Zero Trust in the Context of Firmware

"Firmware may well be the next endpoint battleground..."

—Gartner, Roadmap for Improving Endpoint Security, Peter Firstbrook, November 2020

Without a clear understanding of firmware security posture, any Zero Trust strategy is incomplete.

Everyone knows they need a Zero Trust strategy. But not many understand how Zero Trust strategies apply to the less visible parts of the network, namely hardware and its underlying firmware. Firmware is pervasive in every computing device: a typical laptop computer has more than a dozen internal components such as UEFI/BIOS system firmware, Trusted Platform Modules (TPM), peripheral devices, storage devices, or network interface cards. Each component runs millions of lines of code, developed by a myriad of vendors in a complex supply chain.

Four primary principles make up every Zero Trust strategy and firmware security applies uniquely to each of these principles:

PRINCIPLE 1: "Default Deny" in Firmware

InfoSec practitioners tend to think of the "Default deny" concept as an authentication issue, and in the broadest sense, it is. But we need to look past the act of "authenticating" an entity, whether user or device, using traditional authentication factors of Knowledge, Possession, or Inherence. If authentication means "corroboration of a claimed identity," then we must corroborate all the associated parts of that claimed identity, including, if applicable, the bare metal hardware, its various components, and the underlying, embedded firmware that instructs it on how to run and ensures it has not been tampered with. The principle of "default deny" suggests that firmware that is not correctly signed or certified should not be allowed to run, and should, in turn, prevent the device it serves from booting.

PRINCIPLE 2:
“Contextual Authentication” in Firmware

The concept of “contextual authentication” has a unique application with regard to the firmware. As the general description above states, “An authentication granted yesterday may not work today if the level of detected risks or vulnerabilities has changed.” In a firmware-centric example, if a device attempts to connect Systems assessing for device integrity will include hardware- and firmware-level assessment of not just vulnerabilities, but also anomalies and misconfigurations and it contains a firmware version that has recently been shown to be vulnerable or misconfigured, this authentication request should be denied.

A recent example of this sort of firmware vulnerability can be found in CVE-2019-3707 where multiple vulnerabilities were discovered in firmware supporting Dell systems and their ability to use Dell’s proprietary remote access capabilities. The practice of contextual authentication for devices suggests that a Dell device containing one of the affected firmware versions should be denied access to the network, even if it was allowed access the previous day.

PRINCIPLE 3:
“Granular Control” as it Relates to Firmware

It’s no longer enough to simply acknowledge, “every device has firmware.” In fact, every component of every device — from the ubiquitous Unified Extensible Firmware Interface found in nearly all computers to on-board memory and from networking components to video drivers — has its own firmware. Firmware instances are now nested within numerous integrated containers and it’s not uncommon for endpoints and servers to arrive into service with firmware files that number in the dozens. This deep firmware granularity must be addressed through an effective Zero Trust strategy.

PRINCIPLE 4:
“Dynamic and Real-Time” in the Context of Firmware

Creation, deployment, maintenance, and replacement of hardware has evolved to be a continuous rather than periodic exercise, and is now done in real-time. Virtual servers are spun up and down by the thousands and in a fraction of a second. This includes their firmware. Every device in every household, and every adjacent device in a business network, is dynamic, possibly ephemeral, and likely to be constantly changing. This includes their millions of lines of associated firmware. Static or infrequent inventories cannot secure and assure the integrity of these devices.

Firmware and the devices they support are not only foundational to all compute and networking systems, but a key piece of creating and executing Zero Trust strategies.