The Internet of Things; Epic Change to Follow

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

2015

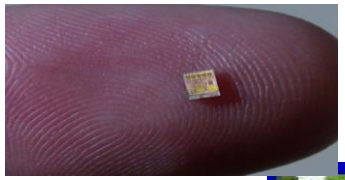
Agenda

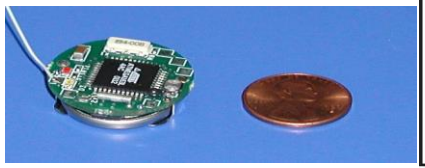
- Four Horsemen of the Apocalypse, **Cloud**, **Mobile**, **Big Data**, **Social**
- What is the Internet of Things?
- Current Landscape
- Other IoT Security Challenges
- Path Forward to Securing IoT
- IOT Primitives & Composition
- Discussion

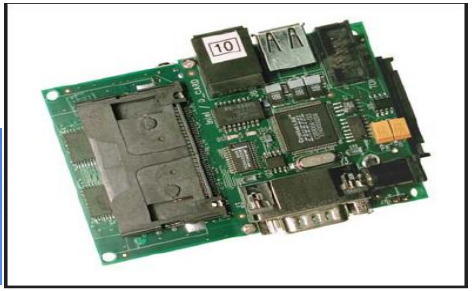
*

Embedded Physical World

New Machines*







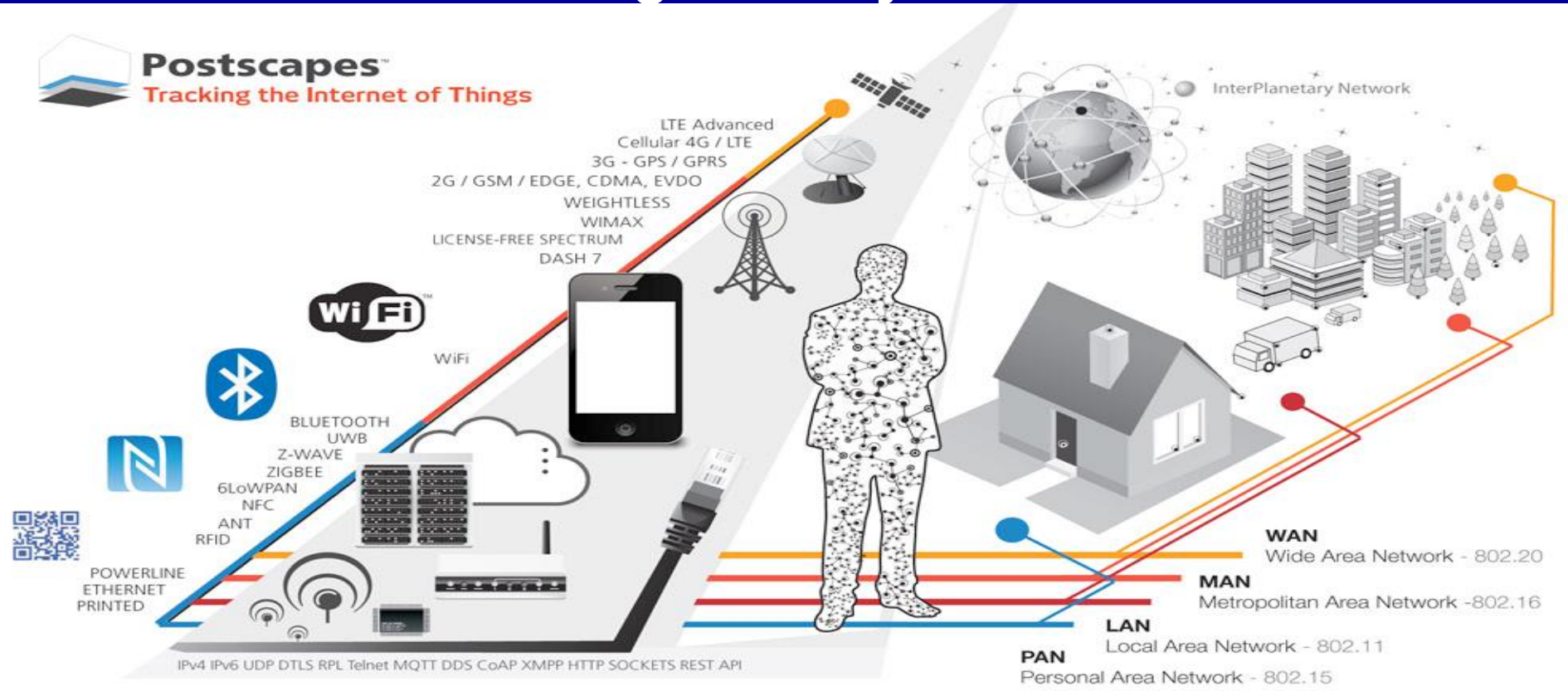
New Environments*
New Applications*

New Scale*

Billion to trillion devices!

