Securing the Internet of Things

Daniel W. Engels, PhD

Associate Professor, **Southern Methodist University**

Member, **AIDC100**

WHAT IS THE INTERNET OF THINGS?

Internet of Things (WikiPedia)

The Internet of Things (IoT, ~~also Cloud of Things or CoT~~) refers to the interconnection of **uniquely identifiable embedded computing like devices** within the **existing Internet infrastructure**.

Accessed 24 July 2014

Internet of Things (ITU)

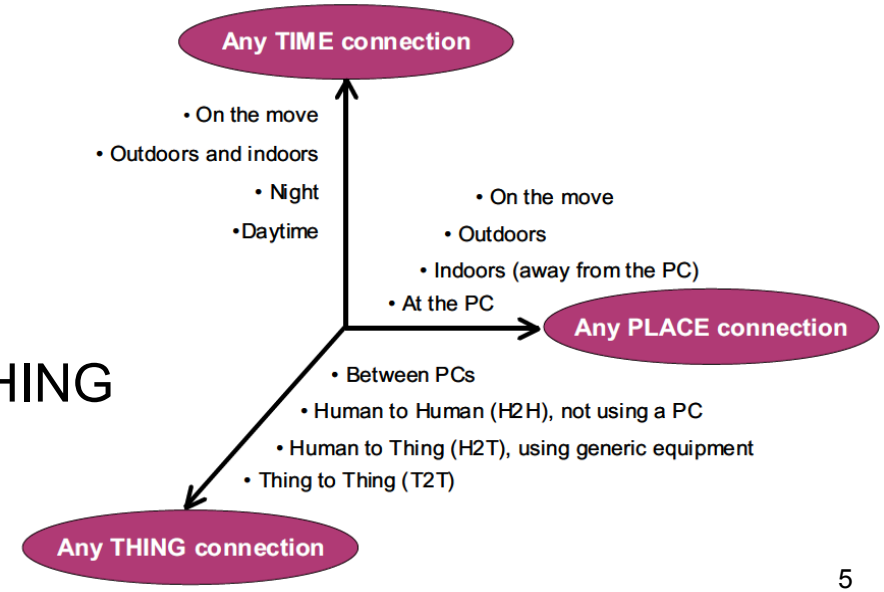
A global infrastructure for the information society, enabling advanced services by interconnecting (**physical** and **virtual**) things based on existing and evolving interoperable information and communication technologies.

