

Musings on the Four Horsemen of the Apocalypse and IOT

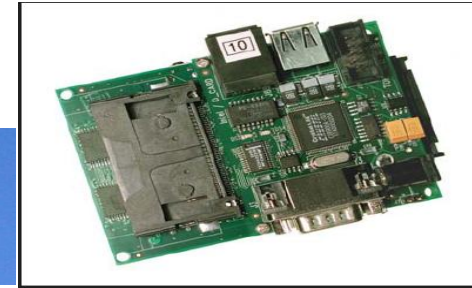
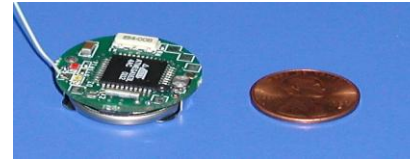
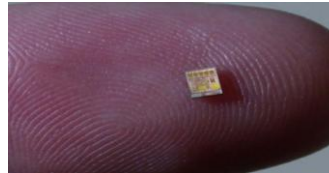
Tim Grance
grance@nist.gov
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Agenda

- Four Horsemen of the Apocalypse, **Cloud, Mobile, Big Data, Social**
- What is the Internet of Things?
- Current Landscape
- Other IoT Security Challenges
- Path Forward to Securing IoT
- IOT Primitives & Composition
- Discussion

