Supply Chain Security at the Hardware Level

Sophia d’Antoine & Ryan Speers
SANS Supply Chain Security Summit
River Loop Security (Program Analysis Lead)

**TL;DR:** specialty in low-level embedded: HW/FW/RF

- HW assessment/pen-testing
- Binary analysis on firmware through Win32
- Cryptographic design & review
- RF reverse engineering
- Security risk assessment
- Vulnerability disclosure response

Supply chain security assessment and evaluation

Pilot Security, Co-Founder

**TL;DR:** Automated analysis of embedded firmware for security vulns.
About this Talk

- Hardware Level Threats
- Discussed Techniques
  - Look at a few approaches for an attacker
  - What are the pros/cons on some of these, and relative difficulty
- Assessment Challenges
  - Some specific examples from our work in assessing these types of systems
- Helping Defenders

All discussions of “Discussed Techniques” and attacks are based only on publicly available data.
“The Big Hack”

How China used a tiny chip to infiltrate America’s top companies
“The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America’s technology supply chain, according to extensive interviews with government and corporate sources.”

“The chips had been inserted during the manufacturing process, two officials say, by operatives from a unit of the People’s Liberation Army.”

Operation ShadowHammer & ShadowPad

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

The Taiwan-based tech giant ASUS is believed to have pushed the malware to hundreds of thousands of customers through its trusted automatic software update tool after attackers compromised the company's server and used it to push the malware to machines.

By Kim Zetter
Mar 25 2019, 9:00am  Facebook  Tweet

Image: Shutterstock
Backdoored ASUS Live Updater executable

Original ASUS code section

Tiny patch of CRT function call

Payload Decryptor

Resource 136: EXE

Encrypted Payload

Remainder of ASUS updater tool code
(broken PE file)

Source: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World

ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide.

Kaspersky Lab experts have discovered a backdoor inserted by hundreds of large businesses around the world. When activated, the backdoor allows attackers to download further malicious modules or steal data. Kaspersky Lab has alerted NetSarang, the vendor of the affected software, and it has promptly removed the malicious code and released an update for customers.

Source: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
Hardware Level Threats
Narrowing our focus

DATA
APPLICATIONS
VIRTUAL MACHINE
OPERATING SYSTEM
VIRTUAL ENVIRONMENT
HYPervisor
FIRMWARE
HARDWARE
Narrowing our focus

- DATA
- APPLICATIONS
- VIRTUAL MACHINE
- OPERATING SYSTEM
- VIRTUAL ENVIRONMENT
- HYPervisor
- FIRMWARE
- HARDWARE
Narrowing our focus

Diagram showing layers of virtual components:
- Hardware
- Firmware
- Hypervisor
- Virtual Environment
- Operating System
- Virtual Machine
- Applications
- Data
General Categories of HW Threats

External

Physical peripherals
General Categories of HW Threats

PCB implants
Discussed Techniques
Regardless of if the alleged incident(s) happened, the claims shed light on what may be possible:

- **Additional microchip**: “Nested on the servers’ motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn’t part of the boards’ original design”
- **Grey or off-white in color**
- **Intercept CPU temporary memory**: “manipulated the core operating instructions [...] as small bits of the operating system were being stored in the board’s temporary memory en route to the server’s central processor”
- “could do all this because they were **connected to the baseboard management controller**”
- “Signal Conditioning Coupler with memory, processing, networking capabilities”
- **Altered operating system**
- **Embedded between PCB layers**: “were thin enough that they’d been **embedded between the layers of fiberglass**”
Regardless of if the alleged incident(s) happened, the claims shed light on what may be possible:

- **Network-related:**
  - “Signal Conditioning Coupler with memory, processing, networking capabilities”
  - Found via suspicious network activity
  - “downloaded firmware […] had been altered”
  - “The malware was on a network card driver”
  - “implant built into the server’s Ethernet connector”
  - “appeared on the network as two devices in one”
  - “Ethernet connector has metal sides instead of the usual plastic ones”
“[Company] offers Wafer Level Chip Scale Packaging (WLCSP), providing a solder interconnection directly between the device and end product’s motherboard”

https://amkor.com/packaging/wafer-level-packaging/wlcsp/
"A 3D package (System in Package, Chip Stack MCM, etc.) contains two or more chips (integrated circuits) stacked vertically so that they occupy less space and/or have greater connectivity... TSVs replace edge wiring by creating vertical connections through the body of the chips. The resulting package has no added length or width."

