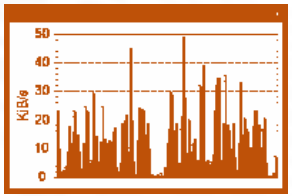
TRAPEZOID
Firmware Integrity Management

4 Ways to Assess Device Integrity

Close the Basement Door

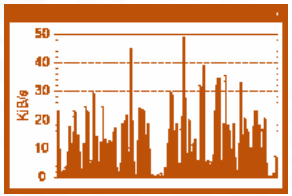
*US Patent Nos. 9,258,331 & 9,674,183; Others pending.

Typical Incident Response Requirements



Network Traffic

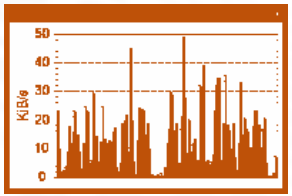
Typical Incident Response Requirements



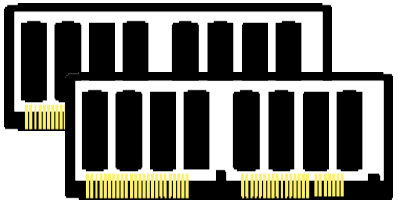
Network Traffic

Disk

Typical Incident Response Requirements



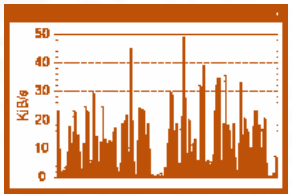
Network Traffic



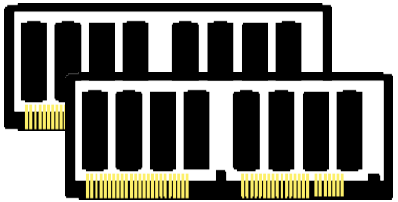
Memory

Disk

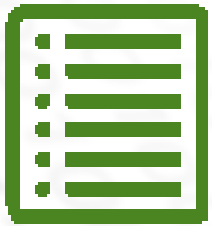
Typical Incident Response Requirements



Network Traffic



Memory



Logs & Events

Disk

What if the incident isn't there?

Firmware:

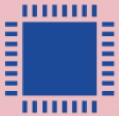
- programmable software stored in non-volatile memory on a device
- persists from boot to boot
- sits below the OS and driver layers
- infrequently updated
- usually physically part of the hardware (versus a hard drive)

What if the incident isn't there?

Firmware:

- programmable software stored in non-volatile memory on a device
- persists from boot to boot
- sits below the OS and driver layers
- infrequently updated
- usually physically part of the hardware (versus a hard drive)

You also can't forget about the hardware itself…..



Firmware Timeline High Level

1998- Chernobyl Virus

Firmware Timeline High Level

1998- Chernobyl Virus

2010- Supplier ships Malware-riddled replacement motherboards

Firmware Timeline High Level

1998- Chernobyl Virus

2014 Leak of
NSA ANT catalog

2010- Supplier ships Malware-riddled replacement motherboards

800-53Rev4 Makes Firmware Hard Requirement

Firmware Timeline High Level

1998- Chernobyl Virus

2014 Leak of
NSA ANT catalog

]HackingTeam[

2015Data breach shows firmware tools for offense

2010- Supplier ships Malware-riddled replacement motherboards

NIST

800-53Rev4 Makes Firmware Hard Requirement

Firmware Timeline High Level

1998- Chernobyl Virus

2014 Leak of
NSA ANT catalog

]HackingTeam[

2015Data breach shows firmware tools for offense

2010- Supplier ships Malware-riddled replacement motherboards

800-53Rev4 Makes Firmware Hard Requirement

2018 ESET finds Fancy Bear Firmware malware in wild

The Simple Truth

You can’t trust your software if you don’t trust your hardware.

Firmware is not visible to traditional tools

Why is Firmware an Attractive Target?

