Smart Nest Thermostat
A Smart Spy in Your Home

Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin
Security in Silicon Laboratory, University of Central Florida

Outline

- IoT Era: Security and Privacy
- IoT Star: Nest Thermostat
- Nest Architecture – Firmware and Hardware
- User Privacy
- Hardware Backdoor
- Demonstrations
- Conclusions and Future Work

Who We Are

- Grant Hernandez: Computer Engineering UG, UCF
- Orlando Arias: Computer Engineering UG, UCF
- Daniel Buentello: Independent researcher
- Yier Jin: Electrical Engineering, Ph.D.

Introduction

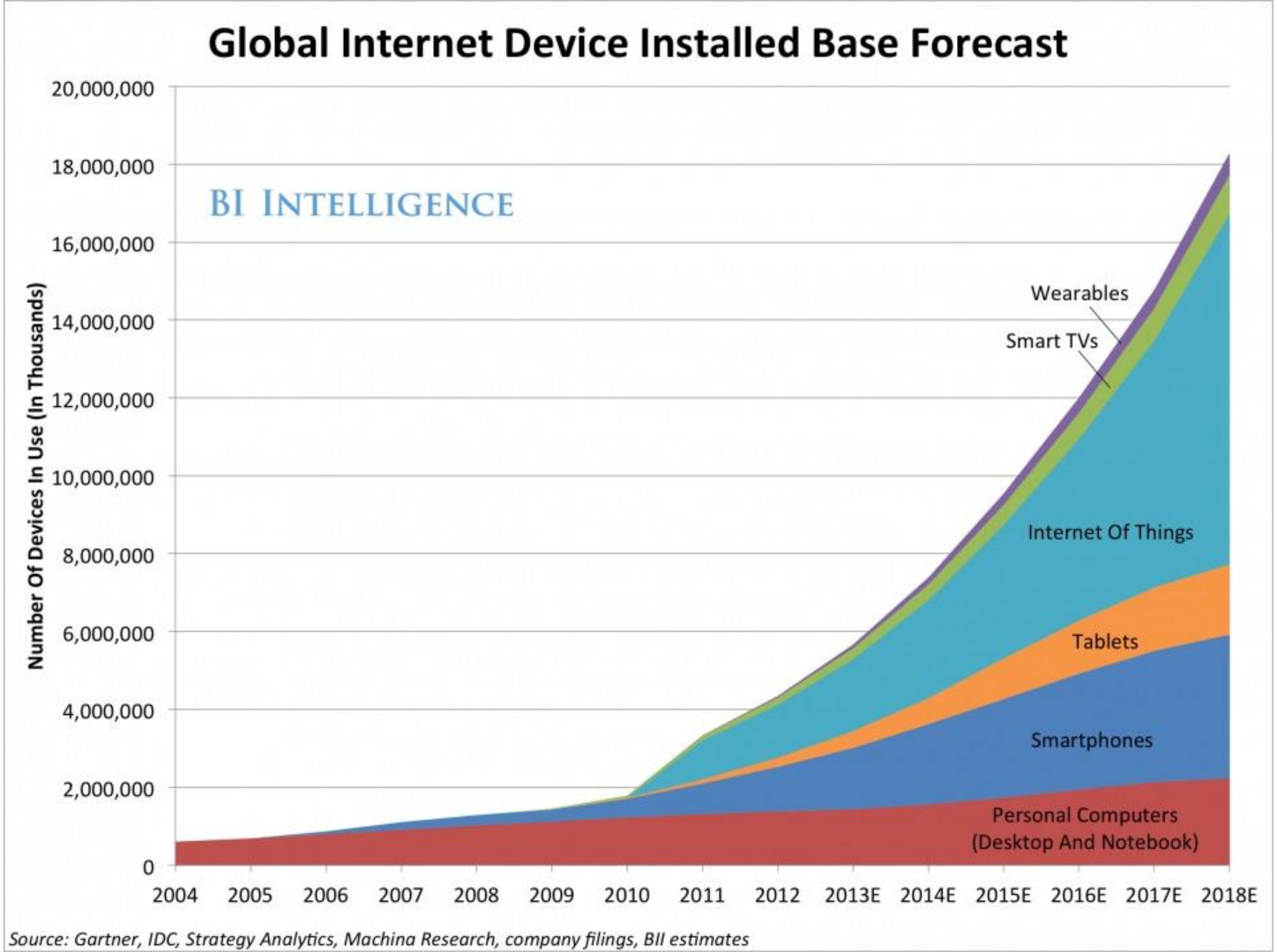
- Internet of Things
  - “When wireless is perfectly applied the whole earth will be converted into a huge brain...and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.”

