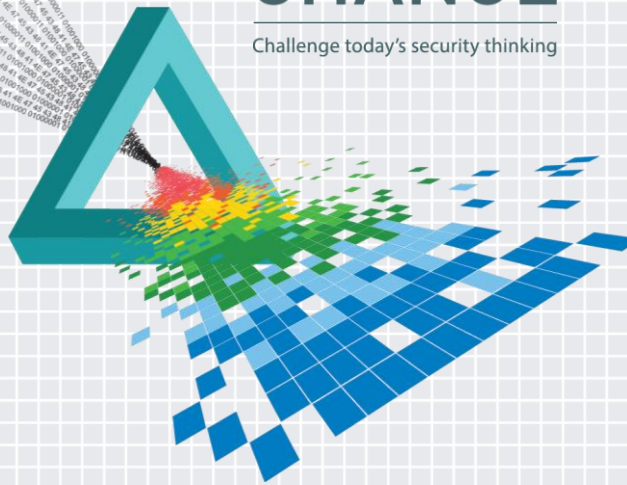
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: STR-F01

IOT: When *Things* Crawl Into Your Corporate Network

Sam Curry

Chief Technology and Security Officer
Arbor Networks
@samjcurry / scurry@arbor.net

Uri Rivner

Head of Cyber Strategy
BioCatch
@UriRivner / uri.rivner@biocatch.com

The upside: Internet of Me

The Promise: from IoT to IoM, a new Chapter in Human Experience

Any sufficiently advanced technology is indistinguishable from magic
-Arthur C Clarke

The shape of the future

- Where does the physical world end and the digital begin?
- Where does the corporate world end and the consumer begin?

RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: STR-F01

IOM:
When *Things* Crawl Into Your Life

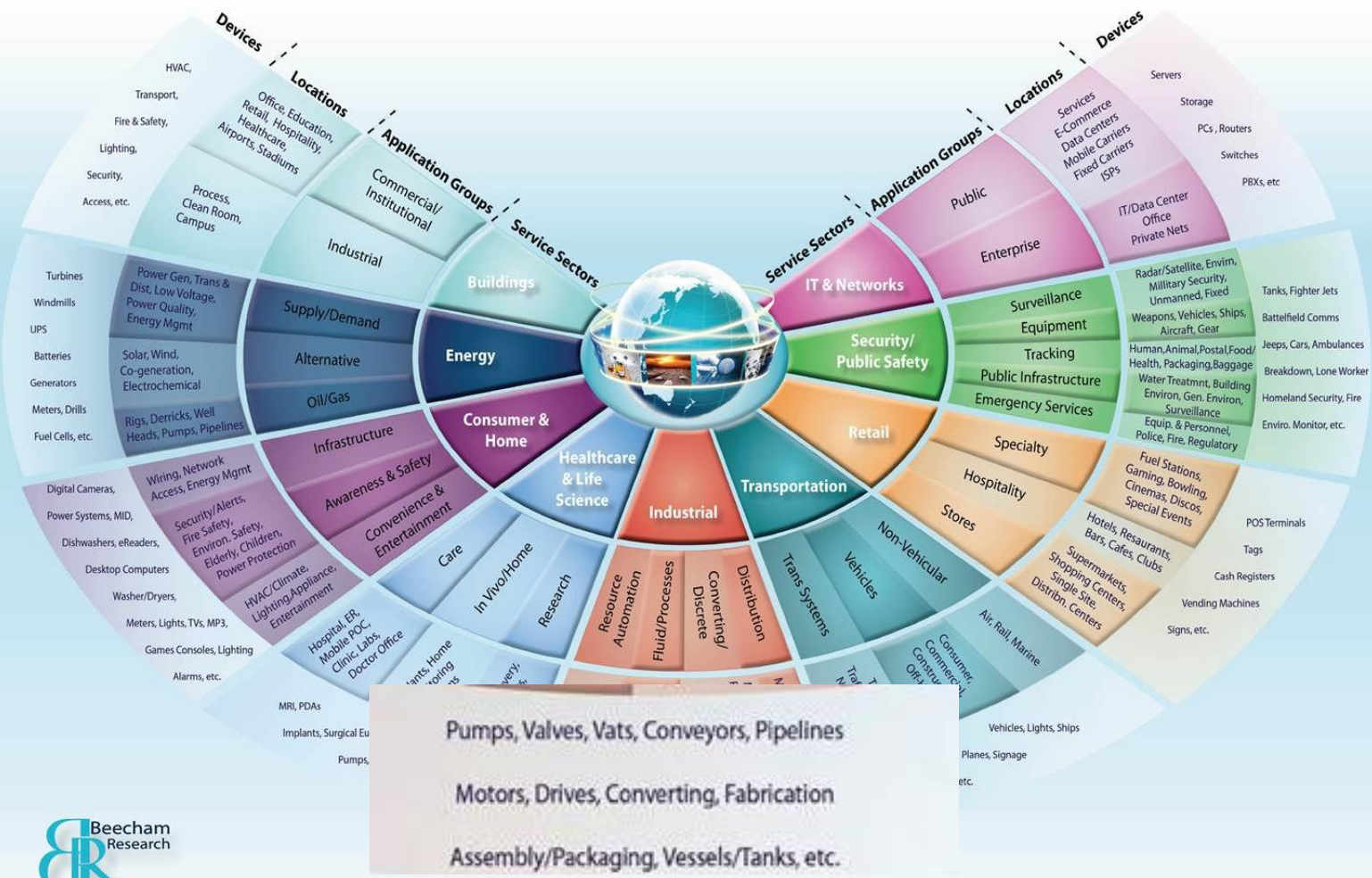
Sam Curry

Chief Technology and Security Officer
Arbor Networks
@samjcurry / scurry@arbor.net

Uri Rivner

Head of Cyber Strategy
BioCatch
@UriRivner / uri.rivner@biocatch.com

Where are we now?



