Firmware Security: Hot Topics to Watch

Spring 2018 UEFI Seminar and Plugfest
March 26-30, 2018
Presented by Dick Wilkins (Phoenix Technologies, Ltd.)
Agenda

- Introduction
- UEFI and the IoT
- Security and UDK2018
- Happenings in NIST Guidelines
- Questions?
Introduction

• There are several security-related topics that we feel should be on all UEFI members’ “radar”

• This presentation calls them out and is intended to raise awareness
UEFI and the IoT
UEFI and the IoT

• The Forum would like to broaden its penetration into IoT and other areas

• I wrote and an article for *Embedded Computing Design* on behalf of the forum

http://www.embedded-computing.com/iot/firmware-security-for-iot-devices

• I also appeared in a podcast for *Security Weekly* where UEFI for IoT was a topic

https://www.youtube.com/watch?v=VG-A6Mkdny4

• In the next few slides, I will summarize my article’s content
Motivation

• The Internet of Things (IoT) has been touted as the *Next Big Thing* as well as the *Internet of Crappy Things*. Both descriptions are justifiable.

• IoT devices have participated in DDoS attacks and have invaded the privacy and exposed the personal information of their users.

• Once fundamental software flaws are corrected, the firmware of these devices will likely be attacked next.
Why IoT firmware is an issue

- IoT devices have all the same attack surfaces as computer systems
- They are NOT cheap, single use, throwaway devices
- They can be used to steal data, spy inside a user’s firewall, or launch attacks on other systems
What to do about it

• Consider using UEFI based firmware
• Security is part of the specification
• UEFI has a proven security design
• Secure Boot prevents corrupted devices from running and compromising networks
• Signed Capsule Update prevents unauthorized firmware replacement or rollback
Why isn’t everyone using UEFI?

• Inertia; many IoT developers are from the embedded & SoC space where U-boot and coreboot are king
• Misinformation, misconceptions and “alternative facts” about UEFI are widespread
Bottom line

• IoT developers should consider using UEFI based designs
• IA and ARM are supported now and open-source code is available
• UEFI on coreboot may even exist
• IFVs (Independent Firmware Vendors) can help
• Call to action for Forum members: Be ready to support UEFI on IoT devices
Security and UDK2018
UEFI Development Kit 2018 (UDK2018)

• UDK2018 is coming and has security implications
• According to the Tianocore site several features will be added to the codebase
• We all should be paying attention and get them into our code ASAP
• Next are some examples of important enhancements
UEFI 2.7 spec related changes

• Deprecate SMM Communication ACPI table
  “The use of the SMM Communication ACPI table is deprecated in UEFI spec. 2.7. This is due to the lack of a use case for inter-mode communication by non-firmware agents with SMM code and support for initiating this form of communication in common OSes.”

• Anything SMM related has security implications
IOMMU based DMA protection

- The possibility of PCI devices with DMA capabilities becoming potential “bad actors” has been known for some time.
- The PI spec was modified to allow blocking some devices by not enabling bus mastering on PCI bridges where it was not needed to boot.
- A more complete solution is described in an Intel public whitepaper using IOMMU based protection.
- An implementation will be in UDK2018.

Stack Guard, Heap Guard, and NULL Pointer Detection

- Phoenix proposed these capabilities in a 2012 Plugfest presentation
- We provided prototype/proof-of-concept implementations at that time
- We are pleased that these capabilities will be in the UDK2018

Happenings in NIST Guidelines
NIST 800-155 BIOS Integrity Measurement

- Draft guidelines published 2011
- Comments submitted years ago, no action from NIST
- Implementations pending final guidelines
- TCG submitted the largest set of comments
- The TCG PC Client Working Group has offered to assist NIST in developing final guidelines. The Server WG may also contribute
- Negotiations are in the late stages and work may begin soon
- Call to Action: Participate with TCG in developing the final guidelines, be aware of their implications, and be prepared to implement the platform firmware guidelines
- FYI, TCG might want to cooperatively work with UEFI

NIST 800-193 Platform Firmware Resiliency

• Describes requirements for firmware Protection, Detection of corruption and Recovery
• Lists requirements for maintenance of Roots and Chains of Trust in firmware (RoT, CoT)
• Provides “guidelines” for requirements to maintain these roots of trust in operation, during updates, when detecting corruption and during recovery
• Platform firmware will be required to meet the standards described in these guidelines
• Broader than 800-147. Includes Option ROMs and other firmware, not just “BIOS”
• Call to Action: Study these guidelines in detail and make sure your product will meet them, in all aspects (TCG is interested in this one too)

Questions?
Thanks for attending the Spring 2018 UEFI Plugfest

For more information on the UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

phoenix technologies