# End-to-End Security for the Internet of Things

**Prabal Dutta**[o]

Dan Boneh[†], Dawson Engler[†], Björn Hartmann[*], Mark Horowitz[†], Philip Levis[†], Raluca Ada Popa[*], Keith Winstein[†]

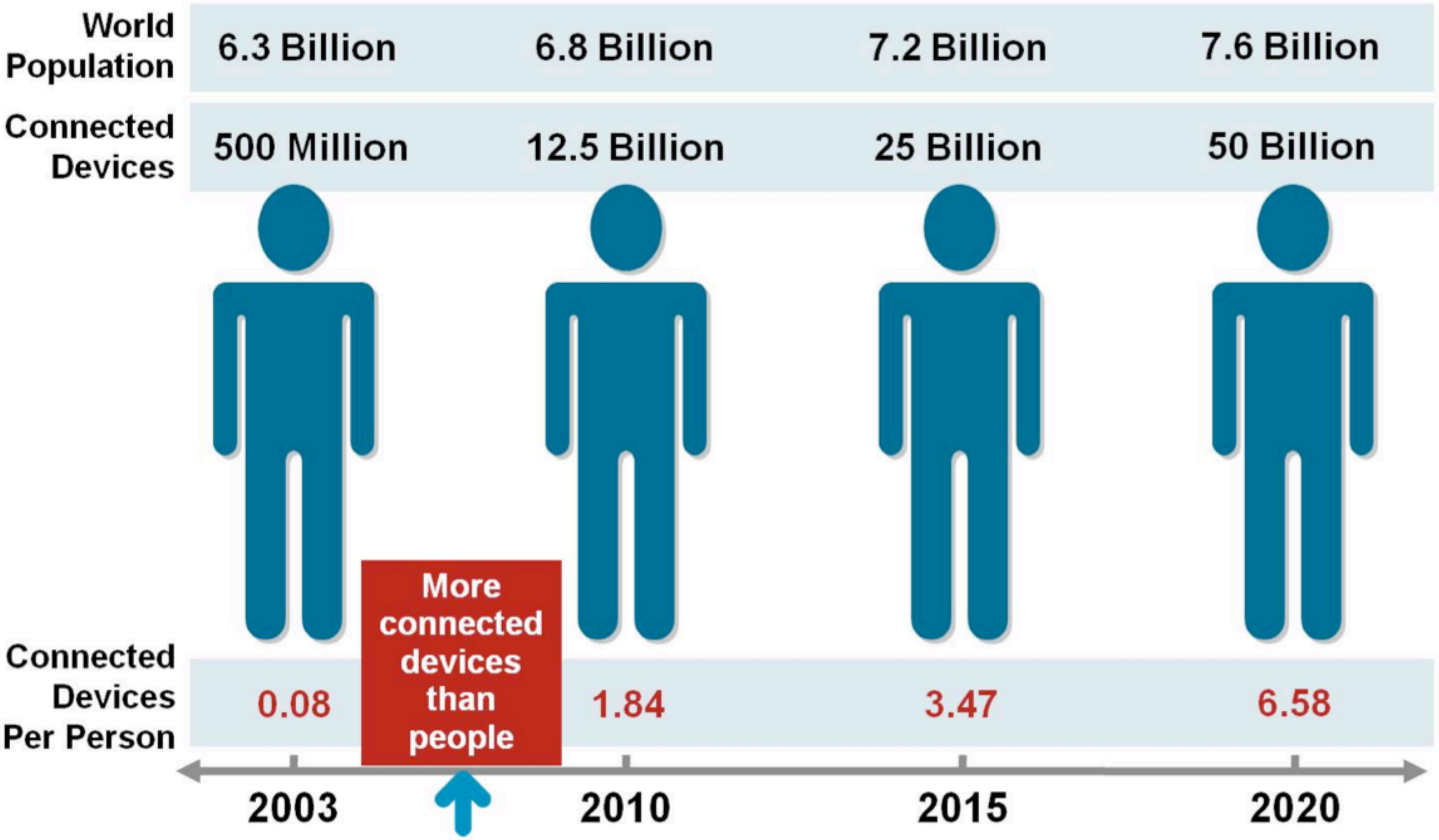
[o]University of Michigan, [†]Stanford University, and [*]UC Berkeley

# The Internet of Things

*“Sensors and actuators connected by networks to computers”*

*- McKinsey & Co.*

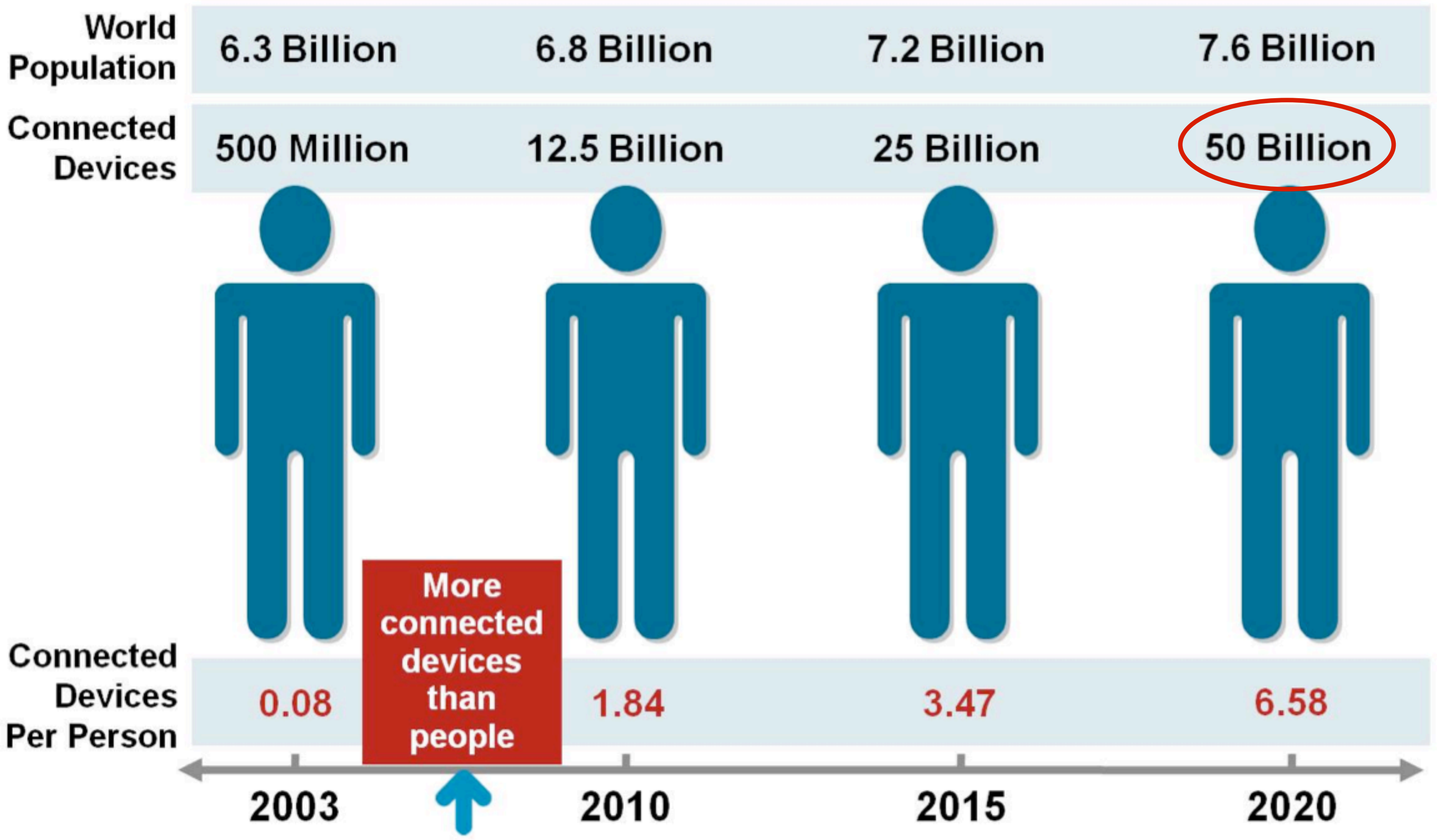
# The Internet of Things (IoT)



| | 2003 | 2010 | 2015 | 2020 |
|---|---|---|---|---|
| World Population | 6.3 Billion | 6.8 Billion | 7.2 Billion | 7.6 Billion |
| Connected Devices | 500 Million | 12.5 Billion | 25 Billion | 50 Billion |
| Connected Devices Per Person | 0.08 | 1.84 | 3.47 | 6.58 |

Source: Cisco IBSG, April 2011

# The Internet of Things (IoT)

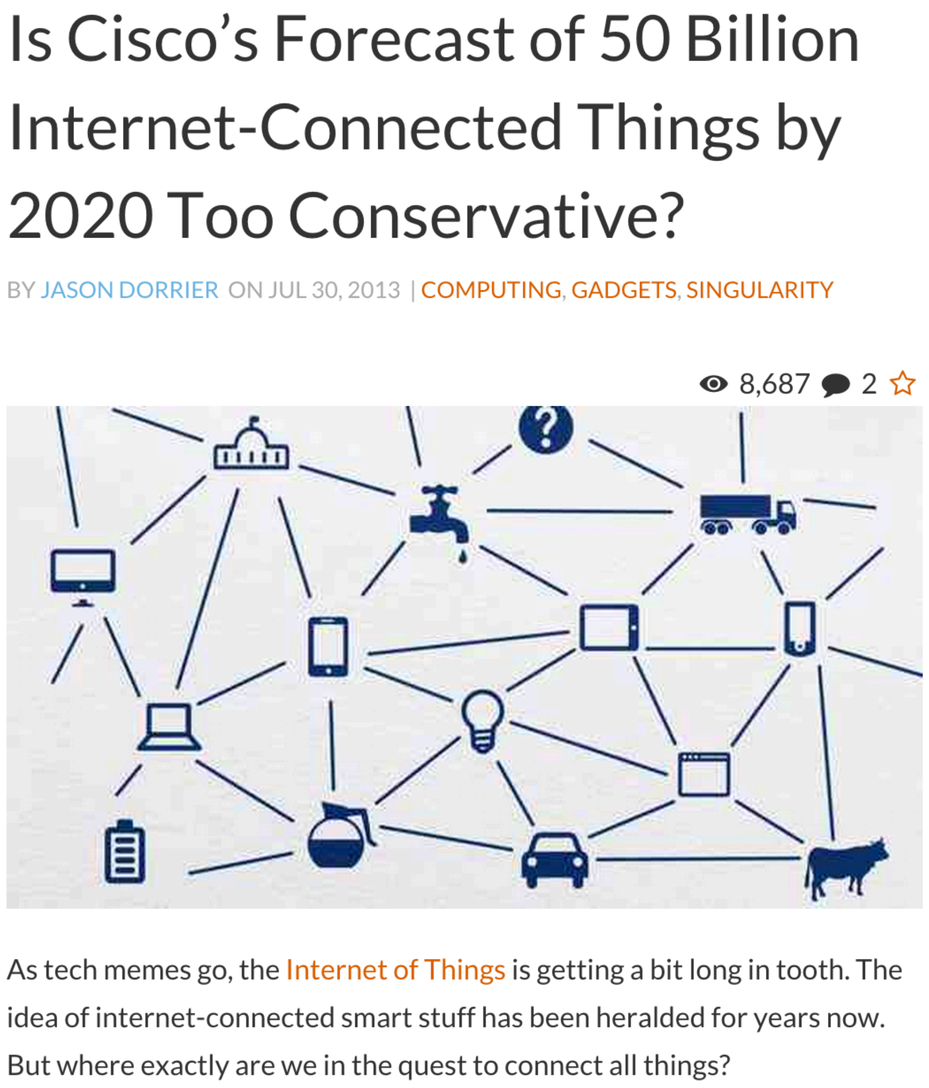


| | 2003 | 2010 | 2015 | 2020 |
|---|---|---|---|---|
| World Population | 6.3 Billion | 6.8 Billion | 7.2 Billion | 7.6 Billion |
| Connected Devices | 500 Million | 12.5 Billion | 25 Billion | 50 Billion |
| Connected Devices Per Person | 0.08 | 1.84 | 3.47 | 6.58 |