Beecham Research

"My god…
It's full of Stars…"
-2001, A Space Odyssey

California

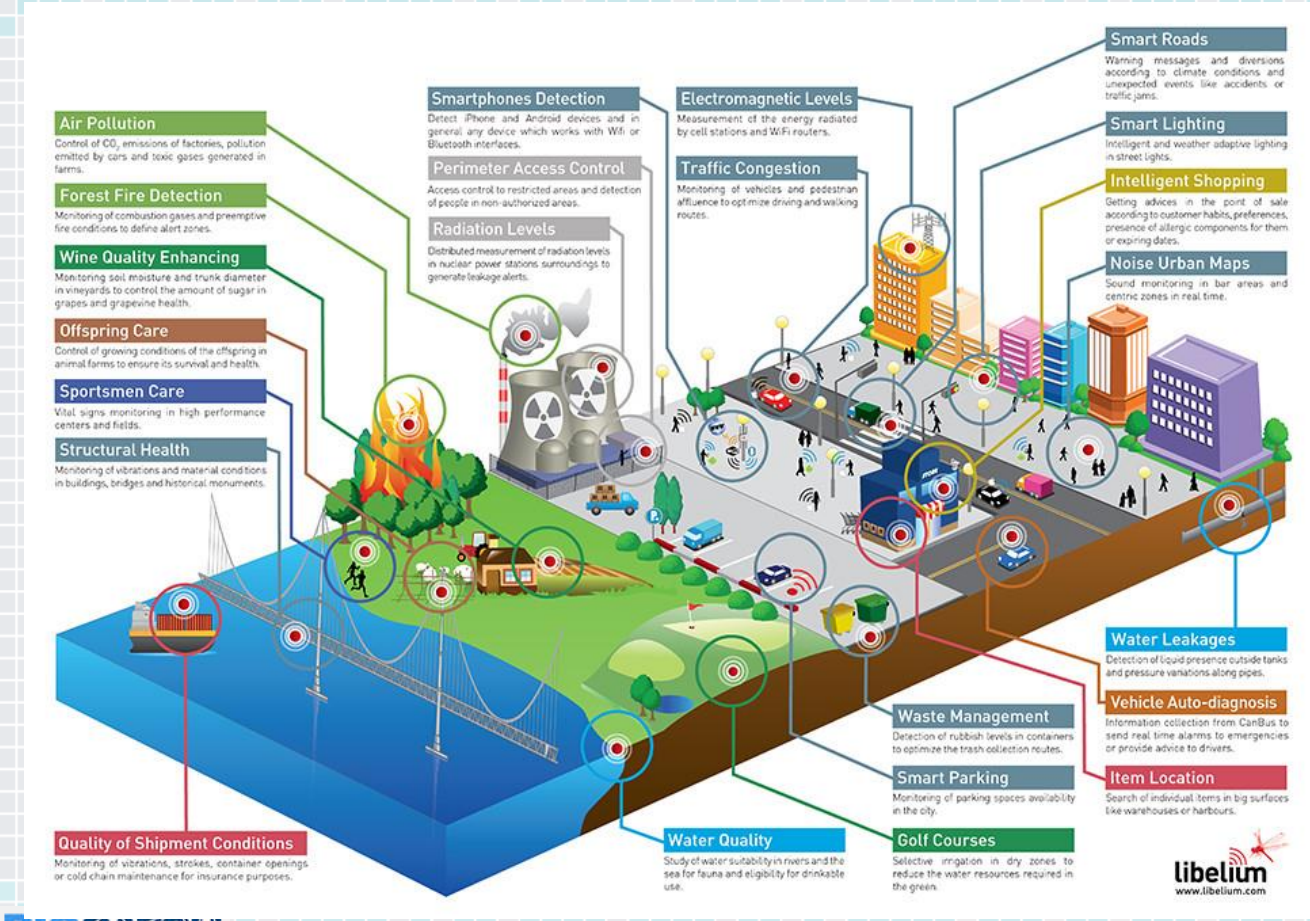
Back Home

National/State

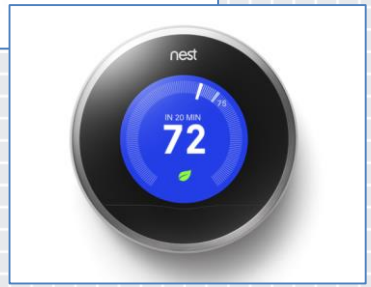
Public sector: $4.6t
National productivity +
Connected military
Cost reductions

Cisco 2013

City


Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.
Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.
Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.
Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.
Sportsmen Care
Vital signs monitoring in high performance centers and fields.
Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.
Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.
Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.
Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.
Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.
Electromagnetic Levels
Measurement of the energy radiated by cell stations and WiFi routers.
Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.
Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.
Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.
Smart Lighting
Intelligent and weather adaptive lighting in street lights.
Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.
Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.
Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.
Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.
Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.
Item Location
Search of individual items in big surfaces like warehouses or harbours.
Smart Parking
Monitoring of parking spaces availability in the city.
Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.
libelium
www.libelium.com

