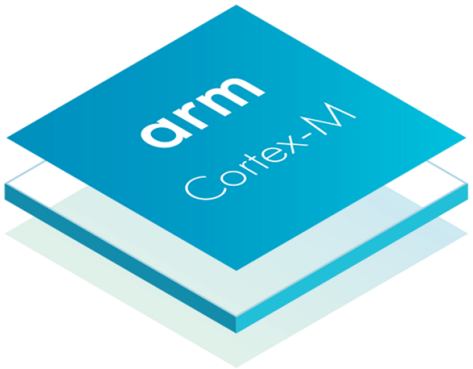
Secure Internet of Things Project Overview

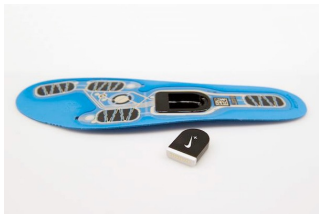
Philip Levis, Faculty Director
SITP 2018 Retreat
Santa Cruz, CA

Four Years Ago



+

=



Security Disaster

The Economist | World politics | Business & finance | Economics | Science & technology | Culture

Cyber-security

The internet of things (to be hacked)

Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition

Timekeeper Like 217 Tweet 594

How the Internet of Things Could Kill You

By Fahmida Y. Rashid JULY 18, 2014 7:30 AM - Source: Tom's Guide US | 5 COMMENTS

Hacking the Fridge: Internet of Things Has Security Vulnerabilities

JESS SCANLON | MORE ARTICLES
JUNE 28, 2014

Philips Hue LED smart lights hacked, home blacked out by security researcher

By Sal Cangeloso on August 15, 2013 at 11:45 am | 7 Comments

HP conducted a security analysis of IoT devices[1]

- 80% had privacy concerns
- 80% had poor passwords
- 70% lacked encryption
- 60% had vulnerabilities in UI
- 60% had insecure updates

[1] http://fortifyprotect.com/HP_IoT_Research_Study.pdf

IoT: MGC Architecture

eMbedded devices

6lowpan, ZigBee, ZWave, Bluetooth, WiFi, WirelessHART

Gateways

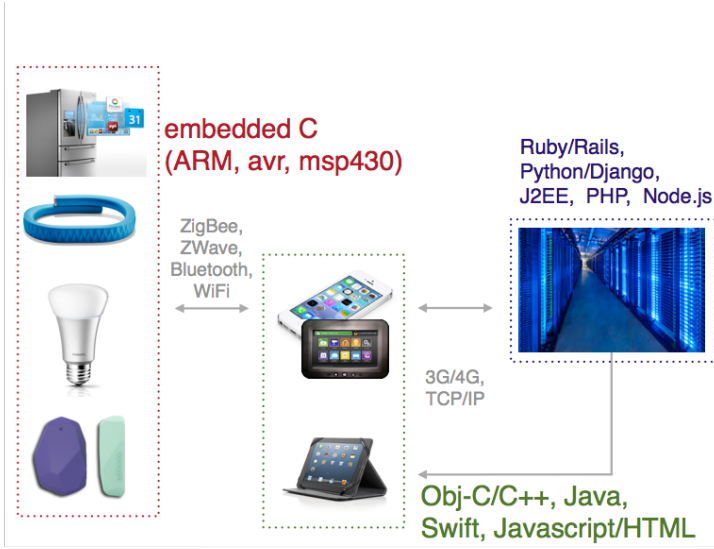
Cloud

3G/4G, TCP/IP

End application

IoT Security is Hard

- Complex, distributed systems
  - 10^3-10^6 differences in resources across tiers
  - Many languages, OSes, and networks
  - Specialized hardware
- Just developing applications is hard
- Securing them is even harder
  - Enormous attack surface
  - Reasoning across hardware, software, languages, devices, etc.
  - What are the threats and attack models?
- Valuable data: personal, location, presence
- Rush to development + hard → *avoid, deal later*



Where Are We Today?

Compromises Are Real

NEWS ANALYSIS

Researchers hack Philips Hue lights via a drone; IoT worm could cause city blackout

Researchers hijack Philips Hue lights with a drone to show how IoT worm could take over smart lights in a city.

IoT Goes Nuclear:
Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*
*Weizmann Institute of Science, Rehovot, Israel
{eyal.ronen,adi.shamir}@weizmann.ac.il
†Dalhousie University, Halifax, Canada
coflynn@dal.ca

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY —WITH ME IN IT

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)

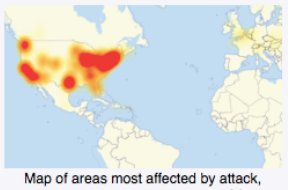
2016 Dyn cyberattack

From Wikipedia, the free encyclopedia

The **2016 Dyn cyberattack** took place on October 21, 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.[2][3] The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.[4]

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses.[5] The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware.

