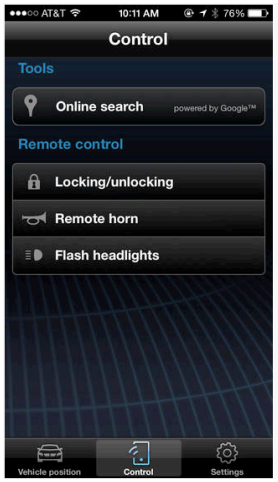
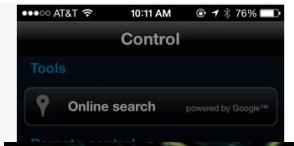
Secure Internet of Things Project (SITP)

Philip Levis
Stanford University

Secure Internet of Things Project Workshop
Stanford University
August 11, 2014

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

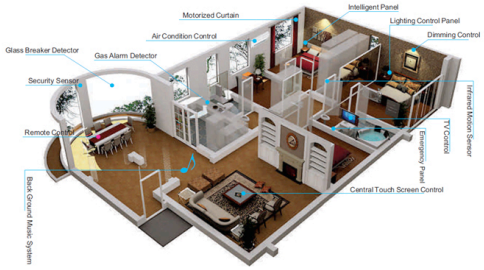
Philip Levis

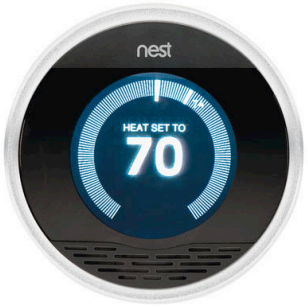
- Associate Professor, Stanford
  - Computer science and electrical engineering
  - Ph.D. in CS from UC Berkeley, 2005
  - Faculty Director, SITP
- Research: embedded systems software and networks
  - Connecting the physical world to the Internet
  - Ultra-low power software and systems
  - Operating systems: TinyOS, Cinder
  - Wireless algorithms: Trickle (RFC6206)
  - Wireless protocols: CTP, RPL (RFC6550)

Outline

- What is the "Internet of Things"? And why is securing it so hard?
- What we plan to do about it
- Overview of rest of workshop

Internet(s) of Things





Industrial Automation

Thousands/person
Controlled Environment
High reliability
Control networks
Industrial requirements

WirelessHART, 802.15.4
6tsch, RPL
IEEE/IIC/IETF

Home Area Networks

Hundreds/person
Uncontrolled Environment
Unlicensed spectrum
Convenience
Consumer requirements

ZigBee, Z-Wave
6lowpan, RPL
IETF/ZigBee/private

Personal Area Networks

Tens/person
Personal environment
Unlicensed spectrum
Instrumentation
Fashion vs. function

Bluetooth, BLE
3G/LTE
3GPP/IEEE

Networked Devices

Tens/person
Uncontrolled Environment
Unlicensed spectrum
Convenience
Powered

WiFi/802.11
TCP/IP
IEEE/IETF

IoT: MGC Architecture

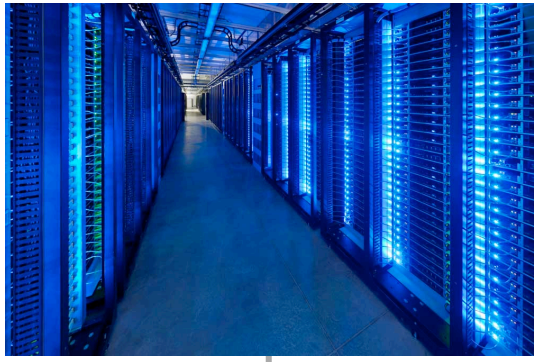
eMbedded devices

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

Gateways

3G/4G, TCP/IP

Cloud



End application

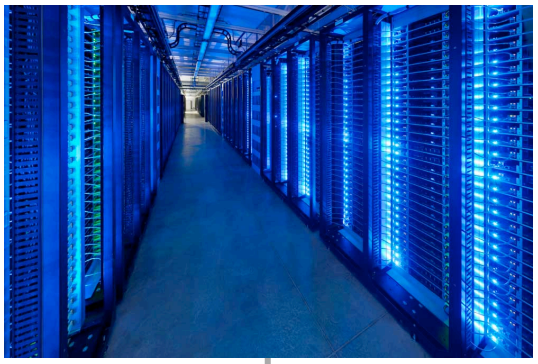
IoT: MGC Architecture

Secure Internet of Things

embedded C
(ARM, avr, msp430)