*NSF

Connecting the Physical World



Current Network not designed to connect the physical world

By the Numbers - Verticals

IHS Automotive: The number of cars connected to the Internet worldwide will grow more than sixfold to 152 million in 2020 from 23 million in 2013.

Morgan Stanley: Driverless cars will generate $1.3 trillion in annual savings in the United States, with over $5.6 trillion in savings worldwide.

Navigant Research: The worldwide installed base of smart meters will grow from 313 million in 2013 to nearly 1.1 billion in 2022.

Machina Research: Consumer Electronics M2M connections will top 7 billion in 2023, generating $700 billion in annual revenue.

On World: By 2020, there will be over 100 million Internet connected wireless light bulbs and lamps worldwide up from 2.4 million in 2013.

Juniper Research: The wearables market will exceed $1.5 billion in 2014, double its value in 2013

Source: Forbes

Courtesy: Dr. Chris Greer

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

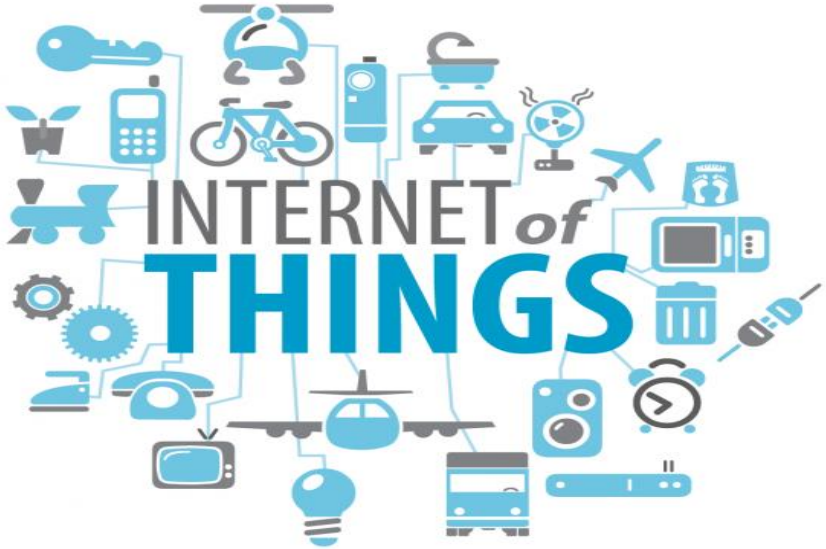
- Mobile, Social, Big Data, Cloud, and IOT/Sensors are/will contribute to the vast increase
- IoT is expected to exacerbate the complexity surrounding the four horsemen - mobile, social, big data, and cloud
- Need advances in math around large datasets, graph theory, machine learning, algorithms, etc.
- 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

What is the Internet of Things (IoT)?

There currently is no single definition of IoT



- Physical Objects (things)
  - Sensors
  - Actuators
- Virtual Objects
- People
- Services
- Platforms
- Networks

*

What is the Internet of Things (IoT)?

Currently, there is no universally-accepted definition of IoT or a "thing"

The Internet of Things (IoT) is the:

- interconnection of uniquely identifiable embedded computing-like **devices** within the existing Internet infrastructure. – *Wikipedia*
- network of **physical objects** that contain embedded technology to communicate and sense or interact with their internal states or the external environment. - *Gartner*
- network of **physical objects** accessed through the Internet. These objects contain **embedded technology** to interact with internal states or the external environment. – *Cisco*
- the networked interconnection of everyday **objects**. - *IETF*

“Thing”

*A “thing” is a (physical) object that contains one or more **devices***

Device Types:

- Sensors (sense the physical environment)
- Actuators (affect the physical environment)
- Combined Sensor/Actuator

Device Characteristics:

- IP-Based (IPv6)
- Resource-constrained (limited memory, processing capability)
- Processor, Embedded OS, IoT platform, firmware
- Wireless protocols, standards, technologies