Dyn cyberattack



Map of areas most affected by attack, 16:45 UTC, 21 October 2016.[1]

Date	October 21, 2016
Time	12:10 – 14:20 UTC 16:50 – 18:11 UTC 21:00 – 23:11 UTC

Understanding the Mirai Botnet

Manos Antonakakis◇ Tim April‡ Michael Bailey† Matthew Bernhard◁ Elie Bursztein○
Jaime Cochran▷ Zakir Durumeric◁ J. Alex Halderman◁ Luca Invernizzi○
Michalis Kallitsis§ Deepak Kumar† Chaz Lever◇ Zane Ma†* Joshua Mason†
Damian Menscher○ Chad Seaman‡ Nick Sullivan▷ Kurt Thomas○ Yi Zhou†

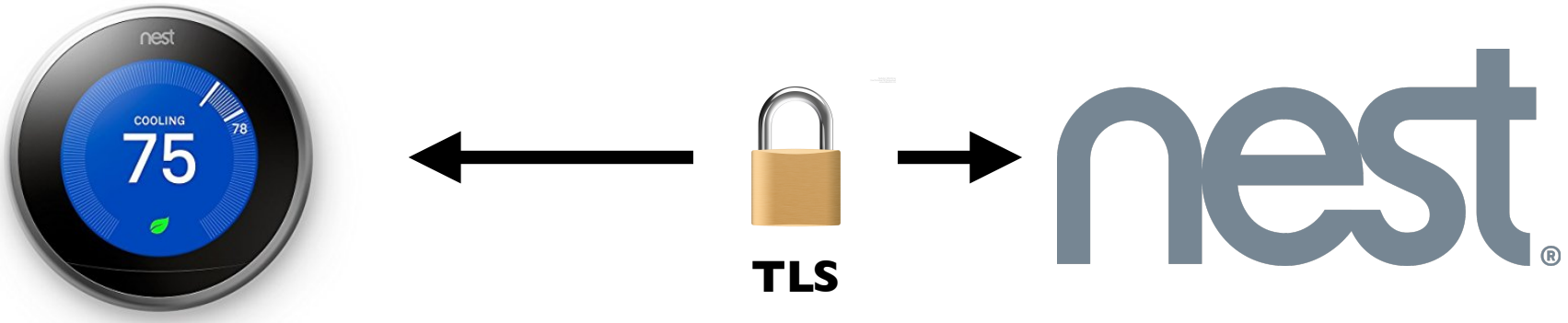
‡*Akamai Technologies* ▷*Cloudflare* ◇*Georgia Institute of Technology* ○*Google*
§*Merit Network* †*University of Illinois Urbana-Champaign* ◁*University of Michigan*

At the Edge

- Embedded devices are the weak link
- Project began with focus on protecting applications and users, but we also need to protect the Internet itself

Tock Operating System

Security Versus Privacy



- Securing IoT devices can raise privacy concerns
- E.g., securing Nest devices makes it difficult for us to monitor and audit them
  - We can't tell what our devices are saying about us

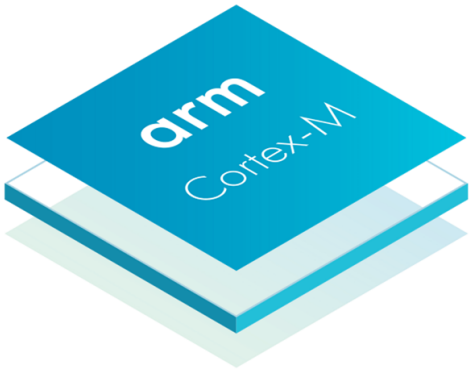
TLS Rotate-and-Release

Security Landscape

- Several breakthroughs transitioned quantum computing from academic question to not impossible
  - 2-qubit silicon gates
  - Google/Martinis simulate hydrogen with 9 bits
  - Intel develops 17-qubit chip
- IoT devices may be deployed for 20 years: need to consider potential reality of quantum attackers

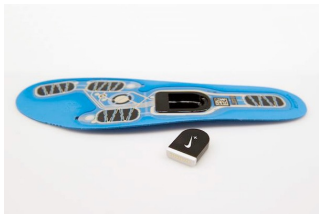
Post-Quantum Cryptography, CESEL accelerator