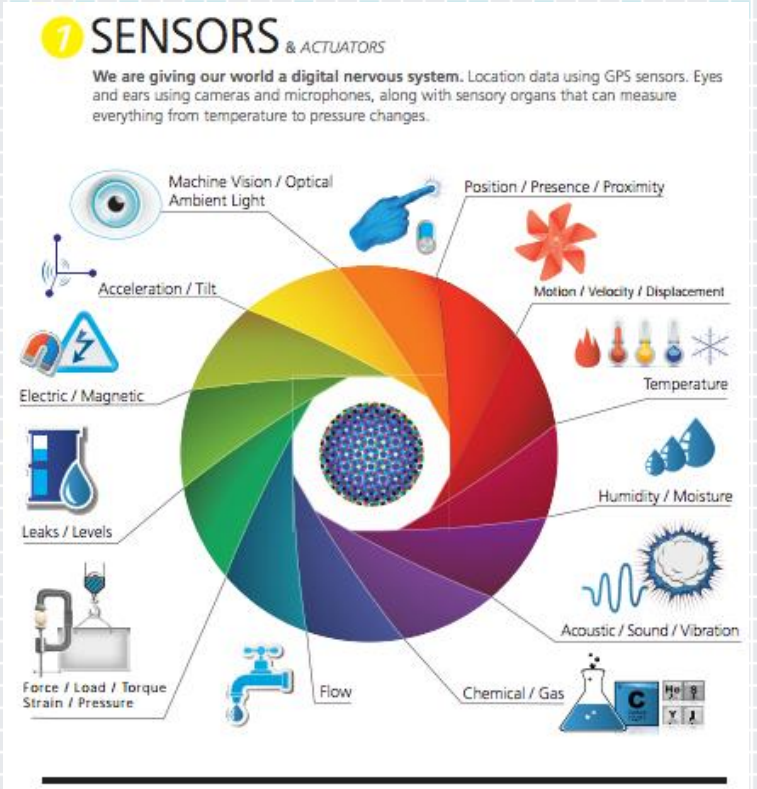
Office & Home



Consumer / Employee

IOT Characteristics

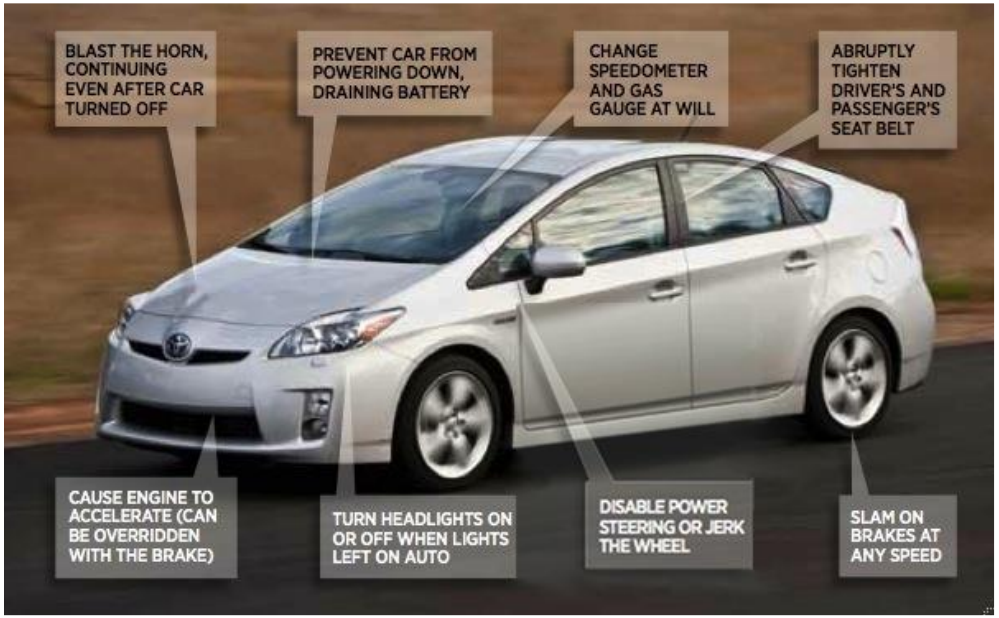
- Thing
- Sensors
- Compute Power
- Network Connectivity (to the cloud)
- Proximity Communication
  (Bluetooth, NFC, etc)




Futuristic video clip:
Search “Sight” on Youtube

Securing *Things*

Stop the FUD!



Source and Inspiration: Josh Corman and "I Am The Cavalry!"

An approach to security for IoT

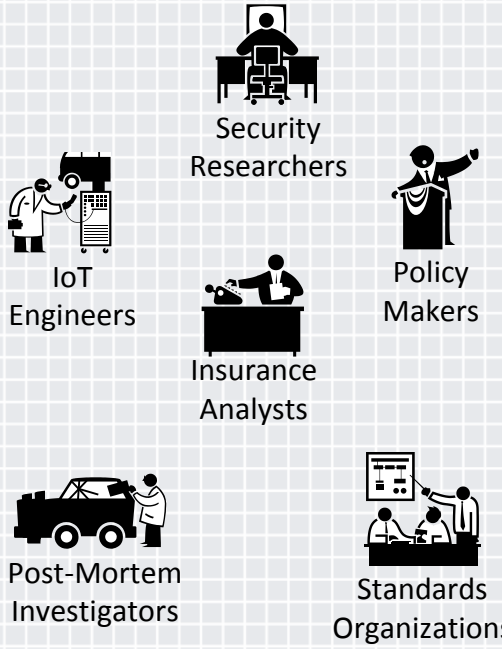
- Scope the problem and implications, without FUD!
- Define countermeasures:
  - Make sure short term fixes are possible (e.g. virtual patching)
  - Make sure processes exist to patch everything*
- Put the right trust models in place
  - Roots of trust
  - Mosaic (not chains) of trust
  - Complex policies that doesn't use a single, ever-present root
  - Complex authorization model
  - Granular enforcement model
- Cost of change curve: get it right now...
  - MQTT, XMPP, DDS, AMQP
  - Thread, AllJoyn
  - OIC, IIC, etc.

* Yes; everything

5-Star Framework…more than cars

Addressing Automotive Cyber Systems

- Automotive "5-Star Capabilities"
  - **Safety by Design** – Anticipate failure and plan mitigation
  - **Third-Party Collaboration** – Engage willing allies
  - **Evidence Capture** – Observe and learn from failure
  - **Security Updates** – Respond quickly to issues discoverer
  - **Segmentation & Isolation** – Prevent cascading failure
- This needs to apply to IoT too!



Source and Inspiration: Josh Corman and "I Am The Cavalry!"

Resistance is Futile

Just follow the rules!

