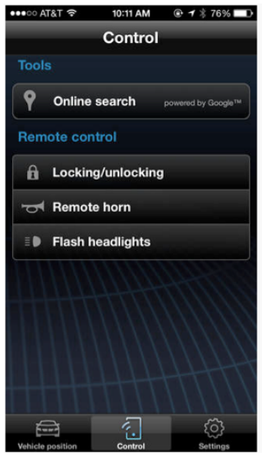
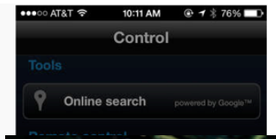
Securing the Internet of Things

Stanford University, UC Berkeley, and the University of Michigan

Philip Levis, Stanford University

The Internet of Things (IoT)





A 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

Securing the Internet of Things

- Secure Internet of Things Project
  - 5 year project (starting now)
  - 12 faculty collaborators
  - 3 universities: Stanford, Berkeley, and Michigan
- Rethink IoT systems, software, and applications from the ground up
- Make a secure IoT application as easy as a modern web application

Who?

Philip Levis
Stanford
Embedded Systems

Mark Horowitz
Stanford
Hardware

Christopher Ré
Stanford
Data Analytics

Dan Boneh
Stanford
Cryptography

Dawson Engler
Stanford
Software

Keith Winstein
Stanford
Networks

Prabal Dutta
Michigan
Embedded Systems

David Mazières
Stanford
Security

Björn Hartmann
Berkeley
Prototyping

Raluca Ada Popa
Berkeley
Security

Greg Kovacs
Stanford
Medical Sensing

Christos Kozyrakis
Stanford
Cloud Architecture

Steve Eglash
Stanford
Executive Director

Philip Levis
Stanford
Faculty Director

What is the Internet of Things?

Internet(s) of Things

Industrial Automation	Home Area Networks	Personal Area Networks	Networked Devices
Thousands/person	Hundreds/person	Tens/person	Tens/person
Controlled Environment	Uncontrolled Environment	Personal environment	Uncontrolled Environment
High reliability	Unlicensed spectrum	Unlicensed spectrum	Unlicensed spectrum
Control networks	Convenience	Instrumentation	Convenience
Industrial requirements	Consumer requirements	Fashion vs. function	Powered
WirelessHART, 802.15.4	ZigBee, Z-Wave	Bluetooth, BLE	WiFi/802.11
6tsch, RPL	6lowpan, RPL	3G/LTE	TCP/IP
IEEE/IIC/IETF	IETF/ZigBee/private	3GPP/IEEE	IEEE/IETF

IoT: MGC Architecture

eMbedded devices

Gateways

Cloud

End application

IoT: MGC Architecture

C, custom embedded software

Gateways

Cloud

End application

IoT: MGC Architecture

C, custom embedded software

iOS, Android, Java, Swift

Cloud

End application

IoT: MGC Architecture

C, custom embedded software

iOS, Android, Java, Swift

Rails, Node, PHP Ruby, JS, Python

End application

IoT: MGC Architecture

C, custom embedded software

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

iOS, Android, Java, Swift

Rails, Node, PHP Ruby, JS, Python

End application

IoT: MGC Architecture

C, custom embedded software

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

iOS, Android, Java, Swift

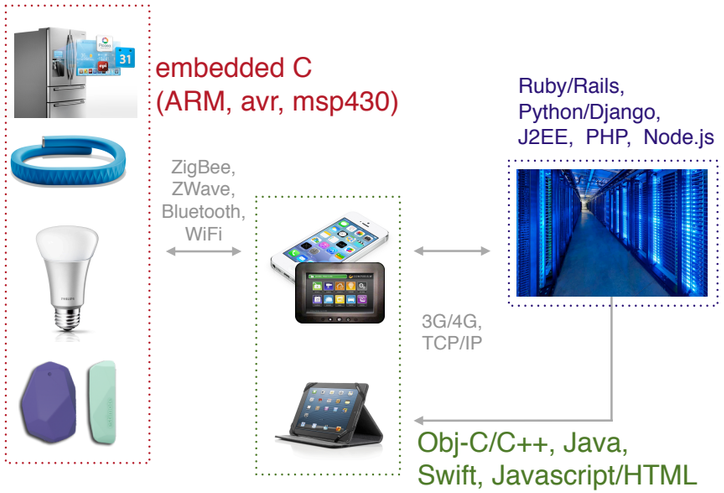
3G/4G, WiFi, TCP/IP, HTTP

Rails, Node, PHP Ruby, JS, Python

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

Two Goals

1. *Data security:* research and define new cryptographic computational models for secure data analytics and actuation on enormous streams of real-time data from embedded systems.

