Instruction-set randomization enhances computer security by enabling system diversity at the lowest hardware/software interface

Due to the computer industry’s increasing reliance on common software tools and hardware architectures, many computer systems to date remain identical and thus vulnerable to the same large-scale security attacks. This technology presents a method to diversify computer systems by providing native hardware support using instruction-set randomization (ISR). ISR randomizes instruction sets that map the lowest-level machine code to computer operations in a unique fashion and decrypts them whenever a task must be performed. In this way, ISR aims to provide a unique random instruction set architecture (ISA) for every deployed system. This technology outlines a number of ways to combat malicious attacks using the ISR diversification approach.

Hardware-based ISR provides faster, more secure system diversification with virtually zero performance overhead

Software-based implementations for system diversification tend to be slow (70% to 400% slowdowns) and insecure because they use weaker encryption schemes that can be turned off. By contrast, ISR performs all encryption within the hardware to prevent malicious programs from turning encryption schemes off. Furthermore, the hardware-based instruction set randomization is several times faster and more secure than software-based implementations. This technology also achieves virtually zero performance overhead using strategic micro-architectural optimizations in which very simple modifications in hardware result in broad security coverage. ISR may be combined with a number of alternative protection schemes, including non-executable data pages and address space layout randomization.

The ISR technique has been implemented on a prototype OpenSPARC FPGA processor.

Lead Inventor:

Angelos Keromytis, Ph.D.
Applications:

- Securing computers against code injection attacks
- Encrypting personal data
- Developing encryption schemes
- Prevent hacking attempts on computers

Advantages:

- Broad security coverage can be achieved through simple modifications in hardware
- Several times faster and more secure compared to software-based instruction set randomization
- Strategic micro-architectural optimizations result in virtually zero performance overhead

Patent Information:

Patent Pending ([WO/2014/210277](http://patents.google.com/original/wo2014210277))

Tech Ventures Reference: IR CU13367

Related Publications:


Inventors

Angelos D. Keromytis