https://en.wikipedia.org/wiki/Through-silicon_via#3D_packages
Image CC-BY-SA Shmuel Csaba Otto Traian
WLCSP + TSV are useful, legitimate, technologies. But an attacker can use them.
“The Sandwich”

- **GPU**
  - Metalization layer

- **Silicon interposer**
  - Through-Silicon Vias (TSVs), μBumps
  - DRAM dice
  - HBM controller die

- **Package substrate**

- **Package substrate**

- **Graphics card**
  - Multi-layer Printed Circuit Board (PCB), up to 8 layers
  - PCI Express
  - Electrical current
  - Display connectors
On a Board?

Can be legitimate: e.g.: move a component from one pad to another

Availability of different package sizes

Slight difference in board design - stability, specs, etc.

Inside a Package?

Can be legitimate: e.g.: flash memory package
- Sold but has different configurations, or different memory internally
- Wirebond down differently

Image credit bunnie Huang @20:40 of https://www.youtube.com/watch?v=RqQhWitJ1As
Trammell Hudson’s example of replacing a 0603 passive with an implant on a motherboard SPI flash to BMC link is just one example...

Well documented and explained on his blog (https://trmm.net/Modchips)
Proof of concept silicon attack at University of Michigan\(^1\)

- Extremely small, likely detectable only with detailed microscopy on the decapped chip
- Change that is done inside a legitimate processor at foundry time

“If any single contractor attempts to modify the designs, the manufacturing process is structured so that those alterations would not match the other design elements in the manufacturing process.”

- Supermicro CEO
Lower cost counterfeit or e-waste parts end up in things

These aren’t a security issue *per se* but is one of the largest risks
But sometimes could be security -- e.g. FTDI chips, BMC, etc

[Image of FTDI chips with a checkmark and an X]
Lower cost counterfeit or e-waste parts end up in things

In some ways it helps incentivize a company to pay attention to the supply chain for a company to have representatives to check / watch in factory but this doesn’t guard against an advanced attacker...
Tech for making fake/forgeries of chips can lower the cost to be able to do HW implants

bunnie’s BlueHat IL numbers:
- low-10ks for wirebonded implant
- mid-100ks for a WLCSP implant
Detection vs Execution

- Easy
  - Add Component
  - Add IC in Package
- Hard
  - Substitute Component
  - Substitute IC in Package

- Easy
  - Mask Edit
  - Hard IP Edit
  - Netlist Edit

Credit to Bunnie Huang’s slide/talk image from https://prog.world/supply-chain-security-if-i-were-a-nation-state/
Challenges of Assessments
1. Assess Security Hygiene
   ○ Poor security practices mean there is no need for a backdoor
2. Assess Supply Chain Risk
   ○ Where would it be most beneficial to the adversary to insert a backdoor?
   ○ How would they likely do it?
3. Focus on those areas
   ○ In code
   ○ In build system
   ○ In programming
   ○ In hardware

“These findings are about basic engineering competence and cyber security hygiene that give rise to vulnerabilities that are capable of being exploited by a range of actors…”

UK, NCSC Report on Huawei
Supply Chain Assessment Points

Software
1. Security Hygiene
2. Backdoors in Code
3. Compilation Time
4. Production Line
5. Program & Provision
6. Reverse Engineering
7. Distribution Channel
8. Installed

Hardware
1. Component Design
2. Hardware Integration
9. Build System
Applying this to Supermicro Case Study
“Pure HW” Stages

- Claims majority of R&D in house
- Offers contract manufacturing and supply chain efficiency
- Huge producer for companies in the US and World
  - ~800 customers total, majority are distributors
  - 4,950 SKU’s, 1,200 server systems, 600 serverboards