Keep them out of the light

Don’t give them any water

And whatever you do, never, EVER, feed them after midnight

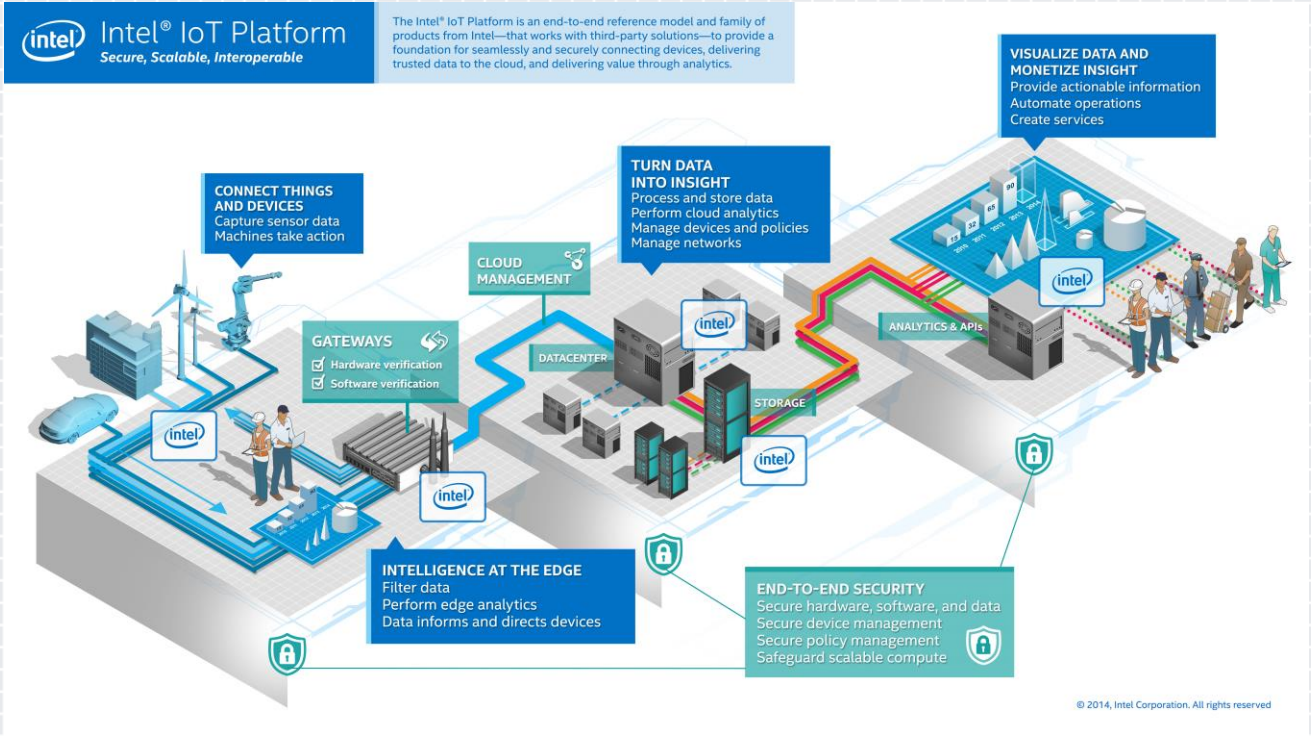
Past waves and tides

- Curse of the were-laptop
- Trojans in your network
- Tidal Wave v. Turn of the Tides
  - Bad guys: follow path of least resistance
  - Good guys: follow path of least security
- Fraud: web v. mobile

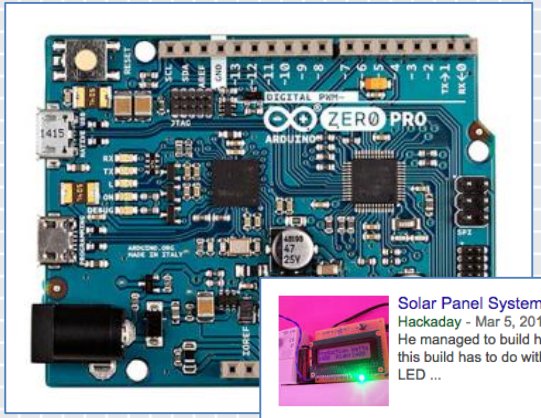
Wake up and Smell the Coffee

Memory
Biometric access
Inventory management
Next step: connecting to Active Directory?

