RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Make Way for The Internet of Things!

SESSION ID: TECH-R02

Benjamin Jun
VP and Chief Technology Officer
Cryptography Research, Inc. a Rambus Company

CRYPTOGRAPHY RESEARCH
a division of Rambus

The Internet of Things

Uniquely identifiable objects and their virtual representation in an Internet-like structure.

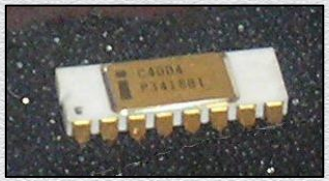
– Wikipedia

The physical world is becoming a type of information system [with] sensors and actuators embedded in physical objects… When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it.

– McKinsey & Company

Brought to you by…

Compute revolution (80's)



Sensor revolution (90's)

Wireless revolution (00's)

Human Internet (http v1.0 1996)

the promise

- Smartgrid + smart home energy efficiency
- Data collected from many sources and analyzed to gain new insights
- Physical world modified for the user
- Real-time marketplace adaptation to data

but…

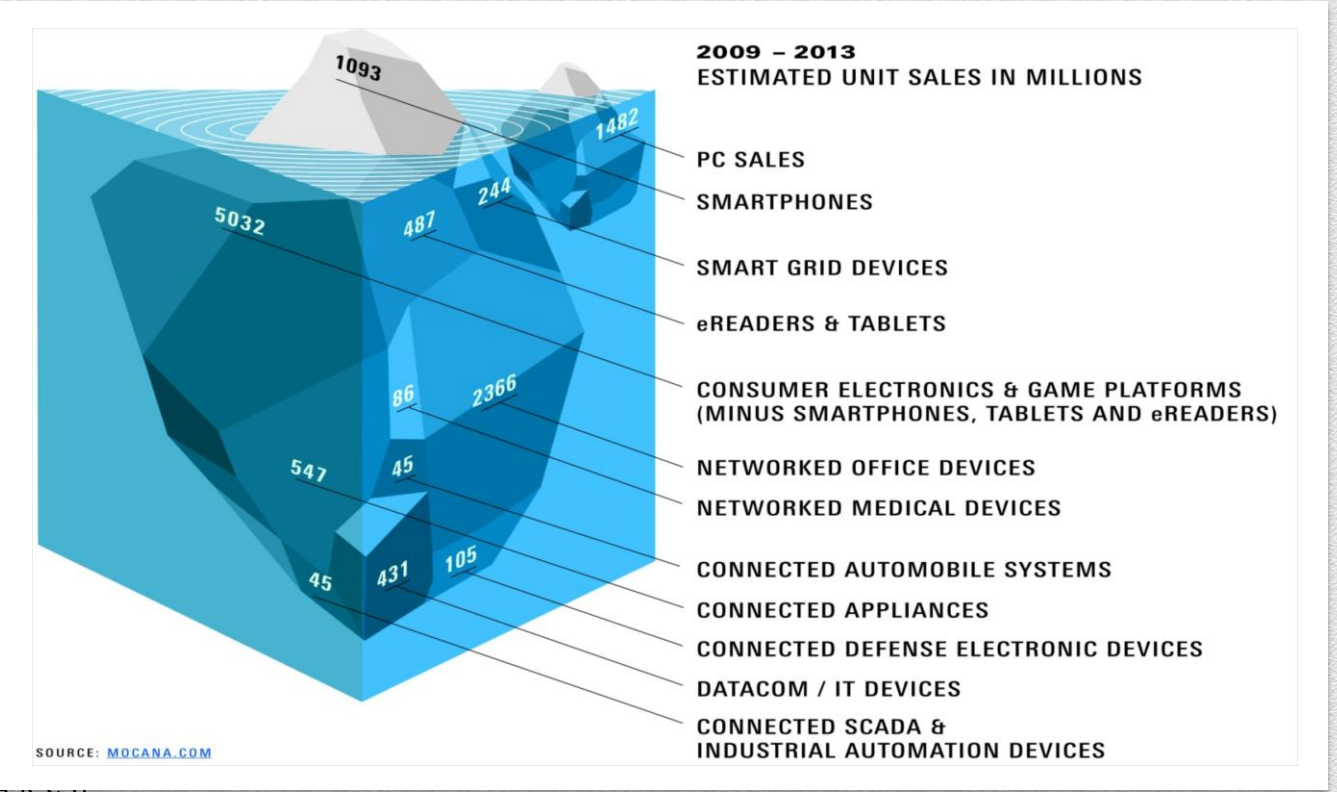
Critical utility DoS?

Invasion of privacy?

Burn down house?

Manipulate markets?

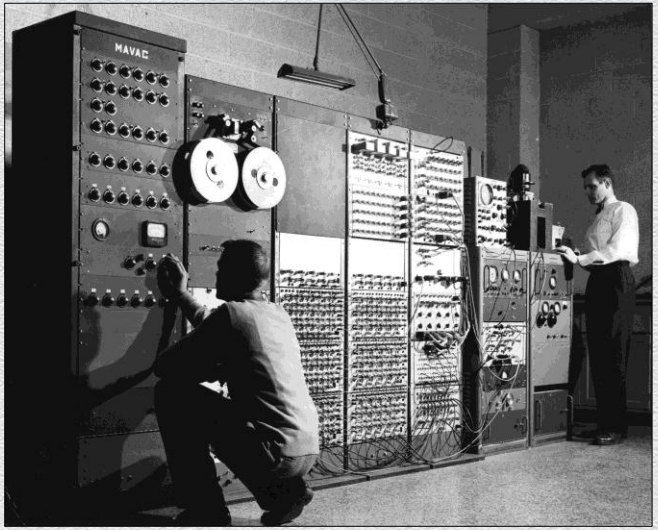
2017: M2M connections x3, traffic x20
2020: 30-50 billion connected IoT