More connected devices than people

Source: Cisco IBSG, April 2011

# Some wild projections



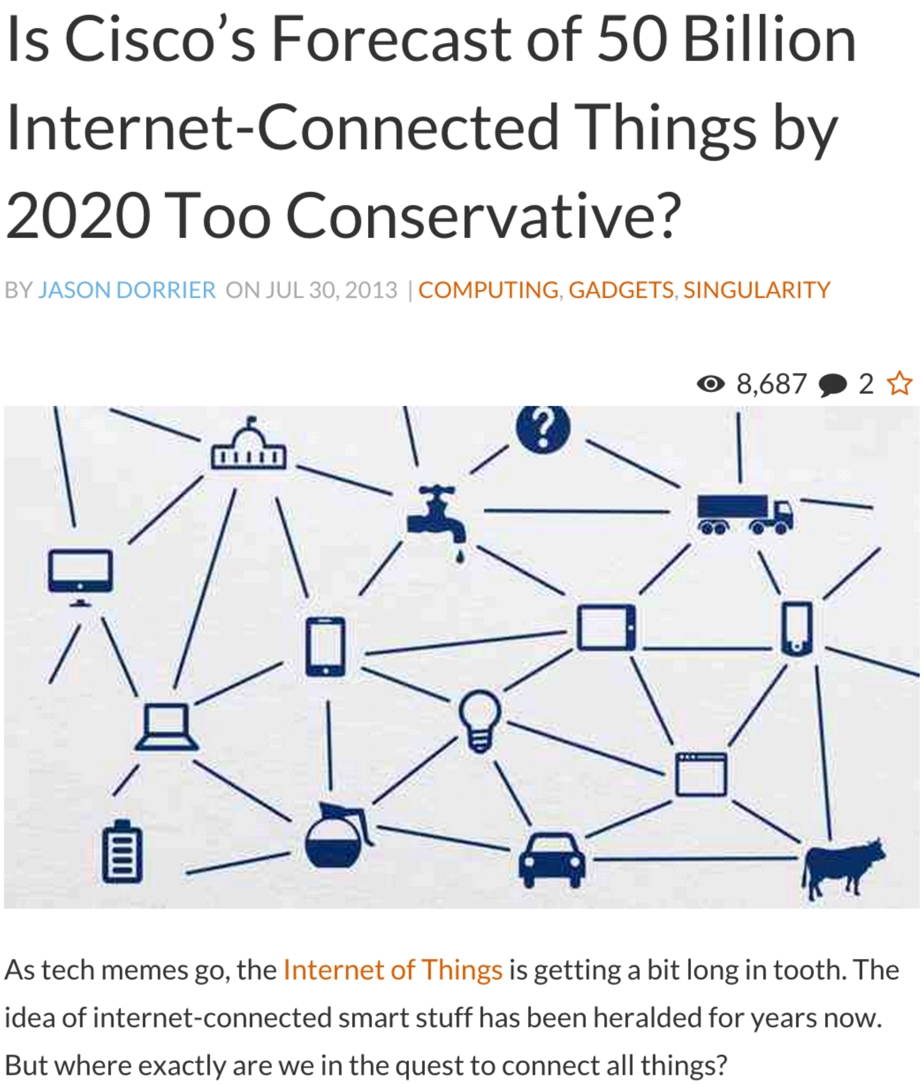
## Is Cisco's Forecast of 50 Billion Internet-Connected Things by 2020 Too Conservative?

BY JASON DORRIER ON JUL 30, 2013 | COMPUTING, GADGETS, SINGULARITY

8,687 2 ☆

As tech memes go, the Internet of Things is getting a bit long in tooth. The idea of internet-connected smart stuff has been heralded for years now. But where exactly are we in the quest to connect all things?

# Some wild projections



## Is Cisco's Forecast of 50 Billion Internet-Connected Things by 2020 Too Conservative?

BY JASON DORRIER ON JUL 30, 2013 | COMPUTING, GADGETS, SINGULARITY

👁 8,687 💬 2 ☆

As tech memes go, the Internet of Things is getting a bit long in tooth. The idea of internet-connected smart stuff has been heralded for years now. But where exactly are we in the quest to connect all things?

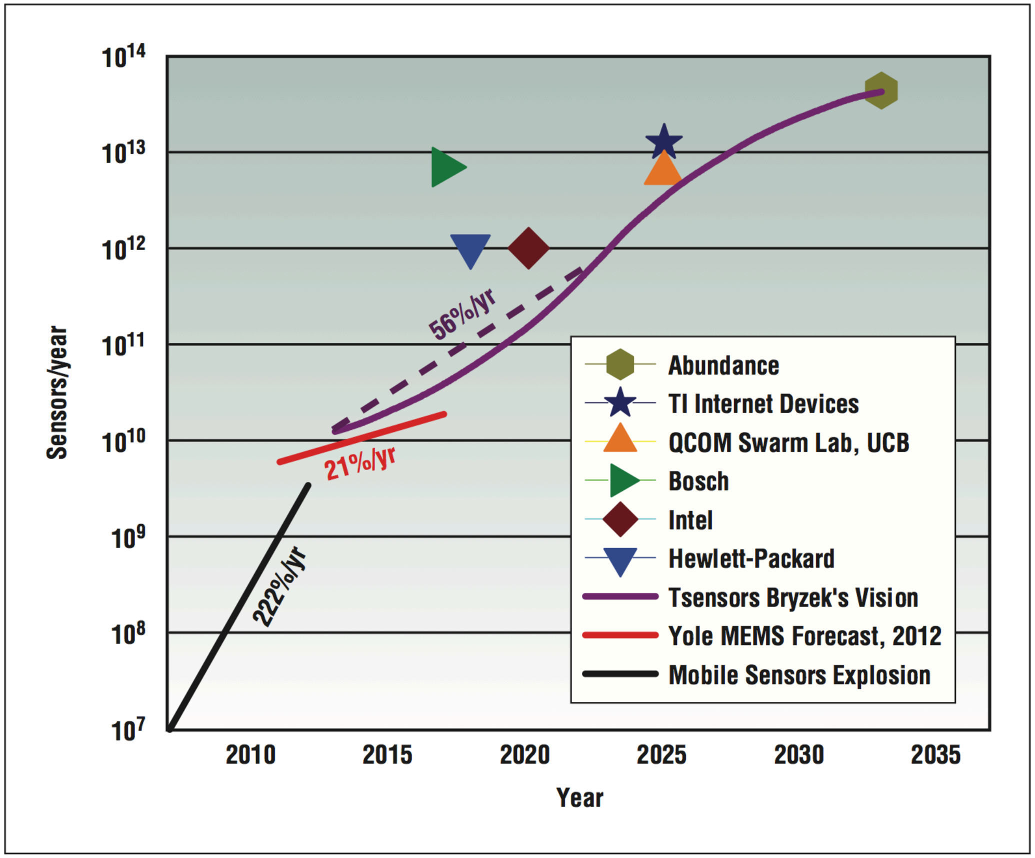
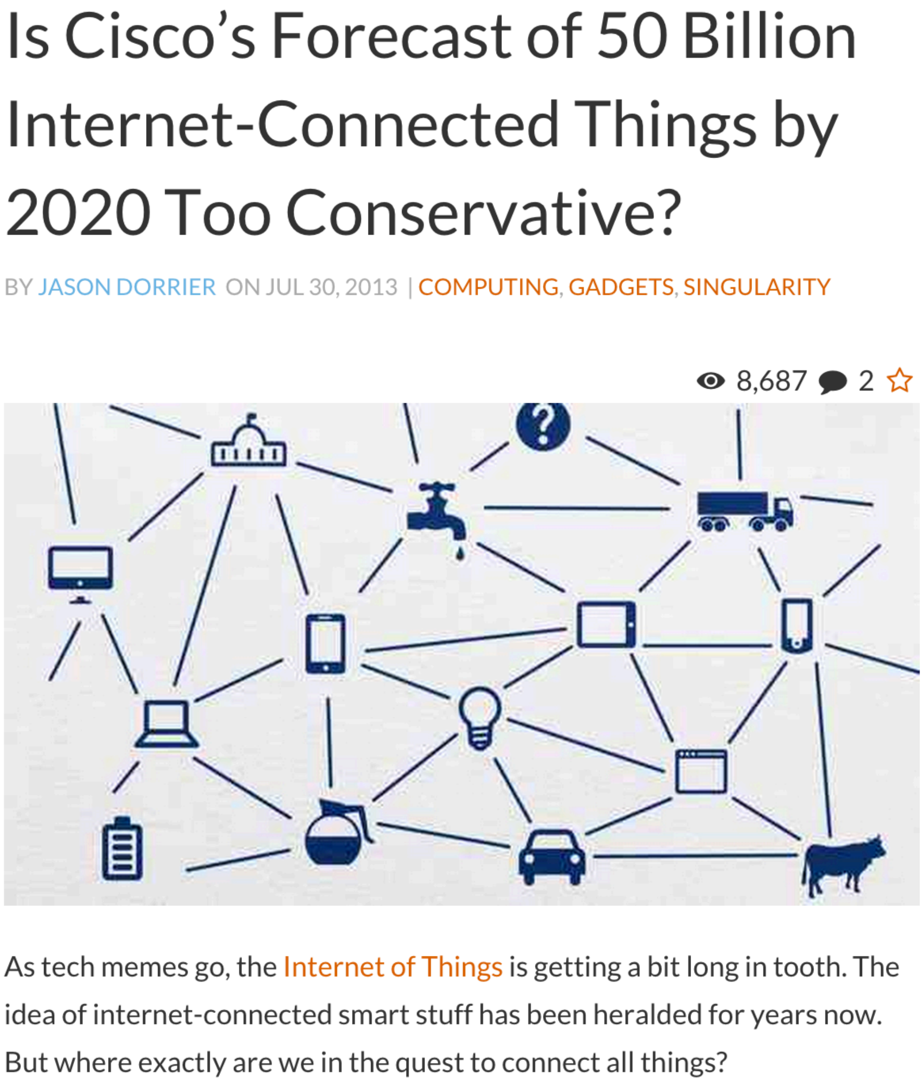


**Figure 2. Actual and projected growth of sensor deployment based on the predictions from a number of leading research labs or companies. (Image courtesy of Janusz Bryzek, Fairchild and chair of TSensors Summit; used with permission.)**

Jan Rabaey, "The Human Intranet – Where Swarms and Humans Meet," IEEE Pervasive Computing Magazine, January—March, 2015

# Some wild projections



## Is Cisco's Forecast of 50 Billion Internet-Connected Things by 2020 Too Conservative?

BY JASON DORRIER ON JUL 30, 2013 | COMPUTING, GADGETS, SINGULARITY

👁 8,687 💬 2 ☆

As tech memes go, the Internet of Things is getting a bit long in tooth. The idea of internet-connected smart stuff has been heralded for years now. But where exactly are we in the quest to connect all things?

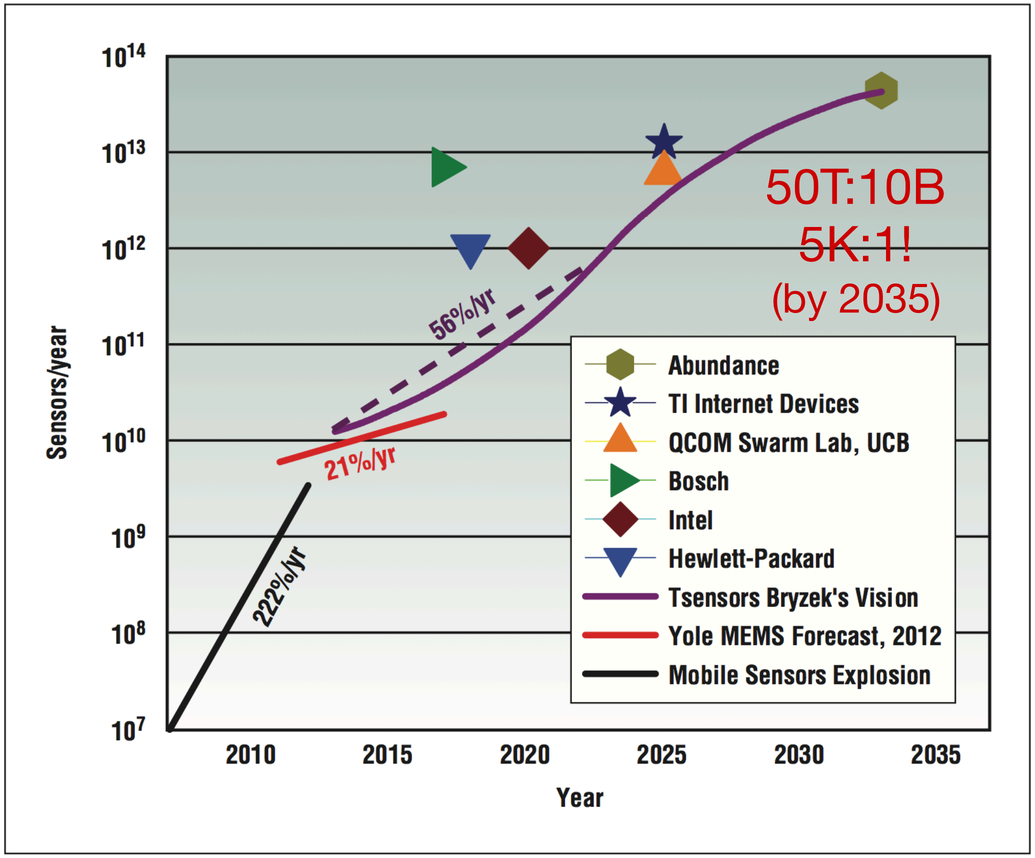


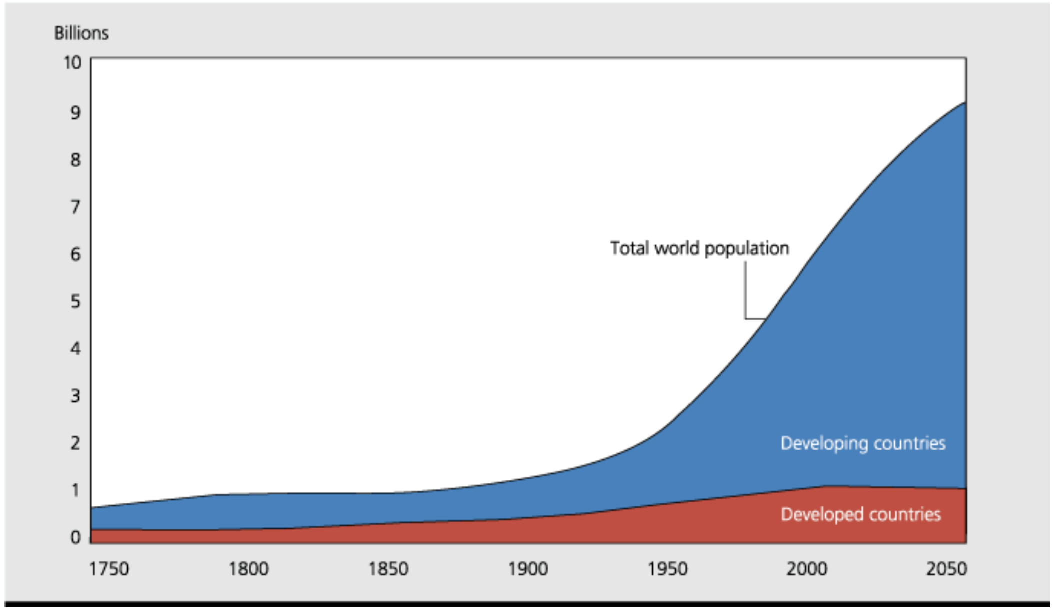
**Figure 2. Actual and projected growth of sensor deployment based on the predictions from a number of leading research labs or companies. (Image courtesy of Janusz Bryzek, Fairchild and chair of TSensors Summit; used with permission.)**