IoT Connects

Any TIME

Any PLACE

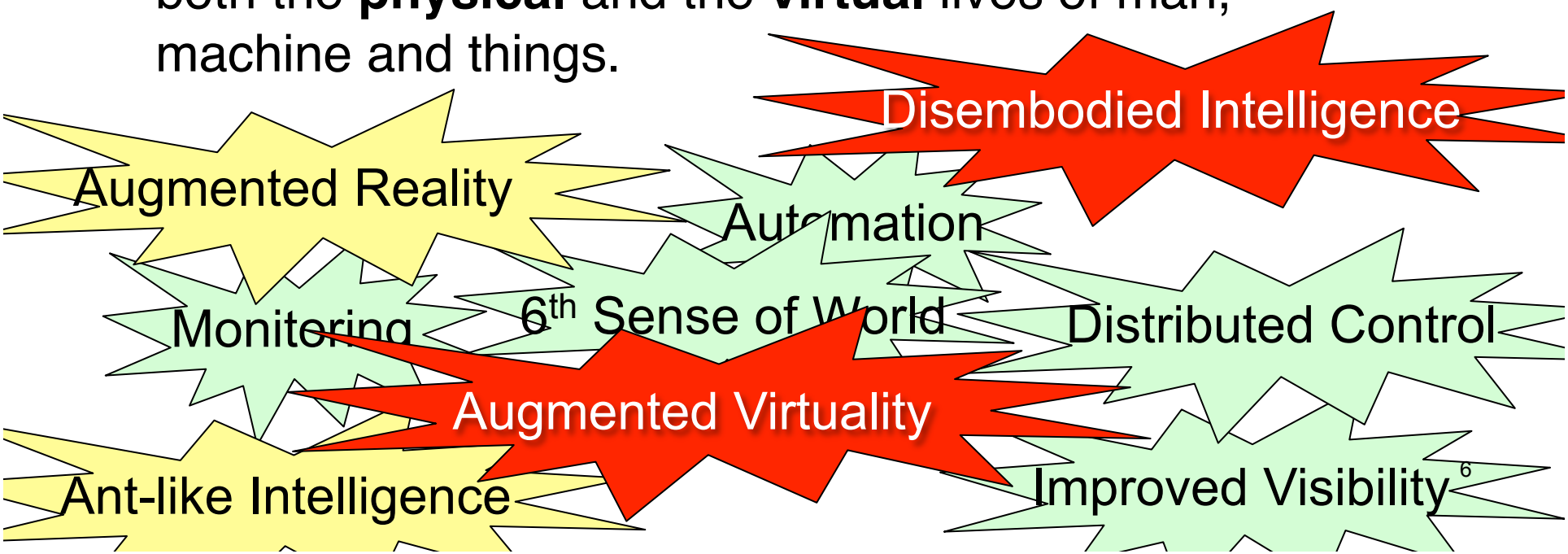
Any THING

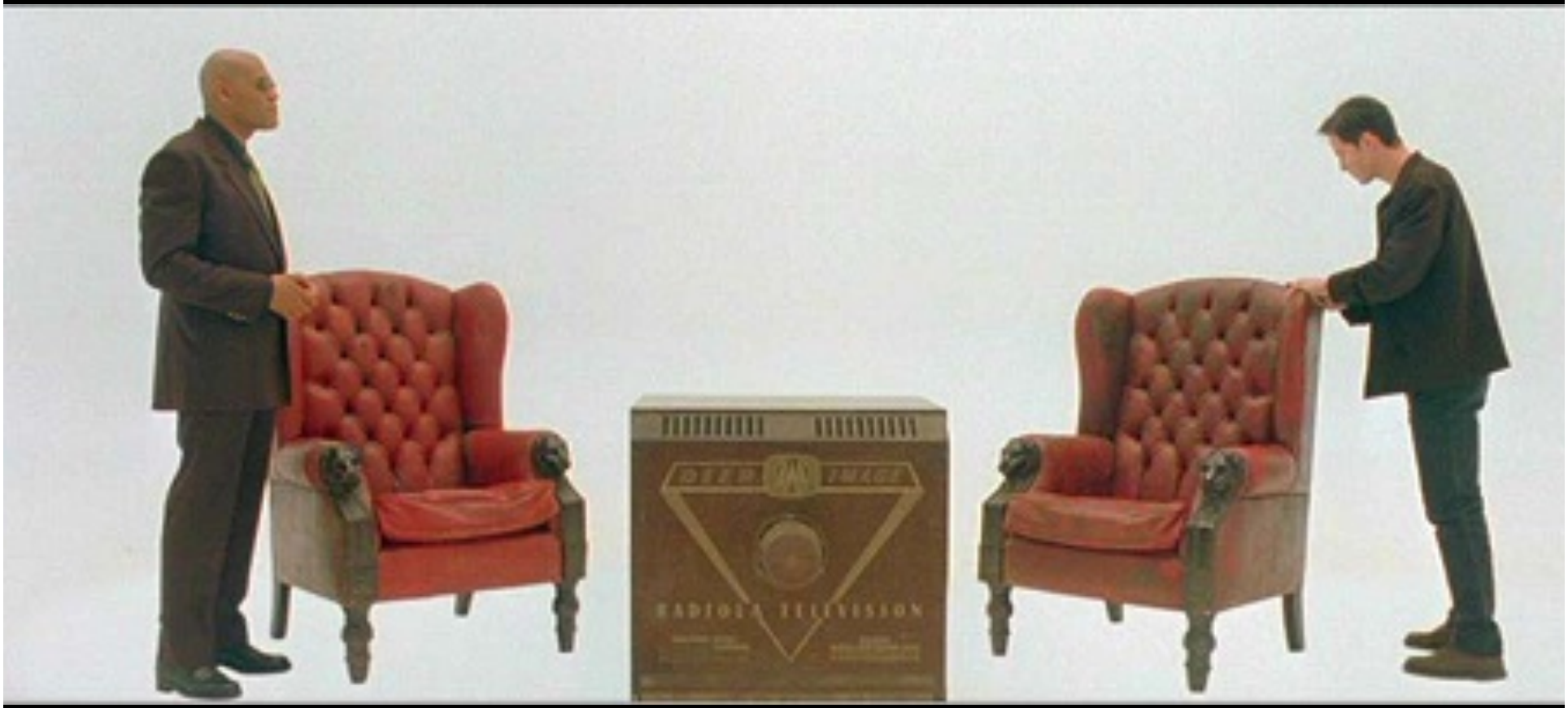


Source: ITU adapted from Nomura Research Institute

Internet of Things (Dragon Files)

Merging of the physical world with the virtual world in order to **give virtual lives to inanimate objects, ideas and concepts** and through those lives to **impact** both the **physical** and the **virtual** lives of man, machine and things.




RADIOLA TELEVISION

Pros
Pros
WORLD OF WARCRAFT
Seal of Vengeance
Magic
Melee attacks have a chance to cause 80 Holy damage over 12 sec.
29 seconds remaining
Azuremyst Isle
You gain Seal of Vengeance.
Forbearance fades from you.
You gain Avenging Wrath.
You are afflicted by Forbearance.
Seal of Vengeance fades from you.
Avenging Wrath fades from you.
You gain Seal of Vengeance.

Pros
Pros
WORLD OF WARCRAFT
Seal of Vengeance
Magic
Melee attacks have a chance to cause 80 Holy damage over 12 sec.
29 seconds remaining
Azuremyst Isle
You gain Seal of Vengeance.
Forbearance fades from you.
You gain Avenging Wrath.
You are afflicted by Forbearance.
Seal of Vengeance fades from you.
Avenging Wrath fades from you.
You gain Seal of Vengeance.

Pros
Pros
WORLD OF WARCRAFT
Seal of Vengeance
Magic
Melee attacks have a chance to cause 80 Holy damage over 12 sec.
29 seconds remaining
Azuremyst Isle
You gain Seal of Vengeance.
Forbearance fades from you.
You gain Avenging Wrath.
You are afflicted by Forbearance.
Seal of Vengeance fades from you.
Avenging Wrath fades from you.
You gain Seal of Vengeance.

Bored

Lost in Translation

It's a second Job

Why would my chair want to play WoW?

Escape from a heavy life

Play with a sitting buddy

Well

How would my chair play WoW?

Integrated Processor

Through its own account

Network

What needs to happen for every chair to be able to play WoW?

Standards

Ubiquitous Networks

Low Cost Computing

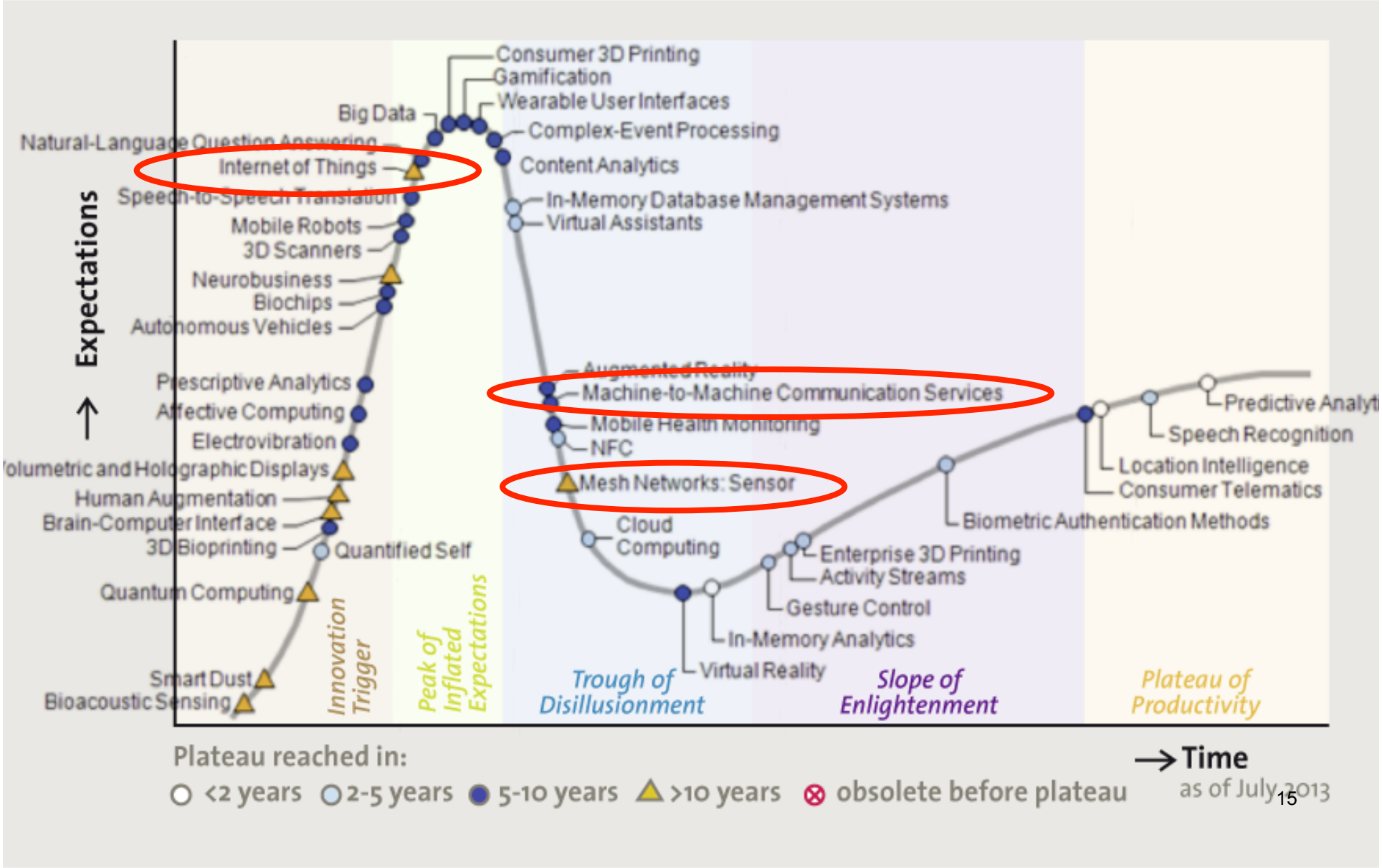
Value to Human Overlords

Talk Outline

- Where is the Internet of Things Today?
- What are we missing?
- What are the technologies of the Internet of Things?
- Defining Security and Privacy
- IoT systems today are lacking that basic security feature
- A closer look at Passive UHF RFID
- Final Thoughts

WHERE IS THE INTERNET OF THINGS TODAY?