Sensors and Actuators

“Thing” = Vehicle (physical object)

Vehicle has multiple devices

Sensors

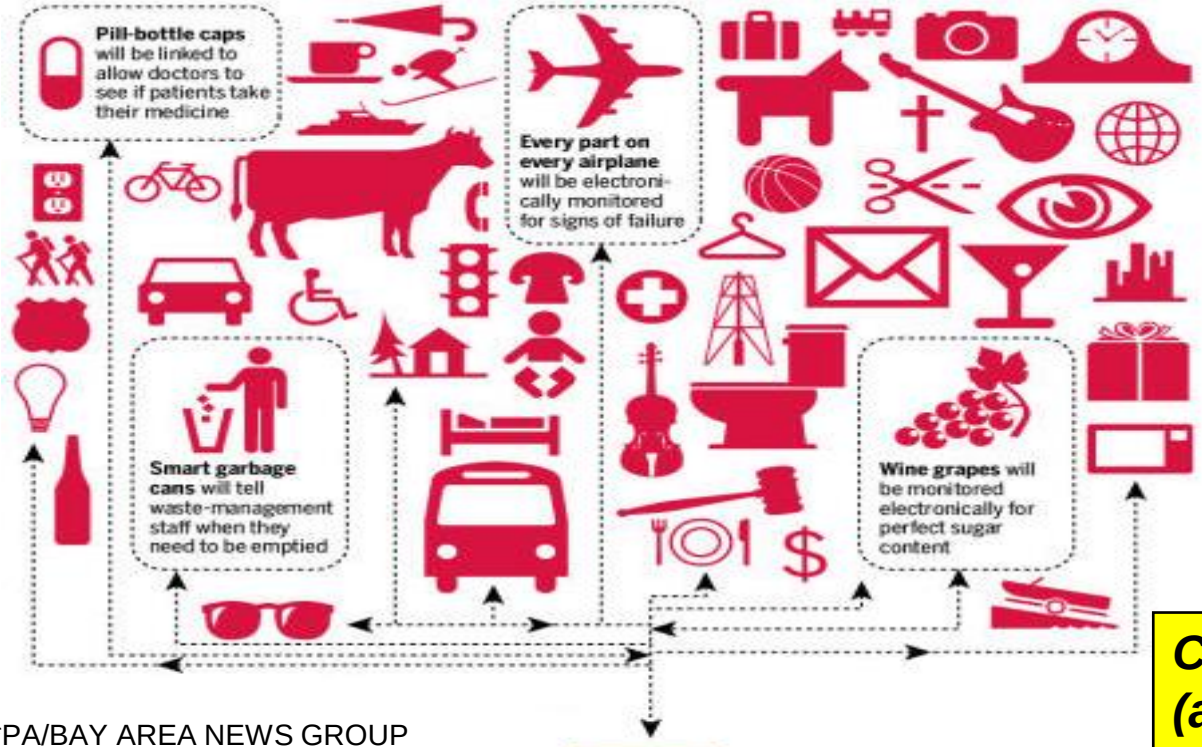
- GPS (location)
- Speed
- Suspension
- Skid
- Collision
- Air Bag
- Emission

In the Internet of Things, all of these devices (sensors and actuators) can be accessed via the Internet!

Actuators

- Brake Controller
- Throttle Controller
- Stability Controller
- Windshield Wiper