Embedded Physical World

New Machines*



New Environments*
New Applications*

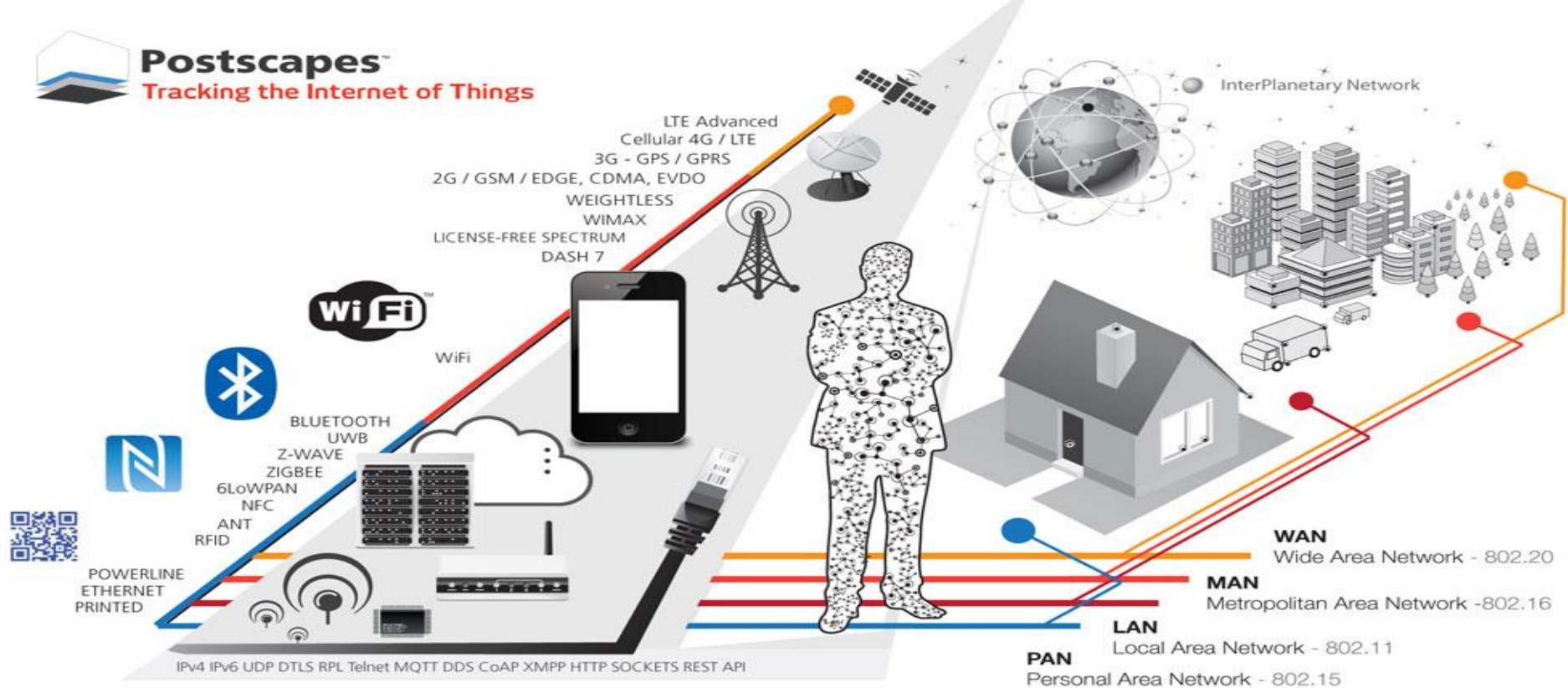


New Scale*

**Billion to trillion
 devices!**

Connecting the Physical World

Postscapes™
Tracking the Internet of Things



Current Network not designed to connect the physical world

Why Four Horsemen?

- Vast change in mobile, second wave of change in cloud, social continues to build, big data gets bigger, and now IOT.
- Complex technology, divergent business models, nervous governments/policy makers, different architectural schemes (API vs Cloud, etc.) many competing ecosystems