Source: ABI / Cisco / Mocana

Anticipating change

50 year-old stove

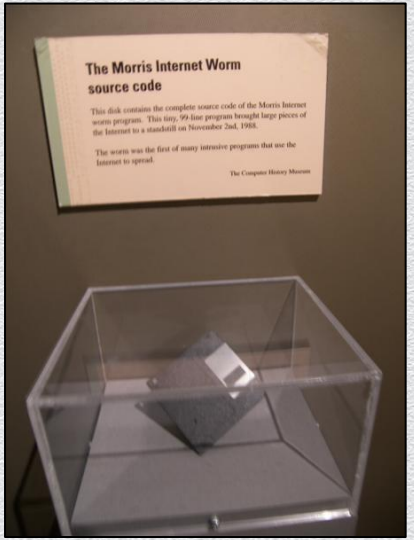


50 year-old computer

NCSU Libraries' Digital Collections: Rare and Unique Materials;
http://doowicky.blogspot.com/

Security challenges

- Connectivity + scale = **huge attack span**
- Ownership is different (BYOD on steroids)
  - Who owns data and device credentials?
- Device lifecycle is different
  - "Zero-step" activation and M2M transactions
- Modularity enables future applications
  - But we don't know what the threat models are!



Source code for Morris Internet Worm

We cannot use PC / IT security as the model

- PC's continuously updated
  - IoT nodes have long service life!
  - Embedded systems have little or no security support, starting with the SoC + BSP
- PC's have high security investment
  - Incremental value of PC node >> IoT node
  - No party willing to spend $
- PC's have good UI, high user mindshare

Data at Rest

Data in Transit

Time and Place

Endpoint Security

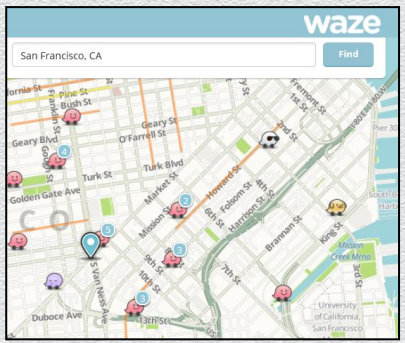
Phase 1: The database of things!

Machine collected

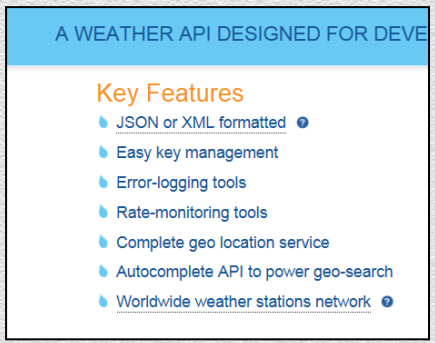
Internet interpreted

Human / machine rendered

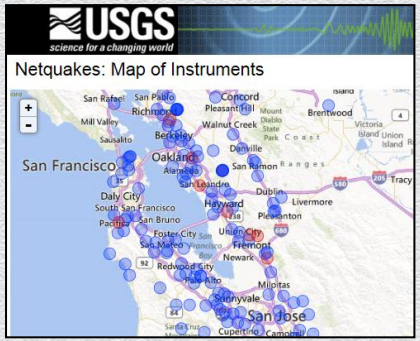
Tile



Waze

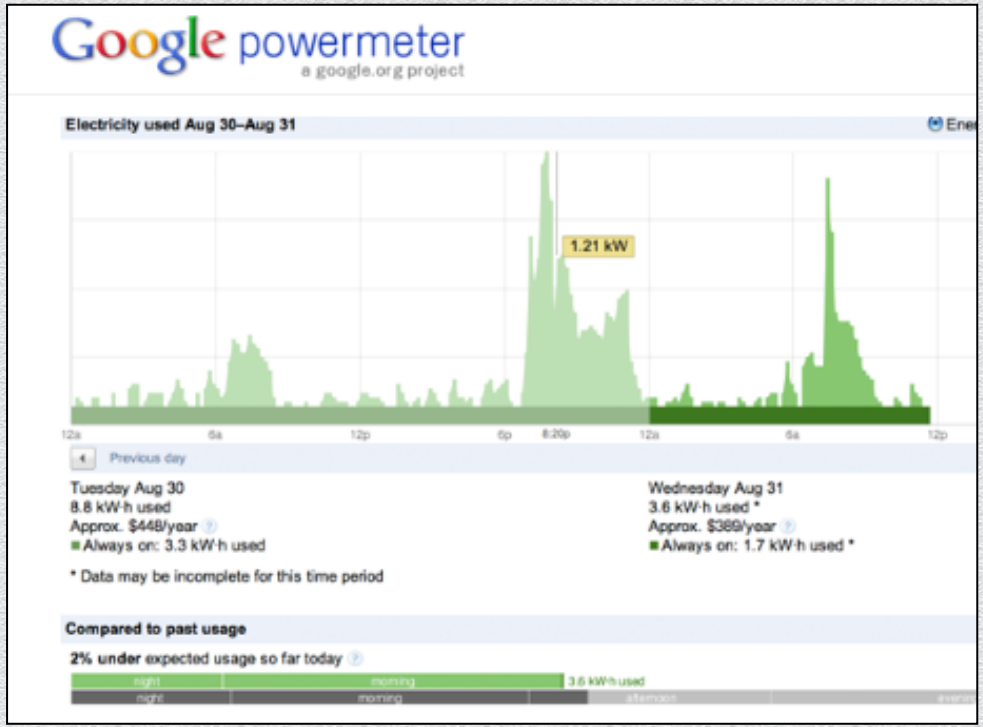


wunderground



USGS netquakes

What can utility data tell us?



