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

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Big Data's Potential in Securing the Internet of Things

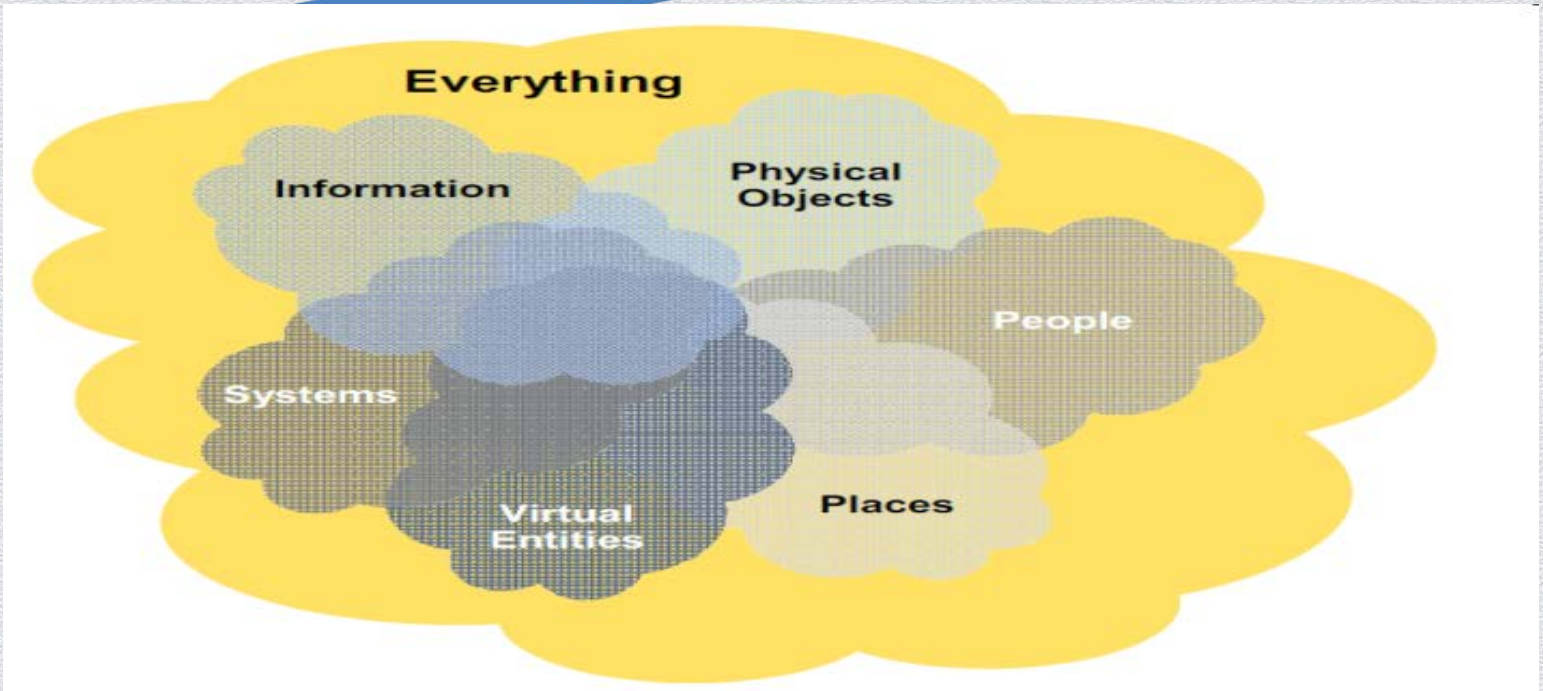
SESSION ID: ANF-W02

James Kobielus
IBM Big Data Evangelist
jgkobiel@us.ibm.com

IBM

The emerging infrastructure of Smarter Planet

Some call this the “Internet of Everything”



So what exactly is the Internet of "Things"?

❑ ***Vision of a Smarter Planet where sensors, intelligence, and connectivity are embedded into every human artifact, every element of the natural world, and even every physical person. (IBM)***

- A network of physical objects that contain embedded tech to communicate, sense, and interact with internal states or external environment (Gartner)
- "Uniquely identifiable objects (things) and their virtual representations in an Internet-like structure." (Wikipedia)

❑ **AKA: Machine to Machine (M2M) Internet, Sensor Internet, Ambient Internet, Industrial Internet,** Pervasive Computing.

What's driving the Internet of Things?

