TRAPEZOID
Firmware Integrity Management

# Exploring the SolarWinds Hack

## *What Did the Bad Guys do Below the OS?*

By José E. González
CEO Trapezoid, Inc.
January 20, 2021

Traditional security tools provide zero visibility into areas below the OS and into the firmware.

Yet sophisticated attackers can easily access this level on any device through a backdoor and lie in wait for months undetected.

### What Traditional Cybersecurity Tools Monitor

- ✓ NETWORK
- ✓ CLOUD ORCHESTRATION
- ✓ APPLICATIONS
- ✓ OPERATING SYSTEM
- ✓ HYPERVISOR / VMs
- X FIRMWARE / BIOS

## The Inherent Weakness of Traditional Cybersecurity Tools

The SolarWinds Orion Network Management System (NMS) breach was the result of a critical supply chain attack that allowed a threat actor to get deep inside thousands of Orion NMS customers via a backdoor. The severity of this attack cannot be overstated, as a compromised NMS gives an attacker a golden perch on the network from where access is basically unlimited.

When an attack like this happens, organizations traditionally respond by first identifying and rectifying the situation, then try to determine exactly what the attacker did after gaining visibility into its devices using incident response data and forensics tools. Traditional approaches focus on four areas:

- **Network Traffic:** Allows organizations to see where the attackers are moving on the network. Sources include NetFlow and other network traffic analysis tools.
- **Memory:** Many malware tools run in the volatile memory of a system, existing tools can track this data.
- **Disk:** Disk forensics can establish a timeline of attacker activity after the fact.
- **Logs:** Logs generated by a system can provide traces of where the attacker has been and what they have done.

Unfortunately, this approach fails to uncover the entire attack surface. The reality is there is another layer of code where attackers can compromise networked devices that organizations have long ignored. This area lies below the Operating System ("OS") in the device firmware.

Sophisticated hackers like those who attacked SolarWinds, are increasingly developing and installing malicious code at the firmware level and exploiting existing firmware vulnerabilities not visible to traditional tools. And this is where modern cybersecurity tools need to evolve.

## Firmware Attacks Are Already Happening

For those unfamiliar with attacks below the OS, consider the 2015 Ukraine power grid attack, which shut down and took off-line multiple substations for several hours and impacted hundreds of thousands of customers in the dead of winter while the power utility frantically tried to get the substations back online. Post-mortem analysis of this attack revealed that the attacker infiltrated the power utility's network and specific devices of interest (serial-to-ethernet converters or IP converters), that gave them access to the central control server that controlled the circuit breakers at remote substations.

The attacker created modified firmware and downloaded it to the infiltrated IP converters, knowing that they were designed to shut down communications to the circuit breakers if they were tripped. All of this work was done well ahead of the attack date and went undetected for months. On the day of the attack, the attacker simply tripped the breakers, knowing that the modified IP converter firmware they installed would prohibit any control server attempts to remotely restart the breakers.

The Ukraine power grid attack is a perfect example of just how devastating a firmware attack can be from an adversary with nefarious inclinations.

Using this example to consider the SolarWinds hack and considering that most organizations are unable to see attacks below the OS, it is impossible to know whether specific devices of interest were compromised or exploited at the firmware layer. And this makes it difficult to quantify the true impact of the SolarWinds attack.

One thing is for certain: organizations without a robust sensing capability below the OS are unable to discover and address malicious implants below the OS. This leaves the backdoor wide open for hackers to get in without detection and achieve persistence so they can reemerge weeks or months later, even after traditional incident response and restoration is supposedly complete.

## Examples of Recent Firmware Attacks

### 2015 Ukraine Power Grid Cyberattack

- Russian adversaries targeted industrial control devices, wrote malicious firmware and uploaded it
- Result: 6-hour heat and power outage across 30+ substations and months of manual rework to fix systems


### 2018 Meltdown/Spectre

- Every chip manufactured since 1995 is vulnerable
- Patches offer limited solutions and impact system performance