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

3G/4G,
TCP/IP

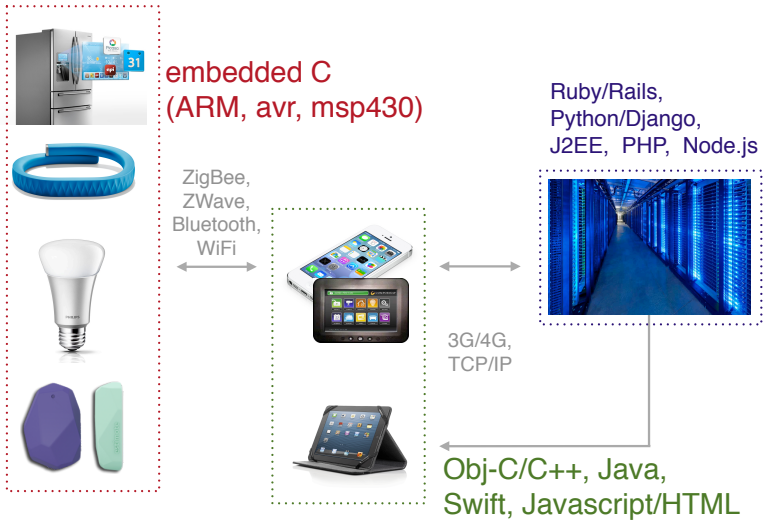


Ruby/Rails,
Python/Django,
J2EE, PHP, Node.js

Obj-C/C++, Java,
Swift, Javascript/HTML

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

What We're Going To Do About it

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.

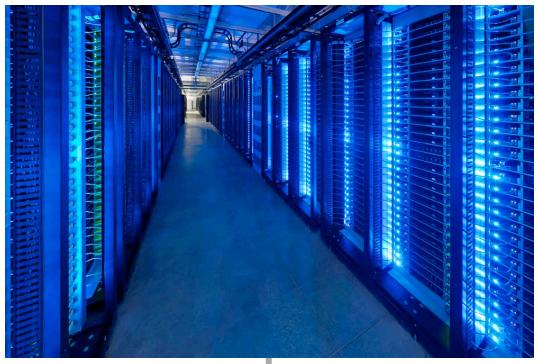
2. *System security:* Research and implement a secure, open source hardware/software framework that makes it easy to quickly build Internet of Things applications that use these new computational models.