    - Nikola Tesla 1926
- Definition
  - Embedded devices with networking capabilities.

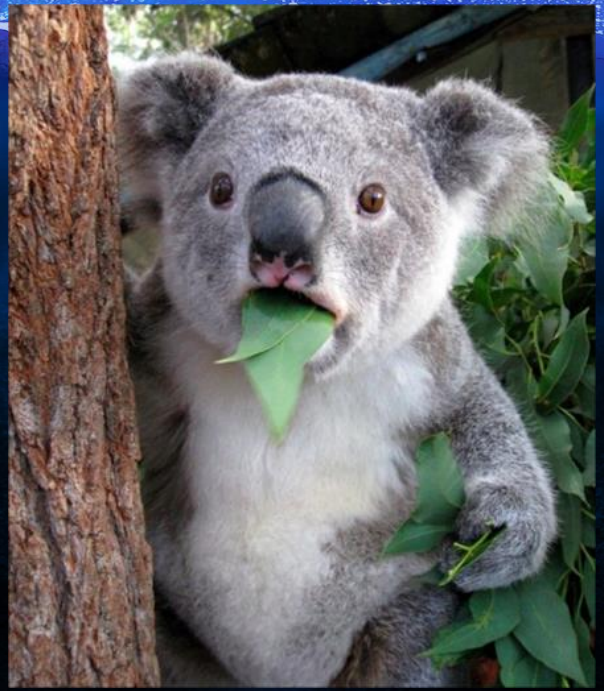
IoT and Wearable Devices

black hat USA 2014

Assorted images found online.


Global Internet Device Installed Base Forecast
BI INTELLIGENCE
Number Of Devices In Use (In Thousands)
20,000,000
18,000,000
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013E
2014E
2015E
2016E
2017E
2018E
Wearables
Smart TVs
Internet Of Things
Tablets
Smartphones
Personal Computers
(Desktop And Notebook)
Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BII estimates

IoT Forecast



Security and Privacy

- Security Concerns
  - "ThingBot": More than 750,000 phishing and SPAM emails launched from "ThingBots" including televisions, fridges
  - IOActive examined the WeMo "Light Switch" firmware and uncovered a series of issues
- Privacy Concerns
  - Personal data is often collected without users' awareness
  - The "big personal data" includes too much information

IoT STAR: NEST THERMOSTAT

Nest Thermostat

- Nest Labs founded by Tony Fadell
- Debuted in October 2011
- Acquired by Google in January 2014 ($3.2B)
- Over 40,000 sold each month

  Data from GigaOM as of January 2013
- Available in UK in April 2014
- Smart home API is released in June 2014