- Proliferation of low cost, smaller, smarter, embeddable sensors, processors, actuators, and communications components
- Explosion of mobile devices
- Rollout of advanced wireless networks

"*Today the connected devices market is dominated by mobile phones, but this will change in the future as a new wave of smartphones, tablets, consumer electronics and M2M devices connect everything from cars to health services and even entire cities*" – **GSMA (link)**

Source: Internet of Things: A 2013 HorizonWatch Trend Report (BP Ready)

Current Internet of Things apps are industry-focused

Industry sector	Applications
Automotive and transport	◆ Fleet tracking, consumer connected cars
Security	▪ Consumer connected alarms, commercial connected alarms, consumer connected security sensors, commercial connected security sensors
Healthcare	◆ Cardiovascular disease monitoring, other disease monitoring, body area networks
Government	◆ Video surveillance devices, police patrol car first responder devices, paramedic first responder devices, fire fighter first responder devices
Utilities	▪ Commercial electric meters, commercial water meters, commercial gas meters, residential utility meters
Retail	◆ Point-of-sale terminals, vending machines
Financial services	◆ ATMs

Source: Analysis Mason, M2M device connections, revenue and ARPU: worldwide forecast 2011–2021, May 2012

Emerging Internet of Things apps in consumer world

Smart vehicles

Smart homes

Smart schools

Smartphones

Smart wearables

Smart healthcare

How big is the Internet of Things becoming?

Approximately 10 billion devices are already permanently connected to the Internet today, with a further 50 billion to 60 billion devices attaching intermittently. These numbers are expected to rise to more than 200 billion by 2015. Source: Gartner

- ***Volumes***: pervasive IoT links driving collection, analysis, transmission, and delivery of increasing volumes of IoT data.
- ***Velocities***: real-time IoT links driving implementation of low-latency connections to support continuous, streaming interactions among physical and digital entities
- ***Varieties***: myriad IoT links driving implementation of standards to support fluid, flexible, contextual, robust, secure interactions among endpoints and infrastructures in diverse consumer, business, and other domains

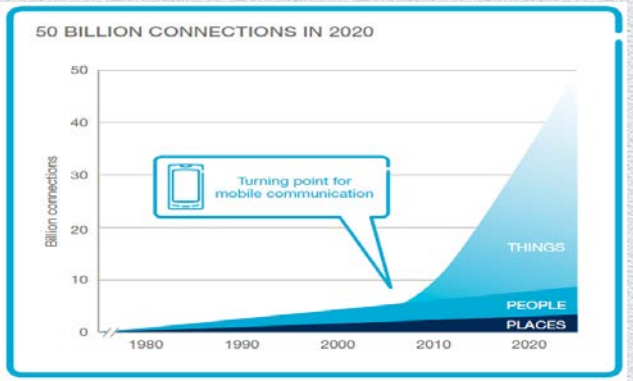
- Throughout the Smarter Planet
- Connecting millions of locations, billions of people, and trillions of devices
- In real time, continuously, often with guaranteed end-to-end latencies
- With embedded analytic intelligence at endpoints and in the infrastructure

Enterprise IT implications: storage, server/compute capacity, network capacity, connectivity, quality of service, *security*, etc.

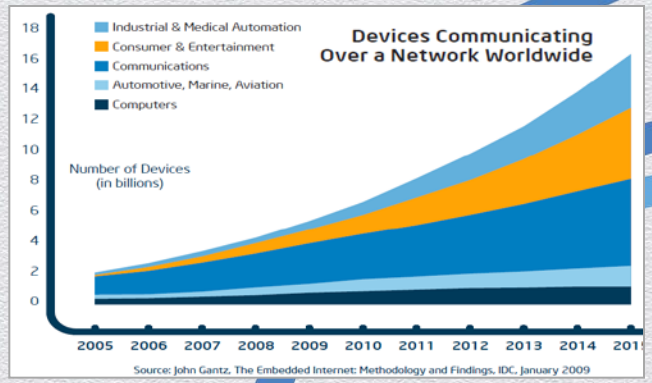
Forecasts call for billions of connected things

"Smart Connected Devices To Reach 13.5 Billion in 2016"
- **Harbor Research** (link)

Ericsson CEO Hans Vestberg estimates 50 billion devices will be connected to the Web by 2020 (link)



50 Billion Connections in 2020 – Ericsson (from page 18 of 2010 annual report)



John Gantz of IDC forecasts 15 billion devices will be communicating over the network by the year 2015 (link)

Source: Internet of Things: A 2013 HorizonWatch Trend Report (BP Ready)

The Internet of Things soon will be everywhere

Impact on Consumers – Top Ten Applications

"The "Connected Life" will be underpinned by seamless and pervasive connectivity between people and processes, enabling a wealth of valuable context-aware services to be delivered immediately and automatically. Individuals will enjoy personalised experiences whenever, wherever and for whatever they are required." – **GSMA** (link)

Impact on Business - Industries

"All of those instrumented and interconnected things are becoming intelligent. They are being linked to powerful new backend systems that can process all that data, and to advanced analytics capable of turning it into real insight, in real time." **- IBM** (link)

Soiurce: Internet of Things: A 2013 HorizonWatch Trend Report (BP Ready)

From a security perspective, is this Pandora's Box?