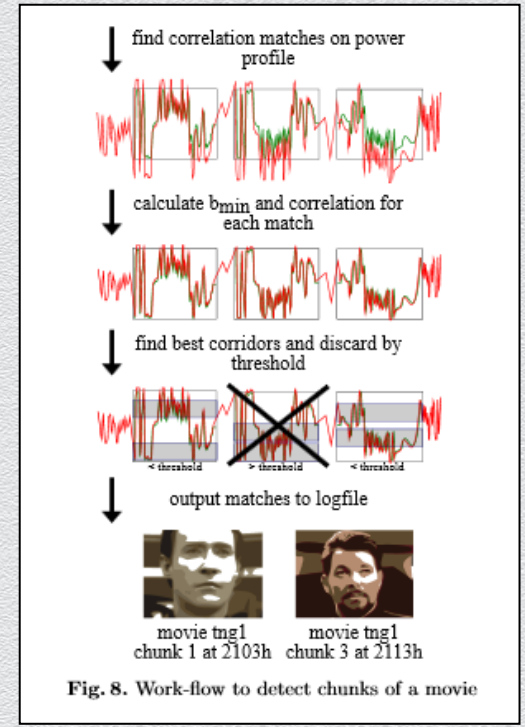


Fig. 8. Work-flow to detect chunks of a movie

Data fusion / Big data

By 2025 Internet nodes may reside in everyday things…

Streamlining—or revolutionizing—supply chains and logistics could slash costs, increase efficiencies, and reduce dependence on human labor. Ability to fuse sensor data from many distributed objects could deter crime and asymmetric warfare. Ubiquitous positioning technology could locate missing and stolen goods.

…

Massively parallel sensor fusion may undermine social cohesion if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search.

Global Trends 2025, US National Intelligence Council

Supply chain

Resource efficiency

Emergency services

Customization

Intelligence gathering

Privacy

Overstepping control

Predictive "creepiness"

Paparazzi

Data poisoning

“Classic” database security issues

Concern	Example
Data ownership	European Communication COM (2012) 9
Data privacy	home occupancy data == PCI PII?
Data theft	“Home addresses + recovery PIN for all users of electronic lock model SU-214”
Data extraction	Facial recognition + city cameras

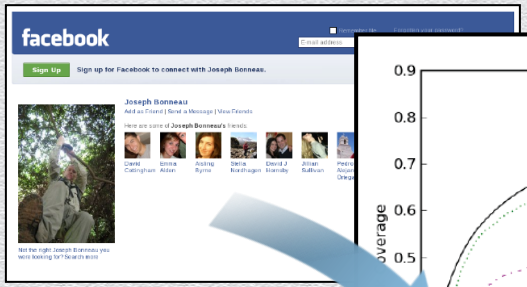
Example:
PCI regulated data

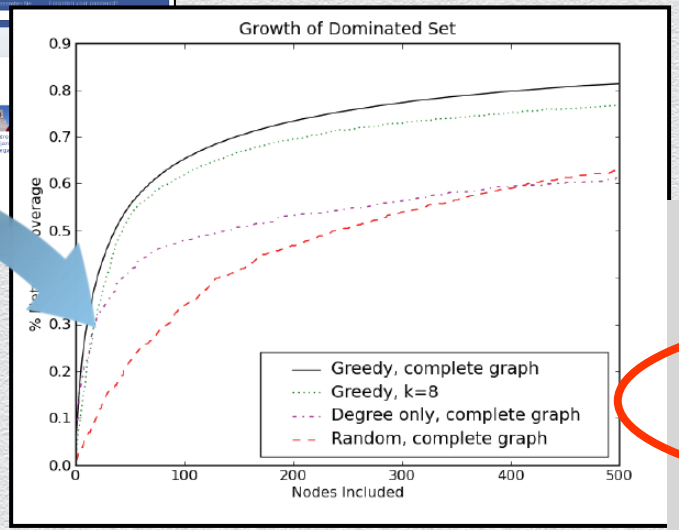
	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

PCI DSS Requirements and Security Assessment Procedures, v1.2

We can't (yet) manage partial data exposure

Graph theory and Facebook (2009)





Eight Friends Are Enough:
Social Graph Approximation via Public Listings

Joseph Bonneau
Computer Laboratory
University of Cambridge
jcb82@cl.cam.ac.uk

Jonathan Anderson
Computer Laboratory
University of Cambridge
jra40@cl.cam.ac.uk

Frank Stajano
Computer Laboratory
University of Cambridge
fms27@cl.cam.ac.uk

Ross Anderson
Computer Laboratory
University of Cambridge
rja40@cl.cam.ac.uk

ABSTRACT

The popular social networking website Facebook exposes a "public view" of user profiles to search engines which includes eight of the user's friendship links. We examine what considerable attention from the media, privacy advocates and the research community. Most of the focus has been on *personal data privacy:* researchers and operators have attempted to fine-tune access control mechanisms to prevent the accidental leakage of embarrassing or incriminating

5. CONCLUSIONS

We have examined the difficulty of computing graph statistics given a random sample of k edges from each node, and found that many interesting properties can be accurately approximated. This has disturbing implications for online privacy, since leaking graph information enables transitive privacy loss: insecure friends' profiles can be correlated to a user with a private profile. Social network operators should be aware of the importance of protecting not just user profile data, but the structure of the social graph. In particular, they shouldn't assist data aggregators by giving away public listings.