The Internet of Things…



Nest

WeMo Belkin

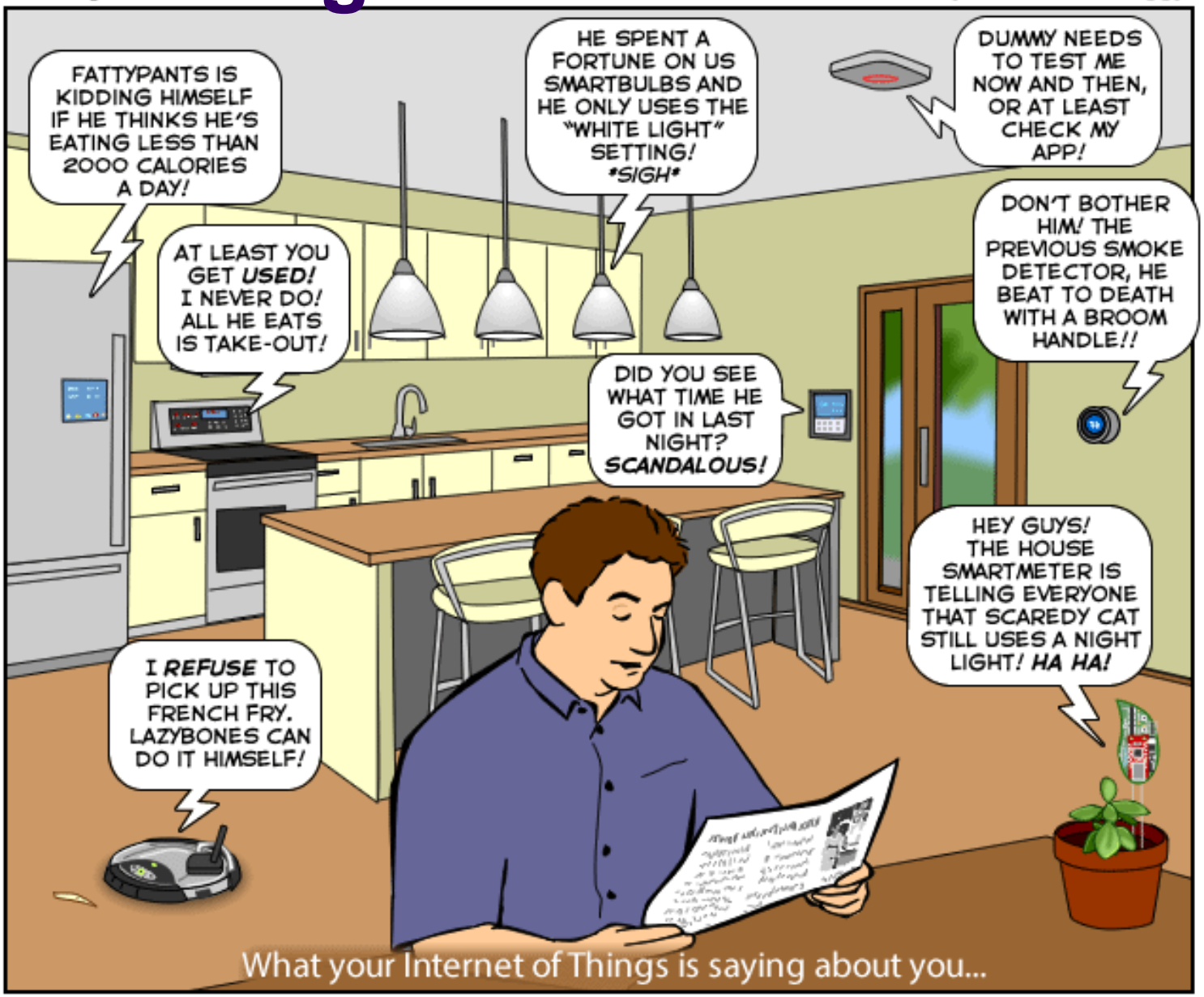
WeMo
SWITCH+MOTION
belkin
The iPhone home remote and motion sensor.
Le détecteur de mouvement et télécommande domotique de l'iPhone.
Heater
OFF
Fan
ON
Lamp
ON
Curling Iron
OFF
Free WeMo app
Application WeMo gratuite

WHER
iPod
11:58 PM
wemo
Edit
Bedroom Lamp
Fan
Iron
Playroom Lamp
Coffee Machine
Radio
Switches
Sensors
Rules
More

Fitbit

1
TRACK YOUR ACTIVITY & YOUR SLEEP
2
SYNC YOUR STATS WIRELESSLY
3
SEE REAL-TIME PROGRESS
4
MAKE FITNESS FUN
Sleep
SLEPT REALLY WELL LAST NIGHT
WIRELESS SYNC
BLUETOOTH 4.0/ BLUETOOTH SMART
12680
fitbit
WORKS WITH MAC OSX AND WINDOWS
SEE SUPPORTED MOBILE DEVICES