- Complexity, metastasizing attack surfaces, and security technology/thinking that is not scaling

Four Horsemen

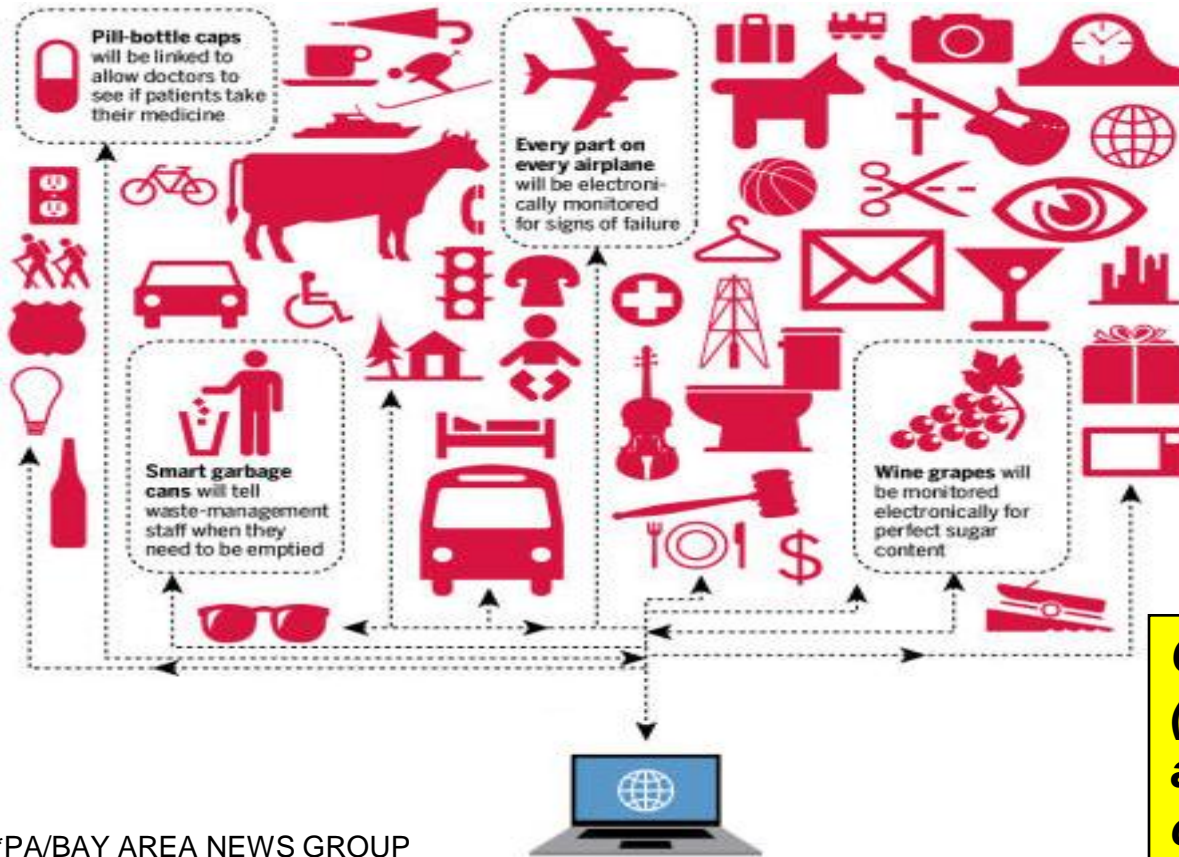
- Mobile, Social, Big Data, Cloud, and IOT/Sensors are/will contribute to the vast increase
- IoT is expected to exacerbate the complexity surrounding the four horsemen - mobile, social, big data, and cloud
- Need advances in math around large datasets, graph theory, machine learning, algorithms, etc.
- Future of computer science is in the **processing**, **analysis** and **safeguarding** of large amounts of distributed data (Hopcroft et al.)

