Itzik Kotler | April 2011

Let Me Stuxnet You

Itzik Kotler
CTO, Security Art

Goodbye World!

- Stuxnet and Cyber Warfare are exploiting the *(it's complicated)* relationship between Software and Hardware to cause damage and sabotage!
- Today it's a country that seeks to destroy another nation and tomorrow it's a commercial company that seeks to make a rival company go out of business. An act of Industrial Cyber Warfare.

Can Software Damage Hardware? Yes!

- Software controls hardware, and it can make it perform damaging operation
- Software can damage another software that runs or operates an hardware
- Software controls hardware, and it can make it perform operation that will be damaging to another hardware

Industrial Cyber Warfare Attack?

- Cyber Warfare is not limited to, or designed exclusively for nations or critical infrastructures
- A successfully delivered Industrial Cyber Warfare attack causes financial loss, operation loss, or both to the attacked company!
- Industrial Cyber Warfare is Logic Bombs, Permanent Denial-of-Service, APT and more

Meet Permanent Denial-of-Service

- Permanent Denial-of-Service is an attack that damages hardware so badly that it requires replacement or reinstallation of hardware.
- The damage potential is on a grand scale, almost anything and everything is controlled by software that can be modified or attacked

Industrial Cyber Warfare: Why & Who?

- Industrial Espionage
  - Rival Companies
  - Foreign Countries
- Terrorism
  - Political/Social Agenda
  - Revenge
- Blackmailing
  - Greed, Power and etc.

Permanent Denial-of-Service 101

- **Phlashing**:
  - Overwriting the firmware of the component and make it useless (i.e. “Bricked”)
- **Overclocking**:
  - Increasing the working frequency of the component and make it unstable and overheat

Permanent Denial-of-Service (Cont.)

- **Overvolting**:
  - Increasing the input voltage of the component and “zap” it or cause it to overheat
- **Overusing**:
  - Repetitively using a mechanical feature of the component and cause it to wear quicker

Permanent Denial-of-Service (Cont.)

- **Power Cycling**
  - Repetitively turn on and off the power supply to the component and cause it to wear quicker (due to temperature flection and spikes)

Local Attacks

Does anyone smell smoke?

Computer Fans

- Not a target, per se.
- Disabling or slowing down the fan RPM speed can result in increased temperature
- Lengthy exposure to high temperature (due to lack of cooling) can lead to Electromigration that in turn will cause a Permanent Denial-of-Service

CPU

- Overheating due to Stressing
- Overheating due to Overclocking
- Overheating due to Overvolting
- Overheating due to (always on) P0 @ APM/ACAPI
- Bricking due to Phlashing (via Microcode Flashing)

CPU: Infinite Loop

x86 Assembly Code:

```
jmp short 0x0
```

Description:

Infinite loop that jump to self

CPU: Microcode Flashing

- Not your typical firmware update
- Microcode goes into the processor, providing a slightly higher level or more complex commands based on the processor's basic ("hard-wired") commands
- Microprogramming can be used to abuse or to damage the microprogram within the processor

RAM

- Overheating due to Overclocking
- Overheating due to Overvolting
- Burnout due to Overvolting

GPU (Graphics Processing Unit)

- Overheating due to Overclocking
- Overheating due to Overvolting
- Bricking due to Phlashing
  - Utilities (e.g. nvflash, NiBiTor, etc.)