2. *System security:* Research and implement a secure, open source hardware/software framework that makes it easy to quickly build Internet of Things applications that use these new computational models.

Data Security

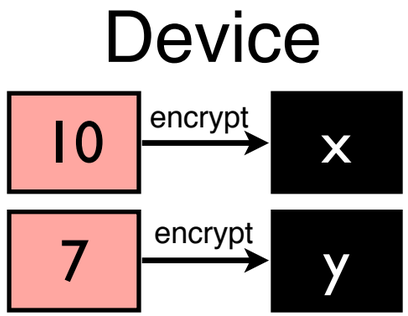
- Security limits what you (or an attacker) can do
- What do IoT applications need to do?
  - Generate data samples
  - Process/filter these samples
  - Analytics on streams of data, combined with historical data
  - Produce results for end applications to view

- Goal: end-to-end security
  - Embedded devices generate encrypted data
  - Only end applications can fully decrypt and view data
  - Gateways and cloud operate on data without knowing what it is

Homomorphic Encryption

(Gentry, Stanford University, 2009)

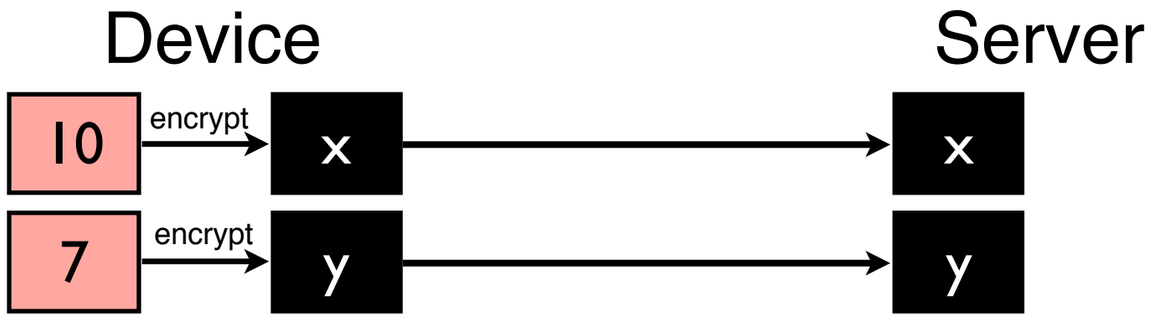
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, Stanford University, 2009)

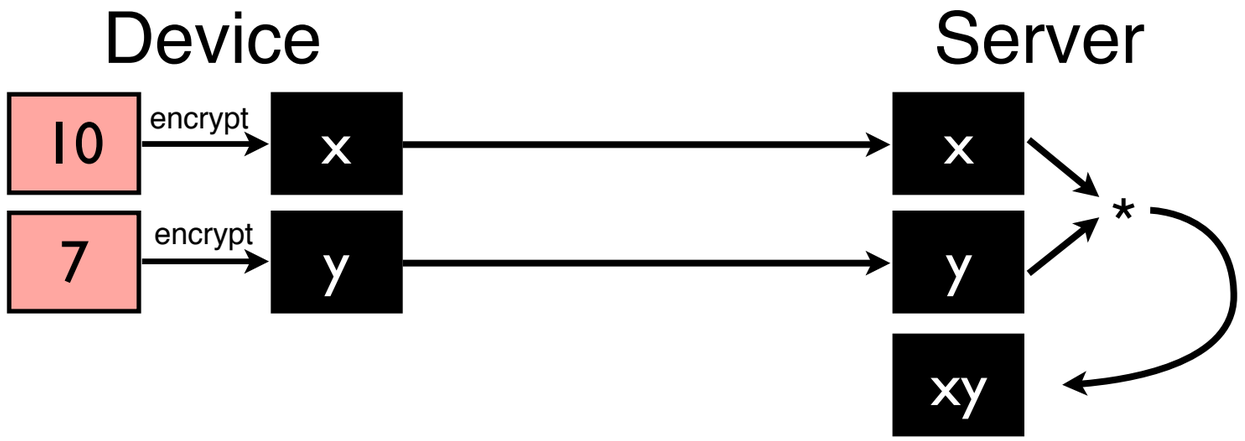
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, Stanford University, 2009)

