE Symposium on Computer Arithmetic, Lee and Yedidya Hilewitz, a graduate student at Princeton, published a paper which proposes a revolutionary design of a fundamental functional unit of microprocessors that greatly expands a computer’s ability to perform "advanced bit manipulation operations,” which are very useful for fast cryptography and cryptanalysis, as well as for many other applications [2].

Lee is also studying computer architecture that prevents leakage of information through covert channels and side channels. At the International Symposium on Computer Architecture in June, Zhenghong Wang, one of Lee’s graduate students, presented a paper describing a hardware approach to preventing so-called “software side-channel attacks” during which attackers exploit the cache memories that are shared between computer programs to leak secret cryptographic keys [3].

In September, at the Cryptographic Hardware and Embedded Systems conference, Lee’s researchers, Reouven Elbaz and David Champagne, presented a hardware memory integrity solution to rebuff memory replay attacks, where attackers try to trick a computer into accepting material as still legitimate even though it has already been officially deleted. [4].

Lee was a member of the Committee on Improving Cybersecurity Research in the United States, a group charged by the National Research Council with outlining a strategy for cybersecurity research in the 21st century. The committee recently issued a report, Toward a Safer and More Secure Cyberspace, published by the National Academy of Sciences. Section 4.1 of the report, which can be found at the url below, describes the earlier user-centric version of the Secret Protection architecture [5] – rather than the authority-centric version described above for emergency response scenarios. Both were developed by Lee's lab at Princeton.

Paper citations:

[1] Jeffrey Dwoskin and Ruby Lee, "Hardware-rooted Trust for Secure Key Management and Transient Trust," to appear at the ACM Computer and Communications Security (CCS '07), Oct 29-Nov 2, 2007.

[2] Yedidya Hilewitz and Ruby B. Lee, "Performing Advanced Bit Manipulations Efficiently in General-Purpose Processors", IEEE Symposium on Computer Arithmetic (ARITH-18), June, 2007.

[3]Zhenghong Wang and Ruby B. Lee, "New Cache Designs for Thwarting Software Cache-based Side Channel Attacks", International Symposium on Computer Architecture (ISCA'07), June 2007.

[4] Reouven Elbaz, David Champagne, Ruby B. Lee, Lionel Torres, Gilles Sassatelli and Pierre Guillemin, "TEC-Tree: A Low Cost, Parallelizable Tree for Efficient Defense against Memory Replay Attacks", Cryptographic Hardware and Embedded Systems (CHES 2007), September 2007.

[5] Ruby B. Lee, Peter C. S. Kwan, John Patrick McGregor, Jeffrey Dwoskin, and Zhenghong Wang, "Architecture for Protecting Critical

Secrets in Microprocessors," Proceedings of the 32nd International Symposium on Computer Architecture (ISCA 2005), pp. 2-13, June 2005.

Source: Princeton University

Citation: New computer architecture aids emergency response (2007, October 31) retrieved 3 May 2024 from https://phys.org/news/2007-10-architecture-aids-emergency-response.html