Internet of Things meets Hardware Cybersecurity

Serge Leef

Vice President and General Manager

- New Ventures
- System Level Engineering Division
IoT: Emergence of Intelligent Systems

- **Intelligent Systems / Internet of Things**
  - 75B Devices will be connected by 2020 (Morgan Stanley)
  - Execute native or cloud-based applications
  - Data collection & analytics
  - Explosive growth potential

- **Internet of Things**
  - Uniquely identified “things”
  - Machine-to-machine communication
  - Cloud infrastructure
  - Cyber-physical systems

- **Edge-node design**
  - Electronics, Controls, Software
  - Multi-physics, Communications
IoT Projected Market Size Generates Excitement

INTERNET OF THINGS

Cisco
$14.4 Trillion

IDC
$8.9 Trillion

Machina Research
$4.5 Trillion

Gartner Research
$1.9 Trillion

Infosys
$300 Billion

to

$300 Billion

to

$14.4 Trillion
Embedded systems moving into IoT world

- Set-top Box (2000)
  - Application: Content access UI
  - Middleware: Linux API
  - Hardware: Linux, HAL, Memory, CPU, Ethernet

- Smart Phone (2010)
  - Application: Mobile garage control app
  - Middleware: MobileOS API
  - Hardware: Mobile OS, Memory, App, WiFi, CPU, Actuators

- Garage Opener (2013)
  - Application: Private interface
  - Middleware: Private interface
  - Hardware: Internet, WiFi, CPU, Sensors, Actuators

- Office Hub (2016)
  - Application: Central Node
  - Middleware: Standard IoT Web API
  - Hardware: Internet, Edge node, CPU, Printer/scanner, Temp control

- Appliance (2017)
  - Application: QR scanner
  - Middleware: Standard IoT Web API
  - Hardware: Internet, HD screen, QR scanner
We used to believe that hardware is the “Root of Trust”, but... not anymore

- Social Engineering (Phishing/bating) - 1 - 100
- Malware / Macros (Information harvesting) - 10,000 – 100,000
- Viruses/ Trojans (Hijacking, DDoS, etc...) - ~100 Million
- IoT - ~100 Billion

We used to believe that hardware is the “Root of Trust”, but... not anymore
IoT World is Already Under Attack

Proofpoint Research: Internet of Things (IoT) Cyber Attack Security

In January 2014, Proofpoint researchers discovered proof of a much-theorized but never before seen Internet of Things (IoT) cyber-attack. Proofpoint has observed what we believe to be an industry first of devices, including some home appliances (TV’s, a refrigerator), sending malicious email spam.

As our researchers were analyzing email threats, they observed a recent cyber attack campaign where more than 25 percent of the malicious email (over 750,000 messages) came from devices that were not conventional laptop or desktop computers, but rather members of the Internet of Things: a “Thingfot-net”.

Specifically, researchers observed a series of cyber attack campaigns:

- From Dec 23rd through Jan 6th
- Three campaigns per day
- Approximately 100 emails per campaign
- Over 45th unique IP addresses, over 100k were from IoT devices

A more detailed examination suggested that while the majority of malware was initiated by “expected” IoT devices such as compromised home-networking devices (routers, NAS), there was a significant percentage of attack mail coming from other non-traditional sources, such as connected multimedia centers, televisions and at least one refrigerator.

Additionally, observing the devices:

- A vast number of the devices are running embedded Linux servers (usually busybox)
- Some use mini-httpd, some apache
- Some are ARM devices, some are MIPS (or something very similar) others are based on an embedded Realtek chipset (for example, media players)
- Some are believed to be game consoles
- Some are N45 devices (with specific brand has open taint, open sn and an SMTW server - all insecure)
- Some set-top boxes were also seen as exploited

This proof of a systematic compromise of IoT devices and its subsequent use of those Thingsbots to further attack other networks is something we’ve never seen before. This suggests an unfortunate future for both home users and enterprises, the latter of whom now faces an even larger volume of maniacal attack capacity.

Worse, these compromised home appliances provide a mechanism where users can unknowingly expose their work environment to such cyber attacks. All a user has to do is use a remote RDP connection and conveniently simply take action likeyching their fronge from their work PC. If a classic drive-by or even a redirect has been installed, the work PC is now compromised (though this is arguably more far fetched). Clearly, as the trend towards smart devices and BYOD increases, the risk of enterprise exposure increases correspondingly.

HP: Most IoT Devices Lack Security, Open To Attack

Thu, 07/31/2014 - 3:16pm
by Jon Minnick, Associate Editor, Manufacturing Business Technology

Get today’s manufacturing headlines and news - Sign up now!