Surround everybody everywhere with everything we've got!!!!!!!!!

Is the Internet of Things too big, diverse, pervasive, and dynamic to secure comprehensively?

What's the problem?

- **Securing everything everywhere forevermore is the ultimate pipe dream.**
- **But securing every "thing" is becoming a critical issue as we move into the IoT era.**
- **Security is critical to IoT's adoption.**
- **How vulnerable are we to security vulnerabilities and privacy violations from the IoT?**

Can we "trust" the sensors, actuators, rules engines, and other connected thingamabobs that we embed in every element of our existence?

How acute is the IoT security problem?

•“Surge of new devices will usher in an unprecedented wave of security concerns.” [Gigacom, Aug 2010]

•“The Internet of Things … has an impact on the security and privacy of the involved stakeholders…Measures ***ensuring the architecture's resilience to attacks, data authentication, access control and client privacy*** need to be established. An ***adequate legal framework*** must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector.” [Computer Law & Security Review, Jan 2010] (emphases added)

Does the general public feel exposed to IoT?

In the post-Snowden age, many people are not reassured by statements such as this from former CIA director David Petraeus, who was discussing the surveillance potential of IoT-equipped "smart homes":

"Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing, the latter now going to cloud computing, in many areas greater and greater supercomputing, and, ultimately, heading to quantum computing."

Source:http://www.wired.com/dangerroom/2012/03/petraeus-tv-remote/

How does IoT complicate the security pro's life?

- So far, nobody has a comprehensive vision for how--or even if--the human race will be able to manage end-to-end security in the coming IoT world.
- The security devil is always in the details of the attack and the IoT is an endless proliferation of details.
- Every new "thing"--sensor, actuator, data source, data consumer, routing intermediary, etc--is a new security-relevant detail that stirs up a wide range of collateral security issues.
- Every new networked IoT endpoint is a new potential attack vector or launching point that the baddies can exploit.

How does IoT complicate the security pro's life? (continued)

- Potentially, every time you plug in a new IoT-networked device that is infected with malware or simply open to unauthorized third-party exploitation, the vulnerabilities start.
- Someone somewhere might exploit the new access point to gain illicit access to sensitive assets, to damage software and data, and to wage distributed denial of service attacks.

Where do we start to address IoT security?

- **“In the past, IT security has been based on establishing secure boundaries and firewalls around internal IT systems.”**
- **“The IoT model is defined by extreme access to many different devices that collect and leverage vast amounts of data.”**
- **“The concept of controlled access is changing with the IoT model to one of controlled trust to enable the wide range of possible solutions.”**
- **“IoT implementations must effectively deal with authorization, authentication, access control, privacy, and trust requirements while not negatively impacting usability objectives.”**

Source: IBM Academy of Technology, “Themes White Paper, Internet of Things” (April 2012)

Are there IoT security standards? Not yet

Considering the ever-expanding diversity of IoT endpoints--in scale, features, deployments, etc.--the security standards should be framed in ***functional terms that are agnostic to underlying physical implementations of the things themselves***.

❖ **IoT networking standards**

- IEEE - 802.15.4 (e-g) - Low-Rate Wireless Personal Area Networks (LR-WPANs)/
- IETF - Internet Engineering Task Force
- IETF - 6LowWPAN - IPV6 over low power wireless personal area network
- IETF- ROLL – Routing over low power and lossy networks
- IETF - CORE – constrained restful environments

❖ **IoT information and data standards**

- OGC SWE - Sensor Web Enablement
- OGC PUCK - standard instrument protocol to store and automatically retrieve metadata
- OASIS - MQTT – MQ Telemetry Transport (M2M)
- DPWS – Devices Profile for Web Services
- RFD – Resource Description Framework
- MQTT – MQ Telemetry Transport