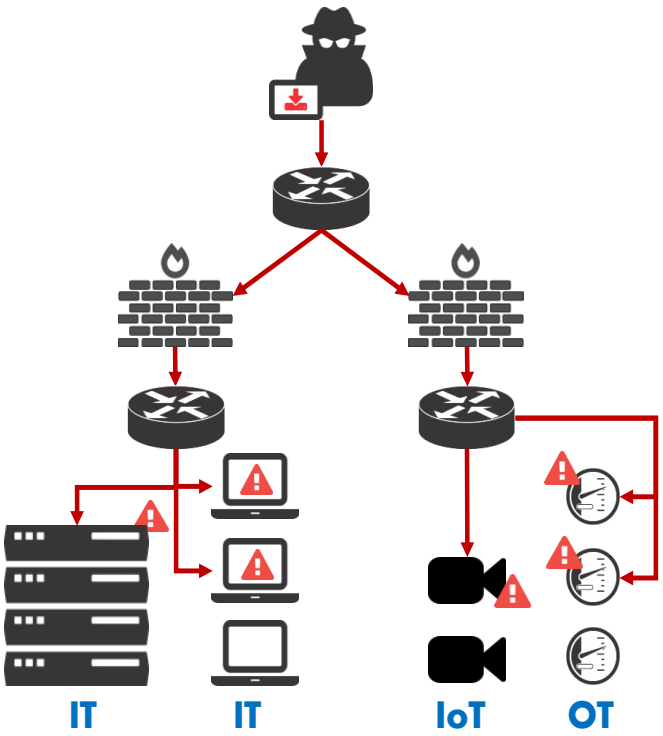
## NIST SP 800-53 Includes Controls for Firmware Integrity

The National Institute of Standards and Technology (NIST) provides technical leadership for the nation's measurement and standards infrastructure. A major part of addressing vulnerabilities below the OS is already contemplated by NIST Special Publication (SP) 800-53 R5 *"Security and Privacy Controls for Information Systems and Organizations."* This publication provides a catalog of security and privacy controls for information systems, including best practice controls for configuration and continuous monitoring of platform firmware (e.g., SI-7 controls) for all devices within an organization.

As more devices become network-enabled, organizations need to apply these controls beyond Information Technology (IT) devices like servers and routers, to Operational Technology (OT) devices such as PLCs and SCADA devices, and to Internet of Things (IoT) devices such as Wi-Fi video cameras, smart TVs and even networked coffee pots. This can become an overwhelming task without the right tools.

*Multiple frameworks call for an integrity verification tool to detect unauthorized changes in firmware, including*
***NIST SP 800-53 R5***

**Breach Example**
**Firmware Payload or Vulnerability Exploit**




**Traditional Incident Response**

- Disk
- Network
- OS/Logs
- Memory

**Currently Monitored Code**

- UI
- Application
- OS/Hypervisor
- Firmware

## Introducing A New Model for Device Integrity

It is precisely the problem of needing to go beyond basic tracking of IT devices into OT devices and increasingly IoT devices, that Trapezoid has been working on since 2012. We have developed a powerful tool that provides organizations with visibility and monitoring of firmware and device integrity regardless of the device type. This tool extends the type of forensic data available to detect and quickly respond to incidents at any layer. We deliver this capability through the **Trapezoid Firmware Integrity Verification Engine (FIVE).** This tool allows customers to detect changes across four critical types of data lacking in the traditional approach. We call these the Trapezoid® Quadrants of Integrity:

**Hardware**

Detects any unauthorized change in the hardware of a device that can introduce malicious capabilities and be an indicator of compromise.

**Firmware**

Monitors any new firmware added or changes to existing firmware. Reviews existing firmware against known unpatched vulnerabilities.

**Configuration**

Analyzes systems for poor configuration, password settings or security settings that can allow an attacker to compromise the system.

**Operational Metrics**

Monitors changes in power, bandwidth, load, consumption and other operational metrics that can be the only indicators of a firmware-based attack. (Booting out of cycle, running hot, strange processing behaviors).

By enhancing the data available to security analysts with data from the Trapezoid Quadrants of Integrity, we can create a trust profile for a device that complements traditional security tools. More importantly, this allows us to abstract devices so that we can treat IT, OT and IoT devices consistently. While the type and amount of data exposed by a manufacturer of a high-end server will vary greatly from that of a Smart TV, Trapezoid FIVE can track specific attack vector data and monitor for unauthorized changes across all four quadrants for both.

As you consider the cybersecurity of your networked infrastructure in the post-SolarWinds hack era, you need to address vulnerabilities below the OS. If not, you will never know what is lurking in the basement.

***José E. González*** *is co-founder and CEO of Trapezoid, Inc., which offers solutions focused on continuous monitoring, detecting and responding to changes in device integrity due to firmware that is compromised either through unauthorized modification or newly discovered vulnerabilities. His LinkedIn profile can be viewed at https://www.linkedin.com/in/jegonzalez/. For more information contact Trapezoid at info@trapezoid.com.*