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

End-to-End Security

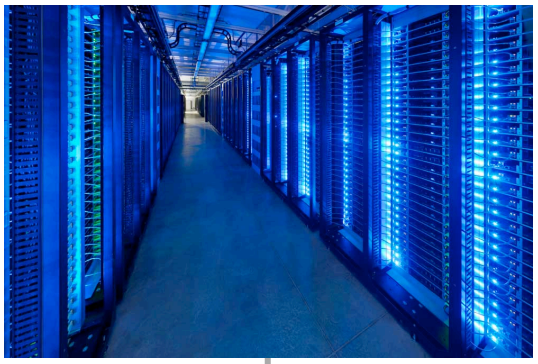
ZigBee,
ZWave,
Bluetooth,
WiFi



3G/4G,
TCP/IP

End-to-End Security

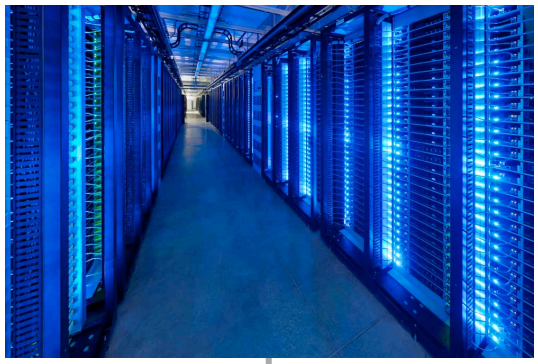
ZigBee,
ZWave,
Bluetooth,
WiFi



3G/4G,
TCP/IP

End-to-End Security

ZigBee,
ZWave,
Bluetooth,
WiFi

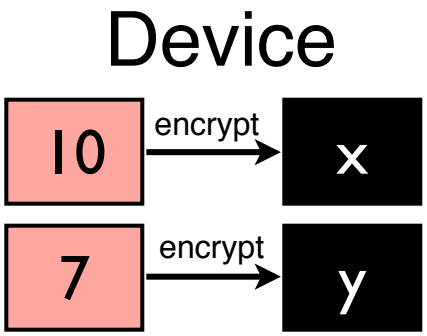


3G/4G,
TCP/IP

Homomorphic Encryption

(Gentry, 2009)

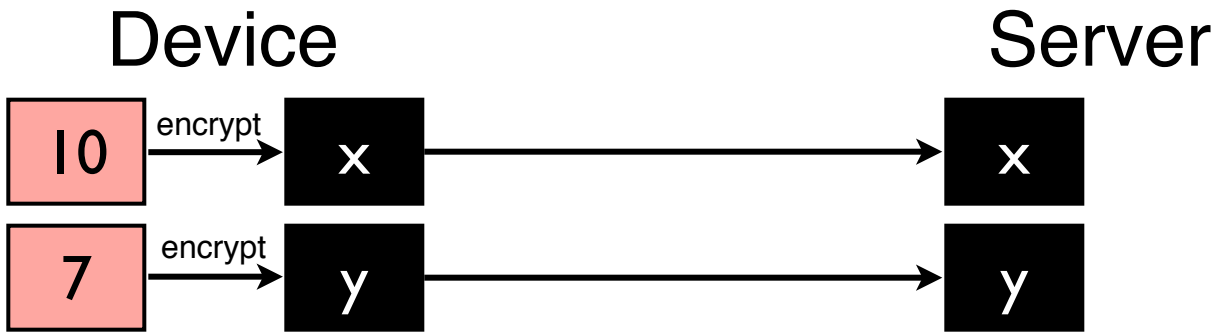
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

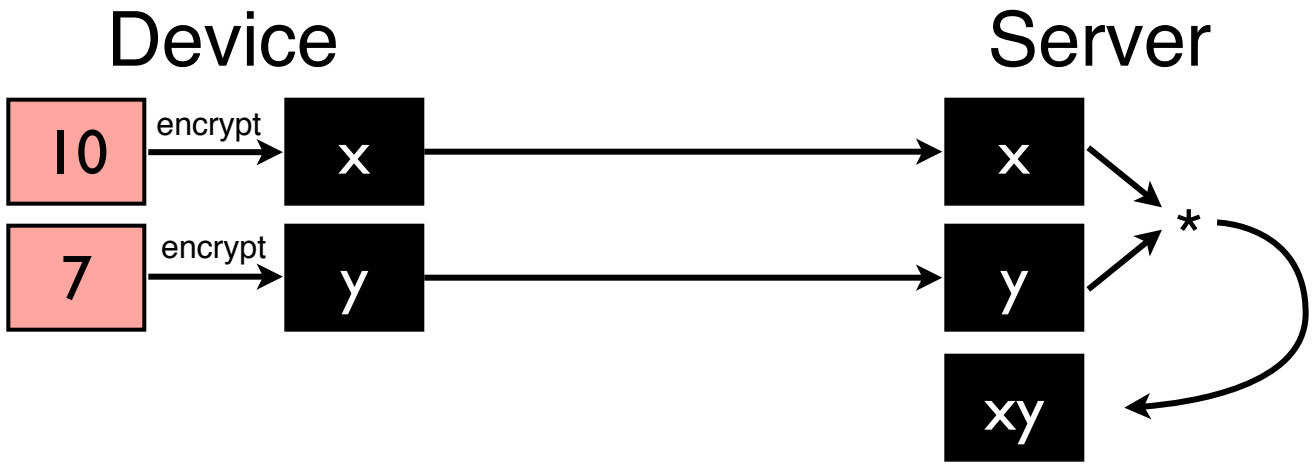
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

