FPGA Implementation of a Secure Microprocessor

Takafumi Iwasa† and Koji Inoue‡
†Dept. of Elec. Eng. and Computer Science Fukuoka University, Fukuoka, Japan
‡PRESTO, Japan Science and Technology Agency

As the popularity of mobile computing devices and the advance in internet information services, considering the security of computer systems becomes more important. Although the internet is a much useful instrument, it also gives an opportunity to malicious persons for attacking remote connected devices. Especially, computer viruses, which invade our computer system and attempt to perform malicious operations, are one of the most serious threats. Although a number of software-base intrusion-detection techniques have so far been proposed, still the threat of computer viruses is spreading in the world. Fundamentally, the viruses are executed on a microprocessor as well as the trusted application programs. Unfortunately, current microprocessors can not distinguish between the trusted and un-trusted programs to be executed by themselves: this is the essence of the virus problem to be solved.

To challenge the security problem, we propose a hardware-base intrusion detection technique which regards the dynamic program-execution behavior as a certification key. Based on secret key information, we determine an execution behavior, e.g. a memory-access pattern. Then an object code which generates the determined execution behavior at run time is constructed by a secure compiler. This means that the successfully compiled source code can be trusted. While the program execution, a secure profiler implemented on a programmable device like FPGA monitors the execution behavior. If the secure profiler can not see the determined behavior, it alarms the microprocessor for terminating the current program execution. Since the viruses do not know the behavior required to continue the execution on the microprocessor, we can detect and prohibit the malicious attacks at the beginning of its execution. We have designed a Strong-ARM base secure microprocessor and a secure profiler in order to verify our concept and evaluate the performance/cost overhead. Figure 1 shows the FPGA evaluation board used in our prototyping. In this presentation, we show and demonstrate the detail of our hardware-base intrusion-detection methodology.

Figure 1: FPGA Board