Challenge: partial "peeks" may leak too much

Who holds the data?

Centralized data provider

- Small # of service providers
- "Security by policy" for data ownership / control / usage
- $ spent on quality, security
- **Data monetization a focus**

Distributed data (in research)

- Data owners maintain "control" of cloud based data
- Fine grained control enforced by crypto, security protocols
- **Who will pay for this?**

802.11s - mesh networking
Internet routing
Root CA

The path to database security

NEAR

- Data clearinghouses will emerge
  - European privacy requirements + business need to aggregate
  - "Security by SLA"
- Devices encrypt data with user keys
  - "Dropbox" for crypto-partitioned IoT data
  - Requires device credential & key management
- Don't hold your breath (yet)…
  - Encrypted data search
  - Homomorphic encryption

FAR

Craig Gentry
Homomorphic Encryption, MIT Technology Review

CRYPTOGRAPHY RESEARCH
a division of Rambus

Data at Rest

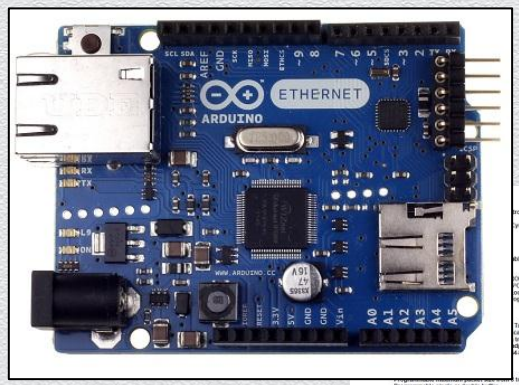
Data in Transit

Time and Place

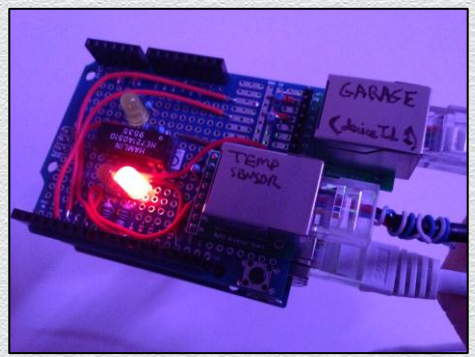
Endpoint Security

Connectivity: My garage door

Arduino Ethernet + sensors + relay



Ethernet
8 bit uP
32KB flash
2KB RAM

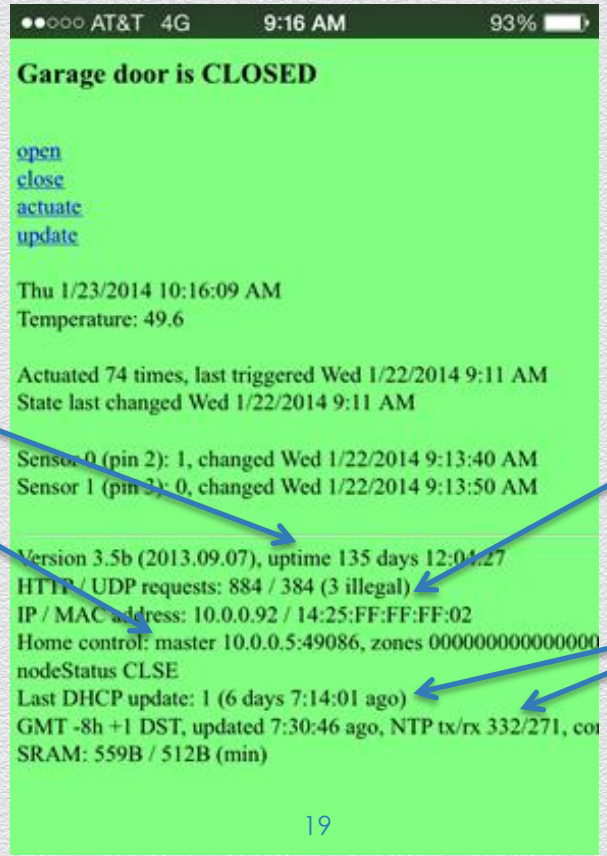


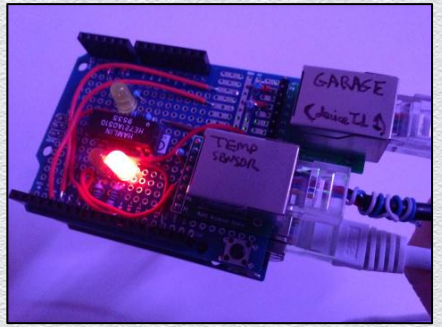
Device as server: Device talks to everybody

User authentication is a big problem

Need infrastructure-class stability with no maintenance

More than a web server: Data sharing requires M2M connections





Requires hardened web server

Dependent on other network resources (time, DNS, DHCP, …)

Device-to-cloud: Device talks to one service

Nest Labs

- Theory: Plug-in, VPN directly to cloud server
- Practice:
  - Not easy to build device that can connect for 20+ years
  - Complexities (WiFi passwords, TLS certificate expiration, DNS, IPv6, …)
- Infrastructure challenges
  - Everything via VPN?
  - What about hacked/spoofed device (PlayStation Network)
- Still may require direct device-to-device connections

Device gateway: Device – Gateway – Cloud

- Gateway to aggregate sensors, actuators
  - Bridge Internet to low-power sensor-friendly protocols
  - "NAT for sensors"

SCADA gateways

- Security model = firewall to keep bad guys out
  - What's our track record of "inside = good" security models?
  - Complexity grows (accumulation of legacy protocols, devices) … which brings security bugs