❖ **IoT identification and tagging standards**

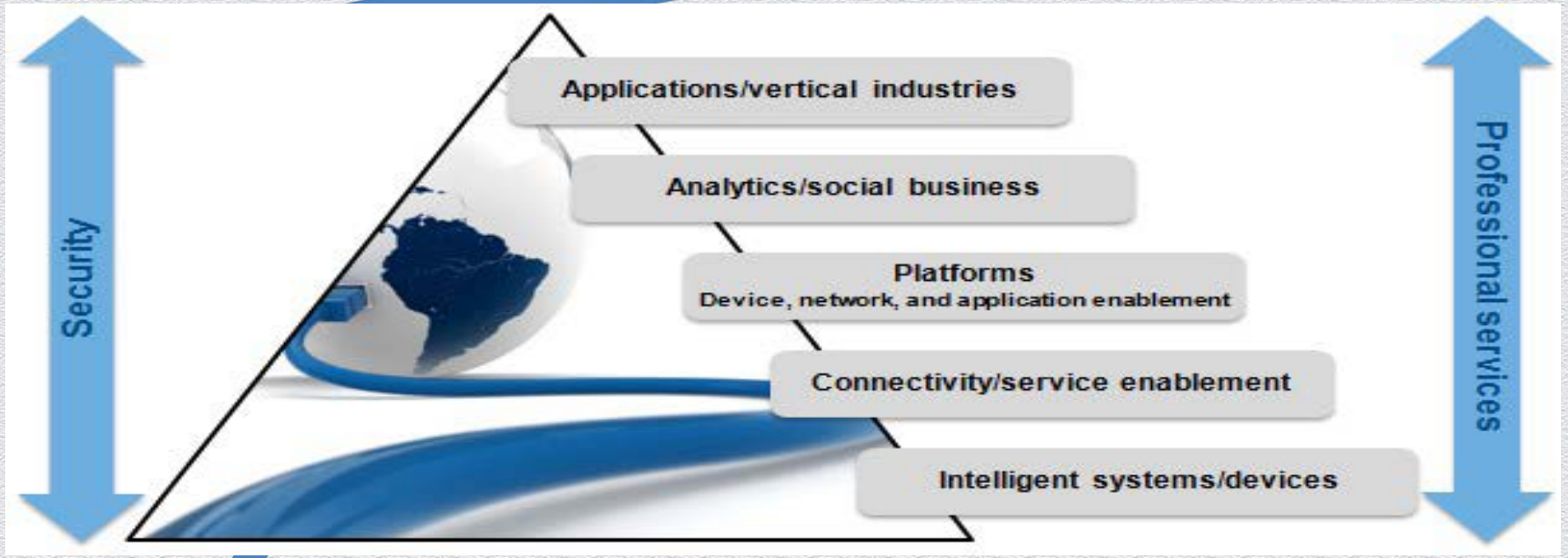
- EPC TDS – Tag Data Standard
- EPC TDT - Tag Data Translation machine-readable version of the EPC Tag Data
- EPC LLPR - Low Level Reader Protocol specifies an interface between RFID Readers and Clients

Ongoing EU effort to define IoT security

“To holistically embed effective and efficient security and privacy mechanisms into IoT devices and the protocols and services they utilise…. Privacy and security are major concerns, in particular to EU citizen. An IoT-A will ensure that appropriate mechanisms are deeply embedded in the IoT architecture, covering the hardware of its devices, communication and interaction protocols and the information level. To implement this goal IoT-A will extensively investigate and take into account service privacy and IoT access security aspects throughout the architecture design activities dealing with service accommodation, indentification and IoT-A platform realisations.”