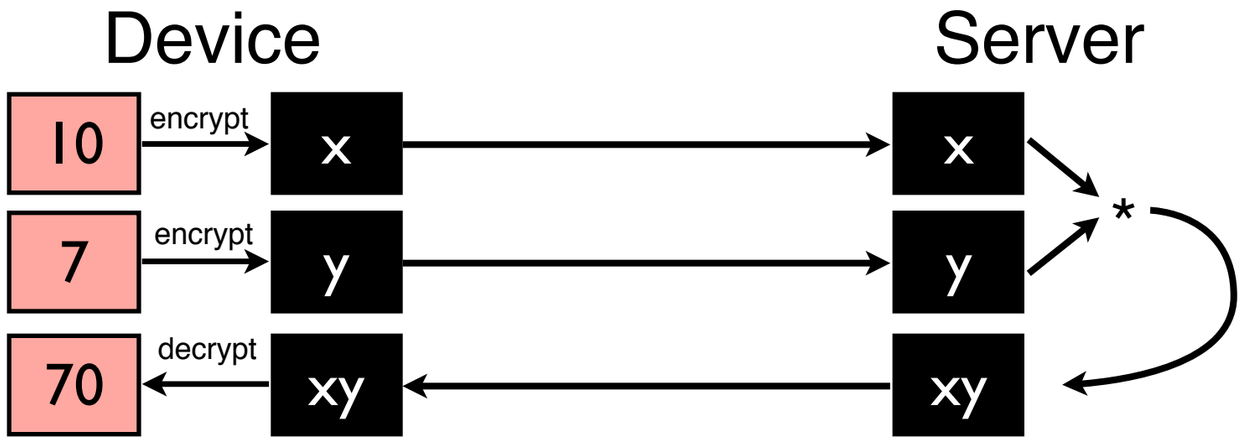
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, Stanford University, 2009)

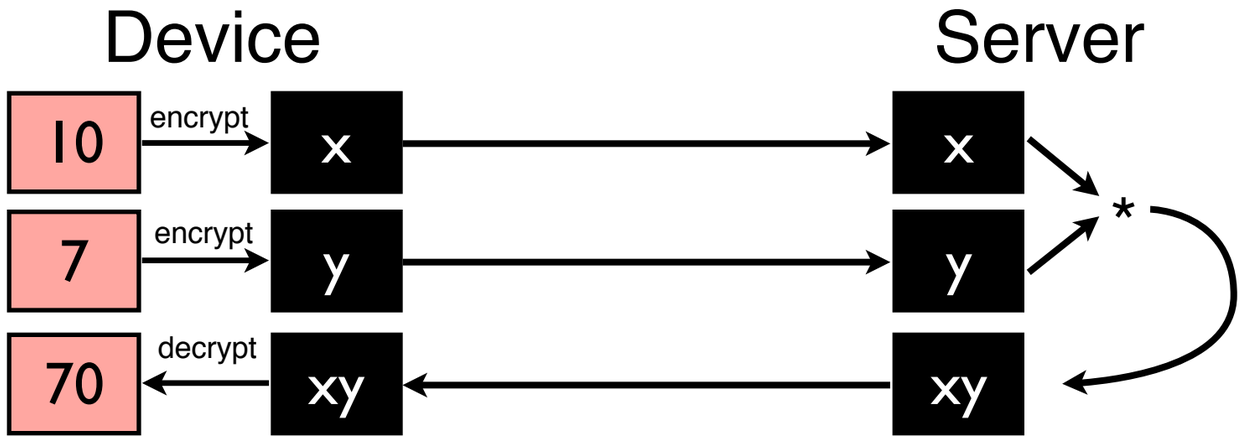
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, Stanford University, 2009)

- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



- So confidential analytics possible, but not yet practical
  - Computations on S_e are 1,000,000 slower than computations on *S*
- But can be fast for *specific* computations (e.g., *)

New Computational Models

- Can we compute statistics on secrets?
  - You're in the 85th percentile for saving water today!
  - Your house consumed 120% of its average energy today
- Distributed computation: many parties compute a value without revealing their own data
- Can we securely compute complex analytics?
- Need new cryptographic computation models
  - Support computations that IoT applications need
  - Open research questions in analytics, cryptography, and energy efficiency

Two Goals

1. *Data security:* research and define new cryptographic computational models for secure data analytics and actuation on enormous streams of real-time data from embedded systems.

2. *System security:* Research and implement a secure, open source framework that makes it easy to quickly build Internet of Things applications that use these new computational models.

