北京大学高能效计算与应用中心学术报告

Invited Talk, Center for Energy-Efficient Computing and Applications

TOWARDS MAKING VULNERABLE PROCESSORS MORE DEPENDABLE

Prof. Sri Parameswaran

School of Computer Science and Engineering

the University of New South Wales

2012年9月14日 星期五 10:30am

理科五号楼410会议室

ABSTRACT: Deep devastation is felt when privacy is breached, personal information is lost, or property is stolen. Now imagine that all of this can happen at once, and the victim is unaware of its occurrence until much later. This is the reality, as increasing amount of electronic devices are used as keys, wallets and files. Security attacks targeting embedded systems illegally gain access to information or destroy information. Such threats in embedded systems could be classified by the means used to launch attacks. Typical launch methods are physical, logical/software-based and side-channel/lateral attacks. Physical attacks refer to unauthorized physical access to the embedded system itself and are feasible only when the attacker has direct access to the system. Logical attacks exploit weaknesses in logical systems such as software or a cryptographic protocol to gain access to unauthorized information. Logical attacks are deployed easily against systems, which are able to download and execute software and have vulnerabilities in their design. Side-channel attacks are performed by observing properties of the system (such as power consumption, electromagnetic emission, etc.) while the system performs cryptographic operations.

A wide range of techniques has been proposed in the past to detect and counter security attacks in embedded devices. They could broadly be categorized into software-based techniques and hardware assisted techniques. Software based techniques use software tools such as code analysers and methods such as proof-carrying-code to overcome these attacks without changing the architecture of the processor. Hardware assisted techniques use additional hardware blocks or micro-architectural support to detect and protect against these security attacks. The talk gives an overview of the most popular attacks on embedded computing systems, and some countermeasures against logical and side-channel attacks.

BIOGRAPHY: Sri Parameswaran is a Professor in the School of Computer Science and Engineering at the University of New South Wales. He also serves as the Postgraduate Research and Scholarships coordinator at the same school. Prof. Parameswaran received his B. Eng. Degree from Monash University and his Ph.D. from the University of Queensland in Australia. He has held visiting appointments at University of California, Kyushu University and Australian National University. He also worked as a consultant to the NEC Research laboratories at Princeton, USA and to the Asian Development Bank. His research interests are in System Level Synthesis, Low power systems, High Level Systems, Network on Chips and Secure and Reliable Processor Architectures. He serves on the editorial boards of ACM Transactions on Embedded Computing Systems, the EURASIP Journal on Embedded Systems and the Design Automation of Embedded Systems. He has served on the Program Committees of Design Automation Conference (DAC), Design and Test in Europe (DATE), the International Conference on Computer Aided Design (ICCAD), the International Conference on Hardware/Software Codesign and System Synthesis (CODES-ISSS), and the International Conference on Compilers, Architectures and Synthesis for Embedded Systems (CASES).