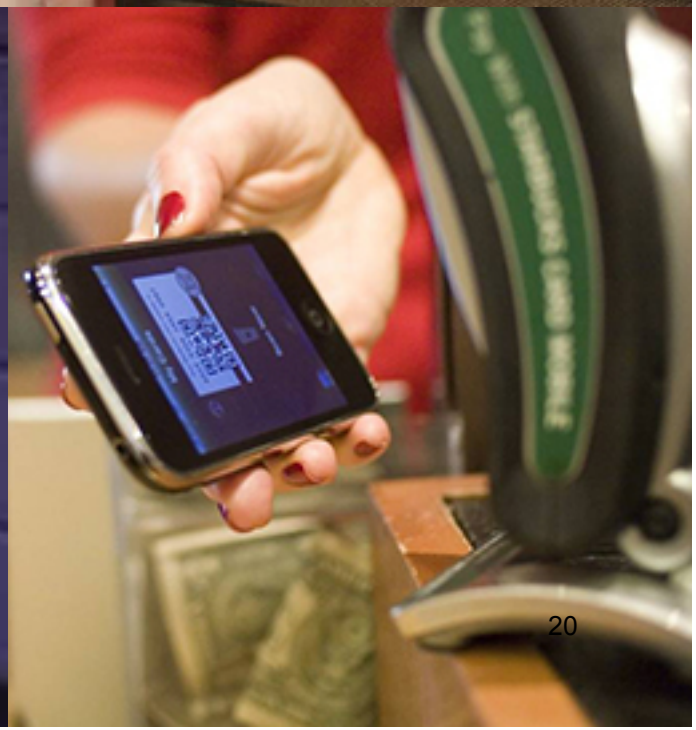
IoT Intelligence Surrounds Us



© 2014 Geek Culture

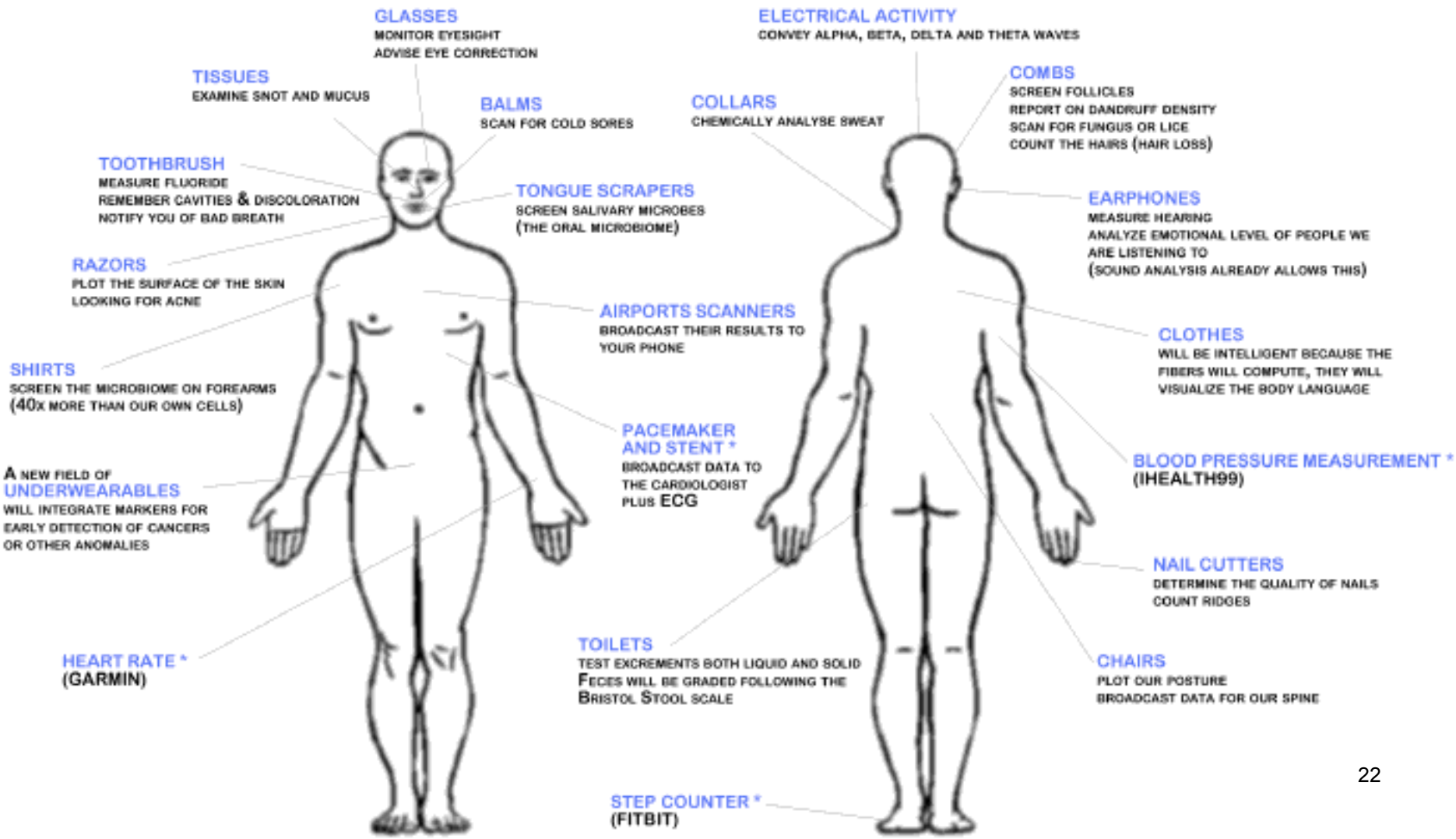
joyoftech.com

IoT Around Us



Connecting Bits and Atoms

IoT Within Us AND On Us



Technology Acceptance in our Lifetimes (adapted from Scott Adams)

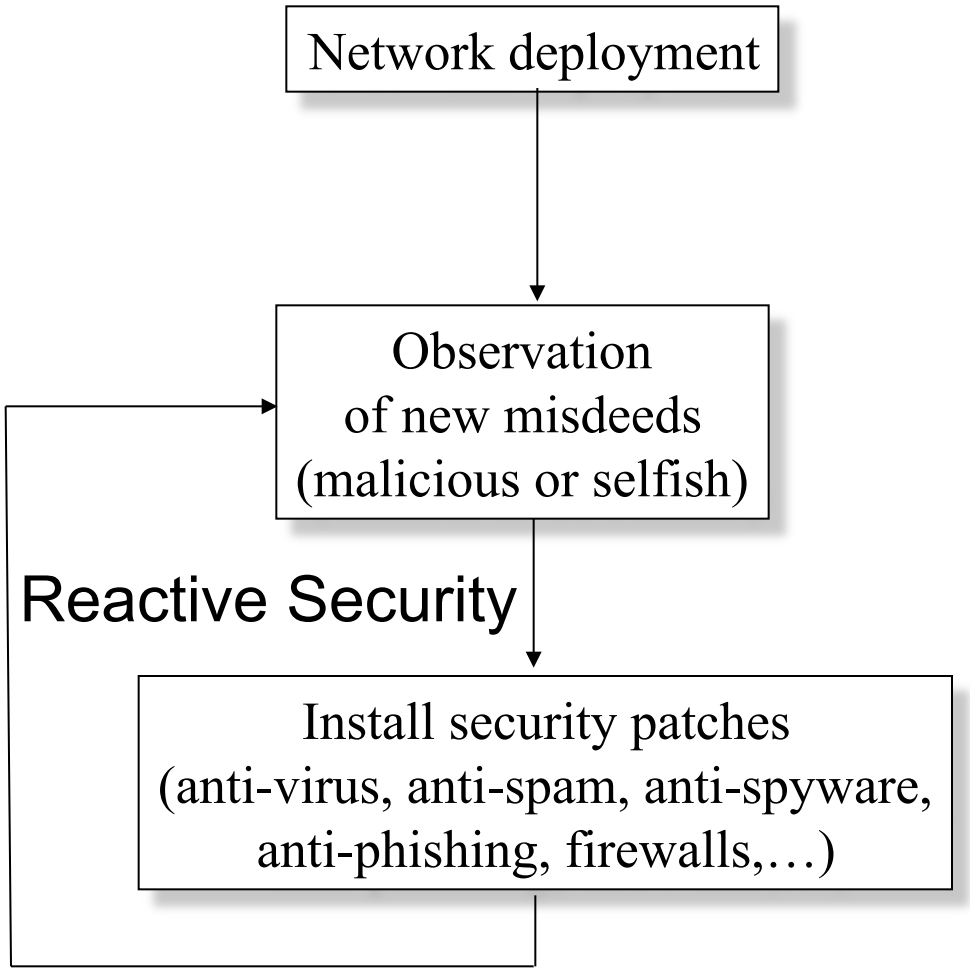
- Anything that is in the world **when you're born** is **normal and ordinary** and is just a natural part of the way the world works

- Anything that's invented between **when you're fifteen and thirty-five** is **new and exciting and revolutionary** and you can probably get a career in it

- Anything invented **after you're thirty-five** is **against the natural order of things**.