Jan Rabaey, "The Human Intranet – Where Swarms and Humans Meet," IEEE Pervasive Computing Magazine, January—March, 2015

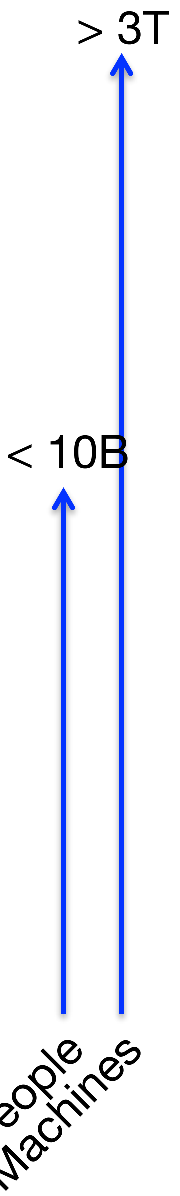
# Computers : People

>300:1 ?!

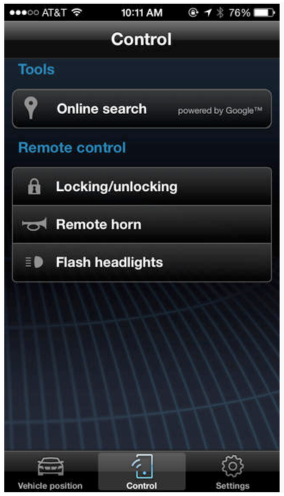
**Figure 3.1** **World population, 1750–2050**



http://www.worldbank.org/depweb/english/beyond/global/chapter3.html



# IoT in Everyday Life


●●●○○ AT&T 10:11 AM 76%

Control

Tools

Online search powered by Google™

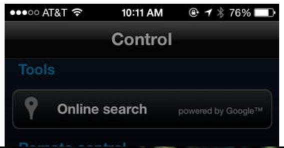
Remote control

Locking/unlocking

Remote horn

Flash headlights

Vehicle position Control Settings


●●●○○ AT&T 10:11 AM 76%

Control

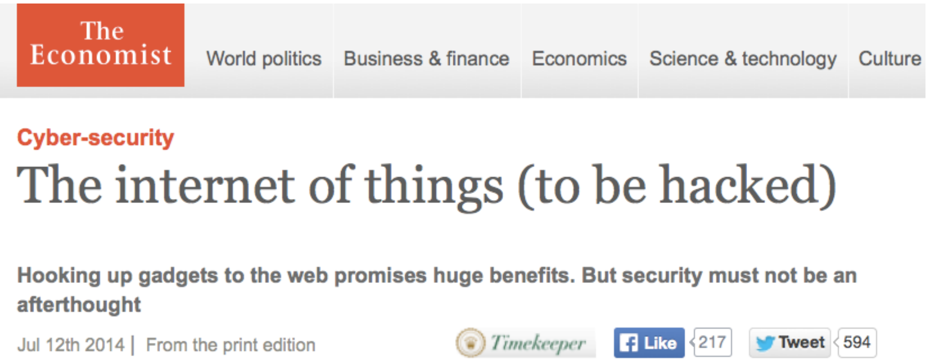
Tools

Online search powered by Google™

# Intranet(s) / Internet 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 |

# A Security Disaster

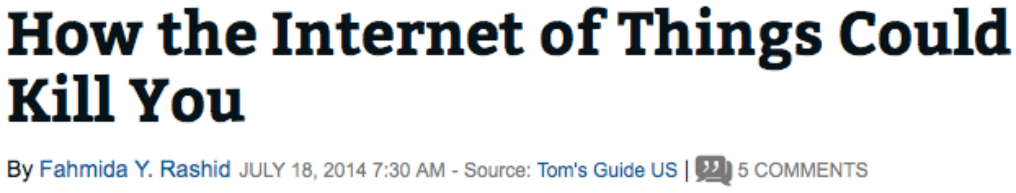


Cyber-security

The internet of things (to be hacked)

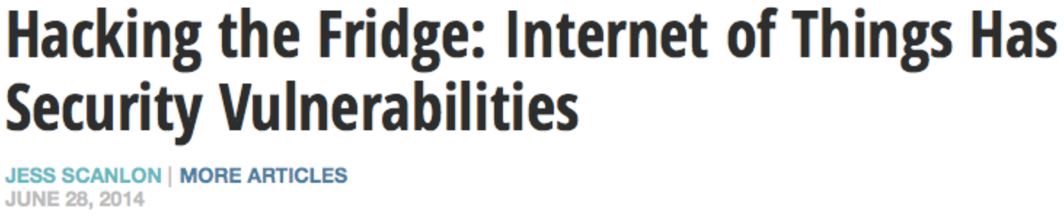
Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition



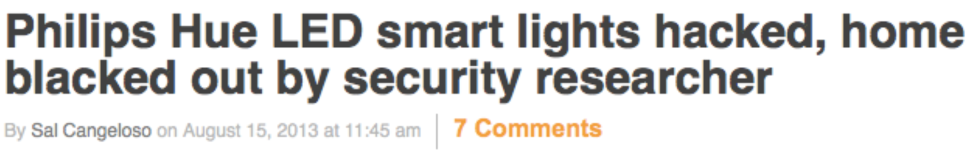
**How the Internet of Things Could Kill You**

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

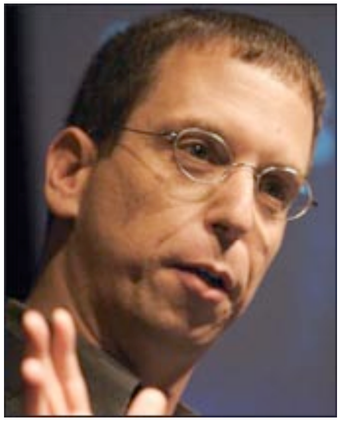
- HP conducted a security analysis of IoT devices[1]
  - 80% had privacy concerns
  - 80% had poor passwords
  - 70% lacked encryption
  - 60% had vulnerabilities in UI
  - 60% had insecure updates

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

# Securing the Internet of Things

- Rethink IoT systems, software, and applications from the ground up
- Overall transformative goal: *end-to-end security*
    - Unencrypted data never leaves embedded devices
    - All infrastructure computation is on encrypted data
    - Data isn't decrypted until viewed by end application
    - Services cannot compromise data because they cannot see it
- Make an end-to-end secure IoT application as easy as a modern web application
- And easy for users to deploy and use

# “Full-Stack” Security Team



Dan Boneh
Stanford
Cryptography

Prabal Dutta
Michigan
Embedded Hardware

Dawson Engler
Stanford
Software

Björn Hartmann
Berkeley
Prototyping

Mark Horowitz
Stanford
Hardware

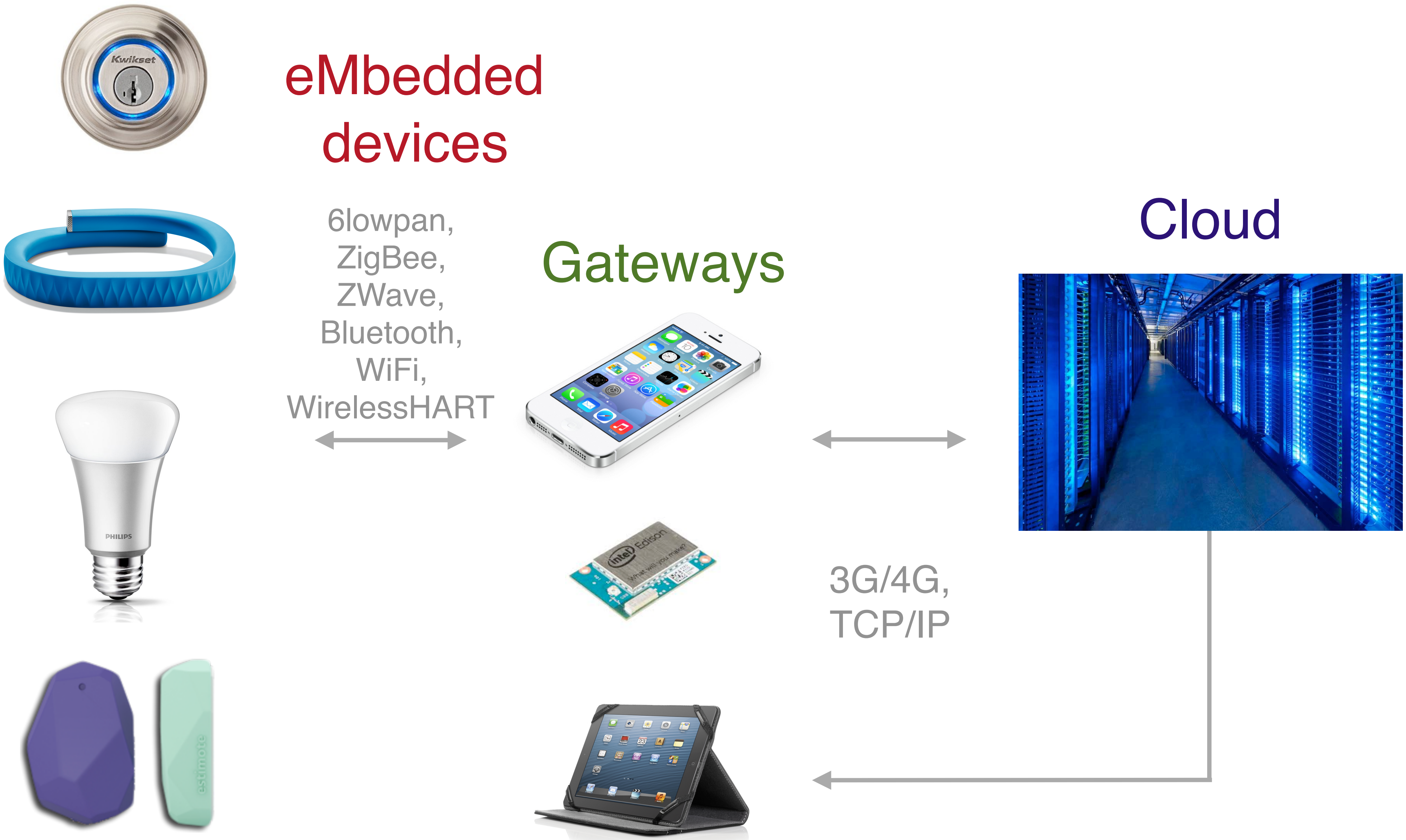
Philip Levis
Stanford
Embedded Software

Raluca Ada Popa
Berkeley
Security

Keith Winstein
Stanford
Networks

Underlined names are on the call

# IoT: MGC Architecture



eMbedded devices

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

Gateways

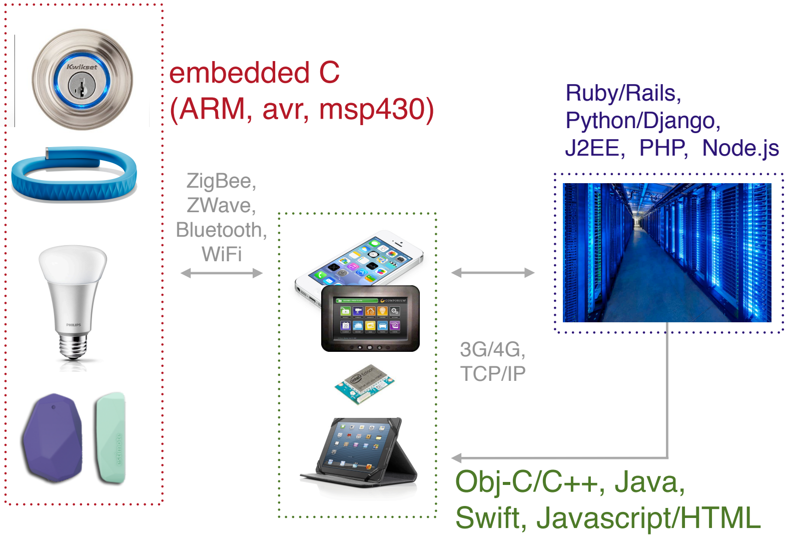
3G/4G, TCP/IP

Cloud

End application

# IoT Security is Challenging

- 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.
- Hardware companies who need software help
- Valuable data: personal, location, presence



- Rush to development + hard ➔ avoid, deal later

# Architectural Principles

- End-to-end: consider security holistically, from data generation to end-user display.