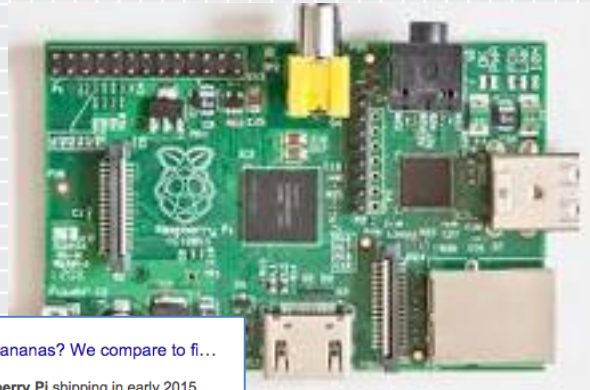
IOT Security Stack:
Visions…



IOT Security Stack:
Reality Check



- Built to agility and wide applicability
- Trust can't be bolted on later
- Standardization of IOT?
  Good luck with that…
- Security not incented here…



Solar Panel System Monitoring Device Using **Arduino**
Hackaday - Mar 5, 2015
He managed to build his own monitor using an **Arduino**. The trick of this build has to do with how the system works. The panel includes an LED ...

Developer Seeks **Arduino** Robotics API Funding
ProgrammableWeb - Mar 6, 2015
Fredrik Per Erik Persson, a Swedish software developer, aims to build an API that will allow **Arduino**/Raspberry Pi robots to be controlled from ...

Tiny IoT SBC runs Linux, offers **Arduino** compatibility
LinuxGizmos - Mar 6, 2015
The credit card sized, open-spec Udoo Neo SBC features Freescale's Cortex-M4-enhanced i.MX6 SoloX, plus **Arduino** compatibility, WiFi, ...

Making **raspberries**, or going bananas? We compare to fi…
Digital Trends - 18 hours ago
With the newer version of the **Raspberry Pi** shipping in early 2015, the maker community has experienced huge expansion as more people ...

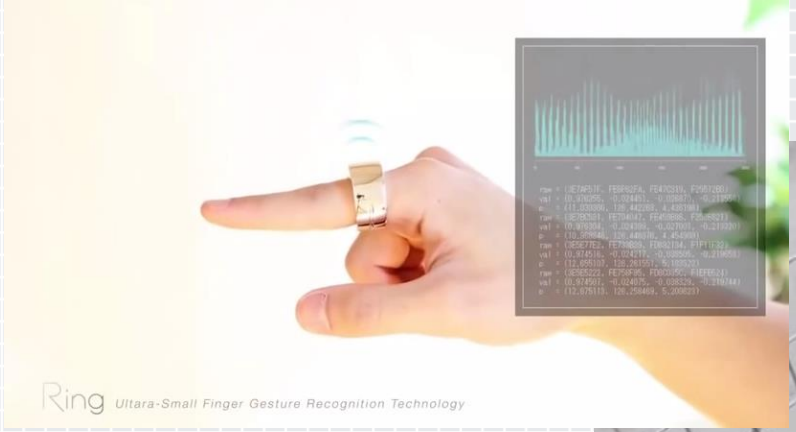
Raspberry Pi Project Ideas: Here Are 10 Cool Things Yo…
Tech Times - Mar 7, 2015
The **Raspberry Pi** 2 is six times faster, with twice the capacity of the Raspberry Model B+. What can be done with the $35 supercomputer?

Is the **Raspberry Pi** 2 a $35 miracle PC, or still a hobby o…
Digital Trends - Mar 7, 2015
The original **Raspberry Pi**, a $35 computer released in early 2012, spurred a revolution in computing. For the cost of a bar tab, an inventor, ...