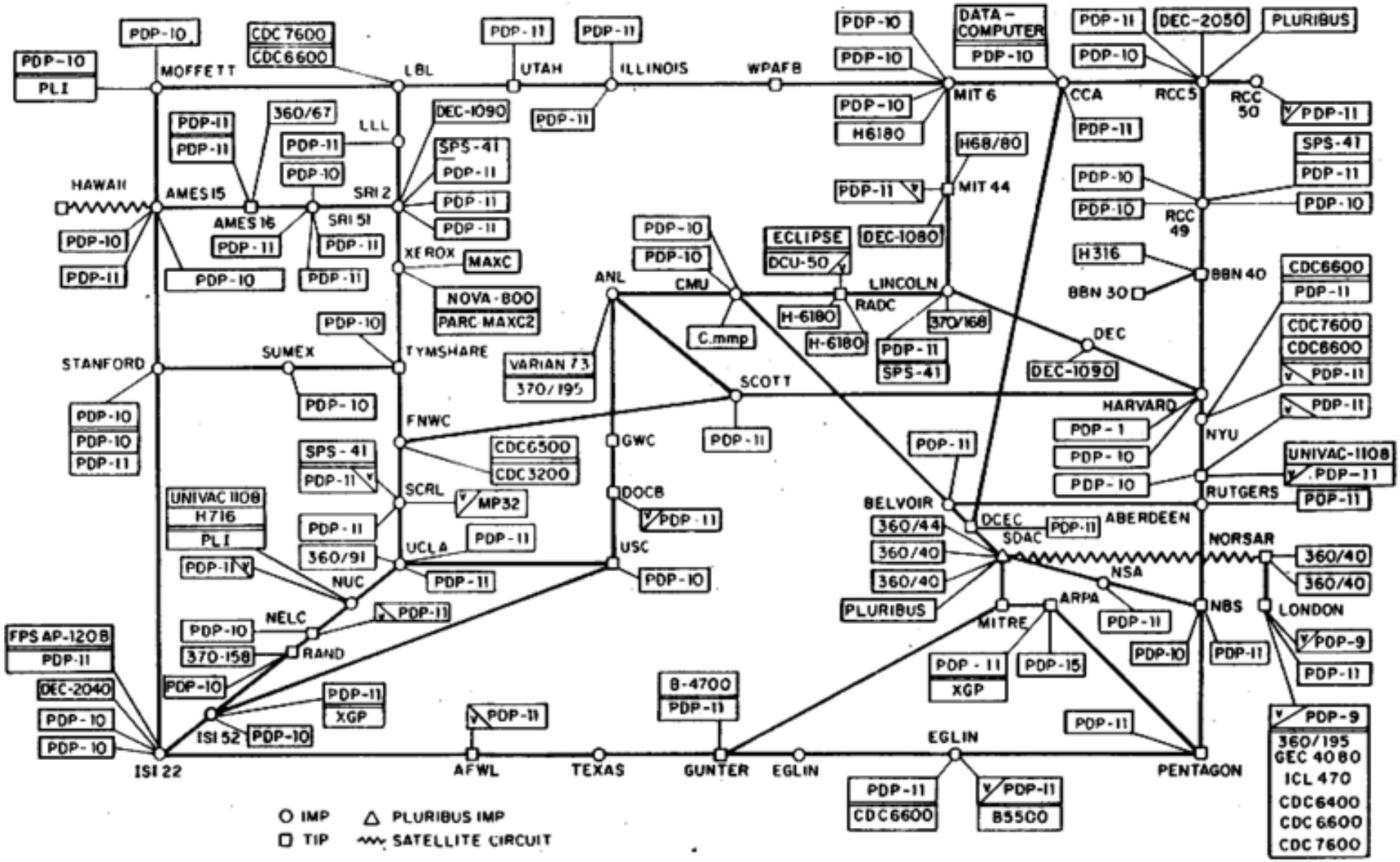
WHAT ARE WE MISSING?

The Internet is Broken



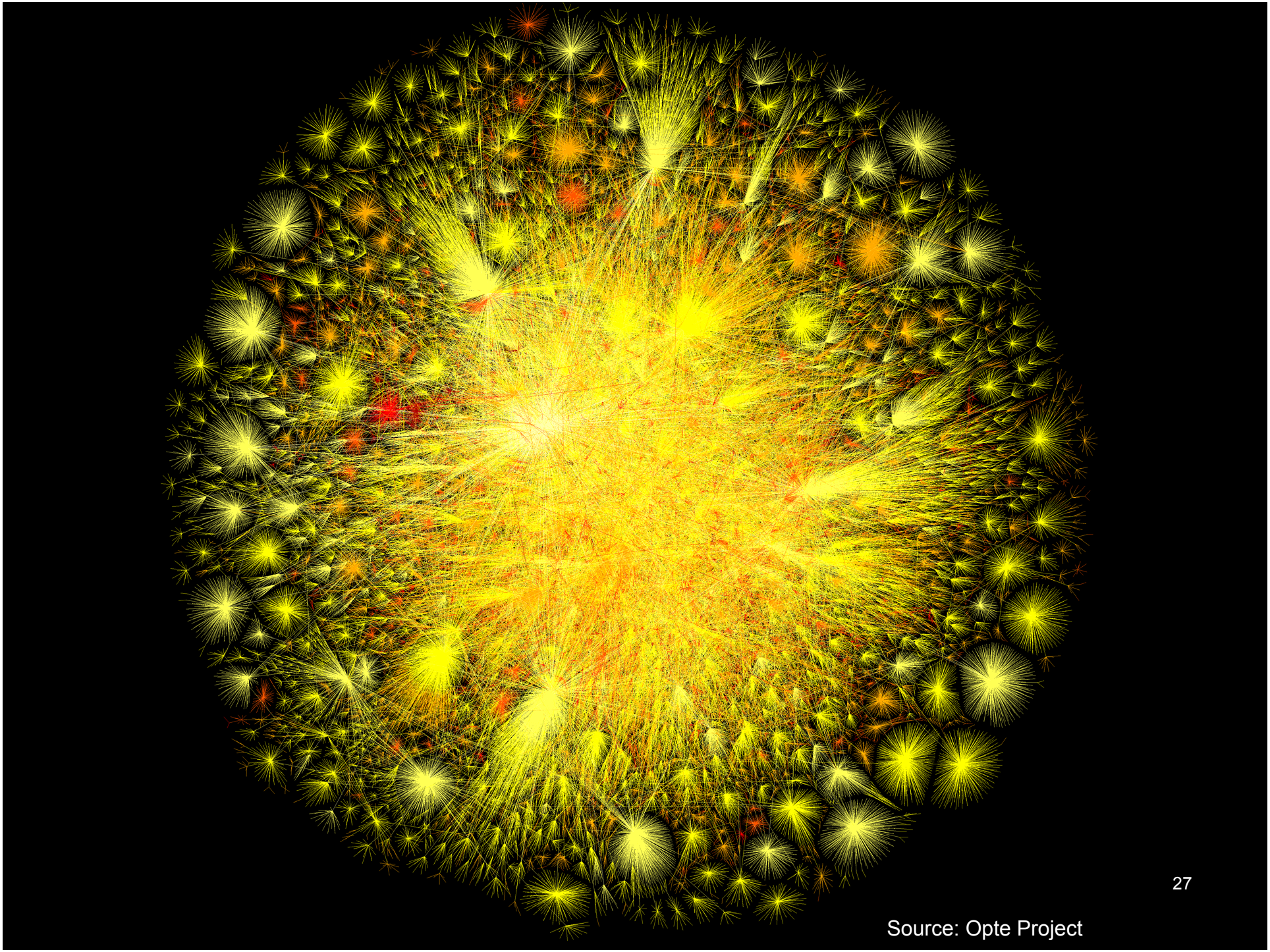
"The Internet is Broken", MIT Technology Review, Dec. 2005 – Jan. 2006