- (Insecure) example: Vehicle TPMS gateways

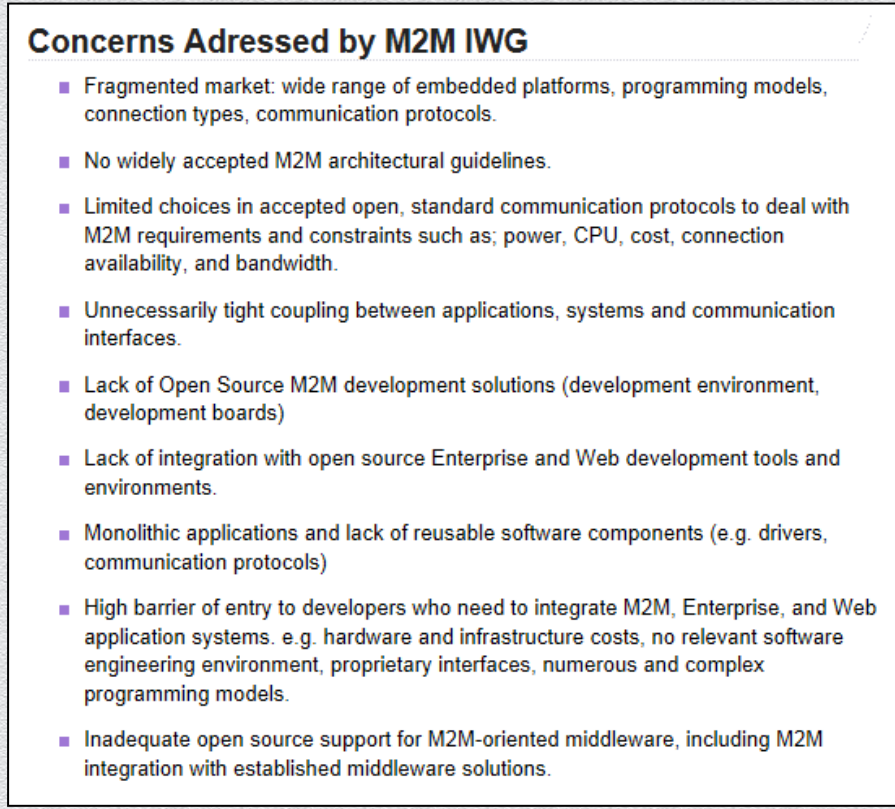
EtherPoll; Abby systems; http://www.cse.sc.edu/~wyxu/papers/TPMSUsenix.pdf

Connection security requires identity management

- We want global **address**ability and global **access**ibility
  - …with appropriate controls!
- What's in a name?
  - Device credentials
  - Identify-specific keys, certs
- Who gets to name it? When?
  - Domain owner, certification authority, issuer, device manager, …

IoT protocols to watch

- Internet of things projects
  - MQ Telemetry Transport (MQTT)
  - Eclipse M2M Industry working group
- Security to follow
  - OAuth 2.0
  - IM messaging security (Off-the-Record, …)



Eclipse M2M Industry working group

Data at Rest

Data in Transit

Time and Place

Endpoint Security

Time and place

- Value proposition: Compute-domain awareness of physical things

- Associations are important
  - The milk bottle in my refrigerator expired
  - Football game will add 8000 more cars to highway at 3:35pm
  - I am standing next to my assigned car-sharing vehicle

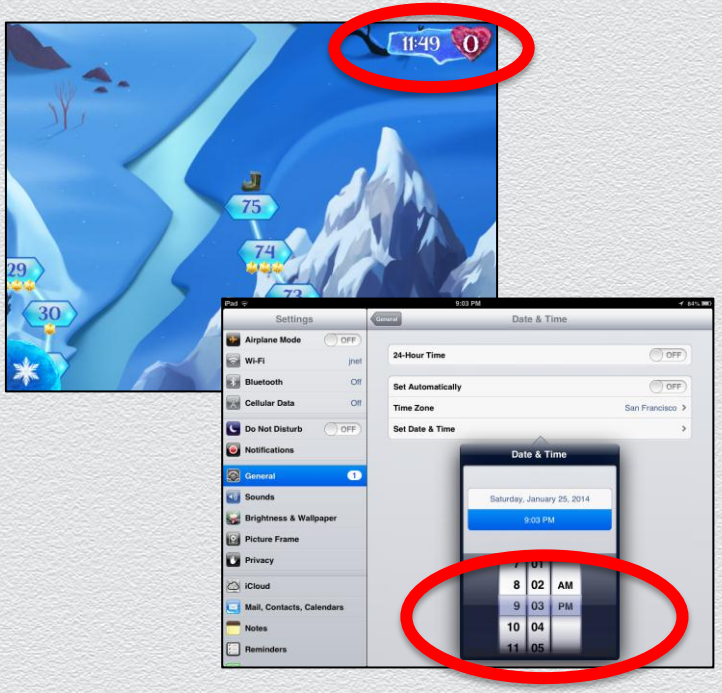
Binding to time and place

- Local services
- Pay-per-impression
- Region pricing
- Relative proximity
- User mobility
- User identity

$85 for time-based energy demand-response

Time

Disney iOS "Frozen" game timeout



Netflix local clock tracking

Common time sources

- Local battery
- User
- NTP server (pool.ntp.org)
- Broadcast: GPS, GSM, NIST WWV/WWVH
- EEPROM (advance only)

Place (GPS)

CJ6 GPS Jammer

jammerstore.com

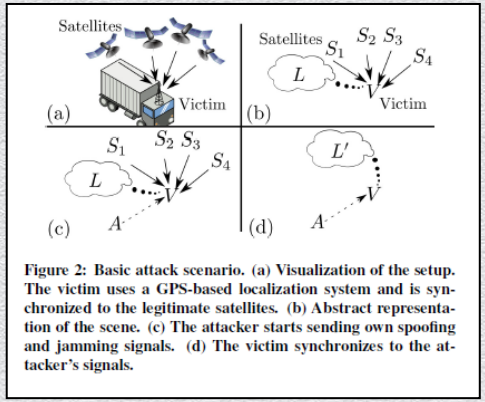


Figure 2: Basic attack scenario. (a) Visualization of the setup. The victim uses a GPS-based localization system and is synchronized to the legitimate satellites. (b) Abstract representation of the scene. (c) The attacker starts sending own spoofing and jamming signals. (d) The victim synchronizes to the attacker's signals.

