Firmware Security 101

The Fundamentals

Presented by UEFI Forum

Tuesday, July 24, 2018

Welcome & Introductions

Moderator: Michael Krau
Chair of the Industry Communications
Working Group (ICWG)
Member Company: Intel

Panelist: Tim Lewis
Member Company: Insyde

Panelist: Eric Johnson
Member Company: American Megatrends Inc.

Panelist: Dick Wilkins
Member Company: Phoenix
Technologies

Panelist: Vincent Zimmer
Member Company: Intel

Audience Poll: *What is your greatest area of concern with UEFI firmware security?*

Select best answer:

A. Maintaining trust

B. Updating firmware

C. Responding to possible exploits

D. Understanding dependencies

UEFI Forum & Security Overview

UEFI Forum Philosophy

- The UEFI community is broad across the computing ecosystem (IHV, IFV, OSVs, Silicon vendors, OEMs, ODMs, and other service and product companies)

- The Forum is focused on creating a cooperative environment for constructively embracing new technology and innovation in the system platform ecosystem and boot process

- The Forum supports the rights and needs of the entire ecosystem: vendors and customers

- The members of the UEFI community collaborate with each other to help provide important security information as well as best practices

- UEFI specification does not “lock” anyone to a single OS, processor, or specific implementation

Firmware As A Point of Attack

Recently there have been reports of Security problems in UEFI firmware

- Reports of exploits found in UEFI implementations
- The improved hardening of “traditional exploit” vectors (OSs and applications) has forced hackers to seek new vectors off attack
- A recent focus on system firmware as a target for hackers and malware
- The integral and inherent nature of firmware, making it an optimal target for hackers
- Security conferences with sessions on exploits and hacks against UEFI implementations

UEFI Firmware Specification

The UEFI Specification is the only current System Firmware plan with security features specified

- UEFI Secure Boot establishes a ‘root of trust’ from the very start of firmware execution
- UEFI Secure Boot can be used to maintain the ‘chain of trust’ through OS boot and application launch

UEFI Specification Security Features

- Capsule Update
- Secure Boot
- User Authentication
- And more…

Firmware Security Panel Discussion

Panel Discussion

- What are the main challenges with firmware security?
- How does each company account for security when they implement firmware?
- How does each company and the UEFI Forum respond to security issues reported to them?
- What are the security benefits of the UEFI specification?
- What are the dependencies of Secure Boot?
- Why should I report security issues to the UEFI Forum?

How Should the Industry Help?

“The whole is greater than the sum of all parts.”
--Aristotle

“Great discoveries and improvements invariably involve the cooperation of many minds.”
--Alexander Graham Bell

"Coming together is a beginning. Keeping together is progress. Working together is success."
--Henry Ford

The UEFI Security Response Team (USRT)

- The UEFI Security Response Team (USRT) is an active team within the UEFI
- The USRT provides a communications conduit between security researchers or others who may discover vulnerabilities and the UEFI community
- The USRT attempts to determine the scope of the vulnerability
- The USRT will also assist member companies in the coordination of responses to reported vulnerabilities
- For more information go to: www.uefi.org/security

Questions?

Thank you!

Join the UEFI Forum and become part of the solution:

- www.uefi.org/membership

Contact the UEFI Forum:

- admin@uefi.org

Contact the USRT:

- For more information go to: www.uefi.org/security
- Email a firmware security issue or vulnerability to: security@uefi.org