Devices will be heterogeneous



*PA/BAY AREA NEWS GROUP

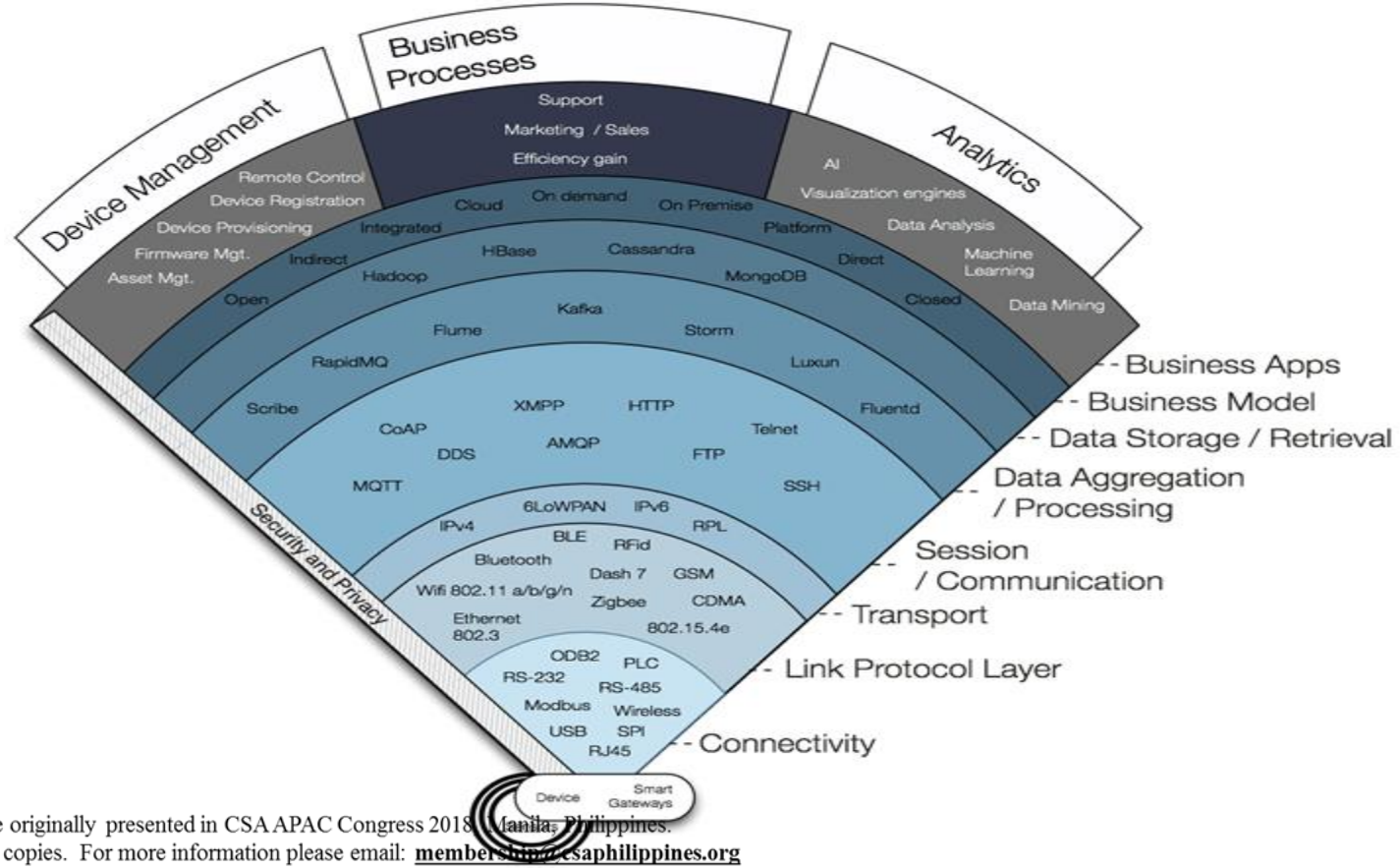
Heterogeneous in:

- 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



*Passemard 2014

*

IoT is Increasingly Present

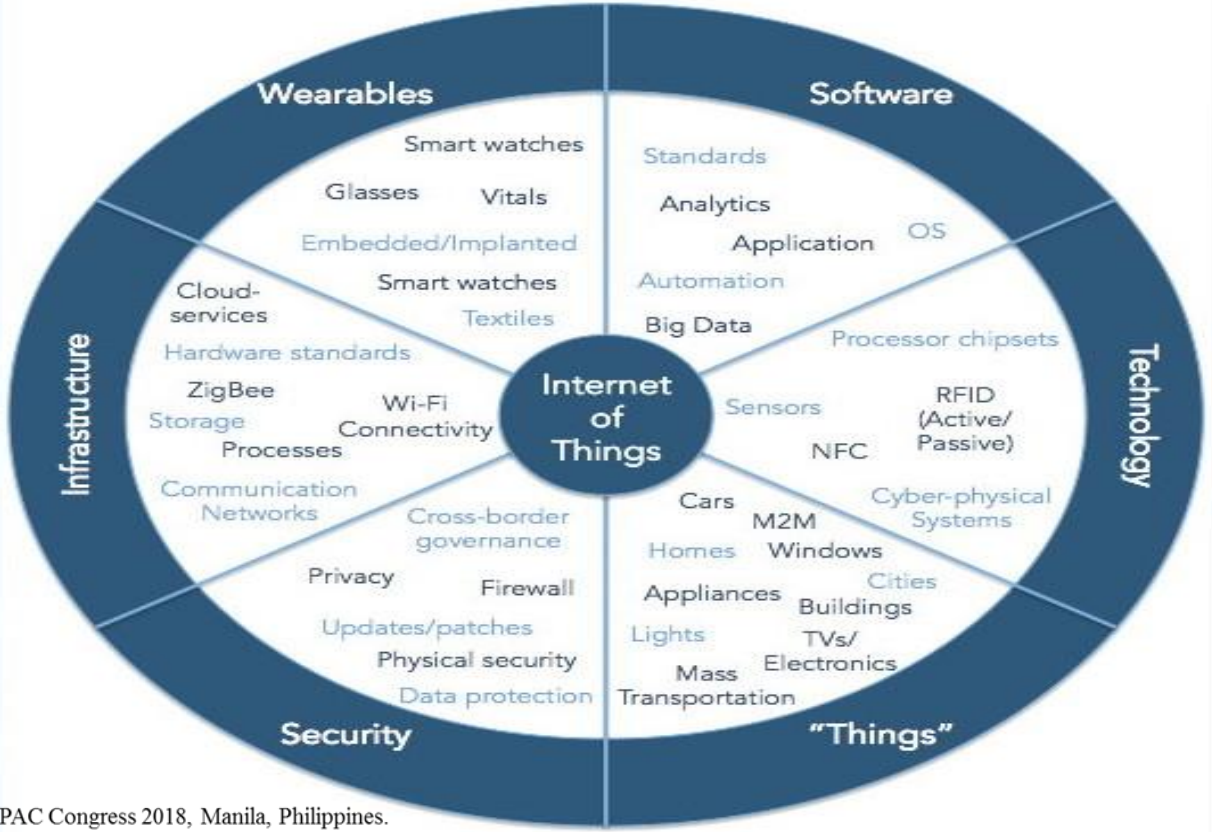
The IoT market by 2020

- The Internet of Things estimated market value: $8.89 trillion

- Wearables estimated market value: $8.3 billion

- If "Wearables" were removed from the estimated IoT value, the IoT overall value would STILL be $8.89 trillion

The sizeable IoT market opportunity is in software, security and infrastructure



@mattceni

Current IoT Landscape

The Good

- IoT Standards Efforts
- Numerous available products, platforms
- Numerous potential benefits

The Bad

- Overlapping IoT standards efforts, platforms
- Numerous incompatible devices with proprietary technologies
- Multiple, complex security challenges

*

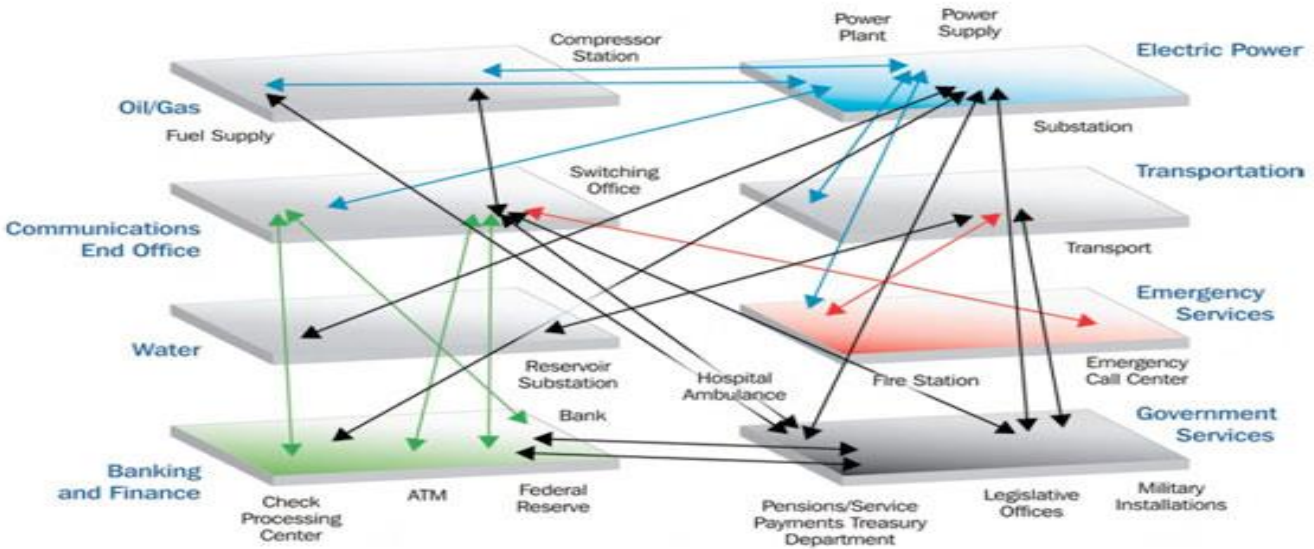
What is the potential IoT threat?