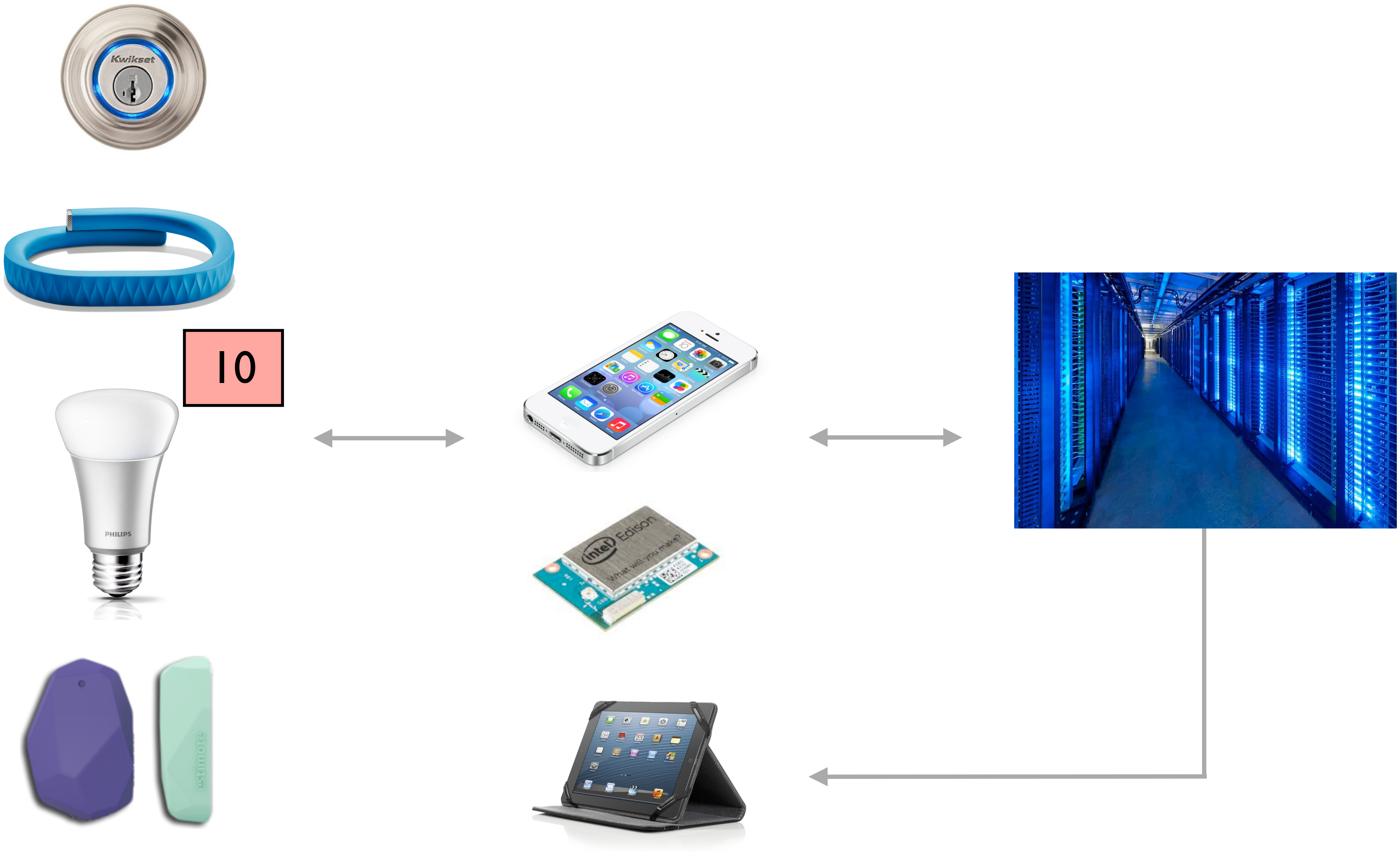
- Transparency: we must be able to observe what our devices are saying about us.

- Longevity: these systems will last for up to 20 years and their security must too.

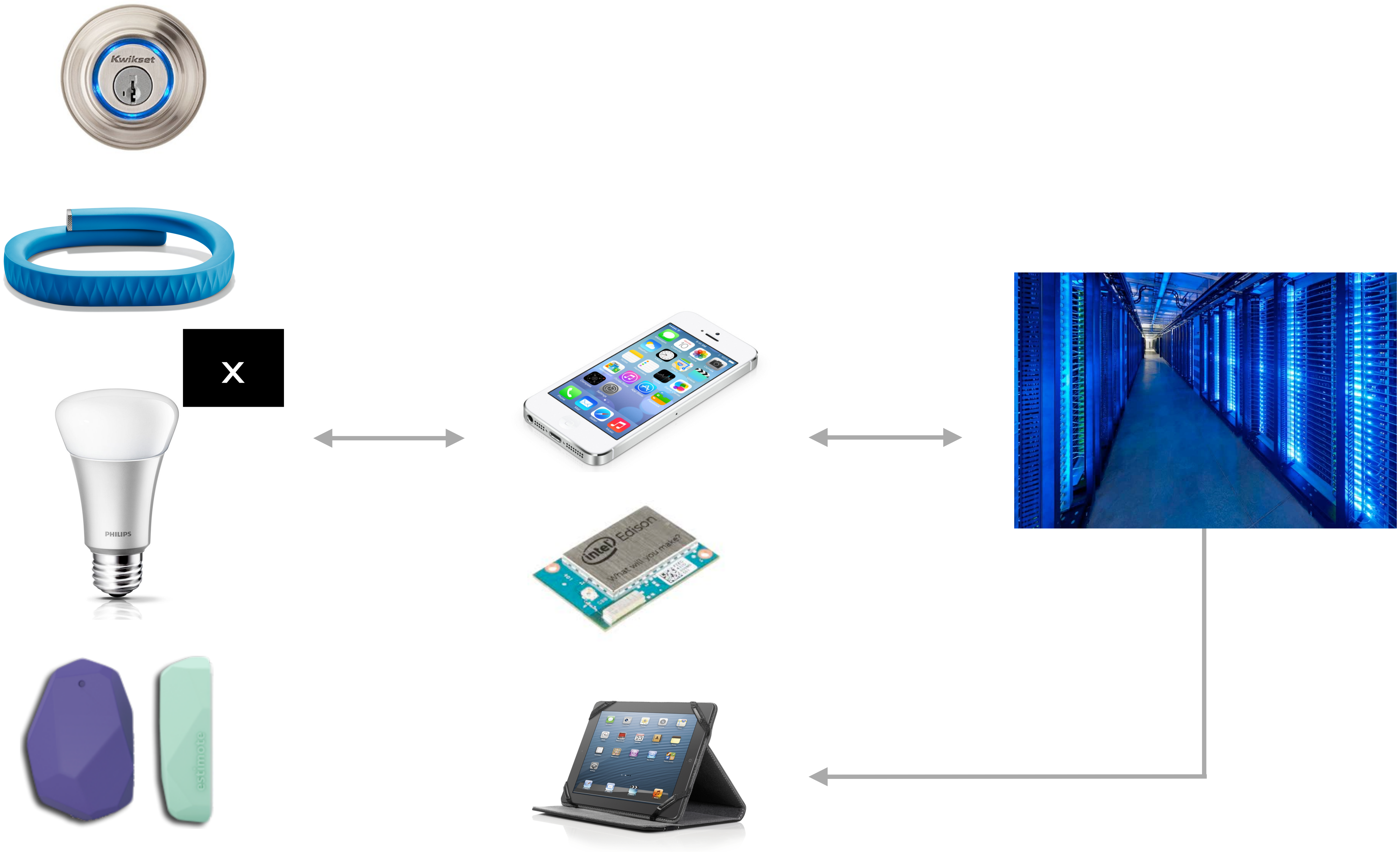
# Architectural Principles

- End-to-end: consider security holistically, from data generation to end-user display.
- Transparency: we must be able to observe what our devices are saying about us.
- Longevity: these systems will last for up to 20 years and their security must too.

