Trusted Computing Technology and Government Implants

TrustyCon 2014
Steve Weis
**Warning:** This talk contains leaked US government classified material. Be aware of your employers’ policy.
Intro

• **Me:** Cryptographer, Co-founder & CTO PrivateCore, Google 2-factor, Keyczar, saweis.net, @sweis

• **Today’s talk:**
  
  • Snapshot of NSA ANT hardware, firmware, & software implants
  
  • “Trusted Computing”: What is it? Can it help? Can we trust it?
  
  • Defensive technologies on the horizon
Can you spot the implants?
NSA ANT

Shopping for Spy Gear: Catalog Advertises NSA Toolbox
By Jacob Appelbaum, Judith Horchert and Christian Stöcker

NSA Hackers Get the ‘Ungettable’ With Rich Catalog of Custom Tools
BY KIM ZETTER 12.30.13  4:11 PM

N.S.A. Devises Radio Pathway Into Computers
By DAVID E. SANGER and THOM SHANKER  JAN. 14, 2014

https://nsa-observer.laquadrature.net/
System Taxonomy Recap

- **Software**: Hypervisor, Operating System, Applications
- **Firmware**: BIOS, SMM, Option ROMs, SINIT ACMs
- **Hardware**: Processor, Memory, Storage, Devices, Buses
(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell PowerEdge servers by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to gain periodic execution while the Operating System loads.

Through remote access or interdiction, ARKSTREAM is used to reflash the BIOS on a target machine to implant DEITYBOUNCE and its payload (the implant installer). Implantation via interdiction may be accomplished by non-technical operator though use of a USB thumb drive. Once implanted, DEITYBOUNCE’s frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

06/20/08
Status: Released / Deployed. Ready for Immediate Delivery
Unit Cost: $0
Why attack BIOS and SMM?

- **Basic I/O System (BIOS):** Persistent firmware that runs first before the OS.

- **System Management Mode (SMM):**
  Special mode of operation that runs with highest privileges, which is installed by BIOS and invisible to OS.
GOURMETTROUGH

ANT Product Data

(TS//SI//REL) GOURMETTROUGH is a user configurable persistence implant for certain Juniper firewalls. It persists DNT’s BANANAGLEE implant across reboots and OS upgrades. For some platforms, it supports a minimal implant with beaconing for OS’s unsupported by BANANAGLEE.

06/24/08

Status: GOURMETTROUGH is on the shelf and has been deployed on many target platforms. It supports nsg5i, nsg50, ns25, isg1000 (limited). Soon: ssg140, ssg5, ssg20

Unit Cost: $0
(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

06/20/08
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

(TS//SI//REL) IRATEMONK Extended Concept of Operations
(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

(TS//SI//REL) Through interdiction, IRONCHEF, a software CNE implant and the hardware implant are installed onto the system. If the software CNE implant is removed from the target machine, IRONCHEF is used to access the machine, determine the reason for removal of the software, and then reinstall the software from a listening post to the target system.

07/14/08

Status: Ready for Immediate Delivery  Unit Cost: $0
COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

CM-I will provide air-gap bridging, software persistence capability, “in-field” re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAIGHTBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

Status: Availability – January 2009  
Unit Cost: 50 units: $1,015K
GINSU
ANT Product Data

(TS//SI//REL) GINSU provides software application persistence for the CNE implant, KONGUR, on target systems with the PCI bus hardware implant, BULLDOZER.

(TS//SI//REL) This technique supports any desktop PC system that contains at least one PCI connector (for BULLDOZER installation) and Microsoft Windows 9x, 2000, 2003, XP, or Vista.

(TS//SI//REL) Through interdiction, BULLDOZER is installed in the target system as a PCI bus hardware implant. After fielding, if KONGUR is removed from the system as a result of an operating system upgrade or reinstall, GINSU can be set to trigger on the next reboot of the system to restore the software implant.

06/20/08
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0
Do-it-Yourself Implants
Can you spot the implant?

- PCI attack device
- Implemented with off-the-shelf hardware
- Boots independently of host
- Exfiltrates data over the network
Can you spot the implant?

- Non-volatile RAM (NV-RAM)
- RAM contents are saved to flash memory on power loss.
- Attackers can capture crypto keys from preserved memory contents
- Several non-volatile memory technologies are in the pipeline
Trusted Computing

Ensure _____’s software is running on _____’s computer.
Trusted Computing for DRM

Ensure a content owner’s software is running on your computer.
Trusted Computing for You
Ensure your software is running on your computer.
Trusted Platform Module

The Coming Civil War on General Purpose Computing:
“A TPM is a nub of stable certainty: If it's there, it can reliably inform you about the code on your computer.”

- Cory Doctorow

- Public-key encryption and signatures
- Random number generation
- Persistent key storage
- Special “Platform Configuration Registers” (PCRs)
Trusted Execution Technology

Firmware and software needed to boot

- BIOS
- Option ROMs
- Platform Config
- Kernel
- SINIT
- OS Config

Remote Attest

TPM

Measure

CPU
Suspension of Disbelief

• What about physical attacks and hardware implants?
• Why do we trust the TPM? Where did it come from?
• Why do we trust the CPU for that matter?
Attack Vectors

Provenance
- BIOS
- Option ROMs
- Platform Config
- SINIT
- Kernel
- OS Config

Forge?
Overflow

Remote Attest
- Hash Collision?
- Extract Keys
- TPM
- Spoof Bus
- Paperclip
- CPU

Spoof CPU

Past
Hypothetical
Current
Where does this leave us?

• State-sponsored actors can circumvent trusted computing.

• Trusted computing still offers protection, although we ultimately have to trust the CPU and TPM.

• In the next 1-3 years: New hardware and platform security features

• Beyond: Practical applications of cryptographic protocols for security computation, e.g. fully homomorphic encryption.
Upcoming Technologies
Software Guard Extensions (SGX)

- Secure “enclaves” protected from other code.
- Enclaves are attested and won’t run if modified.
- Enclaves are backed by fully-encrypted memory.
- Potentially could make DRM hard to circumvent.
Enhanced Privacy ID (EPID)

- Provides ability for CPU to anonymously sign data.
- Could authenticate CPUs as real, without leaking identity.
- Caveat: Rooted in globally unique key material in CPU hardware.
Trusted Platform Module 2.0

- TPM 1.2 is deprecated and banned in several countries.
- TPM 2.0
  - More algorithms and functionality
  - Support for alternate cryptographic suites
  - Better management
  - Easier on-boarding
Summary

• NSA ANT implants target software, firmware, and hardware.

• Trusted computing helps against firmware and software attacks, but not against state sponsors.

• New technologies like SGX and EPID can work for us or against us.
Thank you!