System Security Today

"Currently there is no way of preventing a non-privileged task from creating a privileged task — there is an assumption that the system architecture is familiar with all the code s/he is building into the project. It is therefore unlikely to include malicious code…"

- FreeRTOS discussion forum

A Secure Foundation

(Anderson, Levy, Pannuto, Culler, Dutta, Levis, et al.)

- Tock: a secure operating system for embedded devices, focusing on Cortex M family
  - Memory protection
  - Ultra-low power operation
- Mixture of hardware, software, and language isolation
  - Multi-core platforms for hard isolation
  - Software control of memory protection for application isolation
  - Language type safety (Rust) for isolation within kernel

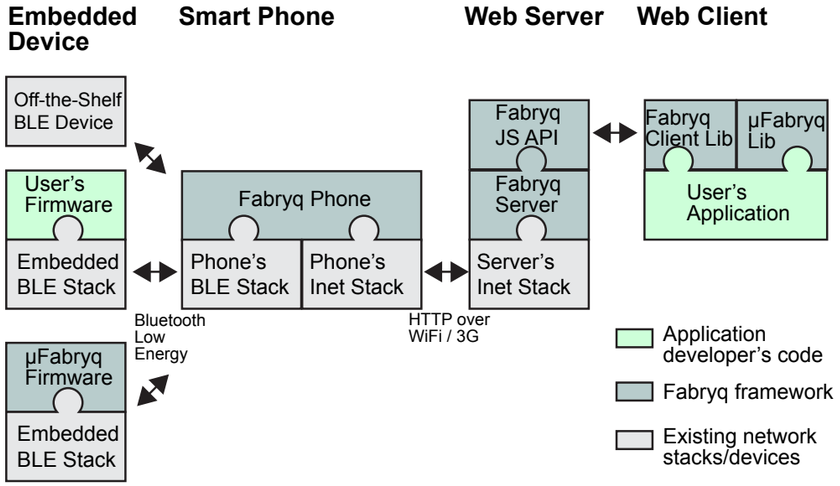
Making It Easy

- Security must be easy
  - Set password to "password", store data in the clear
- Must understand development model
  - Embrace modification, incorporation, low barrier to entry
  - Do so such that prototypes can transition to production
- Research user interfaces and abstractions that make security easy to understand and maintain

One Approach: fabryq

(McGrath, Hartmann, et al.)

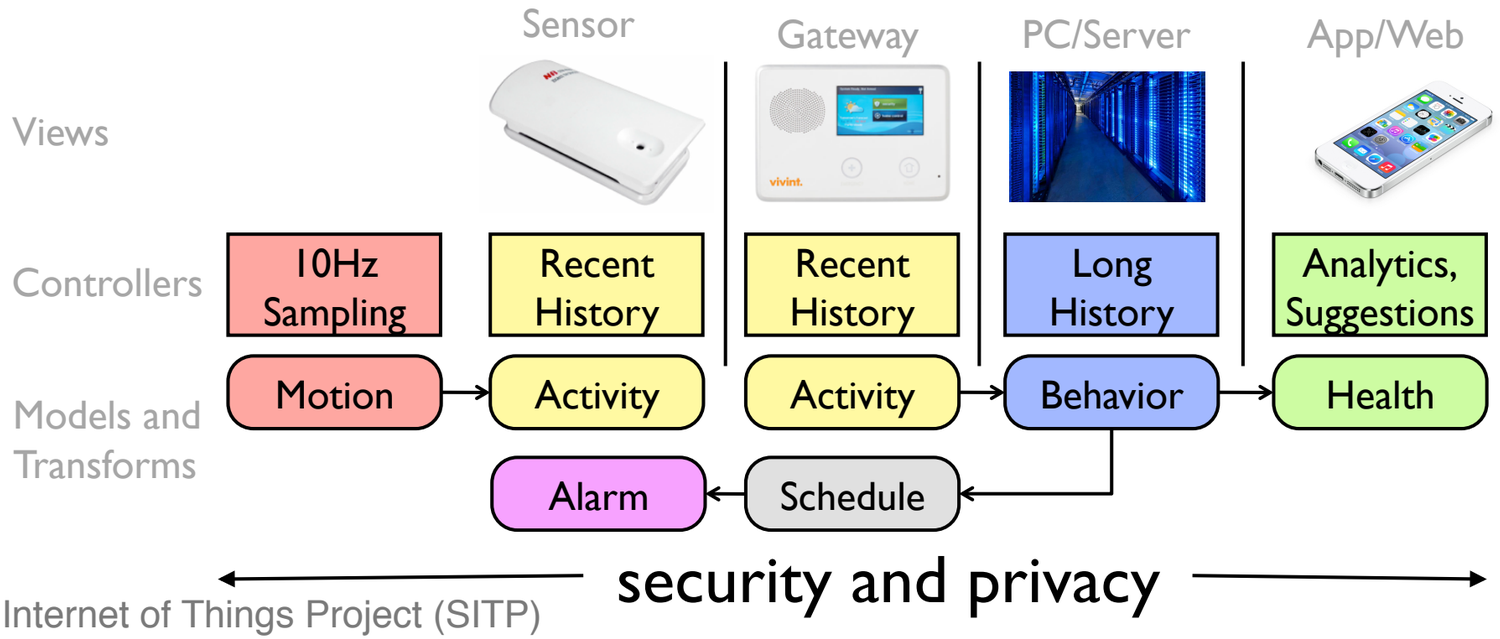
- Rapid prototyping
- Web application directly interacts with embedded device through server and mobile proxy
- Talk: March 2