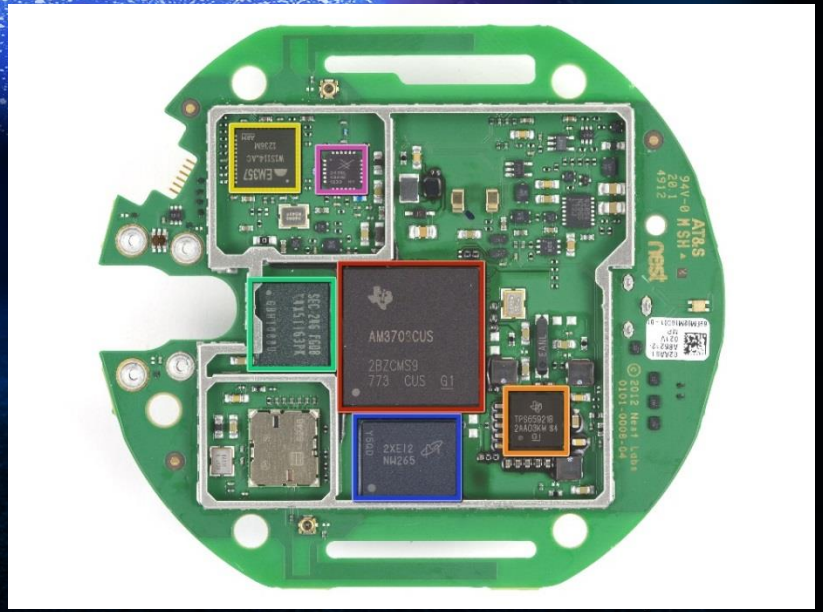
Nest Features

- Self-Learning
- Auto-Away
- Nest App
- Nest Leaf
- Airwave
- Monthly energy report*

NEST HARDWARE

Front Plate

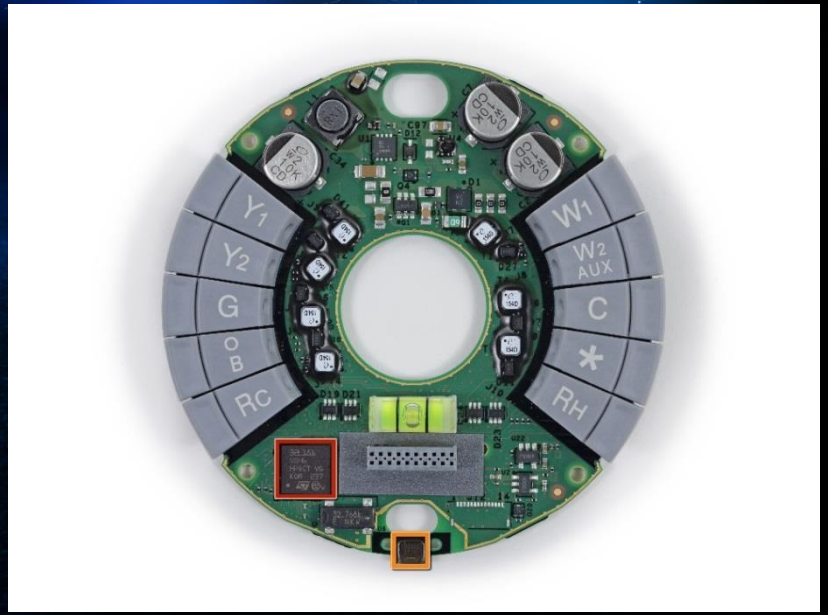
- “Display” board
- Graphics/UI, Networking
- Chips:
  - ARM Cortex A8 app processor
  - USB OTG
  - RAM/Flash (2Gb)
  - ZigBee/WiFi Radios
  - Proximity Sensors
- UART test points (silenced at bootloader)



Courtesy of iFixit

“Backplate” and Comms

- Hooks up to AC/Heating system. Charges battery via engineering wizardry
- Chips:
  - Independent ARM Cortex M3
  - Temp and Humidity Sensor
- Communications
  - Front to Back – UART
  - NEST Weave (802.15.4)
  - USB MSD (FW update)