Secure *this*: Ninja Blocks

Secure *this*: Remotely Controlled Toilets

SpearPhishing 2020



Implications for your company

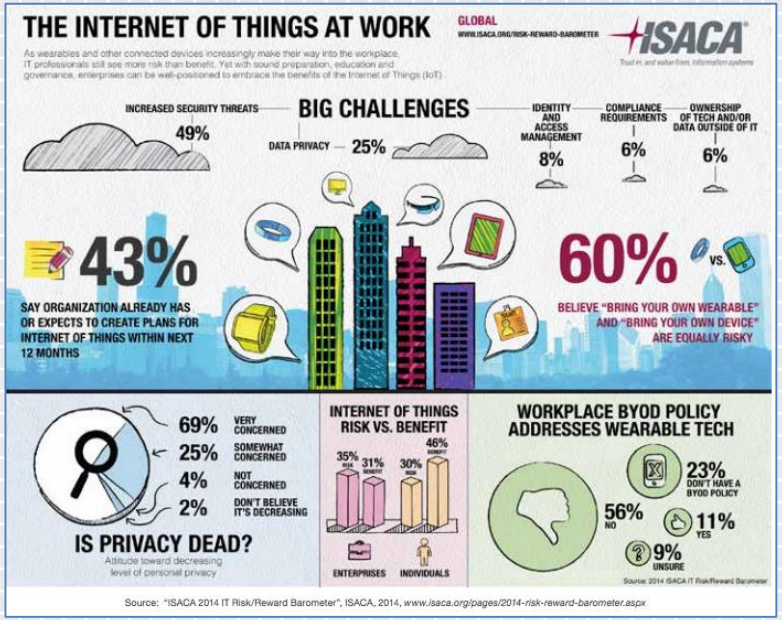
This list should look familiar

- Perimeter… perimeter… perimeter…
  - "You keep saying this word. I don't think it means what you think it means"
  - If it's on its last legs now, it's annihilated with IoT:
    - Drones
    - Wearables
    - Facilities, HVAC, etc.
- What's at risk…?
  - Corporate and National Espionage
  - IP Loss or damage
  - Privacy of employee, partner, customer
  - Availability of IT and basic services
  - Criminal and Civil Liability


DON'T
PANIC

Start with Risk / Benefits

- IoT is coming to the office
- Unlike SmartPhones, they can't be as easily turned off or left outside
- There are benefits from welcoming it

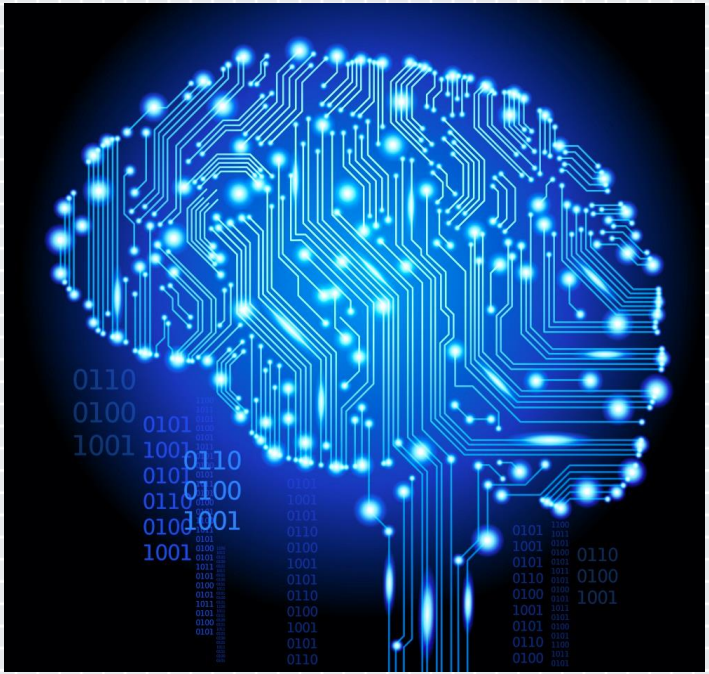


What can we control?

- There is a need for spectrum monitoring, locally
  - IoT storms: I-2-I, I-2-M, M-2-M (cascade)
  - Reflection and Amplification
  - CrowdFlash or attack?
- Qualities in *things* design
  - Resilience
  - Application layer

Real “Intelligence” for security

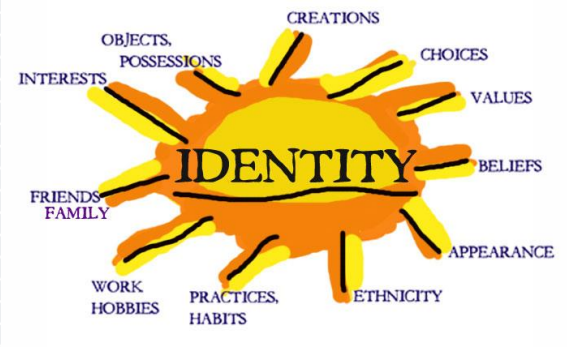
- No – not about Big Data!
- It is about…
  - Authorization models
    - Speed
    - Object models (id, data/app, device)
    - Enforcement
  - Interaction among authorizations models
  - Intelligence (cognition) hubs
    - Opt-in
    - Opt-out
  - Threat Intelligence and context
    - Personal threat intelligence services



Identity & Access Challenges

David Lake, Ammar Rayes, and Monique Morrow, Cisco (The Internet Protocol Journal, Volume 15, No. 3 - Sep 2012)

- It was hard for MF and then for distributed Enterprise environments…welcome to really hard!
  - Probabilistic not deterministic authorization
  - Machine learning, the pragmatic way (ok a little Big Data)
- Acting on a system, affects the system
  - Beware the Mirror Chess problem
  - Manage the contention between data access
- Concurrent multiparty/network security and privacy
  - Authenticate to multiple networks securely
  - Ensure that data is available to multiple endpoints
  - Manage privacy concerns among multiple consumers
  - Provide strong authentication and data protection that cannot be compromised



Can security really know you (and still respect privacy)?