Another Approach: Ravel

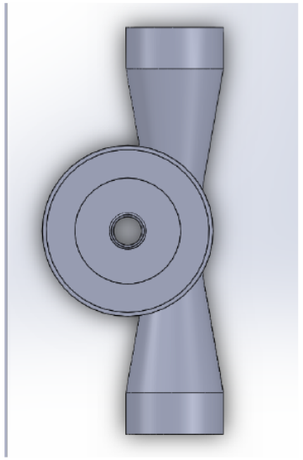
(Riliskis, Levis)

- Write a data processing pipeline
  - Consists of a set of *Models*, describing data as it is stored
  - *Transforms* move data between Models
  - Instances of Models are bound to devices
  - *Views* can display Models
  - *Controllers* determine how data moves to Transforms

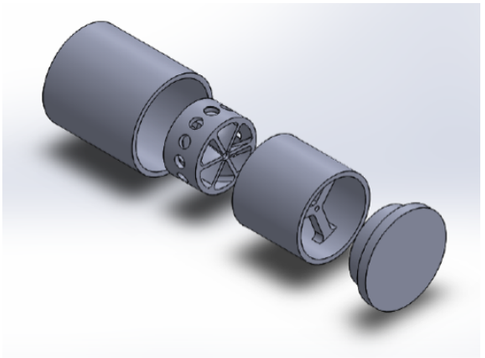


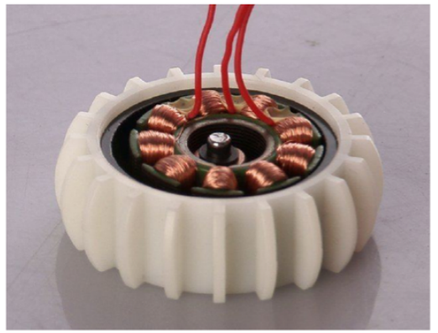
Applications

(Chiang, Hong, Riliskis, Boneh, Diffenbaugh, Horowitz, Levis, Ré)



- Monitor per-tap building water use
- Device harvests power from water flow, records speed and temperature
- Bluetooth Low Energy radio sends data to mobile phones, gateways to cloud storage
- Privacy-preserving analytics on data





Why Now?

- Technology has just reached the tipping point
  - BLE, iBeacon
  - Cortex M series
  - Sensors
  - Harvesting circuits
- We've been waiting
  - Leaders in prototyping, cryptographic computation, IoT networking, secure systems, analytics, and hardware design
  - What are the threats? Application attackers?
- But it's still early enough
  - Most big applications haven't been thought of yet
  - Let's not repeat the web (as good as it is for publications)

Start of a 5 Year Project

- Project starts today!
- Goal: define Internet of Things security for the coming decades
- This seminar brings together faculty, students, and industrial collaborators
  - VMware, Panasonic, SAP, etc.
  - May repeat each year
- Yearly spring retreats

Seminar Schedule

Jan 5	Securing the Internet of Things, Philip Levis
Jan 12	Computing on Encrypted Data - Somewhat Homomorphic Encryption, David Wu
Jan 19	Martin Luther King Day (no meeting)
Jan 26	Cryptographic Computation Systems, Raluca Ada Popa
Feb 2	Affiliate Talk: TBD
Feb 9	Beetle: Many-to-Many Bluetooth Communication, Amit Levy
Feb 16	President's Day (no meeting)
Feb 23	Affiliate Talk: TBD
Mar 2	fabryq: Using Phones as Gateways to Program Smart Devices from the Web, Will McGrath
Mar 9	Analytics on Sensor Data, Christopher Ré