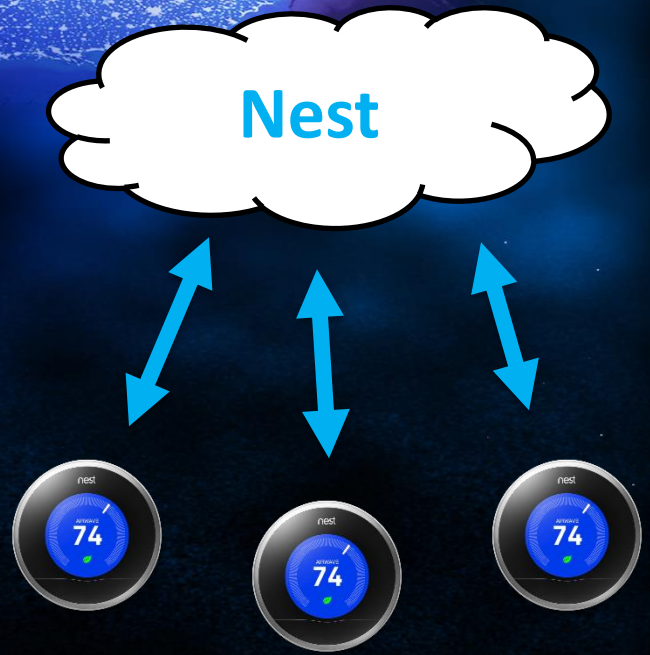


Courtesy of iFixit

NEST SOFTWARE

Nest Client

- Runs on a Linux based platform
- Handles interfacing between device and Nest Cloud services
- Automatically handles firmware updates
- Manual update available
  - Plug Nest into PC
  - Handled as a storage device
  - Copy firmware to drive
  - Reboot



Nest Firmware

- Signed firmware ☹
  - Manifest.plist
    - Hashes contents
  - Manifest.p7s
- Compressed but not encrypted or obfuscated
- Includes
  - U-boot image
  - Linux Kernel image
  - File system
  - nlbpfirmware.plist

Things Done the Right Way™

- Firmware signing using PKCS7
- Pinned Nest certificates for firmware verification
- All critical communications (any with secrets) over HTTPS
  - Other less secure ones over HTTP (firmware, weather)

Things Done the Wrong Way™

- Firmware links downloaded using HTTP and download links do not expire
- Firmware images not encrypted using Nest private key. Could still fall back to unencrypted in the event of a key blacklist
- Hardware backdoor left for anyone with a USB port to use

NEST SECURITY

Remote Update

- A notable quote from Nest Labs founder Tony Fadell:
  - *“Yes, hacking is in our thoughts. When you're talking about the home, these are very private things. We thought about what people could do if they got access to your data. We have bank-level security, we encrypt updates, and we have an internal hacker team testing the security. It's very, very private and it has to be, because it'll never take off if people don't trust it.”*

- Firmware verification
  - Manifest.plist
  - Manifest.p7s

User Privacy

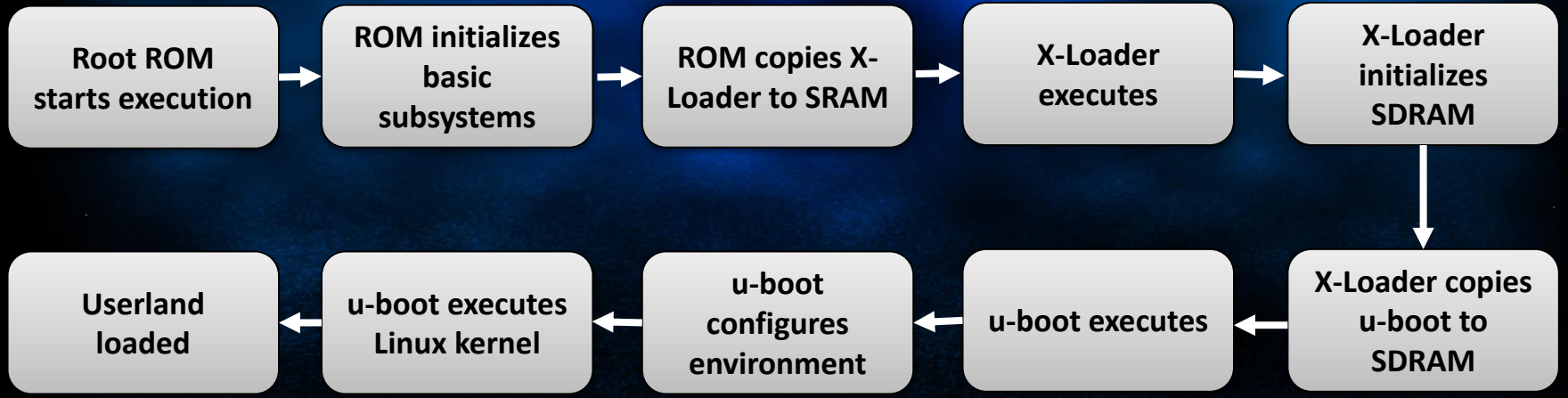
- Log Files
  - Internally stored and uploaded to Nest Cloud when an Internet connection is available
  - Contents
    - Usage statistics
    - System logs
    - Nest software logs (Zip Code, device settings, wired option)
- User Interface
  - Users are unaware of the contents of the log files
  - Users cannot turn off this option
- User network credentials are stored within the device… in plain text!