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

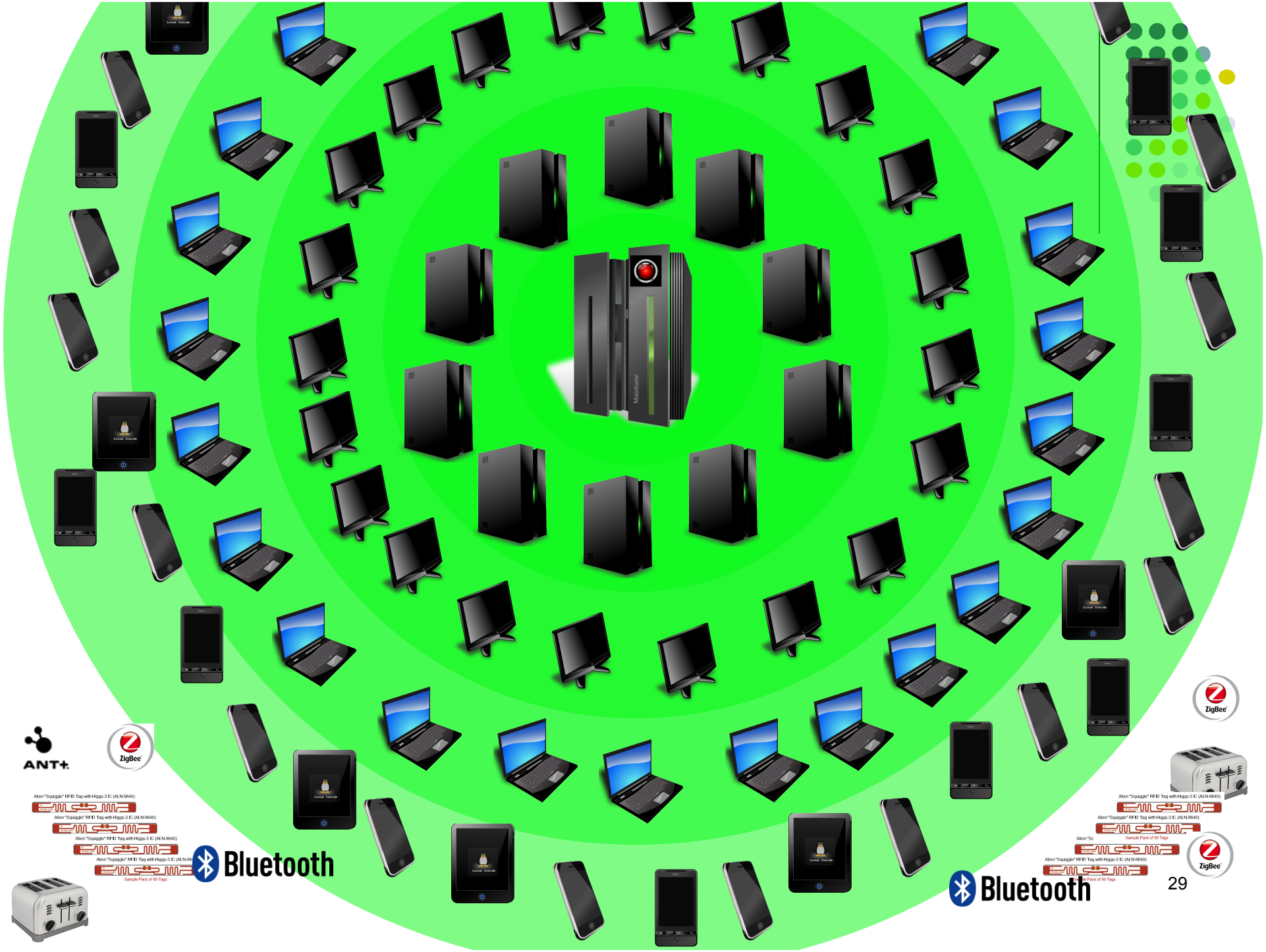


Source: Opte Project

MIT Technology Review,
Dec. 2005 – Jan. 2006

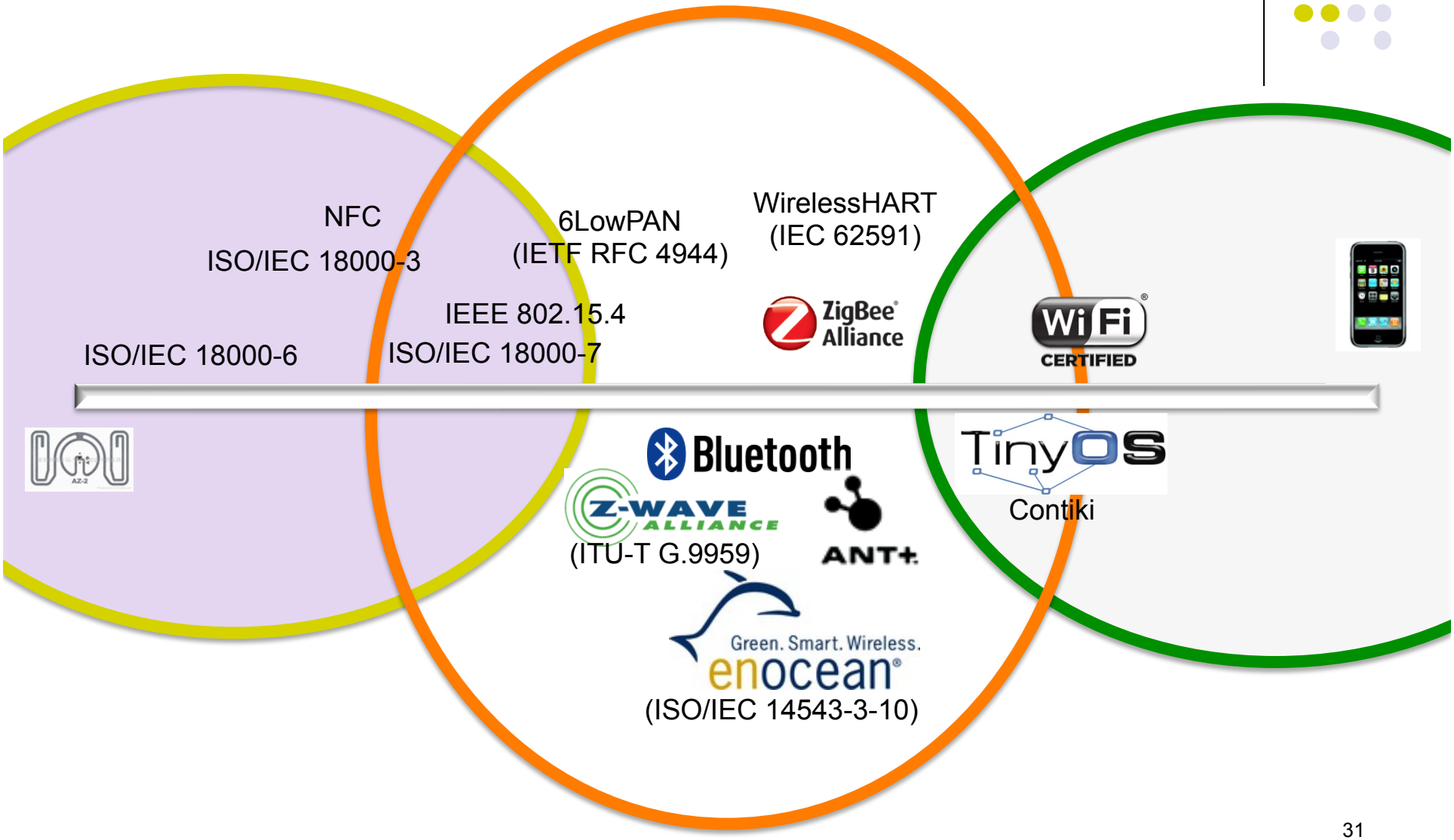
The Economist, April 28, 2007

What if tomorrow's wireless networks are even less secure than today's Internet ?


Mainframe
Linux Inside
ANT+
ZigBee
Bluetooth
Alien "Squiggle" RFID Tag with Higgs-3 IC (ALN-9640)
Sample Pack of 50 Tags

WHAT ARE THE TECHNOLOGIES OF THE INTERNET OF THINGS?

