A Digital PUF-based IP Protection Architecture for Network Embedded Systems

Jason Xin Zheng, Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles (UCLA)
Los Angeles, USA
{jxzheng,miodrag}@cs.ucla.edu

ABSTRACT

In this paper we present an architecture for a secure embedded system that is resilient to tempering and code injection attacks and offers anti-piracy protection for the software and hardware Intellectual Property (IP). We incorporate digital Physical Unclonable Functions (PUFs) in an authentication mechanism at the machine code level. The digital PUFs are used to de-obfuscate, at run time, a firmware that's issued by a central authority with very little performance and resource overhead. Each PUF is unique to the hosting device, and at the same time can be reconfigured with new seeds. The reconfigurable digital PUFs (drPUFs) have much lower risks of side-channel attacks and vastly higher number of usable challenge-response pairs, while retaining the speed and ease to implementation of digital PUFs.

1. INTRODUCTION

Software defined network (SDN) is becoming a new dominant paradigm in the networking systems for two reasons. The first reason is that SDN allows the network equipment maker to deploy systems that can respond to new conditions and traffic patterns. For example, new network features can be supported by uploading a new firmware to the routers. The second reason is that the SDN is inherently resilient against known attacks to the system, as the behavior of the network can be quickly modified to address the system-level mistakes and shortcomings. However, SDN's reprogrammability also presents a new avenue that can be exploited by the attackers. We see increasing needs for securing both the design of the original system to prevent code injection attacks and the mechanisms for the delivering of network hardware and firmware in the context of the SDN.

On the other hand, in the near future, billions more smart devices are becoming connected to the Internet; much of the added intelligence will be in the form of new software Intellectual Properties (IP). In this coming tide of "Internet of Things," parties with commercial interests have great incentives to protect the IPs that they have developed with capital investment and to prevent their smart systems from being wholesale-cloned by competitors.

In this paper we present a secure embedded system architecture that prevents third parties from tempering either the existing or a new firmware being delivered to the system, and from copying the hardware or software designs. The main idea is that while all devices share the same source code, the binaries that are delivered to each device is unique to the device and cannot be run directly by an arbitrary embedded processor. Each device is created with digital Physical Unclonable Functions (PUFs) that is used to translate, at run-time, the unique firmware into the original executable form.

2. DIGITAL RECONFIGURABLE PUF

Physical Unclonable Function (PUF) is a multi-input hardware device that produces difficult-to-predict outputs that are unique to each instantiation of identical devices. PUF is one of the most popular and widely-used hardware security primitives [1]. It is used in a variety of hardware-based security protocols ranging from generation of random numbers to secure storage of privileged information and public key cryptography [4]. However, until recently all PUFs have been analog devices and therefore greatly influenced by operational and environmental conditions and subject to change of their mapping function due to device aging. Very recently, digital PUFs have been developed that eliminate all these drawbacks of analog PUFs. Even more importantly, they are faster, require less energy, and can be easily integrated within conventional digital logic [5].

However, digital PUFs still face certain limitations. Of most importance are potential susceptibility to side-channel attacks and a relatively small number of challenge-response pairs. We address both of these limitations by using multiple Reconfigurable Digital PUFs. While one PUF is in operation mode, other idling PUFs can be continuously updated to prepare for the next activation. Collectively, a set of reconfigurable digital PUFs, by way of run-time reconfiguration, may use an exponential number of seeds to operate without incurring the timing overhead demanded of analog PUFs, and requires a potential attacker to recover all of the seeds in order for a successful attack.

Reconfigurable digital PUF (drPUF) can be used for variety of security, privacy, and trust tasks in many communication and networking applications. For example, drPUF can be used for secure reconfiguration of network elements. It can be also used for trusted data collection by unprotected sensors in sensor networks and the Internet of things.

ANCS'14, October 20–21, 2014, Los Angeles, CA, USA.
ACM 978-1-4503-2839-5/14/10,
http://dx.doi.org/10.1145/2658260.2661776.