Securing the Physical World



Current architecture not designed to secure the physical world

Devices will be heterogeneous

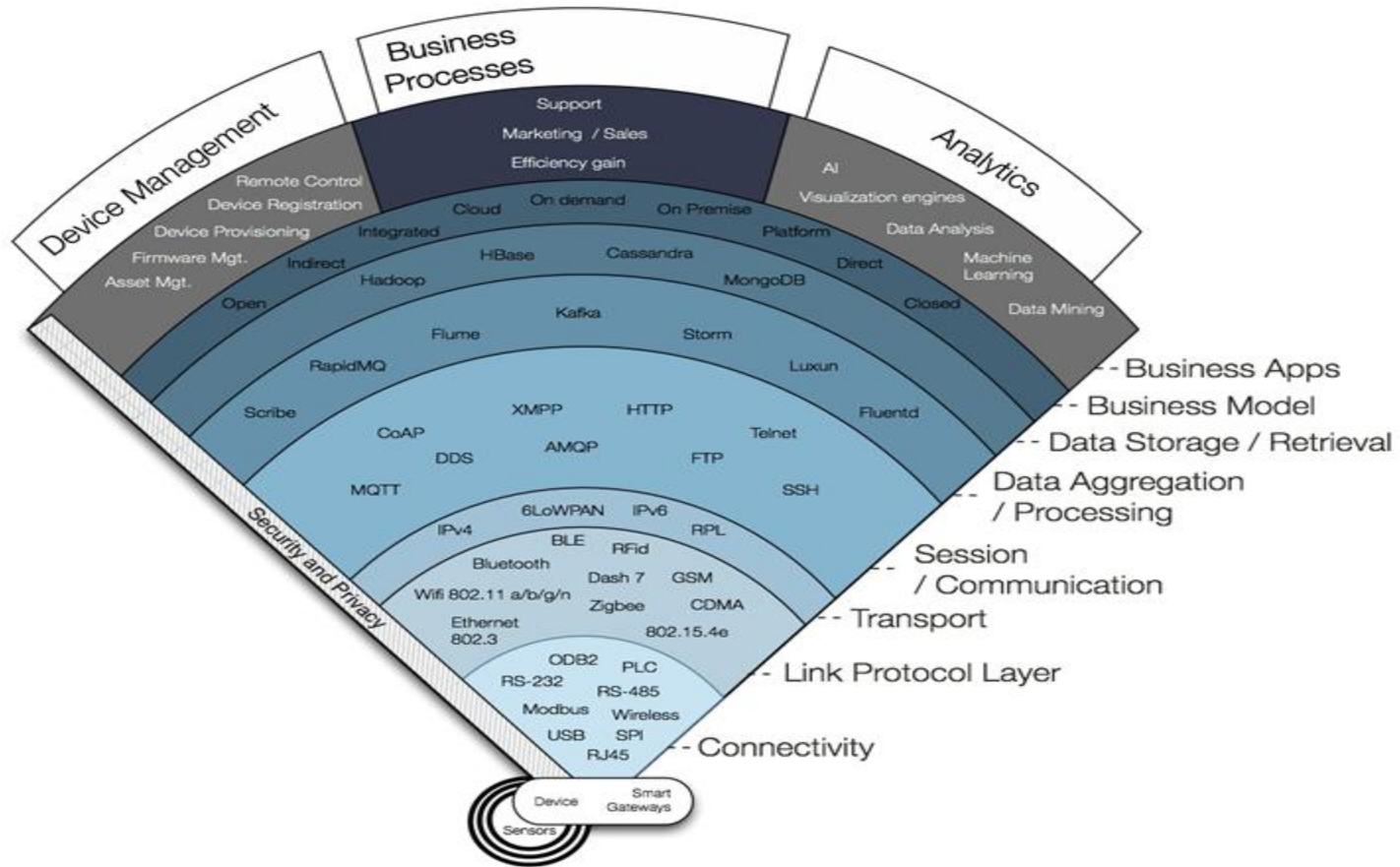


Heterogeneous in:

- Functionality
 - Data sensed
 - Actions invoked
- Processing capability
- Network and platform protocols, standards, technologies
- Applications and services
- Security requirements and capabilities

Combining physical objects (and specifically, their associated devices) will create new capabilities!

Myriad Technologies



Current IoT Landscape

The Good

- IoT Standards Efforts, Active Consortia
- Numerous available products
- Numerous potential benefits

The Bad

- Overlapping IoT Standards Efforts
- Ecosystem and Platform battle
- Numerous incompatible devices with proprietary technologies
- Multiple, complex security challenges

Other IoT Security Challenges

- Standardized IoT-related security definitions, taxonomies/ontologies, nomenclature, report/data formats, risk assessments, design patterns
- Authentication, authorization, and access control between very large numbers of devices
- Analyzing security of resource-constrained devices
- Analyzing and evaluating the security of existing standards and technologies for use in IoT:
 - Network standards, technologies, and protocols
 - Web/Cloud services
 - Mobile applications
 - Identity management, authentication, authorization, access control
 - Privacy

Other IoT Security Challenges

- Scalable security analysis of numerous, disparate resource-constrained embedded devices
- Identity management between devices, IoT platforms, gateways, and cloud services
- IoT platforms (still under development by various organizations)
- Organizational policies regarding IoT security

Path Forward to Securing IoT

- ❖ Categorize the threats in terms of importance
 - ❖ Denial of Service vs Data Loss
 - ❖ Confidentiality (Encryption) vs Availability (Energy)
 - ❖ Quantify the Big Data challenge for security

- ❖ Develop primitives that can allow the IoT devices to be secure on a macroscopic vs microscopic level
 - ❖ Encryption of data vs Authentication of devices
 - ❖ Move expensive security operations on hardware vs software
 - ❖ Understand what is important: connectivity vs usability

Path Forward to Securing IoT

- ❖ Encourage OEMs to make security a top priority during IoT product development
- ❖ Develop scalable approaches for analyzing the security of resource-constrained IoT devices
- ❖ Evaluate the suitability of using existing standards, technologies, and protocols for ensuring the security of IoT components and leverage wherever possible

Path Forward to Securing IoT

- ❖ Develop standardized IoT definitions, taxonomies/ontologies, nomenclature, use cases, design patterns
- ❖ Develop standardized security specifications for IoT platforms, data formats, risk assessments
- ❖ Encourage the development of a smaller set of defacto standards for IoT security
- ❖ Develop and implement policy and practice to ensure the security of IoT, particularly when applied to critical infrastructures including energy grids or national defense systems

'Networks of Things'

Pieces, Parts, and Data



J. Voas
Computer Scientist
US National Institute of Standards and
Technology

jeff.voas@nist.gov
j.voas@ieee.org