The importance of privacy

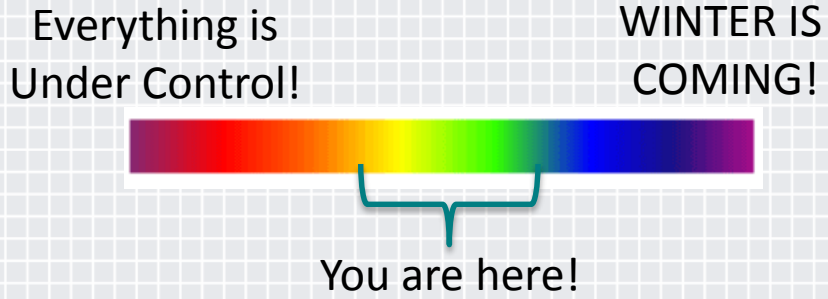
- Privacy and the “cost of getting information about you”
  - Security only one input
  - Sampling your digital wake
- What is mine is mine…
  - Persistence of Identity
  - Inheritance of reputation
- Spying
  - Big brother (government)
  - Step brothers (other governments)
  - Little brother (companies)
  - Cousins (other people)
- De-personalization and Re-identification

Future research

- Patch Wars
- Potential for *better* security with…
  - Continuous, privacy-respecting monitoring
  - PFA, not MFA
  - Smart use of Machine Learning
- Non-Human object authentication and authorization
- Virtual Patching
- Sandboxing
- Signal-to-noise: SIEM writ large
- Centralized (dirigiste) Management
- Retro-viruses?
- Do we want to encourage genetic mutation and drift for resilience

Apply Slide

- Check your risk and threat assessments.
  - Do they cover IoT appliances?
  - Do they balance risk vs. benefit?
  - Think about liability, contracts and vendor
  - Beef up “wireless” protocol monitoring and countermeasures
- Prepare stakeholders, rather than be surprised
  - We’ve been reactive with Cloud and Mobility… time for a change
  - Do your risk / benefit assessment
  - Take a leaning forward approach to architectures *now*
- Resistance is Futile…if you can’t beat them…join them
  - IoT can be tremendously fun; show the business that you’re on top of it
  - Show the benefits of IoT: it opens new vistas for Human experience and new business opportunities
- Trust No One by Default
  - Don’t make *any* assumptions about the security of IOT vendors
  - Think about update cycles and what it takes to be sustainable in a world of constant hacks
  - Think about roots of trust, authorization models and enforcement now
- Work with Peers, Partners and Vendors
  - Standards
  - Regional and Vertical Groups
  - Follow the 5-Star advice
  - Rethink roots of trust and authorization – pressure vendors now

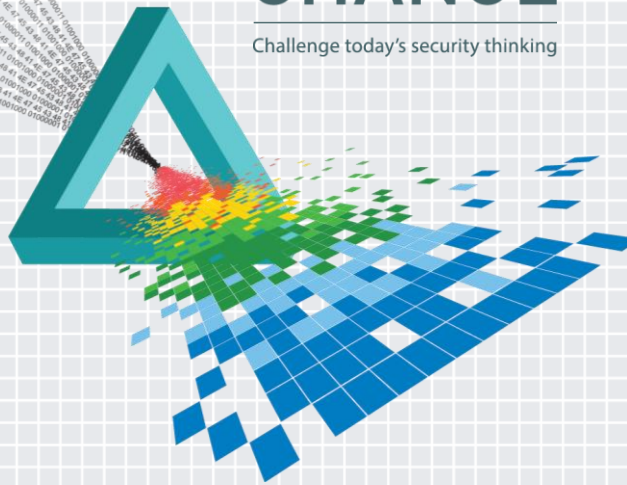


RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: STR-F01

Thoughts?
Feedback?
Any questions?

Sam Curry

Chief Technology and Security Officer
Arbor Networks
@samjcurry / scurry@arbor.net

Uri Rivner

Head of Cyber Strategy
BioCatch
@UriRivner / uri.rivner@biocatch.com