IoT Last Mile Technology Standards



Two Paradigms for IoT are Emerging

- **Brain-Body Merge** – intelligence is added to everyday things in your world, so that your life can be more awesome.
- **Head in the Clouds** – identification and wireless connectivity is added to everyday things in your world and intelligence is supported in the cloud, so that your life can be more awesome.

Brain-Body Merge

HRP-4C Robot

Head in the Clouds

Cloud Data Results in Big Data

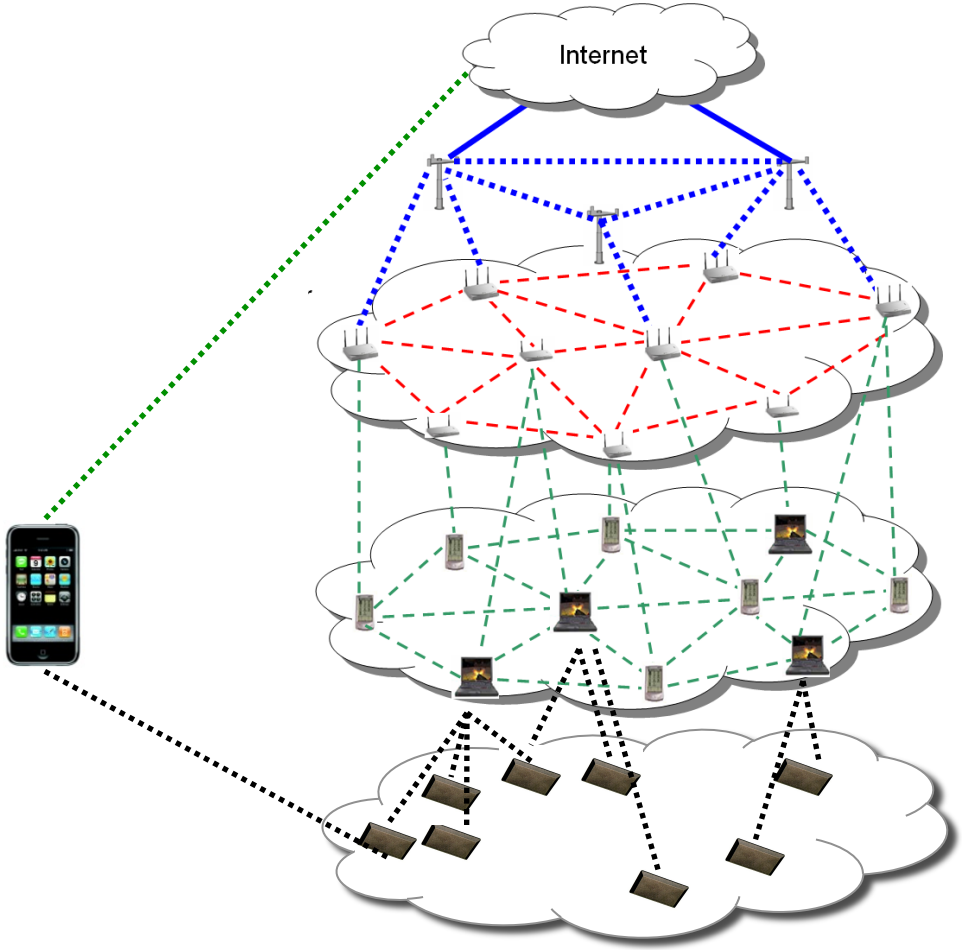
- Big Data – mining the Internet of Things for actionable information
- Trust
  - **do you trust the data you are collecting and/or using?**
  - **do you trust who is collecting the data from you?**

Creating Wisdom Easier When Data is Structured

- Cloud has 4000 Exabytes of data today
  - Stack of books from Earth to Pluto 80 times

- **Challenge** – APIs to find the needed data
- **Challenge** – APIs to move the data from where it is collected and/or stored to where it is consumed
- **Challenge** – Standard formatting of the data
  - John Doe vs Doe, John vs Doe, John H. vs Doe, John Henry

Smart Phone Goes Direct to Cloud

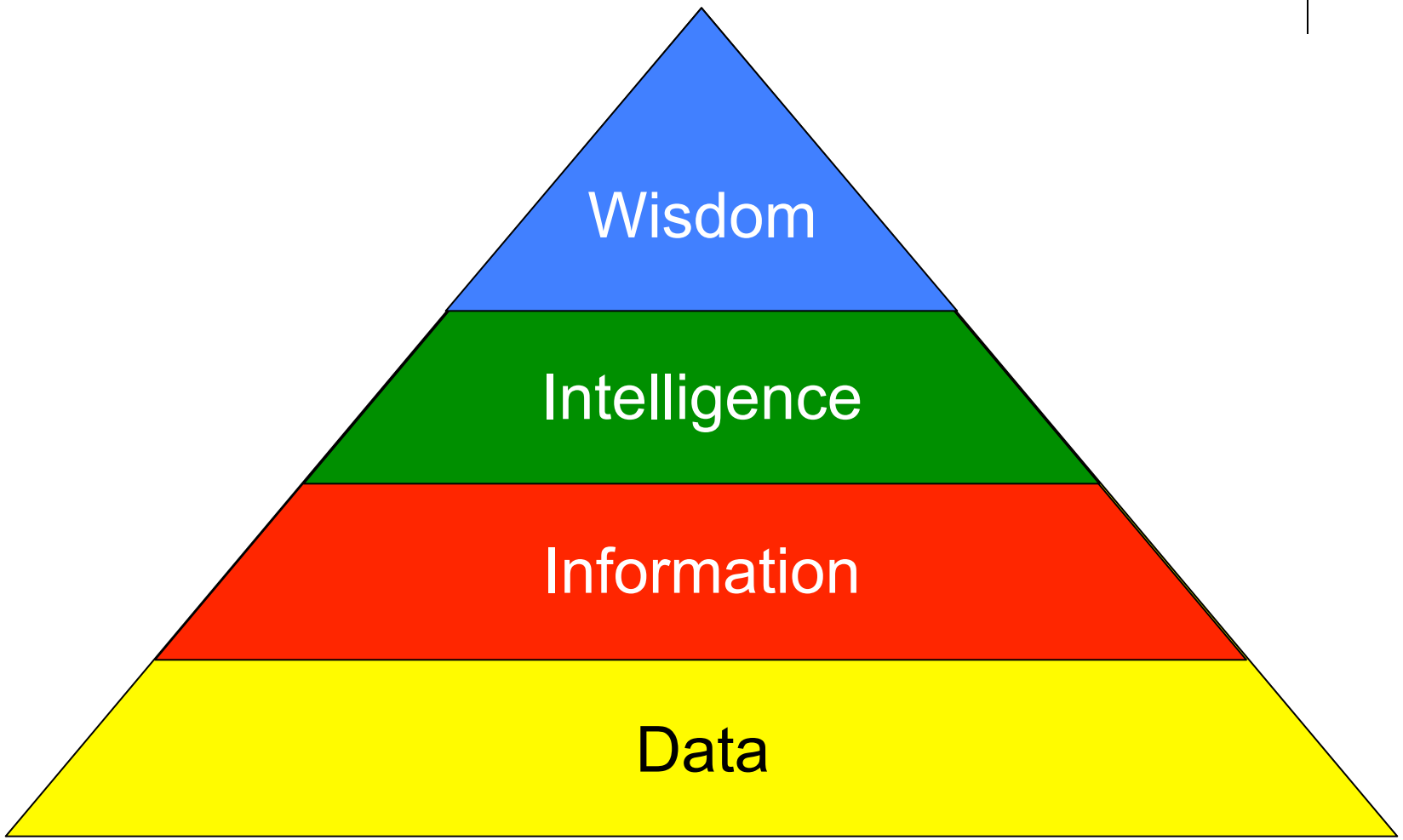


Collecting Data and Moving Data to the Cloud

- **Smart phone is the Tricorder** – allows us to interact with the world through the smart phone to learn all about whatever we point our phone at
  - Allows humans to connect with things and learn about things in a new way
  - All major communication protocols are being integrated into the smart phone
- 90% of earth surface has cell connectivity (not necessarily good, but possible)
- Thing – needs unique identity (IPv6*, EPC), ability to communicate (barcode or wireless or wired), senses (see, hear, smell, touch, talk plus identify)