Hard disk drive

- Traditional (i.e. Mechanical)
  - Overheating due to Excessive Write & Read
  - Wearing out due to Excessive Head Parking
  - Bricking due to Phlashing
- Solid-state drive
  - Wearing out due to Excessive Write

Hard Drive: Pseudo Format Attack

Command:

```
while true; do dd if=/dev/xxx of=/dev/xxx conv=notrunc; done
```

Description:

Infinite loop of read and write requests to disk

Hard Drive: Spindown Attack

Commands:

```
hdparm –S 1 /dev/xxx

while true;  sleep 60; dd if=/dev/random of=foobar count=1; done
```

Description:

Sets disk spindown after 1 minute of inactivity and goes into infinite loop of write requests to disk with 1 minute of sleeping in-between

BIOS: Bricking/Firmware Flashing

- Bricking due to Phlashing

Rouge BIOS Firmware as Platform

- Allows automation of:
  - Overclocking of CPU, RAM and etc.
  - Overvolting of CPU, RAM and etc.
  - Power Cycling (of the whole System)
- Can include a “Self-destruct” function

CD-ROM/DVD-ROM

- Wearing out due to Overusing the drive tray
- Bricking due to Phlashing

CD-ROM: Mechanical Part Attack

Code:

```
while true; do eject; eject –t; done
```

Description:

Infinite loop that opens and closes the CD-ROM tray

Memory Wear

- Flash memory has a finite number of program-erase cycles (aka. P/E cycles).
- Most commercially available Flash products are guaranteed to withstand around 100,000 P/E cycles, before the wear begins to deteriorate the integrity of the storage
- Popular products that are based on, or using Flash memory: USB Disk On Keys, Solid-state Drives, Thin Clients and Routers and more.

Flash: Memory Wear Attack

Code:

```
dd if=/dev/urandom of=/dev/xxx
```

Description:

Infinite loop that excessively writes pseudo-random to a flash memory

NIC (Network Interface Card)

- Bricking due to Phlashing

NIC: TCP Offload Engine

- TCP Offload Engine or TOE is a technology used in network interface cards (NIC) to offload processing of the entire TCP/IP stack to the network controller.
- TOE is primarily used with high-speed network interfaces, such as gigabit Ethernet and 10 Gigabit Ethernet
- TOE is implemented in hardware so patches must be applied to the TOE firmware

CRT Monitor:

- There are problems at scan rates which exceed the monitor's specifications (low or high). Some monitors can blow if given a too low scan rate or an absent or corrupted signal input.

XFree86 Screen Configuration:

```
HorizSync    28.0 - 78.0 # Warning: This may fry very old Monitors
HorizSync    28.0 - 96.0 # Warning: This may fry old Monitors
```

(taken from a real life, XFree86Config file)

Floppy Drive:

- Wearing out due to Excessive Head Rotation
  - On some floppy drives there are no validity checking on sector/track values, and so the floppy head might get hit repetitively against the stopper (See: NYB Virus)

Legacy: Motorola 6800 & 6809

- Motorola 6800 was a 8-bit microprocessor and was part of M6800 Microcomputer System
- The Motorola 6800 and 6809 can damage the computer's bus lines by the instruction 'HCF' (Halt, then Catch Fire).
- HCF successively toggles each of the bus lines, but it does it so fast that it can damage them. It was intended for manufacturer testing.

Summary

- Computer Fans
- CPU
- GPU
- RAM
- Hard Drives
- BIOS
- CD-ROM/DVD-ROM
- External Storage (e.g. Disk On Key)
- Network Cards
- CRT Monitor (Legacy)
- Floppy Disk (Legacy)
- Non-x86 Chip

Itzik Kotler | April 2011

www.security-art.com

Remote Attacks

The long arm of the Permanent Denial-of-Service

Going above and beyond traditional security

Firmware Updates via Web

- Network-attached Storage (NAS) Appliances
- Network Appliances (e.g. Wi-Fi Access Points)
- DSL/ADSL Cable Modems
- Computer Peripherals (e.g. KVM)
- Voice Over IP (VoIP) Phones
- And more …

Open Questions

- How this affects Cloud and Virtualized System?

Countermeasures?

- Hardware:
  - Over-clocking Protection
  - Over-voltage Protection
  - Over-temperature Protection
- Software:
  - Digitally signed Firmware Binaries & Updates

Thanks!

Questions are guaranteed in life; Answers aren't.

mailto: itzik.kotler@security-art.com