On the Requirements for Successful GPS Spoofing Attacks

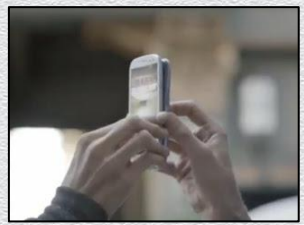
Tippenhauer, Pöpper, Rasmussen, Capkun

Captured RQ-170 Sentinel

Christian Science Monitor, 12/15/2011

Three things the world needs…

- Protocols to selectively prove you were somewhere at some time
  - Need: User authentication, proximity based automatic enrollment
  - Concern: Can I turn off the tracking bug?
  - **Two strikes: today's tech is not private and very spoofable**
- Secure means to federate devices in close proximity
  - …auto pair milk and fridge!
- Trusted time and location
  - From application OR from server

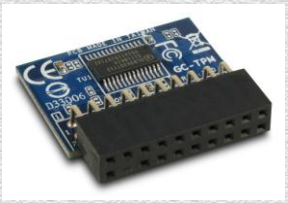


Samsung SIII advertisement

Crypto to the rescue?

- Trusted Computing Group made some inroads in attestation + privacy
  - TPM v1.1 pseudonymous machine credentials (requires TTP)
  - TPM v1.2 direct anonymous attestation

- **Not much infrastructure exists for pseudonymous modes, still problematic in real world use scenarios (revocation)**



Coming soon

Time & place attestation without user / OS / application trust

- **Approach 1: Chipsets w/ built-in environment attestation resource**
  - Independent core on CPU maintains GPS + time history
  - Hardware module can offer a high-valued attestation (digital signature) on data, traceable to module's security certification
  - User opts to share data with app environment

- **Approach 2: Infrastructure (caution – privacy)**
  - Cell tower geolocation services
  - Crowdsourced? (bitcoin block chain)

Data at Rest

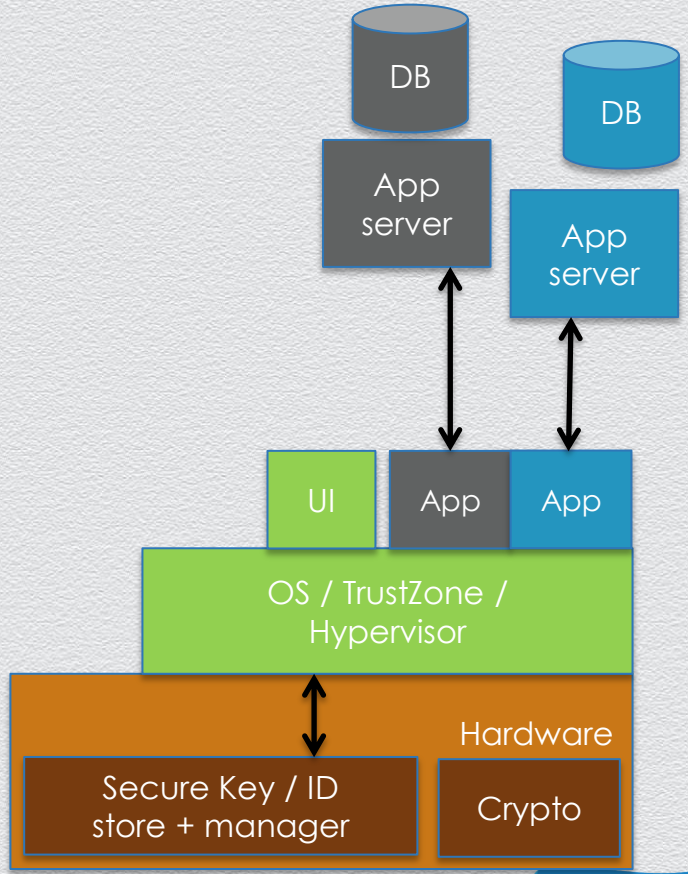
Data in Transit

Time and Place

Endpoint Security

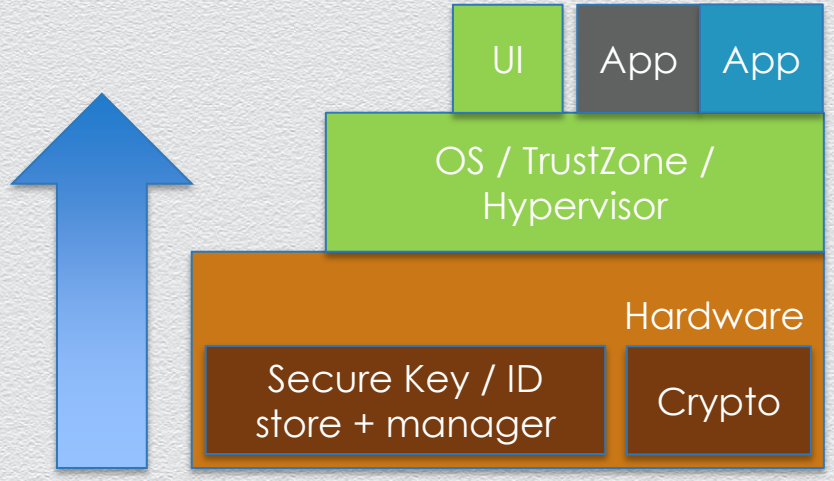
Trust means ?