- Attacks will aim to acquire private information and control IoT components
- Attacks will affect the physical world
- Unlike most of today's endpoints (e.g., mobile phone), many IoT devices will work autonomously with little or no human intervention making it difficult to detect an attack
- By 2020, 50 billion IoT devices are expected. This proliferation vastly extends the attack surface.

*

IoT Security and Critical Infrastructures

IoT attacks can target critical Infrastructures



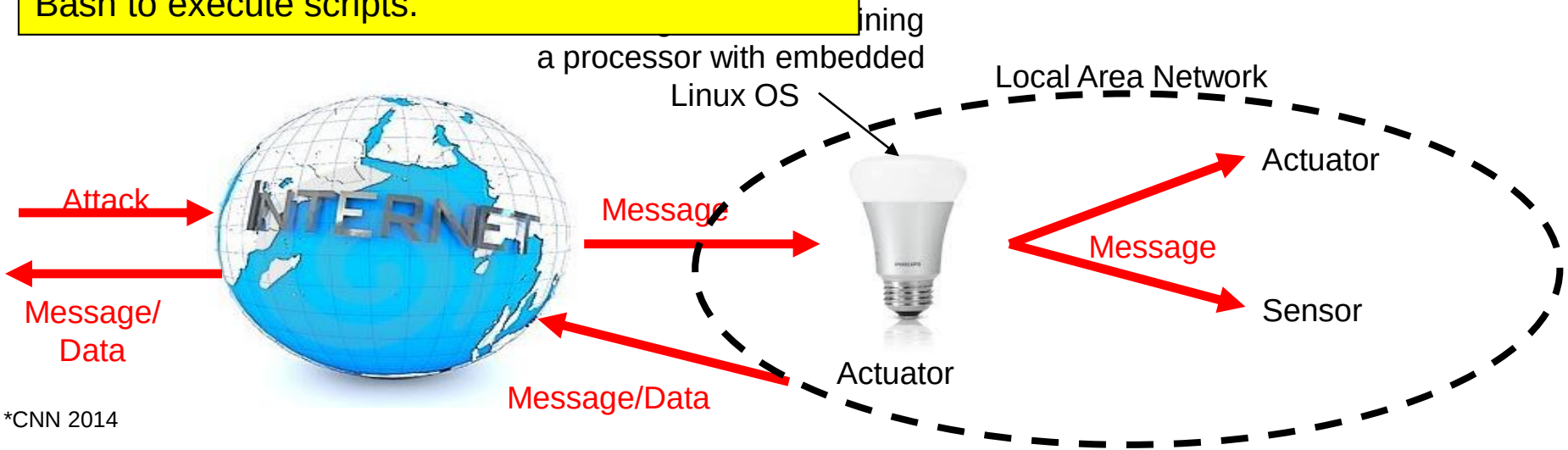
Connections and interdependencies across the economy. Schematic showing the interconnected infrastructures and their qualitative dependencies and interdependencies. SOURCE: Department of Homeland Security, National Infrastructure Protection Plan, available at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

*

Example: Bash Bug Vulnerability

Bash Bug is a vulnerability associated with the Linux Bourne Again Shell (Bash)

If Bash is configured as the default system shell, it can be used by network–based attackers against Unix and Linux devices via Web requests, secure shell, telnet sessions, or other programs that use Bash to execute scripts.



*CNN 2014

Other IoT Security Challenges

- Standardized IoT-related security definitions, taxonomies/ontologies, nomenclature, report/data formats, risk assessments
- 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
- What are the roles/limits of cryptography in IOT?
- 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

IoT Primitives

‘Networks of Things’

Pieces, Parts, and Data

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

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

Eight Primitives

1. Sensor
2. Snapshot (time)
3. Cluster
4. Aggregator
5. Weight
6. Communication channel
7. *e*Utility
8. Decision

First Primitive: Sensor – an electronic utility that digitally measures physical properties such as temperature, acceleration, weight, sound, etc. Cameras and microphones are also treated as sensors.