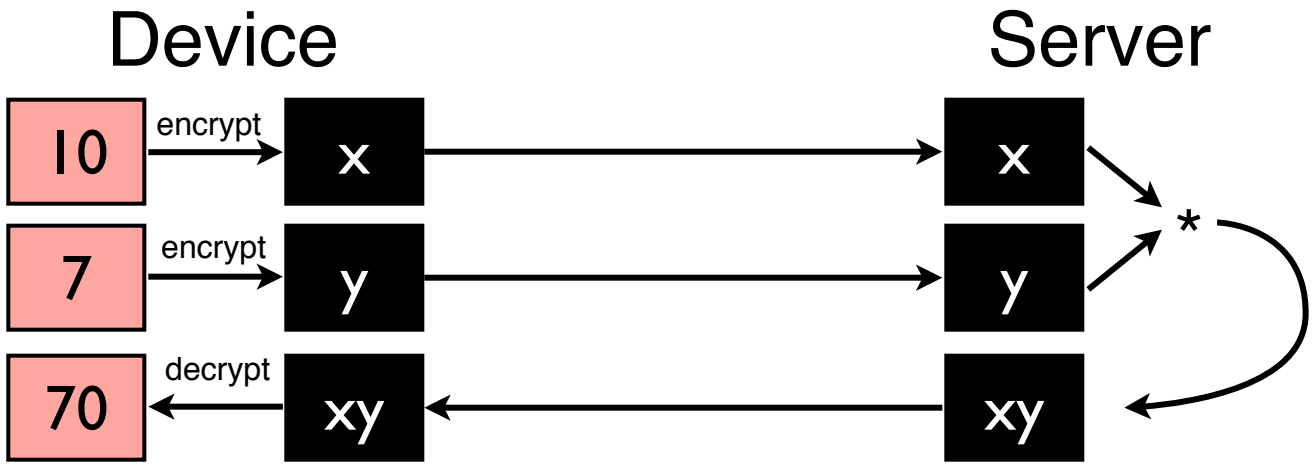
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

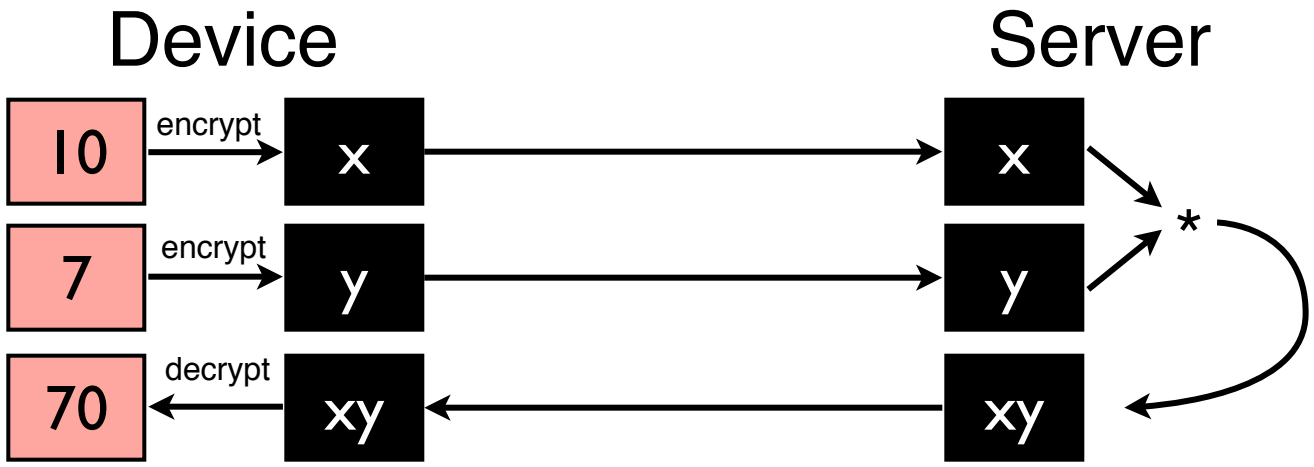
- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 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
- Can we securely compute complex analytics?
- Need new cryptographic computation models
  - Support computations that IoT applications need