PROCESSOR AND BOOT

Hardware Analysis

- TI Sitara AM3703
  - ARM Cortex-A8 core
    - Version 7 ISA
    - JazelleX Java accelerator and media extensions
    - ARM NEON core SIMD coprocessor
  - DMA controller
  - HS USB controller
  - General Purpose Memory Controller to handle flash
  - SDRAM memory scheduler and controller
  - 112KB on-chip ROM (boot code)
  - 64KB on-chip SRAM

Boot Process



Device Initialization

- Boot Configuration read from sys_boot[5:0]

Selected boot configurations					
sys_boot [5:0]	First	Second	Third	Fourth	Fifth
001101	XIP	USB	UART3	MMC1	MMC1
001110	XIPwait	DOC	USB	UART3	
001111	NAND	USB	UART3	NMC1	
101101	USB	UART3	MMC1	XIP	DOC
101110	USB	UART3	MMC1	XIPwait	
101111	USB	UART3	MMC1	NAND	

Device Programming

- ROM is capable of booting device to boot from USB!
- Boot configuration pins are set by Nest hardware
- Device will boot from USB if sys_boot[5] is high

Device Programming

- ROM is capable of booting device to boot from USB!
- Boot configuration pins are set by Nest hardware
- Device will boot from USB if sys_boot[5] is high
- Circuit board exposes sys_boot[5] on an unpopulated header…

Hardware Backdoor

- It is possible to boot the processor from a peripheral device, such as USB or UART!

Implications

- Full control over the house
  - Away detection
  - Network credentials
  - Zip Code
  - Remote exfiltration
  - Pivoting to other devices

Control over all Nest devices

- Unauthorized ability to access Nest account
  - we now have the secrets
- Ability to permanently brick the device
  - we can modify NAND
- Persistent malware in NAND
  - Modify x-loader in NAND

THE ATTACK

Attack

- Device Reset
  - Press the button for 10 seconds causing sys_boot[5] = 1'b1
- Inject code through the USB into memory and execute
  - Have a short timeframe

Initial Attack

- X-Loader
- Custom U-Boot
  - Utilize existing kernel
  - Load our ramdisk (initrd)
- Ramdisk
  - Mount flash and write at will
- We have netcat!

Refining a Backdoor

- Rebuild toolchain
- Port dropbear (SSH server)
- Add user accounts and groups
- Reset root password

Linux Kernel Modification

- A custom Linux kernel
- Custom logo
- Debugging capabilities (kgdb)
- Polling on OMAP serial ports


black hat
USA 2014
DEMO

Modding: Graphics and Input

- Full 2D framebuffer control
- Unfortunately, no 2D acceleration, so no heavy per-pixel calculations
- Easy access to the rotary dial, button, piezo, and LED

Double-Edged Sword

- Positive View
  - The backdoor provide legitimate users to opt-out of uploading logs files
- Negative View
  - The backdoor may be maliciously exploited
- A Relief to Nest Labs
  - The backdoor needs physical access to the device (although remote attack is under investigation)

A Solution – Chain of Trust

- Code Authentication
  - Processor must authenticate the first stage bootloader before it is run
- Use public key cryptography
  - Userland protection
    - Only execute signed binaries
    - Filesystem encryption
  - Processor-DRAM channel protection

Conclusions and Future Work

- About the Nest Thermostat
  - A lot of things done right
  - Not enough focus on hardware security
- Future work
  - Find remote attacks
  - Look at other devices

Thank you!

Yier Jin

yier.jin@eecs.ucf.edu

Links

http://hardwaresecurity.org/iot/

https://nest.com/legal/compliance/

https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html

http://www.mentor.com/embedded-software/sourcery-tools/sourcery-codebench/editions/lite-edition/