Four Years Ago

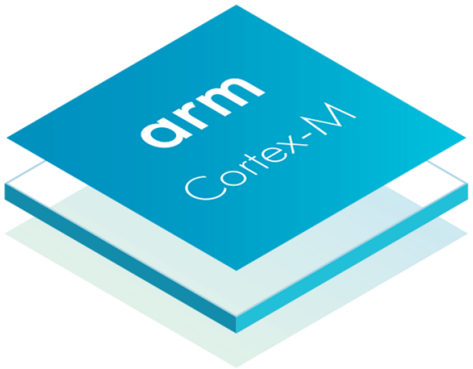


+

=



Today


arm
Cortex-M


RISC-V

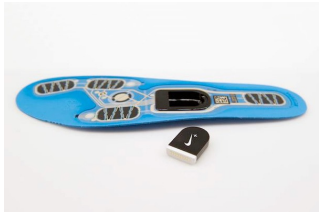

PHILIPS


Picasa
epi
31

+

=


LE




DEBIT
CREDIT


SHOP


ViewSonic

RISC-V

- Completely open-source architecture, instruction set
- Impressive industrial adoption (modern tools, etc.)
- Opens possibility of entirely new architectural designs for IoT security
  - Memory isolation/protection
  - Tagged memory: enforce software protection in hardware
  - Hardware IFC support?

Voice-Controlled IoT

Deep Learning

The Switch

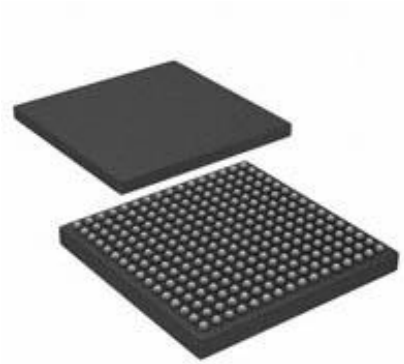
Can Amazon Echo help solve a murder? Police will soon find out.

- Size of learned models requires sending data to cloud for inference, where it is no longer under 5th Amendment protections
- But pushing models to the edge requires orders of magnitude reduction in model size

NLP model reduction

Distributed and Embedded

- Securing embedded devices is made harder by the fact that they are increasingly distributed systems
  - Multiple SoCs on a board (e.g., imix, Signpost)
  - Multiple cores in an SoC (e.g., NXP LPC4367JET256)



IoT Video

- IoT cameras are an increasingly important device class
  - Mirai botnet
- Video quality remains poor
  - Today, only large corporations can see the Internet
  - Protocol/encoder design

Large-scale measurement, video system design

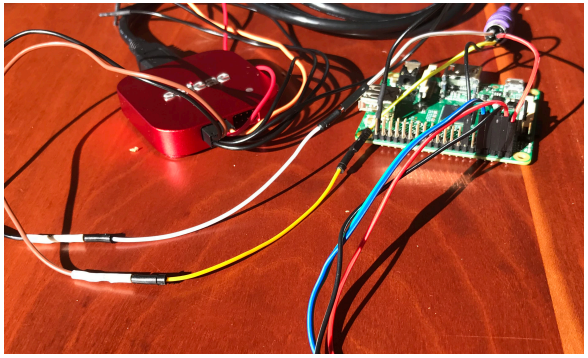
Secure Data Processing

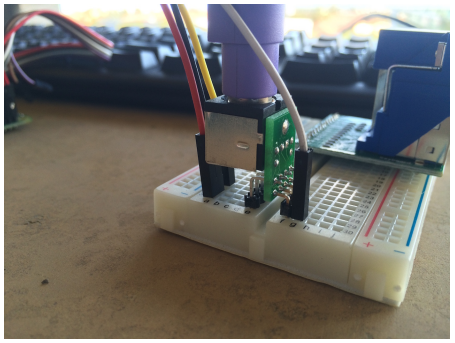
- Secure data analysis: centralized computations (e.g., cloud) on encrypted data
  - Allows interesting applications
  - Does not leak private information
  - Predicated on narrow computations, lots of research
- Distributed computation
  - Much less computationally intensive, but requires communication
- Enclave-enabled systems
  - Can trust 3rd party systems to secure data

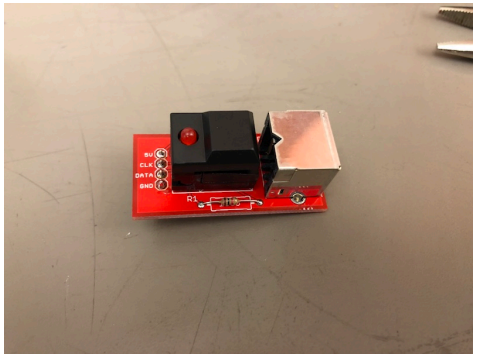
SGX-based cloud systems

Device Design

- Want to make building an IoT application as easy as building a modern web application
- Several years of instructional experience: hardware/ software boundary is the hardest part







Tools for HW/SW debugging, tools for EDG

Summary

- The hardware landscape has changed
  - Opportunities for new, security-based MCU designs, multi-core
- The security landscape has changed
  - Need to consider drastic changes in cryptography in 20 years
- The data landscape has changed
  - Prevalence of deep learning, training versus interference
- Identified achilles heel in building applications
- Ongoing research on tackling all of these problems

Rest of Today

- A series of talks by students and faculty on recent research results
- Several breaks (and lunch) to talk in greater depth