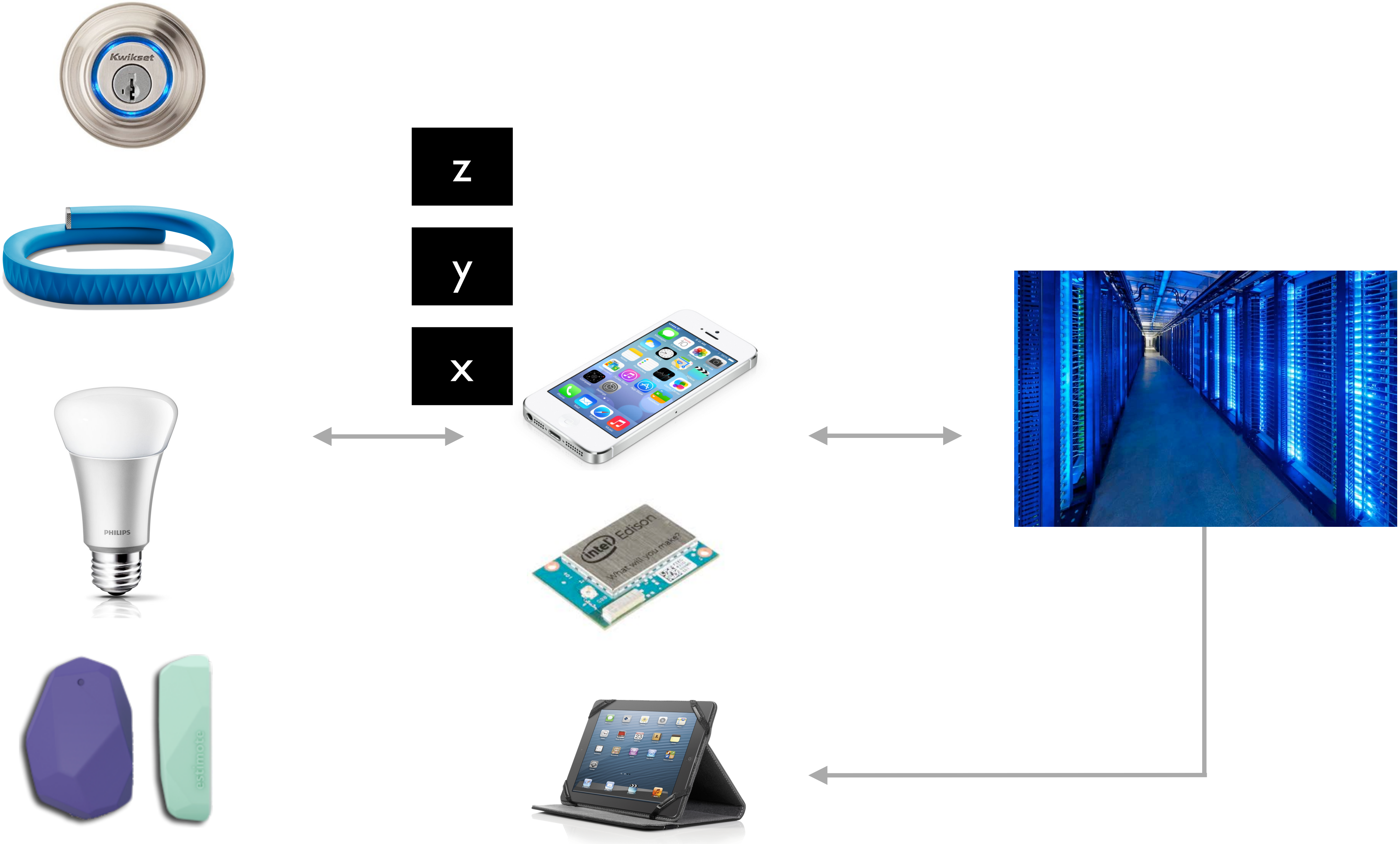
# End-to-End Security



# End-to-End Security



# End-to-End Security

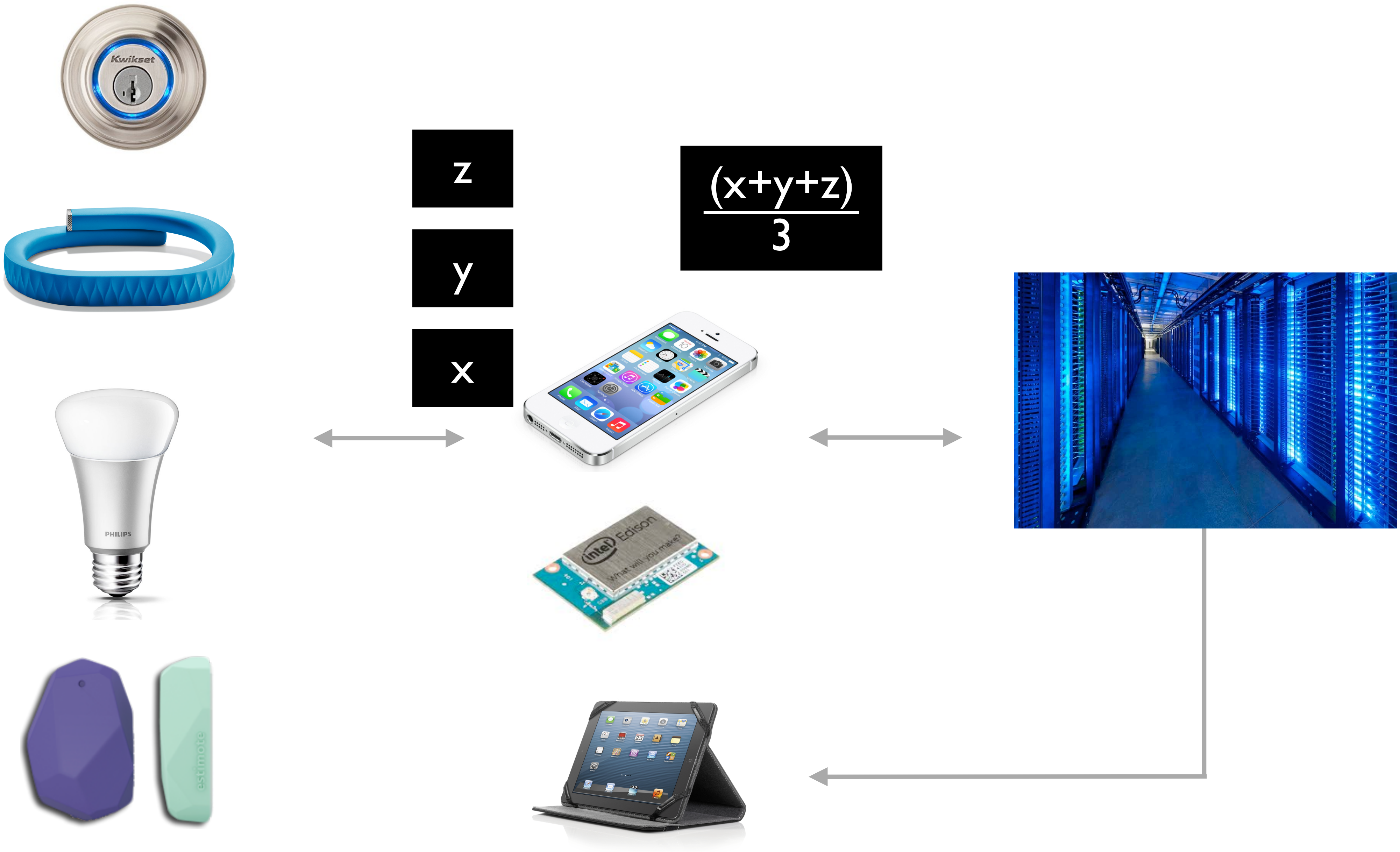


z

y

x

# End-to-End Security



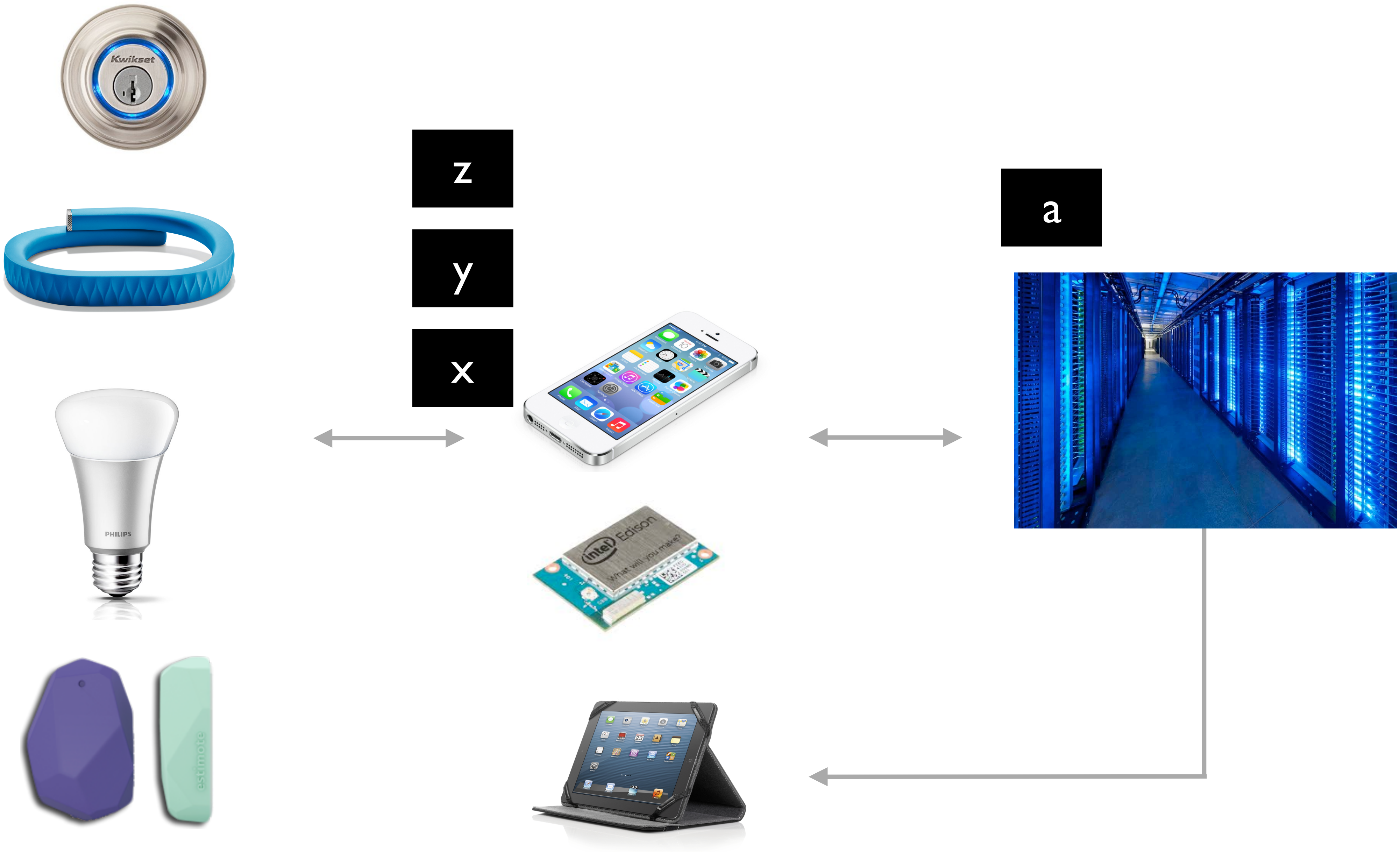
z

y

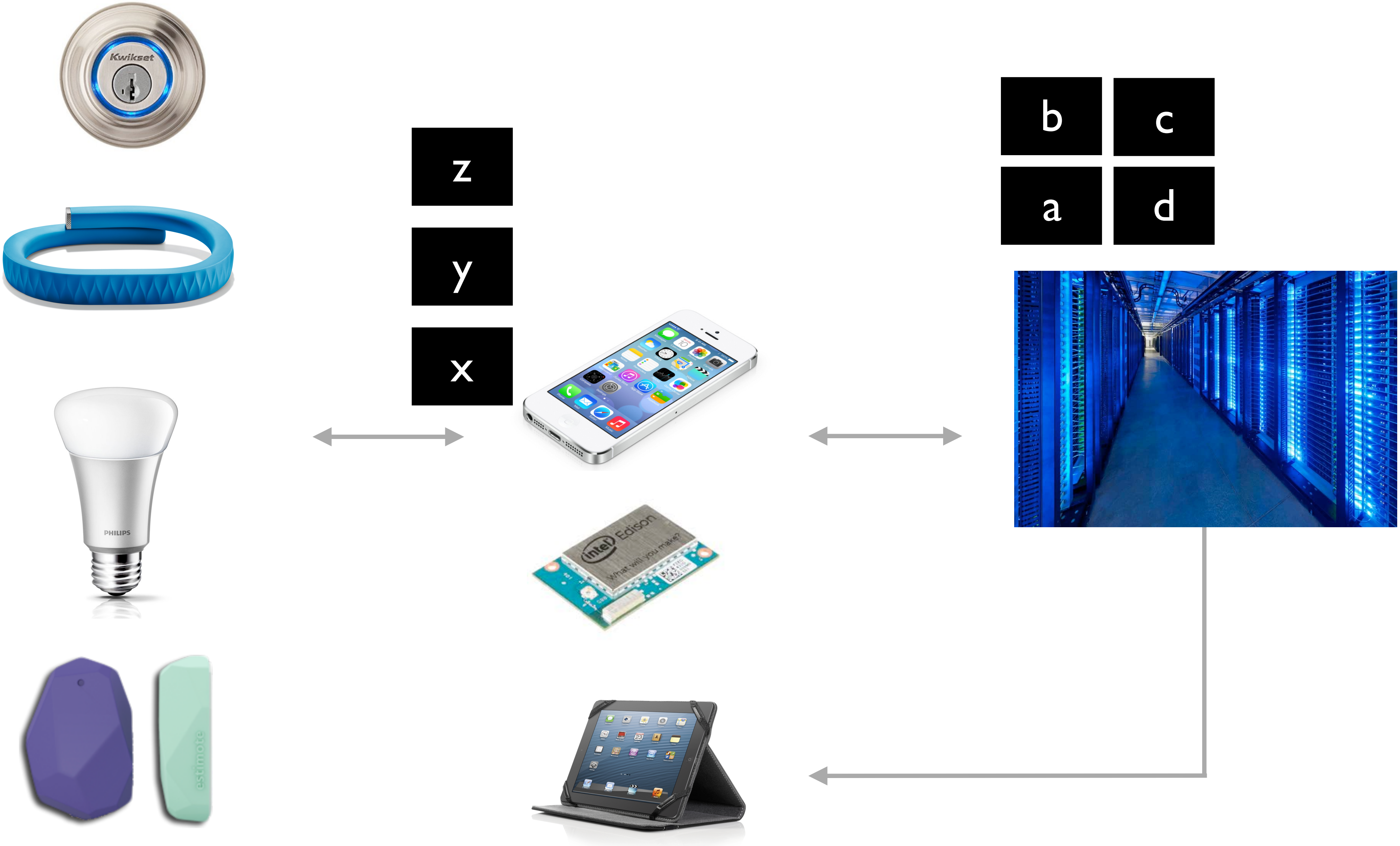
x

$$\frac{(x+y+z)}{3}$$

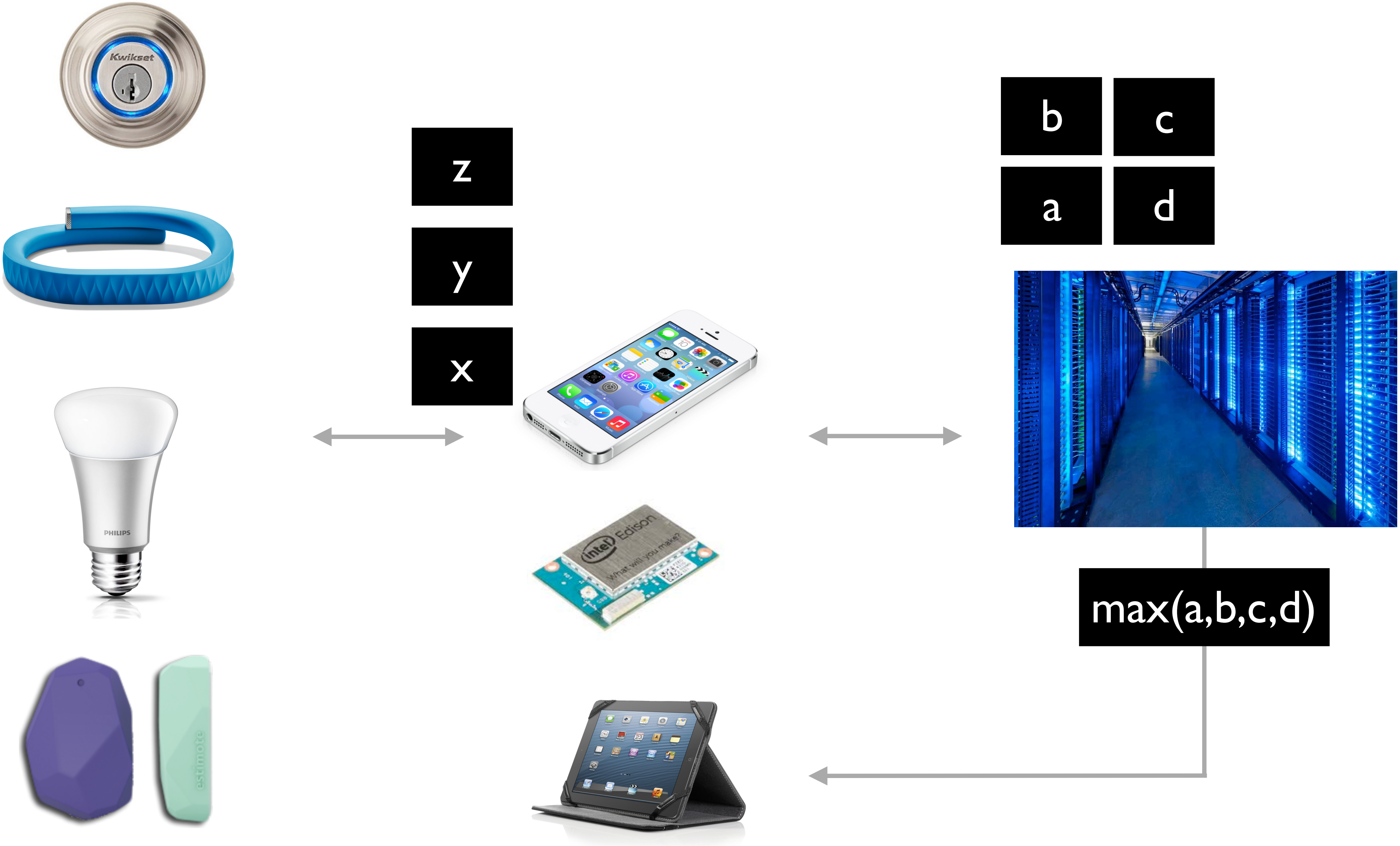
# End-to-End Security



# End-to-End Security



# End-to-End Security



z

y

x

b

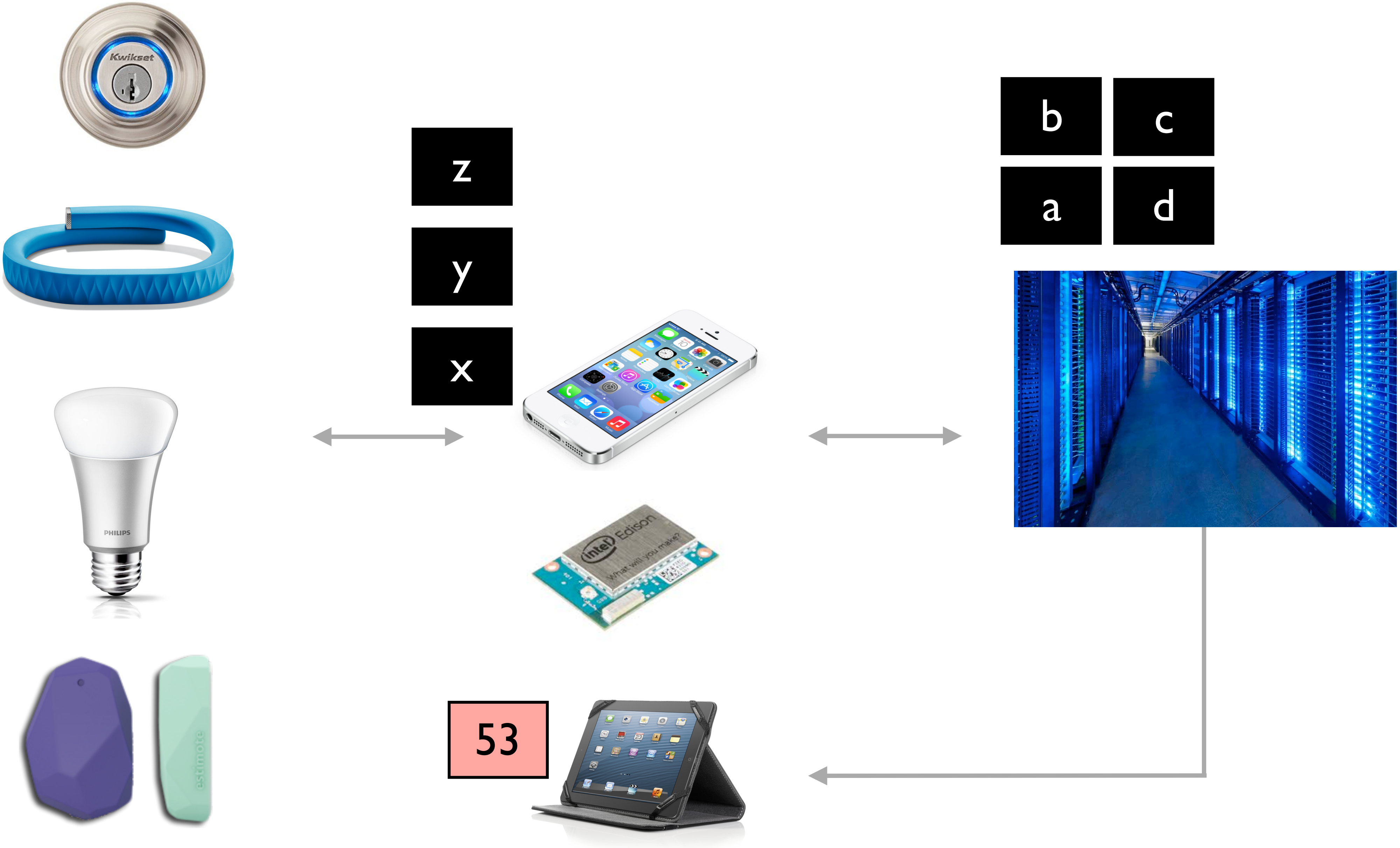
c

a

d

max(a,b,c,d)

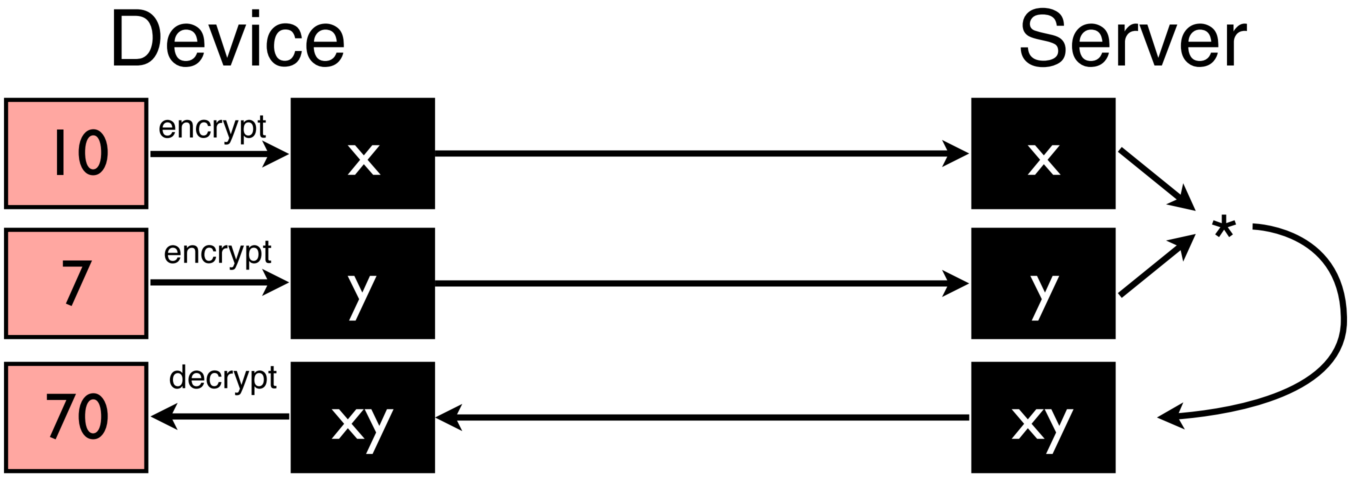
# End-to-End Security



# Homomorphic Encryption

(Gentry, Stanford University, 2009)

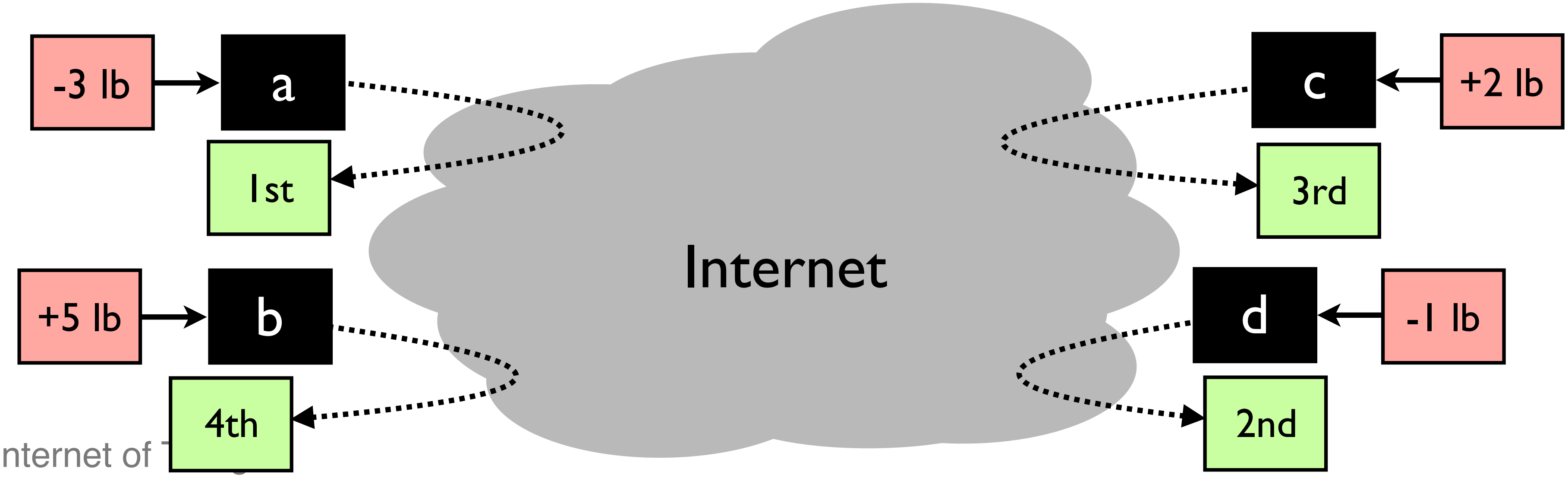
- Take a sensor value *S*, encrypt it to be $S_e$
