ARM TrustZone in an SOC Environment

Stephen Donchez, *Member, IEEE,*

***Abstract*—ARM's TrustZone platform is a well-known platform for the implementation of security functionality in embedded systems. Although the platform is widely used in the larger embedded development industry, it has been less widely studied with regards to its use in Field Programmable Gate Array (FPGA) based embedded systems, which have widespread popularity. This paper analyzes current research work being done in this field, which has demonstrated that there are numerous potential vulnerabilities exposed by such a system. It then analyzes the countermeasures recommended by those conducting said research, as well as proposes avenues for future work.**

***Index Terms*—ARM TrustZone, Embedded System, System on a Chip, FPGA Security**

I. Introduction

IT has rapidly become common knowledge within the technology industry, and to some extent in society at large, that the phrase "secure IoT device" is an oxymoron. Recent advances in computer technology have led to a massive surge of smart devices, with a particularly rapid growth in the consumer electronics sector. However, this rapid proliferation of such devices has led to an unfortunate discovery – many of them fail to adequately address security concerns, leading to vulnerabilities that are often harnessed by malicious actors.

As a result, the industry has begun to take a second look at security in embedded systems. To this end, ARM ltd., the organization that oversees the development of the ARM processor family, has introduced the ARM TrustZone platform, which seeks to offer "an efficient, system-wide approach to security with hardware-enforced isolation built into the CPU." [1] This platform effectively partitions the processor into two discrete "worlds", one for secure operations and one for nonsecure (or normal) operations.

TrustZone has enjoyed tremendous success since its inception, and forms the basis for the security of many common devices, including Android based smartphones. However, the concept of Field Programmable Gate Array (FPGA) based System-on-a-Chip (SoC) devices introduces a host of complexities into the implementation of a TrustZone enabled system. The presence of in-situ reprogrammable hardware in such a system creates drastically increased potential for malicious actors to attempt to compromise the integrity of said system.

Beyond the vulnerability created by having logic that can be altered present in such a system, the FPGA development process introduces several additional concerns. First and foremost, the industry as a rule relies heavily on third party logic designs, known as intellectual property (IP), for abstracting much of the intricacies of these complex systems. The presence of this IP brings with it a host of potential security concerns, both as a result of maliciously compromised IP and also defects in otherwise genuine IP that may expose the larger system to exploitation. Furthermore, the nature of the FPGA development process is heavily automated by a complex buildchain not dissimilar to a compiler. This poses another avenue for attack - compromised buildchain software could result in a device that performs as expected but presents additional avenues for exploitation.

A. Structure of the Paper

This paper is structured into 6 major sections. The introduction in Section I seeks to provide essential context as to the purpose of the ARM TrustZone platform, as well as the additional complexities introduced by using the platform in combination with a FPGA based SoC. Section II provides an explanation of the principles governing the operation of the TrustZone platform itself. Section III and IV discusses the state of current research on the effective implementation of the ARM TrustZone into FPGA-based Embedded Systems, while sections V and VI discuss potential avenues for further research. Section VII concludes the paper.

II. Details of the TrustZone platform

III. Related Research in Embedded Systems

IV. Related Research in FPGA-Based Embedded Systems

V. Avenues for Future Research in TrustZone Enabled Systems

VI. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] "TrustZone," library Catalog: developer.arm.com. [Online]. Available: https://developer.arm.com/ip-products/security-ip/trustzone

S. Donchez is with Villanova University, Villanova, PA 19085 USA e-mail:sdonchez@villanova.edu

Manuscript received May 6, 2020

PLACE
PHOTO
HERE

Stephen Donchez (M’20) was born in Bethlehem, PA, USA in 1998. He anticipates receiving his B.S. in computer engineering from Villanova University, Villanova, PA in 2020.

In the summer of 2018 he was a software engineering intern at Harris Coroporation (now L3Harris Technologies, Inc.). He returned to L3Harris for the summer of 2019 as a systems engineering intern, and anticpates returning to the same position for the summer of 2020 at their facility in Clifton, NJ. His research interests include FPGAs, embedded software development, and embedded systems with a focus on System-on-a-Chip technologies.