- Talks today
  - Christopher Ré on analytics
  - Dan Boneh on cryptographic computational models

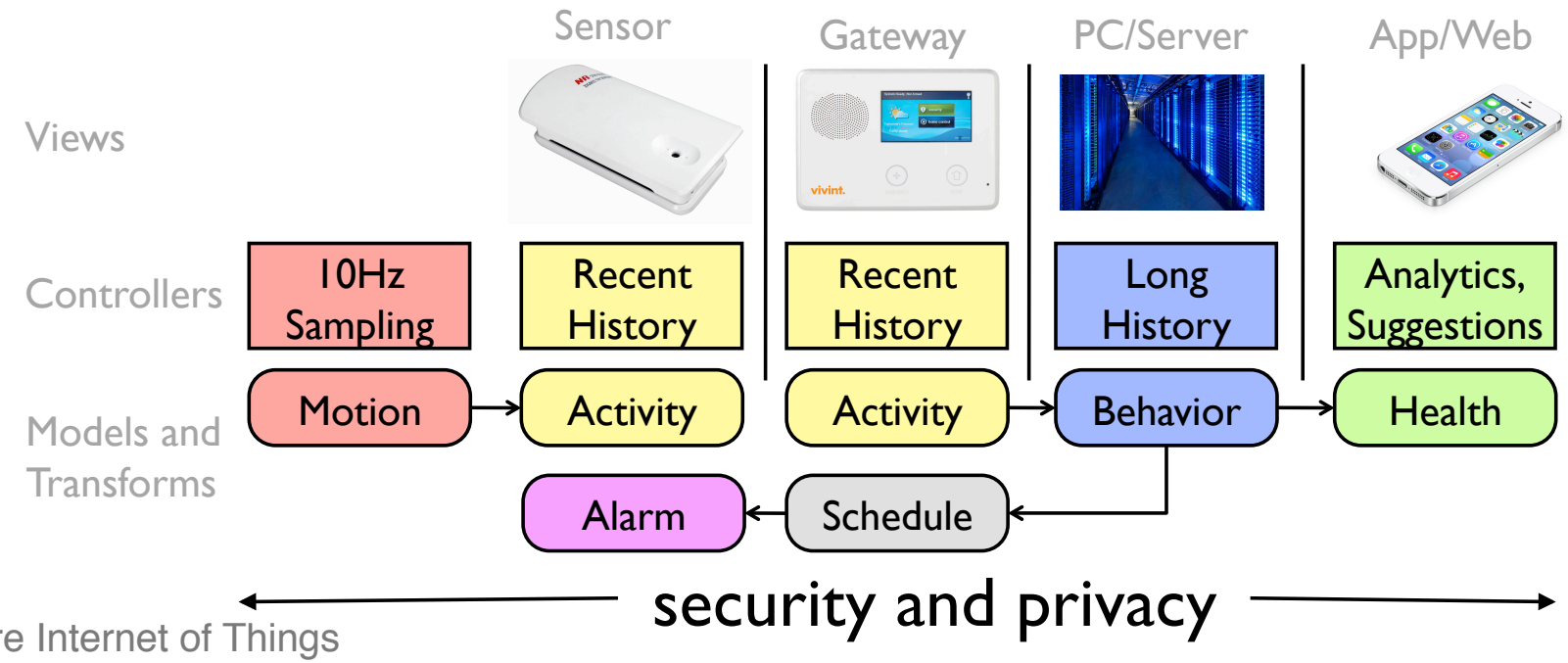
Two Goals

1. Research and define new cryptographic computational models for secure data analytics and actuation on enormous streams of real-time data from embedded systems.

2. 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.