A recent study from Hewlett-Packard reveals that 70 percent of Internet of Things (IoT) devices — including sensors and connected infrastructure — are seriously vulnerable to attack. The Internet of Things State of the Union Study from HP’s Fortify on Demand division came about after hearing a lot about IoT, but saw nothing that focused on the complete picture of IoT security.
IoT Topology Coming into Focus and Edge Nodes are wide-open to attacks
Syrian Radar Case

“September 2007, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of Syrian radar, supposedly state of the art, to warn the Syrian military of the incoming assault. It wasn’t long before military and technology bloggers concluded that this was an incident of electronic warfare and not just any kind. Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar”

Source: IEEE spectrum, 2007
**Stuxnet Virus** Likely Delivered by “Infected” USB Flash Drive

“*Stuxnet, a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran*”

IEEE, “The Real Story of Stuxnet”, February 26, 2013
The “Candy Drop”

- Security firm hired to test data security of credit union
  - Scattered 20 infected USB flash drives in parking lot, picnic and smoking areas
  - 15 were plugged into company computers
  - Passwords, logins and other information were compromised

- U.S. Department of Homeland Security Test
  - USB flash drives scattered in government parking lots
  - 60% of those found were plugged into networked computers
  - 90% of those with official logos were plugged in

Source: Information Week, June 7, 2006 & Business Insider, July 24th 2013
Hardware Attack Types

- ‘Side-Channel’ Attacks - (SECRET EXTRACTION)

- Counterfeit Chips - (SUPPLY CHAIN VULNERABILITY)

- Malicious Logic inside Chip - (TROJANS)
Side-Channel Attacks

To crack safes, it’s essential to know how they work.
DPA: Differential Power Analysis

- Thermal images can help in locating cryptographic circuits
  - Attempts to enter candidate keys should exercise crypto
  - This results in visible power dissipation

- Subsequently, different power dissipation patterns can be observed based on correct or incorrect key entry attempts
- Keys can then be inferred
Set-Top Boxes Side-Channel Attacks
Delaying Time-to-Crack Is Measure of Success

STRONG Digital HD TV Receiver
PVR Recorder Set Top Box
Decoder Media Player
From Australia

H.264/ MPEG-4 HD PVR TV Receiver Set Top Box FTA Media Player
From China

Wintal STB14HD h3 HD PVR set top box w/ Multimedia USB Playback/Player
From Australia
Countermeasures for Side-Channel Attacks

- Decrease signal-to-noise ratio
- Incorporate randomness into cryptography
- Pre-charge registers and buses to mitigate power-leakage signatures
- Use fixed-time algorithms to reduce data-related timing signatures
- Camouflaging structures from reverse engineering
Global nature of supply chain makes chain-of-custody unworkable

Component changes hands 15 times before final install
Counterfeit and recycled chips

More than a Backyard Industry!

- Millions of Scrap Boards
- Component Removal
- Sorted by size, similarity and lead count
- Re-processed
Creating Secure Silicon in an Untrusted Environment — VPN for Silicon

Secure Tunnel (VPN)

“VPN” for Trusted Silicon

Supply Chain Protection Solution

IC Design

Data

Untrusted Network

Users

Users

© 2010 Mentor Graphics Corp.
www.mentor.com
**Possible Activation Solution: Logic Encryption**

- Add gates throughout a design connected to a key
  - Generate a 256 bit encryption key
  - Inject 256 gates throughout the design
    - Gates inserted are pre-determined by the bit in the key

- Manufacturing
  - Use potentially un-trustworthy fab
  - Place a 256 bit key in tamper-proof location in the design after fabrication

- Global key vs. unique key (PUFs)
What Are Hardware Trojans?

- Rogue hardware injected into the design/chip
  - Untrusted cores (design phase)
  - Untrusted fab (fab phase)
  - Triggered subsequently
    - Special date/time
    - Receipt of special signal

- Payload = Malicious Action

- Types of Attacks
  - Kill switch: Breaking the system
  - Backdoor: Gaining access to the system. e.g., sending confidential data off-chip

The Hacker in Your Hardware, Villasenor, Sci. American 2010
Threat Example

- Unpublished control message travels around the internet and is unrecognized and ignored by most routers.
- When a router containing a hardware Trojan in the control plane sees such a message, it takes action to re-direct data.
Run-time Detection via Co-processor

- **Co-processor for run-time Trojan detection**
  - Include co-processor in the design as an IP block

- **Issues targeted**
  - Peripherals with hidden functionality
  - Prevention of undeclared communications

![Diagram showing CPU, Memory, Input / Output, Control Bus, Address Bus, Data Bus, System Bus, Rules, EDA Tool, Micro Code, Cybersecurity Co-processor]
Countermeasures

Malicious Logic inside Chip
(\textit{TROJANS})

Counterfeit Chips
(\textit{SUPPLY CHAIN VULNERABILITY})

‘Side-Channel’ Attacks
(\textit{SECRET EXTRACTION})

Detection of \textit{over-produced, cloned re-marked, recycled} or otherwise unauthorized IC’s
- Authentication
- Activation

Design-time Detection
- Formal methods
- Algorithmic test

Run-time Detection
- Insertion of logic to monitor run time activity

Defenses against attempts to leak out secrets stored on the chip
- Use of hardened IP or altered design
- Simulation of attacks to identify weaknesses
Countermeasures Don’t Need to Be Perfect

Based on my calculations, we can’t out run this bear!

I don’t need to outrun the bear. I only need to outrun you.
Summary

System design and integration take new forms with evolution and pervasiveness of cloud, sensors, social networking, gaming and mobility enabled by rapidly advancing silicon.

A huge opportunity exists to combine all these technologies in intelligent ways to create high-value, domain-specific user experiences.

Edge node security needs to be considered up-front.