- It is possible to perform arbitrary computations on $S_e$



- 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., *)

# Distributed Computation

- Multiple parties want to jointly compute a statistic, aggregate, or value (e.g., average)
- Each party encrypts value, performs multi-round communication with cloud and/or other parties
- Each party obtains result without revealing value
  - Trades off communication for less computation



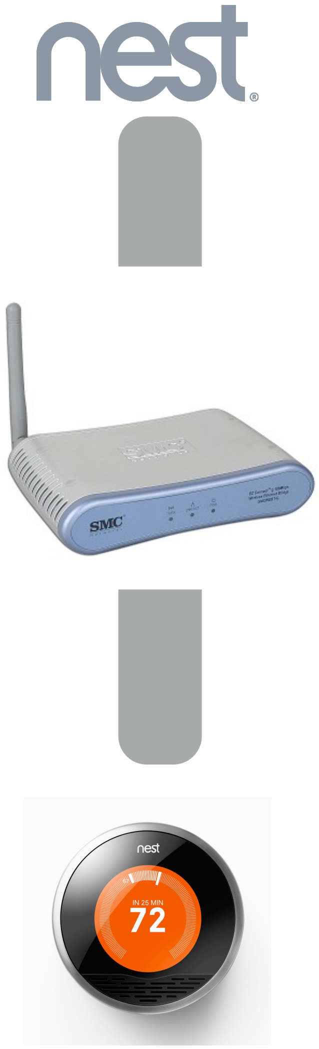
# Architectural Principles

- End-to-end: consider security holistically, from data generation to end-user display.

- Transparency: we must be able to observe what our devices are saying about us.

- Longevity: these systems will last for up to 20 years and their security must too.