Building an Application

- 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



Code Generation

- Framework generates (working) skeleton code for entire pipeline
- Developer can modify this generated code
  - Framework detects if modifications violate pipeline description
  - E.g., data types, information leakage, encryption
- Talks today
  - David Mazières: software abstractions for security
  - Dawson Engler: verifying software without hardware

The *Internet* of Things

- Networking is one of the hardest development challenges in IoT applications
  - Ultra-low power protocols
  - Difficult link layers (4G, BLE), protocol mismatches
- Framework handles this automatically
  - Novel network algorithms
- Talks today
  - Keith Winstein, reliability in challenged networks
  - Pat Pannuto, low power wireless

Software-defined Hardware

- Hardware (boards, chips, power) is a daunting challenge to software developers
  - It easier to modify something than create it from scratch
- The data processing pipeline is sufficient information to specify a basic embedded device
  - Sensors, networking, storage, processing needed
- Talks today
  - Mark Horowitz: underlying technology trends
  - Pat Pannuto: embedded device design
  - Björn Hartmann: prototyping new applications

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
- Talks today
  - Björn Hartmann: prototyping new applications

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

Schumpeter
Business and management

Previous | Next | Latest Schumpeter | Latest from all our blogs

The "internet of things"

The internet of hype

Dec 9th 2010, 12:42 by Schumpeter

Why Now?

- Technology has just reached the tipping point
  - BLE, iBeacon
  - Cortex M series
  - Sensors
  - Harvesting circuits
- We've been waiting
  - RPL experience: I wrote the security section
  - 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)

Who Are We?

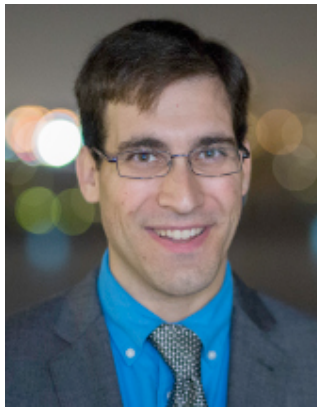
Philip Levis
Stanford

Mark Horowitz
Stanford

Christopher Ré
Stanford

Dan Boneh
Stanford

Dawson Engler
Stanford



Keith Winstein
Stanford

Prabal Dutta
Michigan

David Mazières
Stanford

Björn Hartmann
Berkeley

Raluca Ada Popa
Berkeley

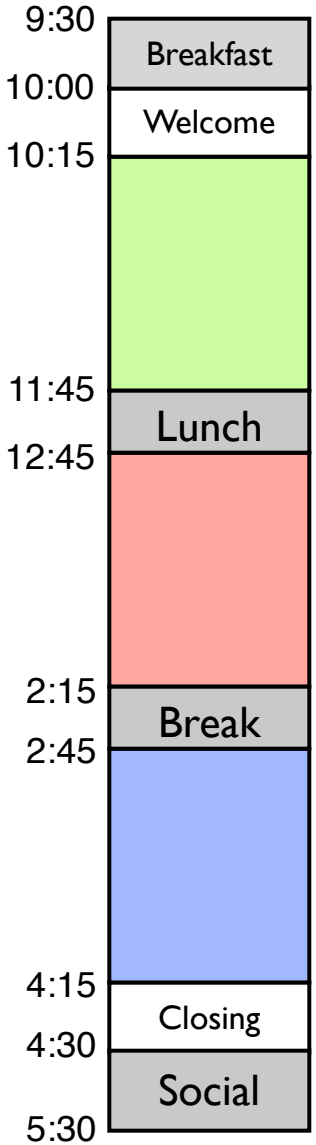
Greg Kovacs
Stanford

Christos Kozyrakis
Stanford

We Need Your Help

- Rethink building IoT systems from the ground up, researching the foundations of a secure IoT
- We are starting an industrial affiliates program
  - Affiliates financially support the research (we are also applying for governmental funding: DARPA, NSF, etc.)
  - Affiliates invited to yearly project retreats to hear the latest results and provide feedback as well as guidance
  - Affiliates collaborate with us, drive our research towards the practical and vexing problems
- Today will give you much greater detail on our goals: talk with researchers and ask questions!

Schedule



Technology and Applications

Philip Levis: Overview of SITP
Mark Horowitz: Technology push: silicon
Christopher Ré: Application pull: analytics

Security and Networks

Dan Boneh: Computing on secure data
Dawson Engler: Software verification
Keith Winstein: Challenged networks

Hardware, Software and Users

Pat Pannuto: IoT device design
David Mazières: Secure software
Björn Hartmann: Prototypes and security

Questions