Second Primitive: Snapshot – an instant in *time*. Because a network of things is a distributed computing system, different events, data transfers, and computations occur at different times. Therefore it is necessary to consider time as a primitive.

Third Primitive: Cluster – a grouping of sensors that can appear and disappear instantaneously.

Fourth Primitive: Aggregator – is a software implementation based on mathematical function(s) that transforms various sensor data into *intermediate* data.

Fifth Primitive: Weight – is the degree to which a particular sensor's data will impact an aggregator's computation

Sixth Primitive: Communication Channel – any medium by which data is transmitted (e.g., physical via USB, wireless, wired, verbal, etc.).

Seventh Primitive: *e*Utility (external utility) - a software or hardware product, or service, that executes processes or feeds data into the overall dataflow of the NoT.

Eighth Primitive: Decision - a decision is the final result from data concentrations and any other data needed to satisfy the purpose and requirements of the specific NoT. Decisions are the outputs of NoTs and the reason for the existence of NoTs.

Six Other Actors

1. **Data** – the flow of information in a NoT workflow; data may be virtual or physical,
2. **Environment** – the universe that all primitives in a private NoT operate in; this is essentially the *operational profile* of the private NoT,
3. **Cost** – the expenses, in terms of time and money, that any specific private NoT architecture incurs in terms of the non-mitigated reliability and security risks, as well as the costs of each of the actors and the architecting of the private NoT,
4. **Geographic location -** Place where a sensor or *e*Utility operates or was manufactured. The operating location may change over time. Note that a sensor's or *e*Utility's geographic location along with communication channel reliability may affect the ability to move data throughout the workflow in a timely manner,
5. **Owner** - Person or Organization that owns a particular sensor, communication channel, aggregator, decision, *e*Utility, or computing platform. There can be multiple owners for any entity in a Not. Note that owners may have nefarious intentions, and
6. **Device_ID** – a unique identifier for each entity associated with a NoT.

Composition and *Trust*

Primitive or Actor	Attribute	Pedigree an Issue?	Reliability an Issue?	Security an Issue?
Sensor	Physical	Y	Y	Y
Snapshot (time)	Natural phenomenon	N/A	Y	?
Cluster	Abstraction	N/A	?	?
Aggregator	Virtual	Y	Y	Y
Weight	Variable constant	N/A	Y	?
Communication channel	Virtual or Physical	Y	Y	Y
eUtility	Virtual or Physical	Y	Y	Y
Decision	Virtual	Y	Y	Y
Geographic location	Physical (possibly unknown)	N/A	?	?
Owner	Physical (possibly unknown)	?	N/A	?
Data	Virtual	Y	Y	Y
Environment	Virtual or Physical (possibly unknown)	N/A	Y	Y
Cost	Partially known	N/A	?	?
Device_ID	Virtual	Y	?	Y

Summary

1. A common vocabulary is useful to foster dialogue concerning IoT
2. 8 primitives that impact the trustworthiness of NoTs are proposed
3. 6 actors that impact the trustworthiness of NoTs are proposed
4. NoTs are the likely means by which IoT will be delivered
5. IoT is in part a *big data* problem (maybe “overwhelming” is better than “big”)
6. As mentioned at the beginning, the goal is to build a definition(s) of IoT.

Future

1. Three diverse use case studies are being architected that have these properties: (1) acute healthcare (high security, medium reliability, and safety concerns), (2) smart home (high security, medium reliability, and safety concerns), and (3) crop agriculture (low security, medium reliability, and little to no safety).
2. If from this effort we can understand the composability issues of only 2 “ilities”, reliability and security, given the scalability and homogeneity concerns, we hope to map it to composing other “lesser” known but equally important “ilities.” This might once and for all begin to “chip away” at the age-old IT composability problem.