# Model Today



- Transport-layer security (TLS) between devices and cloud services
- Internet applications: we control one end point
  - Can install new certificates, observe data
- IoT applications: we are a transit network
  - Can't see or control what happens on either end

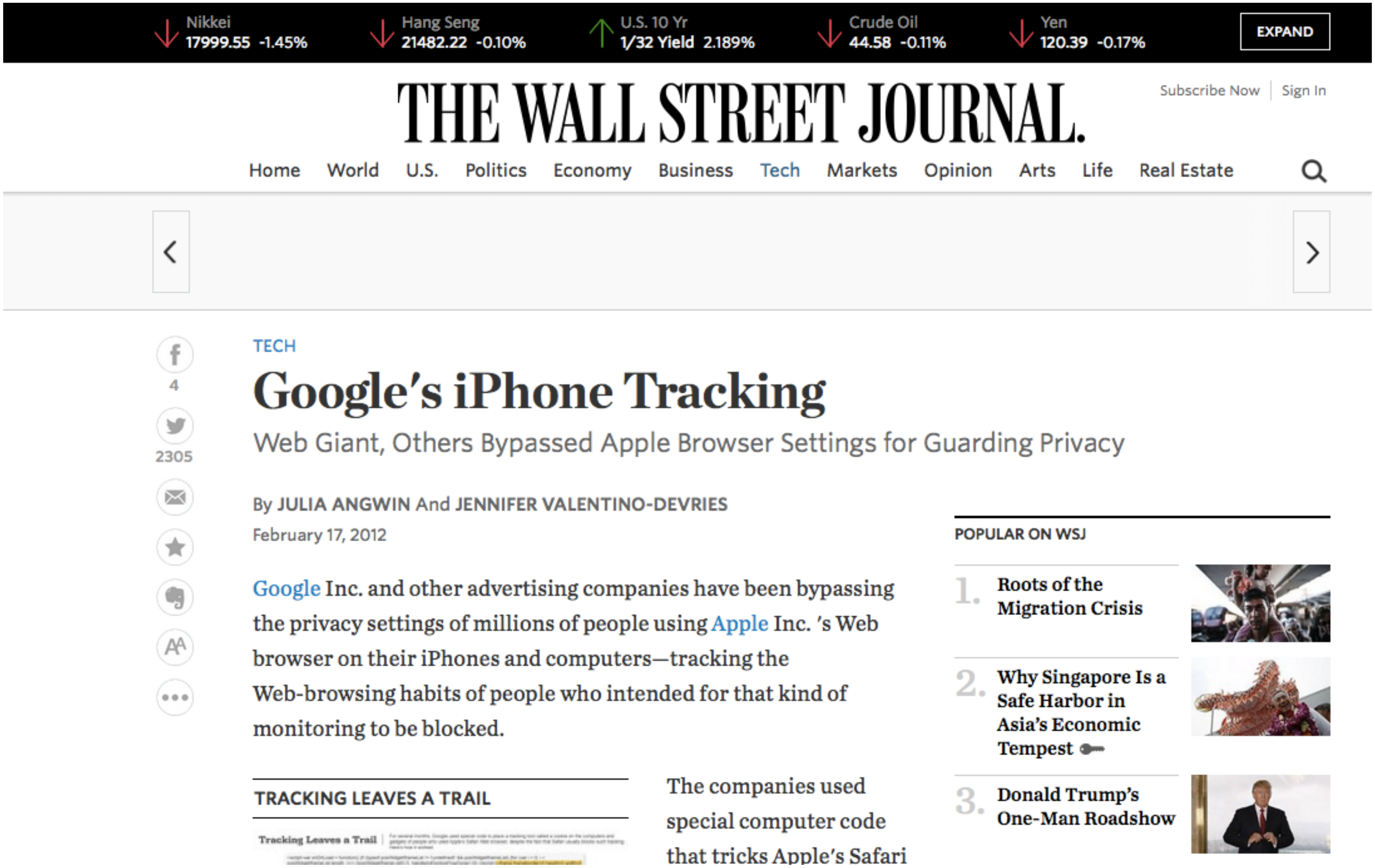
# Intrusion Detection

- How do we build an intrusion detection system for our smart home?
  - Can’t see what data our devices are transmitting
  - They could be compromised and we’ll never know
- Enterprises solve this by installing new certificates on endpoints, allow IDS to look inside TLS, filter trojan horses from email, etc.
  - We don’t control these devices, can’t install new certificates

# Independent Checks

> “Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie.”
>
> - Google, 2012

# Stanford Student Eavesdrops on his PC….


Nikkei 17999.55 -1.45%
Hang Seng 21482.22 -0.10%
U.S. 10 Yr 1/32 Yield 2.189%
Crude Oil 44.58 -0.11%
Yen 120.39 -0.17%
EXPAND
Subscribe Now | Sign In
Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate
4
2305

THE WALL STREET JOURNAL.

TECH

## Google's iPhone Tracking

Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy

By JULIA ANGWIN And JENNIFER VALENTINO-DEVRIES

February 17, 2012

Google Inc. and other advertising companies have been bypassing the privacy settings of millions of people using Apple Inc. 's Web browser on their iPhones and computers—tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked.

TRACKING LEAVES A TRAIL

The companies used special computer code that tricks Apple's Safari

POPULAR ON WSJ

1. Roots of the Migration Crisis

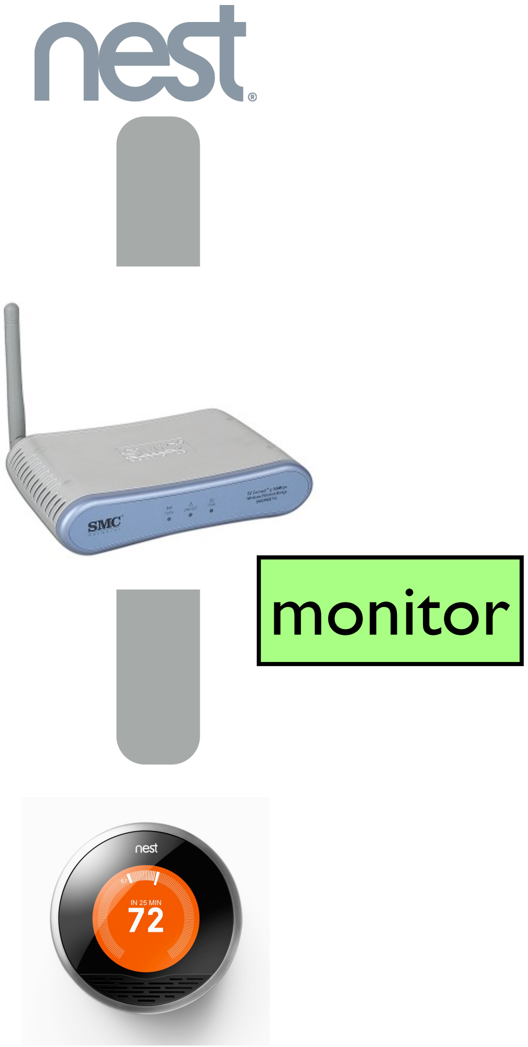
2. Why Singapore Is a Safe Harbor in Asia's Economic Tempest

3. Donald Trump's One-Man Roadshow

# This is a big deal

- Federal penalty (2012): $22.5 million
- State penalty (2013): $17 million
- Class-action consumer lawsuit:  ???
- Europe:  ???

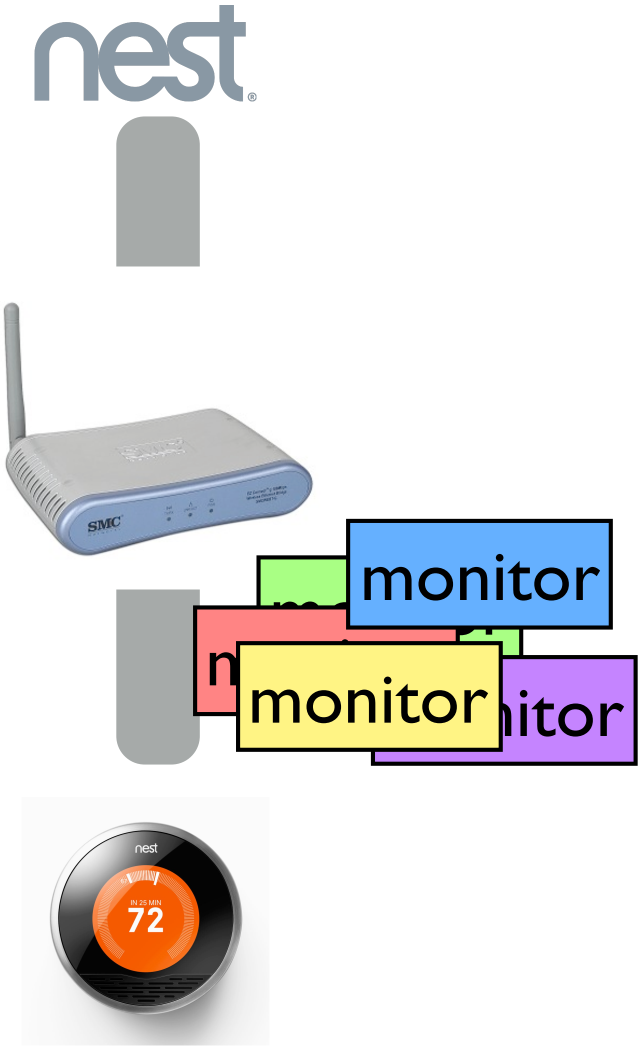
# Communication Architecture



monitor

- Allow us to
  - Inspect
  - Audit
  - Interdict
  - ~~Modify~~

# Communication Architecture



- Defense in depth
- Need new crypto constructions

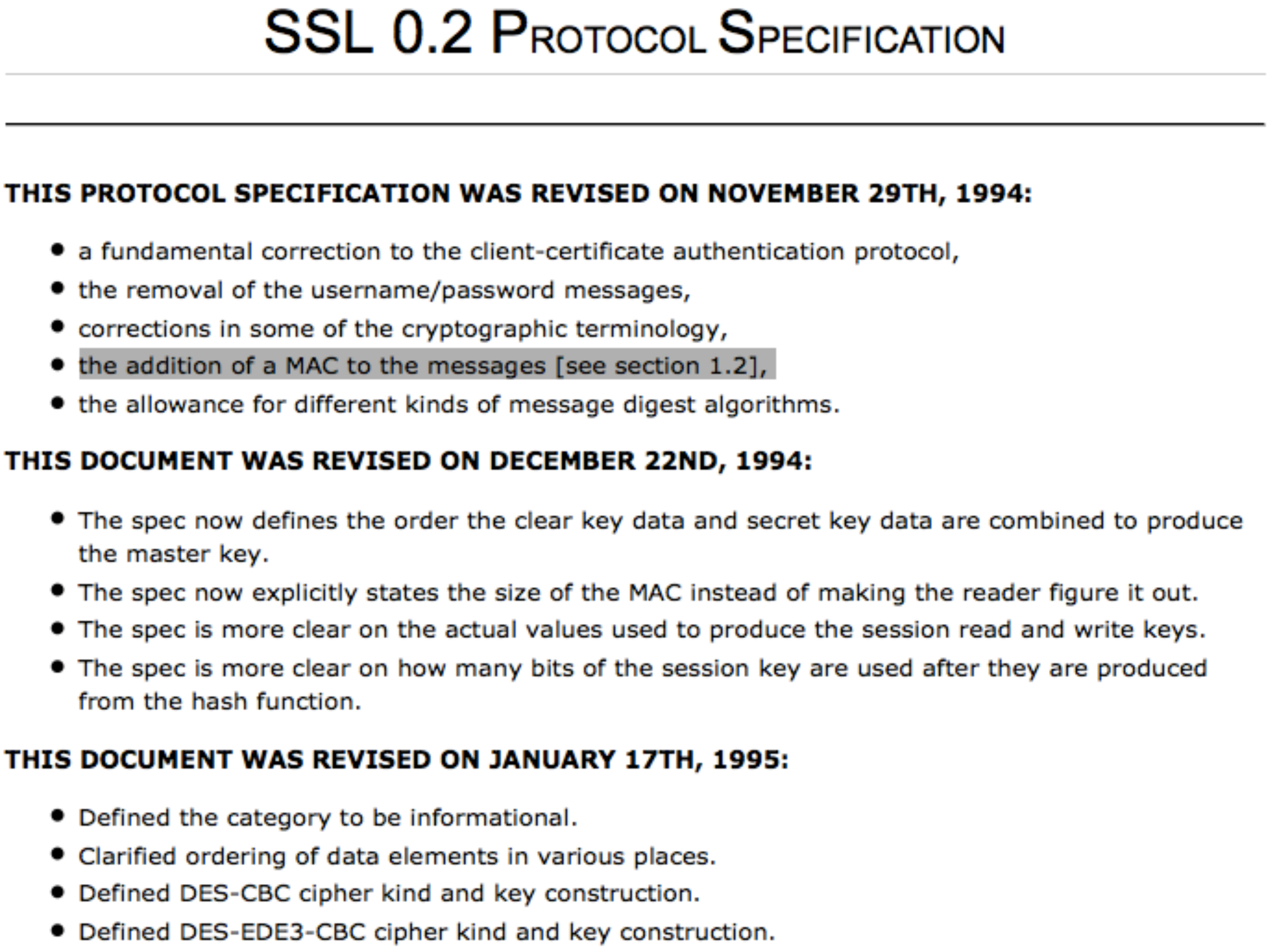
# Architectural Principles

- End-to-end: consider security holistically, from data generation to end-user display.

- Transparency: we must be able to observe what our devices are saying about us.

- Longevity: these systems will last for up to 20 years and their security must too.

# 1995: SSL 0.2



## SSL 0.2 Protocol Specification

**THIS PROTOCOL SPECIFICATION WAS REVISED ON NOVEMBER 29TH, 1994:**

- a fundamental correction to the client-certificate authentication protocol,
- the removal of the username/password messages,
- corrections in some of the cryptographic terminology,
- the addition of a MAC to the messages [see section 1.2],
- the allowance for different kinds of message digest algorithms.

**THIS DOCUMENT WAS REVISED ON DECEMBER 22ND, 1994:**

- The spec now defines the order the clear key data and secret key data are combined to produce the master key.
- The spec now explicitly states the size of the MAC instead of making the reader figure it out.
- The spec is more clear on the actual values used to produce the session read and write keys.
- The spec is more clear on how many bits of the session key are used after they are produced from the hash function.

**THIS DOCUMENT WAS REVISED ON JANUARY 17TH, 1995:**

- Defined the category to be informational.
- Clarified ordering of data elements in various places.
- Defined DES-CBC cipher kind and key construction.
- Defined DES-EDE3-CBC cipher kind and key construction.