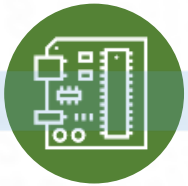
- **Persistence** – firmware can persist malware even after normal remediation actions.
- **Stealth** – sits below OS and traditional malware detection tools don't examine this layer.
- **System control** – If you control system firmware it can bypass any existing measures you put into place.

Firmware on many devices is vulnerable today but organizations do not know

Assessing a Device

Hardware changes can only occur via direct physical access to the device, which could afford a bad actor the opportunity to inject malicious firmware onto the device.

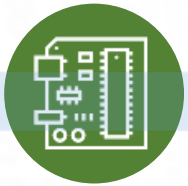
Hardware



Assessing a Device

Some devices may have methods to validate their firmware against the manufacturer's known-good measurements to attest to the integrity of the code.

Hardware

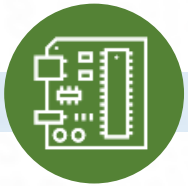


Firmware

Assessing a Device

Many devices ship with security settings turned off by default, which, if not changed, allows bad actors to take over the unsecured system and introduce malware firmware.

Hardware



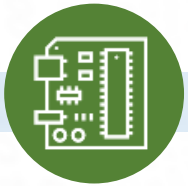
Firmware

Configuration

Assessing a Device

Unexpected variances in a device's behavior – e.g. power consumption, bandwidth usage, heat profile – may be indicators of compromise.

Hardware

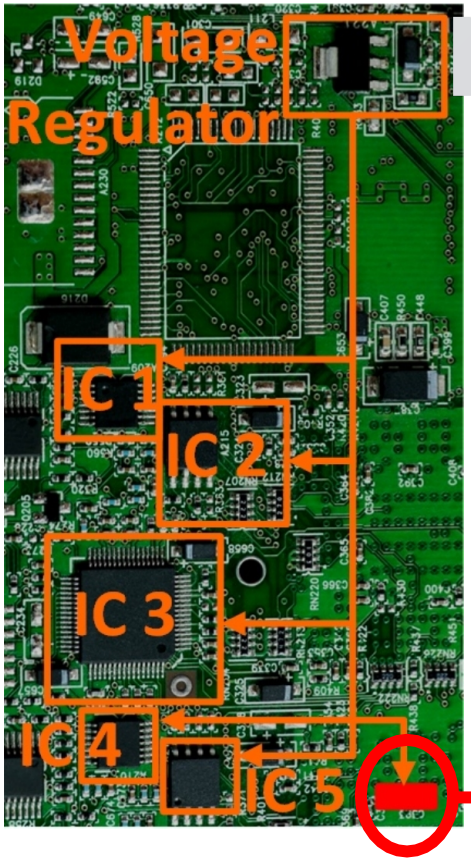


Firmware

Configuration

Operational Metrics

PCB Trust Verification



Potential Malicious IC

1. Create Models of Malicious Changes

2. Build Machine Learning (ML) based Classifier

3. Run ML Classifier on Reverse-engineered PCB Design

Trust Report

Source: https://makezine.com/2016/08/15/7-fatal-mistakes-avoid-printed-circuit-board-pcb-design/

Challenges Assessing Device Integrity

- What are manufacturers doing?
- How can you access the data?
- What is the quality and quantity of the data?
- How can you access the data?
- What is the shape of the data?
- How can you manage it at scale?

Time between capabilities and when OEM's and ISV's make use of them:
Trusted Execution Technology:
Mentioned pre 2005 as feature on some Intel platforms.

What can you do?

Leadership:

Make sure procurement is taking this into consideration.

Procurement:

Ask the manufacturers, OEM's and ISV's what they are doing in this space.

Ask what standards they are developing to?

Audit:

Understand your compliance requirements.

Organizations are starting to fail compliance audits.

(Hardware, Software, Firmware)

Operations:

Understand your inventory.

Some systems replaced because they cannot be secured.

TRAPEZOID
Firmware Integrity Management

Thank you.

Robert Rounsavall
Trapezoid
rrounsavall@Trapezoid.com