LABSCON

LABScon Replay | Breaking Firmware Trust From The Other Side: Exploiting Early Boot Phases (Pre-Efi)

LABSCON / DECEMBER 29, 2022

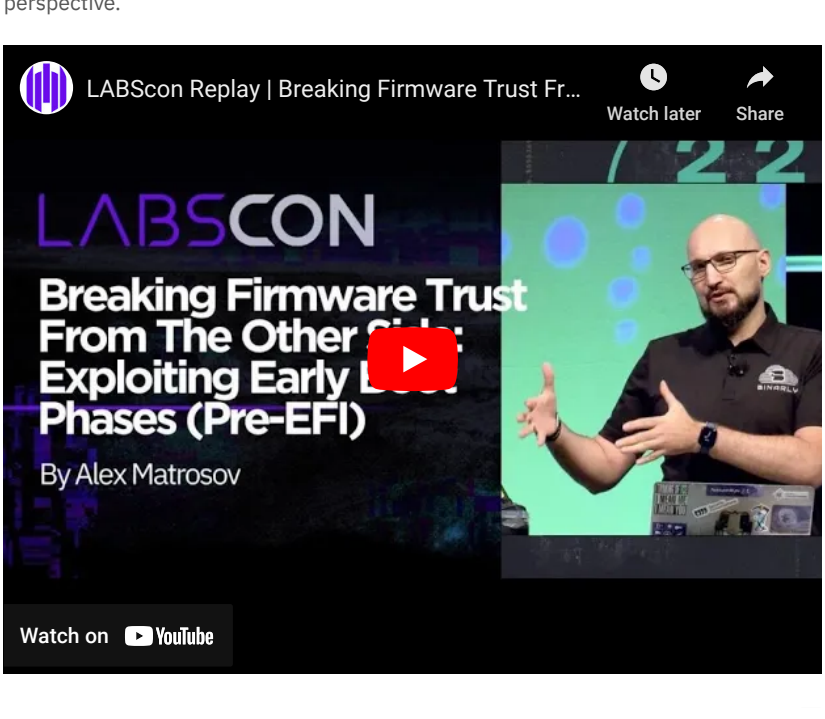
Vulnerabilities in System Management Mode (SMM) and more general UEFI applications/drivers (DXE) are receiving increased attention from security researchers. Over the last 12 months, the Binarly efiXplorer team disclosed 107 high-impact vulnerabilities related to SMM and DXE firmware components.

However, newer platforms have significantly increased the runtime mitigations in the UEFI firmware execution environment (including SMM), and the new Intel platform firmware runtime mitigations reshaped the attack surface for SMM/DXE with new Intel Hardware Shield technologies applied below-the-OS.

The complexity of the modern platform security features is growing every year. The general security promises of the platform consist of many different layers defining their own security boundaries. In many cases, these layers introduce inconsistencies in mitigation technologies and create room for breaking general security promises, allowing for successful attacks.

In this presentation, Alex Matrosov explores recent changes in the UEFI firmware security runtime using one of the most recent Intel CPUs as an example. The presentation covers the evolution of firmware mitigations in SMM/DXE on x86-based CPUs and a discussion about the new attacks on Intel Platform Properties Assessment Module (PPAM), which are often used in tandem with Intel SMI Transfer Monitor (STM).

These topics have never been publicly discussed from the offensive security research perspective.



Breaking Firmware Trust From The Other Side: Exploiting Early Boot Phases

Transcript

00:00:05 **Alex Matrosov**
I think after system internals, we need to dive deeper into firmware internals and we have a very interesting stuff today. We'll dive even deeper than just as system management. What we will be talking about the pre-EFI firmware and how actually that works and where is the breaking point and how actually it can be broken and what are the attack surfaces and of course, new vulnerabilities. All right.

00:00:32 I will probably just make a chart. So it's the Binarly research team which has been involved. Google remembers all my research better than me. You can just Google my name. All right.

00:00:43 So this is a short agenda for today. And I think we will start with some introduction and why this topics are important and then dive deeper into

SentinelOne

1.00x

00:00:00 00:20:53

About the Presenter

Alex Matrosov is CEO and co-founder of Binarly Inc., where he builds an AI-powered platform to protect devices against emerging firmware threats. Alex has more than two decades of experience with reverse engineering, advanced malware analysis, firmware security, and exploitation techniques. He served as Chief Offensive Security Researcher at Nvidia and Intel Security Center of Excellence (SeCoE).

About LABScon

This presentation was featured live at LABScon 2022, an immersive 3-day conference bringing together the world's top cybersecurity minds, hosted by SentinelOne's research arm, SentinelLabs.

UEFI

LABSCON

LABScon brings together the world's top cybersecurity minds to share cutting-edge research and push the envelope of threat landscape understanding.