- Independent security certification
- Key integrity
- Auditability / traceability
- Strong device identity credentials
- Robust application sandboxing
- System reliability
- Secure UI
- Data integrity



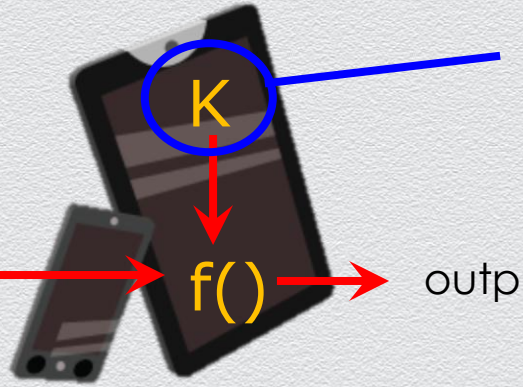
Apps require a secure, reliable foundation

- What gets to run on the platform?
  - Boot / code authentication
  - Secure debug lock
- Am I in the real world or the matrix?
  - Environment attestation
  - Peripheral authentication
- Do my secrets remain opaque?
  - Application partitioning
  - Hardware-based secure key storage



Example: Key protection

- Devices using secret or private key cryptography must protect their secret keys



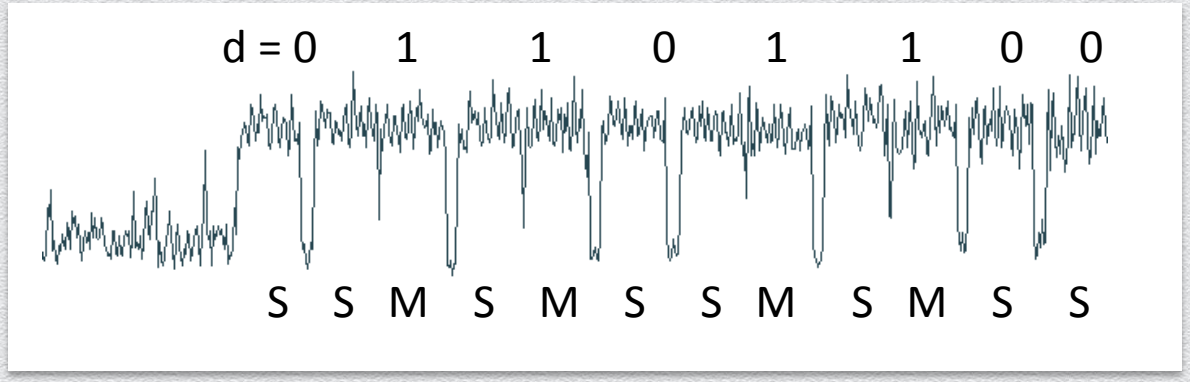
Device computes with key K, but
bad guys must never extract K

inputs → f() → outputs

Attackers should not get K, even if they use mathematics, invasive attacks, external monitoring…

Example: EM analysis of an RSA implementation

- Android app with RSA implementation on modern 4G phone
- Magnetic field pickup coil
- Measurements collected during computation of M^d mod N



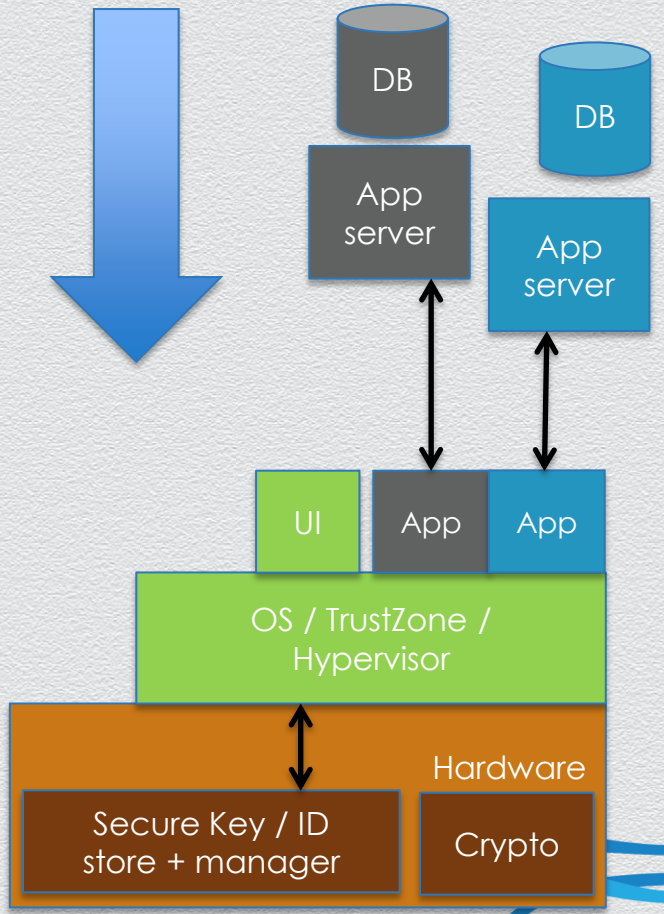
CF = 36.99 MHz | Acq BW = 500 KHz | Filt BW = 250 KHz | Smoothing = 10

