Test. Tactics. Training.

TITLE: Hardware Exploits: Can you trust your devices?

DATE: 7 March 2018

Author: Christina Witt
Author Office: Information Assurance Documentation & Validation
Author Phone: 661-277-5148

Approved for public release; distribution is unlimited.
412TW-PA No.: 18095

Agenda

- **Introduction: Christina Witt, CISSP**
- **Hardware Exploits**
- **Supply Chain Security**

Hardware Exploits

Intel ME

- Intel Management Engine (aka Intel ME)
  - Contains an Intel Active Management Technology (AMT) which is the heart of Intel ME
  - Runs closed source, proprietary firmware
  - Access at the lowest level
  - Runs on standby power
  - Full network device access with the ability to intercept network traffic without CPU's knowledge
  - Has its own IP and MAC address to handle everything
  - Remains functional in the background even if the system is off

Intel ME (cont.)

- Installed not just on enterprise or server applications since 2008-2009
  - Found in devices with Intel Core vPro processor family including Intel Core i3, i5, i7, and Intel Xeon processor E3-1200 product family
- Uses compression and encoding to thwart reverse engineering
- Intel ME firmware is throughout the hardware on the system

Why is Intel ME a Concern?

- Does not allow end users to monitor for activities of malicious hardware components
- End users have no control over the access Intel ME has due to proprietary firmware
- AMD also has similar firmware which extends concern beyond Intel systems
- New government systems cannot turn it off either
- Vulnerabilities already found

Is There A Solution?

- This is a risk built in by Intel and AMD chipsets with proprietary, closed source OS
- Disable AMT
- Do not install LMS. If installed, uninstall it.
- Update ACAS Plugins
  - Ensure plugins are properly configured for credentialed scan
  - Plugin 97999 – Intel ME Authentication Bypass. This requires an update to the default port scanning preferences to probe ports 16992, 16993, and 623 in addition to the default ports.

Hardware Security Modules (HSM)

- **What is a Hardware Security Module?**
  - A special “trusted” network computer performing a variety of cryptographic operations: key management, key exchange, encryption etc.
  - An HSM is trusted because it:
    - Is built on top of specialized hardware.
    - Has a security-focused OS.
    - Has limited access via a network interface that is strictly controlled by internal rules.
    - Validated to Common Criteria EAL 4+ & FIPS 140
    - Actively hides and protects cryptographic material.
    - Tamper-proof, tamper-resistant, and have tamper-response

HSM Concerns

- **6 Steps of the HSM Private Key Lifecycle:**
  - **Someone designs IC**
  - **IC is fabricated**
  - **IC is delivered to hardware vendor**
  - **Vendor loads firmware & assembles device**
  - **Device is sent to customer**
  - **Customer generates and stores keys on the device**
- **There have been cases where the vulnerabilities of HSMs have been exposed within the first four steps. The actual security of the device has been completely broken down or made nonexistent during this time.**
- **HSMs only protect the last two steps of the private key lifecycle.**

HSM Solution

- **DEFCON Speaker Vasillios Mavroudis's ("Trojan Tolerant Hardware: Supply Chain Security in Practice") ingredients for a solution are:**
  - **Independent fabrication where fabrication is done in different facilities and their supply chains do not overlap.**
  - **Hardware must be programmable**
  - **Affordable**
  - **COTS is a bonus**

HSM Solution (cont)

- ***Vasillios Mavroudis's* final ingredient:**
- **For cryptographic protocols, no single chip has the private key, but rather that private key is sectioned out to the various chips. To use that private key, a designated number of chips must send out their piece of the key to complete the private key. None of the chips knows which part of the key the other chip has thus making it harder for a compromised HSM to discover the private key and decrypt confidential information.**

Supply Chain Security

Supply Chain Security

- University of Michigan Study called A2: Analog Malicious Hardware
  - Creates distrust at the manufacturer level
  - One employee can backdoor a chip at the fabrication center
- FLUXBABBITT created by the NSA is a piece of hardware built for one specific server that is implanted during shipment

Hardware Exploit Concerns

- **Enemy Nation States can backdoor a product through manufacturing depending on the situation but attacks are generally done at the shipping state of delivering a product by switching additional components.**
  - **CPUs**
  - **Chipsets**
  - **Network interface cards**
  - **ROM**

Government-Level Adversaries

- Have deep access to fabrication facilities
- Can intercept the products in shipping
- Use sophisticated techniques
- Nation State backdoors and Trojans are hard to detect
- Abilities are highly classified

Conclusion

My Thoughts

- **Social engineering, hardware exploits, and IoT exploits can be used in tandem for an attacker to gain enough intel that achieves their goals**
- **Education, training, and awareness can help deter confidential information from getting into the hands of a persistent adversary**

PRESENTATION FINISHED
...ANY QUESTIONS?
makeameme.org