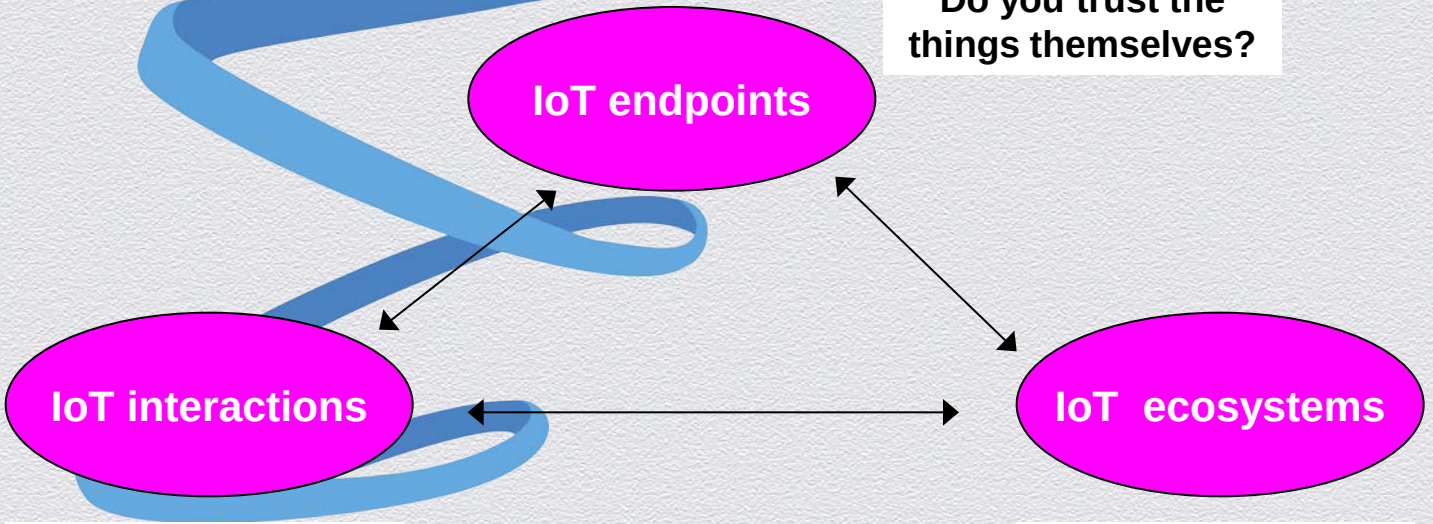
Source: http://www.iot-a.eu

IoT security must be comprehensive, multi-level



Source: IDC "Worldwide Internet of Things (IoT) 2013-2020 Forecast: Billions of Things, Trillions of Dollars" (October 2013)

Overall IoT security reference framework



Do you trust the things themselves?

Do you trust the things' interactions with the world around them?

Do you trust the things' value chains in the physical and virtual world?

Securing IoT endpoints






- **Everybody recognizes that the first line of IoT security must be built into the things themselves.**
- **At the very least, we should:**
  - rely on standardized IoT interfaces
  - incorporate robust security and attack-protections safeguards in the development of IoT products;
  - leverage widely vetted open security standards in IoT products;
  - embed modular security-aware hardware and software designs in IoT products; and
  - conduct independent review, auditing, and penetration testing of security in IoT products
  - Implement policy-driven bulk IoT device provisioning, configuration, & security patching

A big-data repository of thing identities, profiles, configurations, privileges, histories, and other metadata will prove essential for endpoint security.

Securing IoT interactions

- **Security vulnerabilities are consequences of how IoT endpoints interact with users, local &remote applications, cloud &other infrastructures, and each other.**
- **At the very least, we should:**
  - Leverage identity, authentication, access control, message encryption, transport-level security, key exchange, digital signatures, de-identification, privacy, intrusion detection, alerting, auditing, monitoring, malware prevention, DDoS prevention, and other infrastructure services in IoT environments
  - Use analytic and trend-analysis tools to identify threats across the entire IoT cloud under your purview.
  - Monitor and log IoT security-relevant events
  - Embed and continuously update analytics algorithms that detect various security issues, predictively pre-empt attacks, and automatically alert, escalate, and log all priority issues.
  - Escalate exceptional, unprecedented, and undiagnosed IoT issues to human security analysts for further investigation.

A big-data security incident & event management repository will be the foundation for logging IoT events for predictive, real-time, & historical analysis.

Securing IoT ecosystems

- **Security vulnerabilities may introduced anywhere in the constellation of solution providers, service businesses, certification authorities, and others who build, deploy, test, manage, and vouch for the endpoints and infrastructures.**
- **At the very least, we must:**
  - Assemble the compliance, legal, contractual, trust, reputation, governance, operational, and risk management frameworks to handle the interlocking responsibilities of all these parties for ensuring end-to-end IoT security.
  - Inspect, certify, vet, monitor, and audit the suppliers of IoT components and life-cycle services for conformance to generally accepted IoT security practices
  - Implement strong authentication, permission management, content encryption, tamperproofing, and other technical safeguards to prevent unauthorized parties in the value chain from gaining access to sensitive data

A big-data ecosystem registry will facilitate tracking of all value-chain parties who “touch” security-sensitive things throughout their life cycles.

Summary

- **Comprehensive IoT security is multilayered: device and application endpoints, middleware and infrastructures, vendor ecosystems.**
- **Fortunately, the IoT industry and security professionals are beginning to address these challenges on many fronts.**
- **As new IoT technologies take hold and new threats reveal themselves, the global security framework will grow more complex.**
- **Ongoing refinement of IoT security standards, practices, and tools will go on indefinitely.**

James Kobielus
jgkobiel@us.ibm.com

@jameskobielus