Standards requiring side-channel resistance

- PCI
- Movie Labs
- FIPS 140-3
- Common Criteria

Trust from the top down

- Device enrollment
- System auditing & risk management
- Online revocation
- Remote management & updates



Lifecycle considerations for "Internet Things"

"Direct to field"

Limited UI for administration steps

Early provisioning of dev. credentials

- Inject keys, certificates
- Enroll device
- May be done before OS load
- Often an outsourced (faraway) manufacturing site

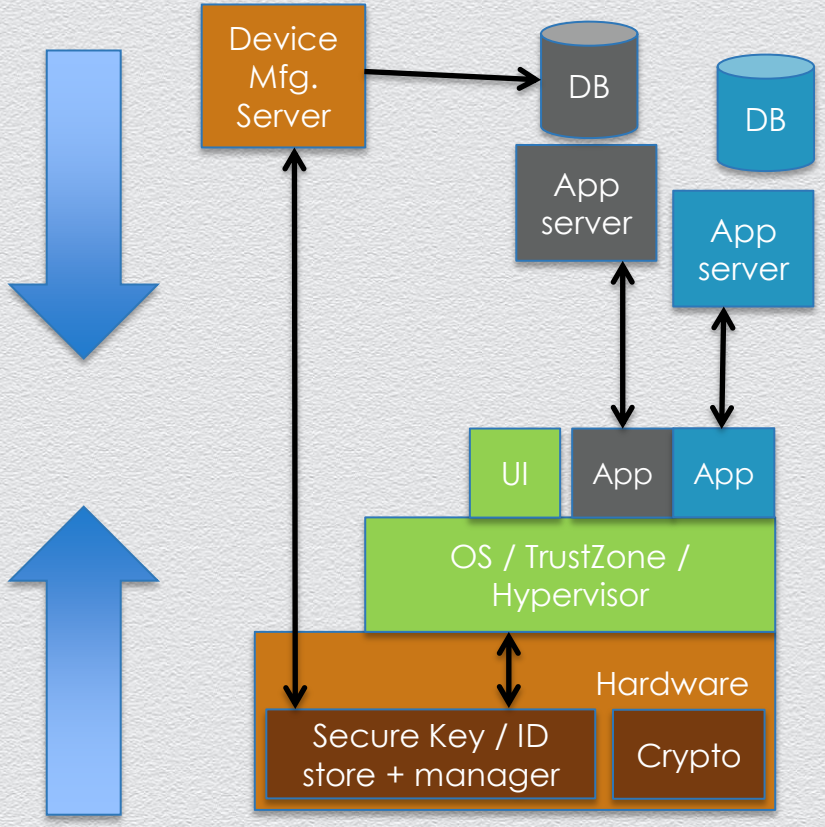
Device administration secured by base credentials

- In-field challenge/response authentication
- Add/update user credentials
- Send signed updates

Trust meets in the middle

Identity + key provisioning
Authentication service
Secure session management
Security updates

Identity + key management
Sandboxed secrets
Partitioning of critical state
Reliability & integrity



Data at Rest

Data in Transit

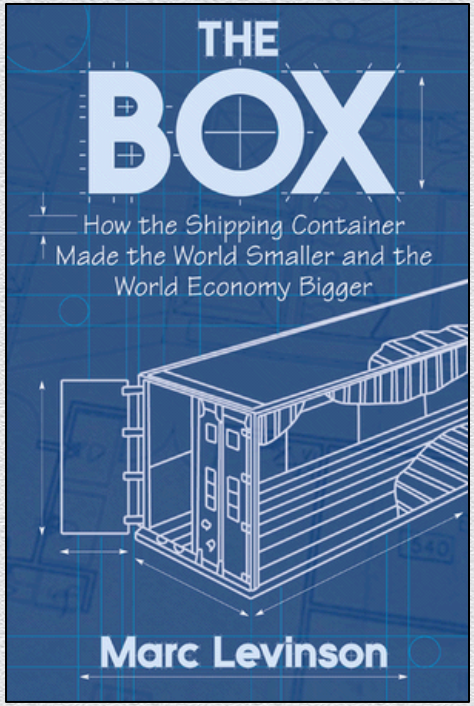
Time and Place

Endpoint Security

What's next?

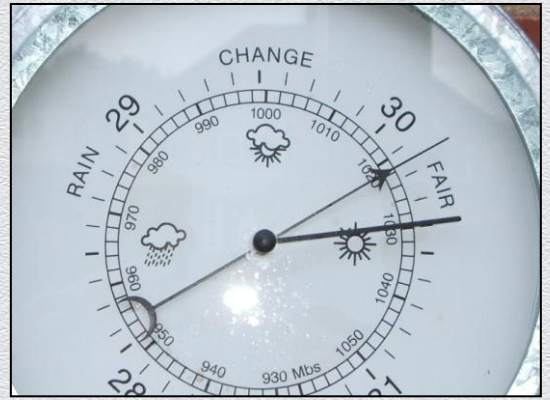
- The human Internet is a success story
  - Yay for standards: TCP/IP, IETF, Apache, SSL/TLS
  - But security has always played catch up!

- The Internet of Things is still the wild west…
  - Largely without security
  - Proprietary and not interoperable
  - And mashups always bring security challenges!



Internet++

- We have many building blocks to secure the Internet of Things
- But they must be applied to solve a different (and changing) set of challenges!
- Think carefully before you build tomorrow's legacy problems!



Questions?

Benjamin Jun

Chief Technology Officer
ben@cryptography.com

CRYPTOGRAPHY RESEARCH

a division of Rambus