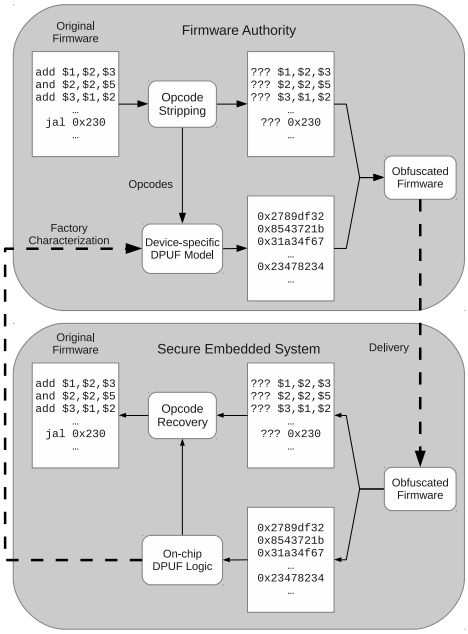

Figure 1: Protection Mechanism

A notable advantage of PUF-based IP protection to crypto-based solutions is that PUFs are truly unique devices. While cryptographic engines can employ unique keys for each device instantiation, once one device is compromised, an attacker can relatively easily make copies of the system by cloning both the hardware and the software components. Cloning PUF-based systems are inherently difficult as the operational secret is embedded in the silicon.

3. PROTECTION MECHANISM

The basic protection mechanism is illustrated in Figure 1. First, the device manufacturer characterizes the digital PUF on each device instance to build a device-specific model for the firmware authority to use. By using the device-specific models, the firmware authority can process the original firmware by stripping away all instruction opcodes and replace them with an obfuscated version that's unique to each device. Finally, when the obfuscated firmware is executed on the intended embedded system, the original instruction opcodes are recovered by using the obfuscated opcodes as challenges to the device's digital PUF logic.

The strength of the obfuscation mainly rests on two points. First, for each opcode, there exists millions of different choices to choose from as the obfuscated opcode. Therefore each occurrence of the same opcode will look completely different from another, making any statistical attack very difficult. Secondly, the on-chip PUF devices are unique physical devices that cannot be easily copied. This has great implications on code-injection attacks; an attacker who successfully attacks one of the devices cannot simply replicate the attack on another device without incurring the same amount of engineering effort for the first attack.

This mechanism is further enhanced by two facts. The first is that multiple digital PUFs are used to obfuscate the firmware. For each instruction, one active PUF is chosen based on a logical combination of the instruction's address.

Benchmark Program	Original Runtime (Seconds)	Modified Runtime (Seconds)	Performance Penalty
FFT	24281.5	25968.25	4.62%
search_lg	8706.5	8888.5	2.09%
search_sm	303.5	311.75	2.72%
bitcount	24331	24331.75	0.00%
basicmath_sm	99091	107023.75	8.01%

Table 1: Performance Penalty for ORPSoc

In addition, while one digital PUF is used for a segment of the firmware, the idling PUFs can be modified by using a different set of initialization seeds. The dynamic transformation of the digital PUFs makes it more difficult for an attacker to collect all the seeds necessary to attack the PUFs.

4. RESULTS

A demonstration and evaluation system is implemented by incorporating real-time instruction de-obfuscation with the OpenRISC Reference Platform System-on-Chip (ORPSoC) project [3]. The implementation targets a Xilinx Spartan-6 FPGA on a Digilent Atlys development board.

We show that the on-line de-obfuscation has low performance overhead by running an embedded benchmark suite based on MiBench [2]. Table 1 shows a comparison of the benchmark results running on the original and modified systems. The effects of the modification are similar to that of a slow instruction memory interface. The performance impacts are well contained within 10% as most of the memory latency is hidden by the instruction cache.

5. CONCLUSIONS

We have presented a novel use of the reconfigurable digital PUFs as instruction-level authentication devices. This mechanism offers temper protection on the firmware and prevents the software and the hardware IP from being copied by third parties with very little performance impact.

6. ACKNOWLEDGMENT

This work was supported by the NSF Award CNS-0958369, Award CNS-1059435, and Award CCF-0926127.

7. REFERENCES

[1] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, pages 148–160, New York, NY, USA, 2002. ACM.

[2] M. R. Guthaus et al. MiBench: A free, commercially representative embedded benchmark suite. In *IISWC*, pages 3–14, Dec. 2001.

[3] D. Lampret and J. Baxter. OpenRISC 1200 IP core secification, rev. 0.12, 2011.

[4] M. Potkonjak and V. Goudar. Public physical unclonable functions. *Proceedings of the IEEE*, 102(8):1142–1156, Aug 2014.

[5] T. Xu, J. B. Wendt, and M. Potkonjak. Secure remote sensing and communication using digital pufs. In *ANCS*, pages 1–11, 2014.