Rough outline based on public filings
- Ablecom Technologies
  - Offers warehousing & coordination of contract manufacturing
  - Private Taiwanese company
    - Run by brother of Supermicro CEO
  - 15%+ of cost of sales
  - Accurately forecasts and warehouse parts from various contract manufacturers to be able to create their products

Rough outline based on public data
1. Supermicro designs
2. Ablemicro coordinates manufacturing with contract manufacturers
3. Contract manufacturer produces and ships to Ablecom for warehousing
4. Ship to Supermicro facility (San Jose, Netherlands, or Taiwan) for assembly
5. Distribution to distributor, OEM, or customer

Rough outline based on public filings
“Gray or off-white in color, they looked more like signal conditioning couplers, another common motherboard component, than microchips, and they were unlikely to be detectable without specialized equipment.”


Inspecting for something exactly matching that appearance is likely to be ineffective.

Our Typical Methods:
Spend the time to understand the supply chain, motivations, risk factors, and then select where to focus inspection.
Methods - Hands-On

- Follow traces
- Reverse for net list
- Visual inspection - hands-on and images
- Electrical testing - on vs off board
-...

Prepared by River Loop Security. Confidential
“The Add” - Inside an IC

Finding it with X-rays?
- Can’t see on image top-down on PCB
- Can’t image side on PCB
- Can’t see well on image top-down off PCB
- Likely can see on side-image off PCB

NOTE: Image here shows a legitimate multi-stacked chip!
X-Ray to Identify Passive vs Active

- Labor intensive
- Requires skilled evaluators
- Removal of components
  ...DESTRUCTIVE

We can’t show our x-ray images from past assessments here, but …
  ... they are much more complex than this example
In one assessment we did:

- ~76 presumed-active components per motherboard
- plus ~12 on network card
- plus other cards
- each board visually inspected with many macro lens photos
- ~500 xray images per PCB for overview
- ~450 xray images per PCB for communications port detail

Xray analysis focused on mounting elements (wires, bonds, balls, discontinued tracks)

Takes significant time and experience, e.g.:

- Each inspector conducting x-ray analysis had 10 to 15 years of experience in electronics, failure analysis, and/or electronics x-ray, electron microscopy, and depackaging
- Each image analyzed twice
Trammell Hudson’s example of replacing a 0603 passive with an implant on a motherboard SPI flash to BMC link is just one example...

Well documented and explained on his blog (https://trmm.net/Modchips)

Images from https://trmm.net/Modchips
CC-BY Trammell Hudson
The Big Hack: The Software Side of China's Supply Chain Attack

- It wasn’t just hardware. An online portal for firmware updates hid and distributed malware.

By Jordan Robertson and Michael Riley
From a **Hardware** Validation perspective...

...Hardware backdoors often don’t operate alone...

(take for example Trammell’s POC - uses HW to set config on boot)
“Work to validate them by HCSEC is still ongoing but has already exposed wider flaws in the underlying build process which need to be rectified before binary equivalence can be demonstrated at scale... Unless and until this is done it is not possible to be confident that the source code examined by HCSEC is precisely that used to build the binaries running in the UK networks.”

- UK HCSEC 2019.03 (emphasis added)
<table>
<thead>
<tr>
<th>In Source Code</th>
<th>In Compiled Firmware</th>
<th>In Chips</th>
</tr>
</thead>
<tbody>
<tr>
<td>An attacker could hide via a subtle logic bug; require multiple preconditions</td>
<td>If a reproducible, signed build chain using trusted components isn’t available...</td>
<td>When reading from the chips, differences 0x00 vs 0xFF for memory vs firmware</td>
</tr>
<tr>
<td>Very difficult to audit for -- especially when the general code quality is poor.</td>
<td>Reverse engineer and do program analysis to align <em>all</em> parts of binary firmware to code -- while dealing with compiler optimizations/etc</td>
<td>Wear leveling, old versions not cleared, etc.</td>
</tr>
</tbody>
</table>
We don’t have time to cover all the aspects....

- Radio Frequency (RF)
- Network
- ...

Prepared by River Loop Security. Confidential
Possible Solutions
Questions

team@riverloopsecurity.com