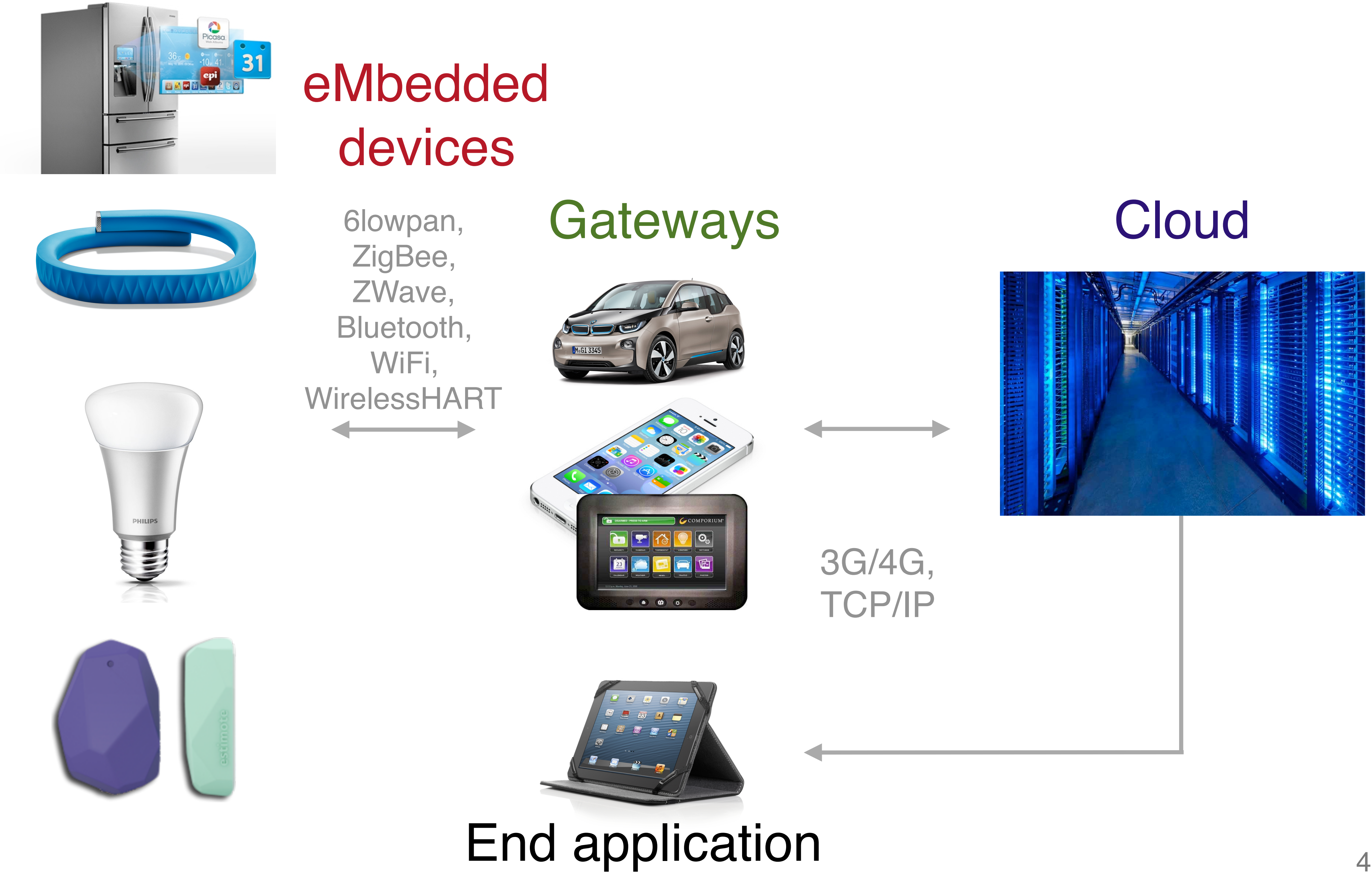
# A Truism

Anything connected to the Internet needs to be patched regularly to bugs, or it becomes vulnerable to vandals who will break in and commandeer it to their own ends.

# 20-year Cryptography

- Devices need to be able to support ciphers that are used 20 years from now
- Add extensible cryptographic accelerator: silicon is cheap and BLE dominates the SoC
- Designing a 20-year crypto processor
  - Symmetric crypto: S-boxes and P-boxes, an instruction set
  - Public key crypto: several very different constructions
  - What if quantum computers are real in 20 years?

# IoT: MGC Architecture



eMbedded devices

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

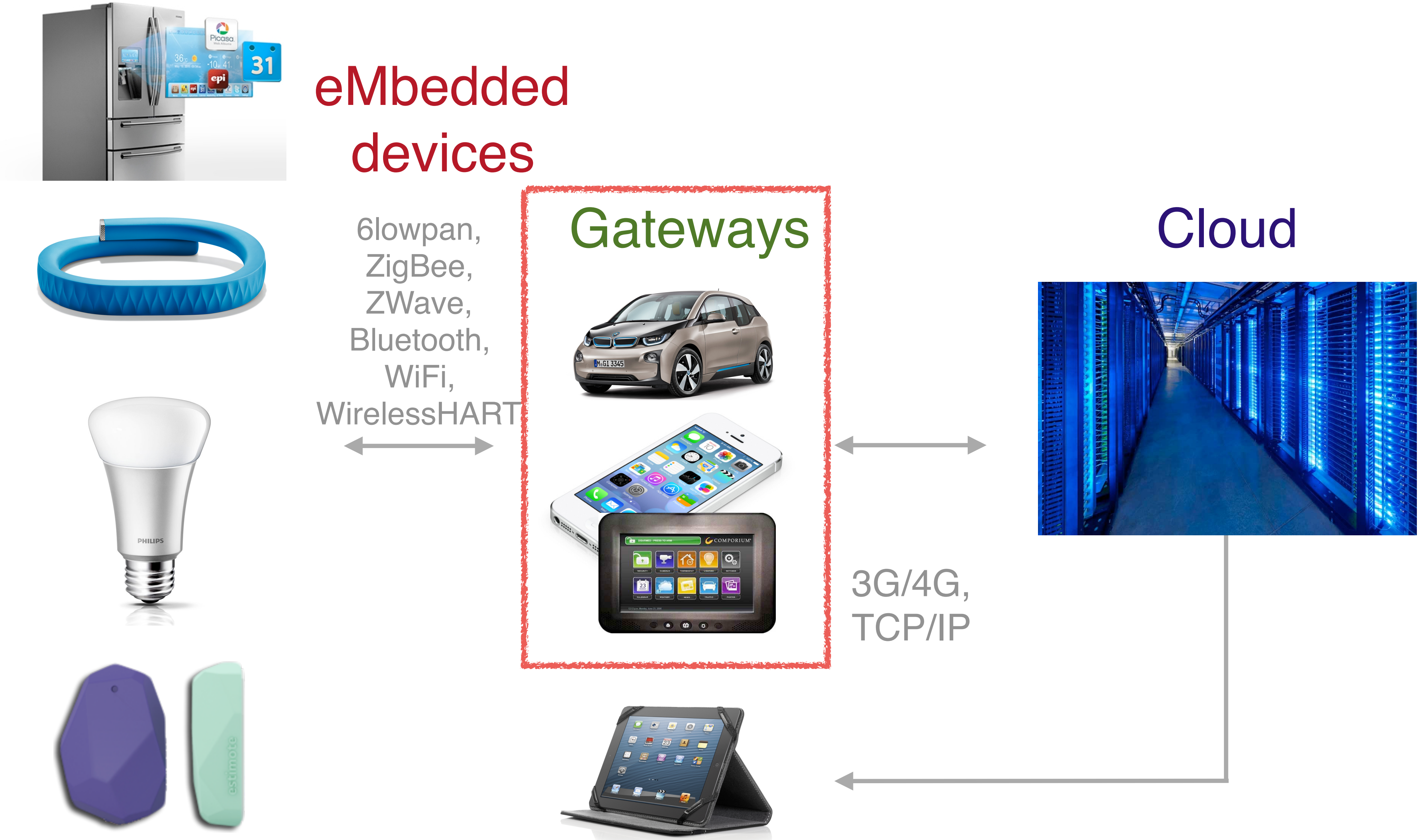
Gateways

3G/4G, TCP/IP

Cloud

End application

# IoT: MGC Architecture



eMbedded devices

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

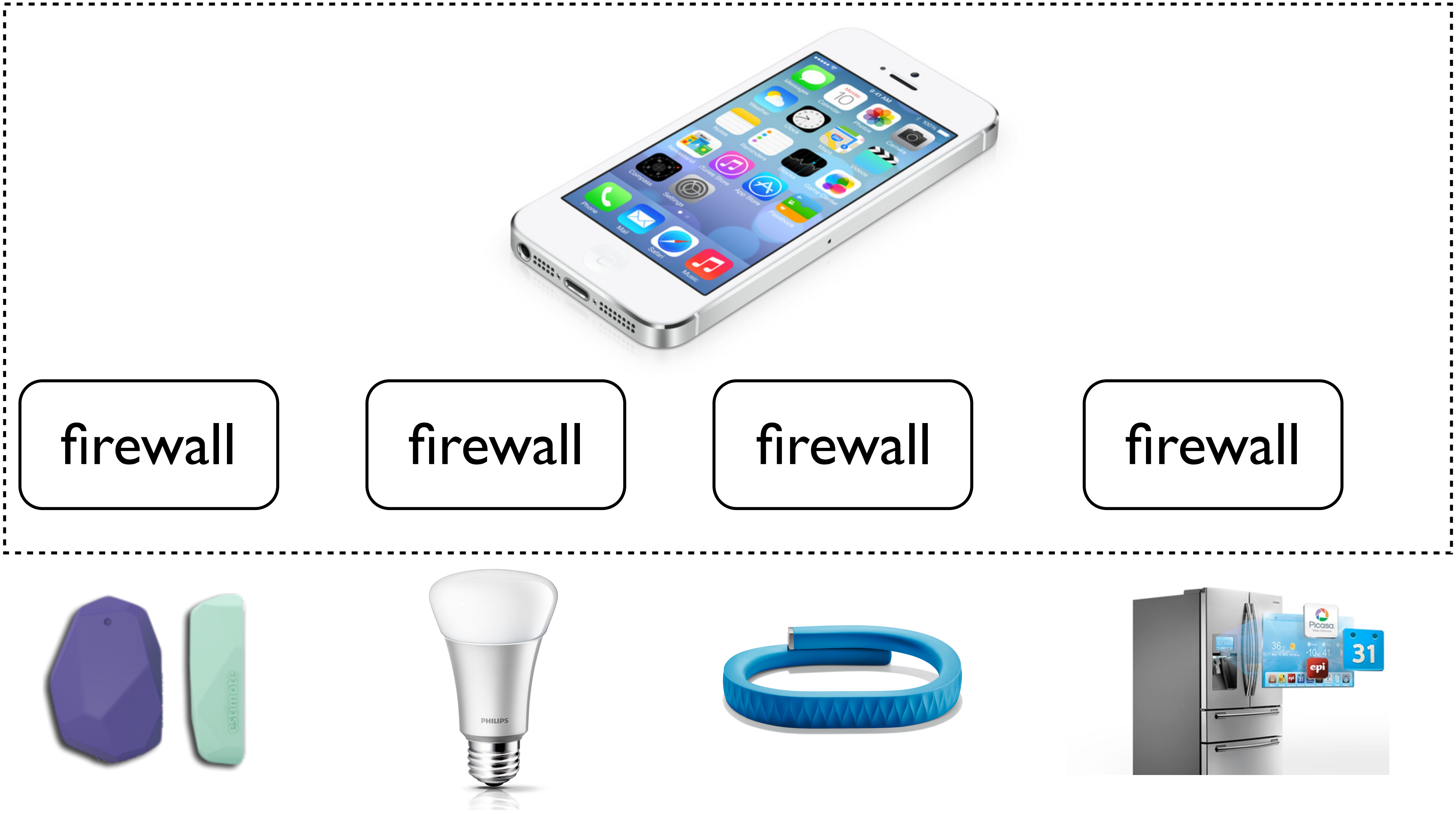
Gateways

3G/4G, TCP/IP

Cloud

End application

# Gateways to the Rescue



firewall

firewall

firewall

firewall

# Many Challenges

- Limited energy
- Limited storage
- Delay-tolerant networking
  - disconnection, not always on
- End-to-end security
- Handle them once
  - avoid repeated errors and security flaws

# Why Now?

- Technology has just reached the tipping point
  - BLE, iBeacon, 6LoWPAN
  - 32-bit Cortex M series (embedded: 500 nA sleep current)
  - Intel Edison (gateway: 15 $\mu$A sleep current)
  - Sensors, energy harvesting circuits
  - Cloud capabilities: future Xeon with FPGA
- We've been waiting
  - Leaders in prototyping, cryptographic computation, IoT networking, secure systems, analytics, and hardware design
- 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)

# Our goal

A team of two developers can develop a complete, secure IoT application, from hardware to cloud services, in 3 months, using tools developed by the project. All user data will remain secure and confidential even if the gateway or cloud servers are compromised.

# Thank you!

NSF

intel®