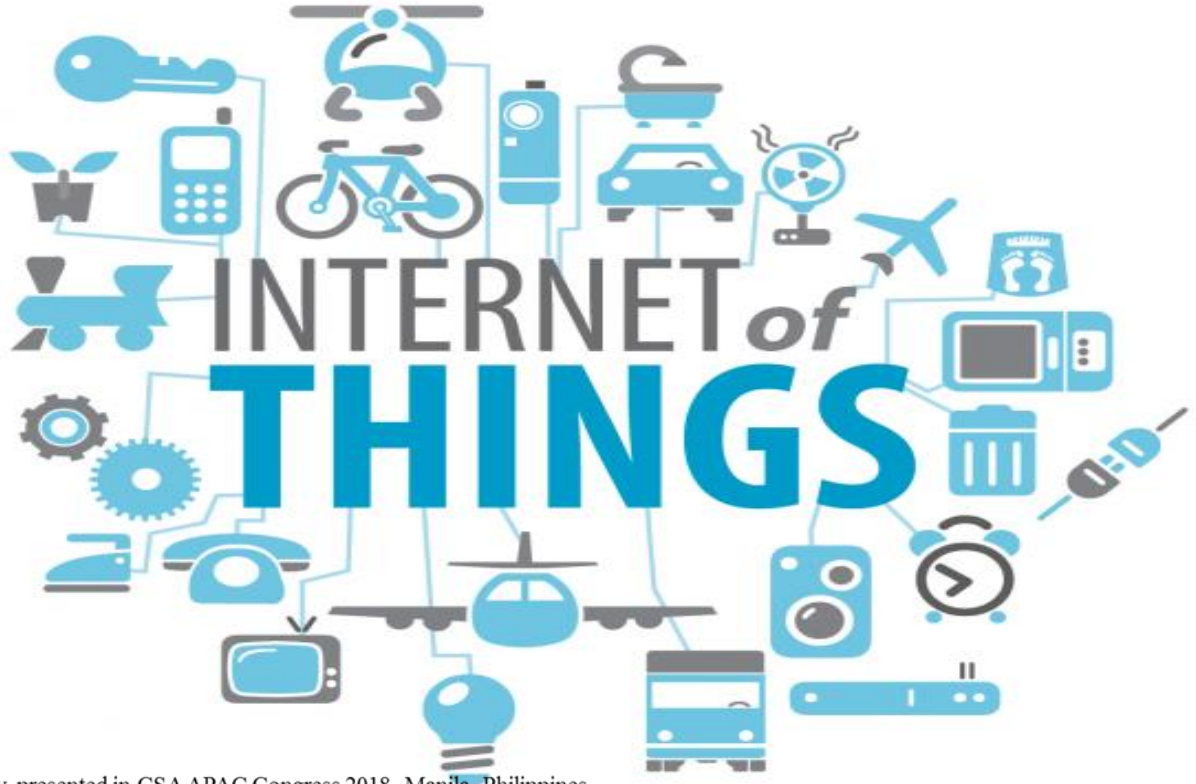
Appendix: Additional Points to Ponder

1. Things may be all software or hardware, a combination, or human.
2. Things may have a stealth/invisible mode when coming and going thus creating near-zero *traceability*.
3. Threats to previous genres of distributed, networked systems apply to NoTs. Security threats in NoTs may be exacerbated as a result of composing seemingly limitless numbers of 3rd party things. This may create *emergent* classes of new threats.
4. Successful functional composition of things does not suggest the secure composition of the same things.
5. Forensics concerning security, for seemingly limitless numbers of late-binding heterogeneous things, is unrealistic.
6. 'Counterfeit things' is a *supply-chain* problem, even for software [Skyba].
7. *Authentication* addresses the 'Who's Who' and 'What's What' questions. Things may misidentify, for faulty or nefarious reasons.
8. *Actuators* are things; if fed malicious data from 'other things', issues with life-threatening consequences are possible.
9. The workflow in NoTs is *time*-sensitive. Defective local or semi-global clocks (timing failures) can lead to deadlock, race conditions, and other classes of system-wide NoT failures.
10. Some NoTs may have the ability to self-organize and self-modify (self-repair). If true, NoTs can potentially rewire their security policy mechanisms and implementations or disengage them altogether.

Conclusion

- http://www.nist.gov/cps/
- http://csrc.nist.gov
- http://bigdatawg.nist.gov/home.php
- Major opportunities especially in industrial internet and capital intensive industries
- Security composition does not equal functional composition. Current security thinking will not scale to IOT. Cryptography will need to adapt beyond confidentiality to integrity/availability.
- Use cases, domain knowledge, advances in machine learning, algorithms, etc needed,
- Assert that this is data phenomenon. Scale is everything.
- Opportunities abound in many traditional areas such as smart cities, transportation, medicine, construction, and agriculture

Discussion



*