*IPv6 poses a security problem

The Progression of Data



Humans Interact with the IoT

- Learn about things – using their smart phones
- Monitor things – data driven life
- Search for things – reality search
- Manage things – supply chain adoption of RFID is first step in this direction
- Control things – automation
- Play with things – www.layar.com (augmented reality – Layer is first to have augmented virtuality where virtual world is impacted by physical world around us)

Security is in the Future of IoT

- Future – each person will be surrounded by 3000 - 5000 smart things (source: Dragon Files)
- Weapon of mass destruction
  - Hacked – RFID, barcodes, smart meters, pacemakers, cars, SCADA, Cloud
- IoT will (and is) changing our lives

DEFINING SECURITY & PRIVACY

Types of Security

- Human/Societal
- Physical
- System
- Operational
- Data

Our Focus Today (Cyber Security)

www.kaltoons.com

Cartoon used without permission

Cartoon used without permission

Security

[Definition] Security – 1) **Freedom from risk or danger.** 2) Measures taken to guard against espionage, sabotage, crime, attack, escape, modification, duplication, or interception.

[Definition] Privacy – 1) The state of being free from unsanctioned intrusion. 2) **The right of an entity to decide when and on what terms its attributes should be revealed.**

Terminology

[definition] Policy – a definition of security

[definition] Mechanism – a measure that implements all or a portion of the policy

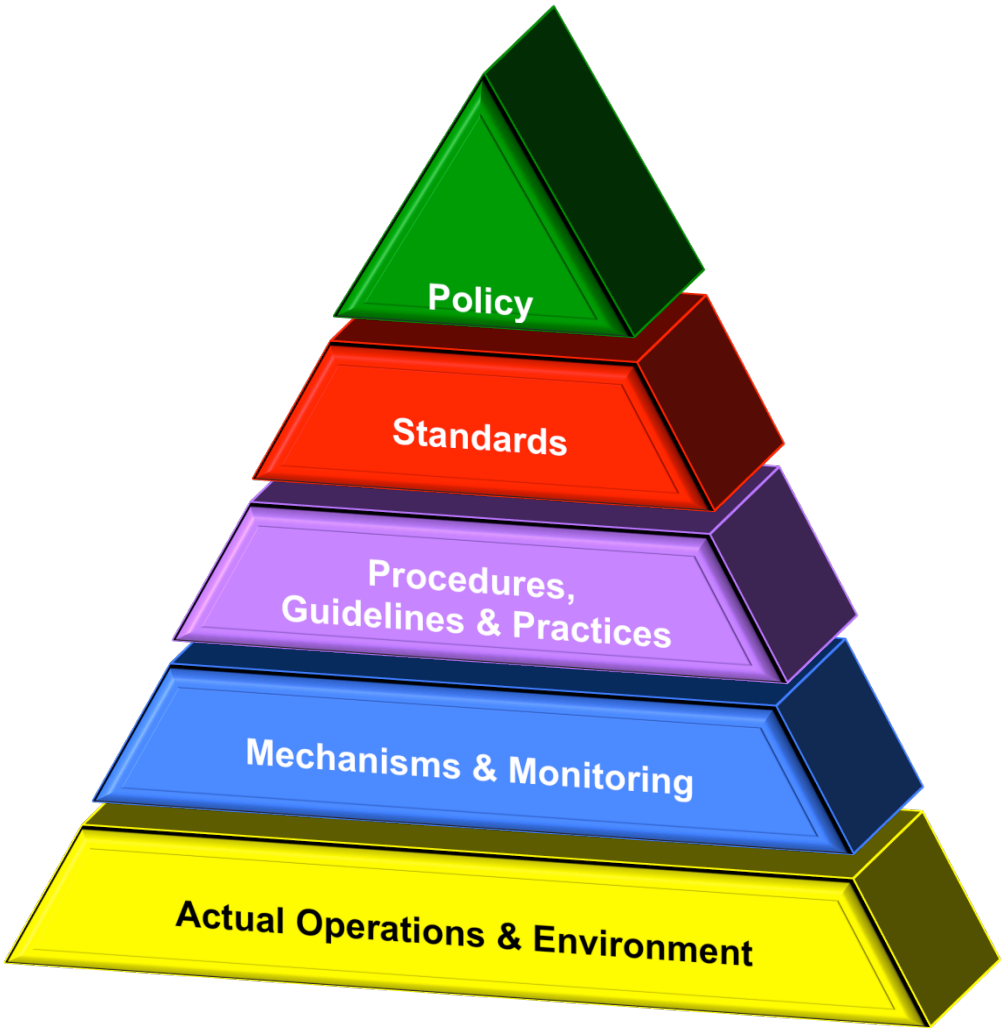
Terminology

[definition] Vulnerability – a weakness in the system security

[definition] Threat – a set of circumstances that has the potential to cause loss or harm, typically by exploiting a vulnerability

[definition] Attack – the exploitation or attempted exploitation of a threat

Security Policy Pyramid



IOT SYSTEMS TODAY ARE LACKING THAT BASIC SECURITY FEATURE

GOOD AFTERNOON MR. HENFENNEL! HEMORRHOID CREAM AISLE SIX!
BEEP!
TOO MUCH INFORMATION IN MY MEDICAL I.D. CHIP.
TOLES
10-6 © 2004 THE WASHINGTON POST
DON'T FORGET MOUTHWASH. I FIGURED THAT ONE OUT BY MYSELF. —

(Simple) IoT Data Attacks

Eavesdropping	• Listen to a conversation without the participants' knowledge or consent
Snooping	• Illicit reading of a device's identity and data
Tracking	• Determine where a specific device is currently
Tracing	• Determine where a specific device has been
Replay	• Repeat a recorded conversation
Counterfeit	• Create a duplicate device
Spoofing	• Masquerade as a tag, reader, or other device

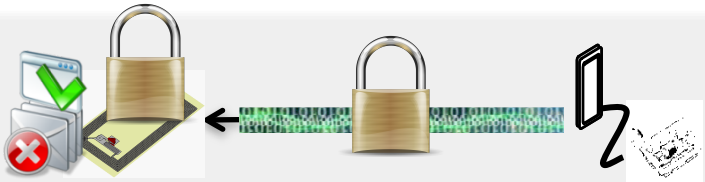
Some Security Mechanisms

Over the Air Encryption: over the air data and commands are encrypted with full data authentication (**secure communication channel**)

Device Authentication: validates devices as TRUSTED before data divulged or accepted. (**identity authentication**)

Secure Identification tags communicated identifier changes securely over time – identity never sent in the clear. (**secure identification**)

Cloaking enables device to determine whether it is SAFE to respond to a request or remain silent (**cloaking**)



Information Assurance authenticate data integrity and data origin. (**data authentication**)

Multiple Mechanisms Required

- No mechanism protects against all attacks.
- Complex systems often require multiple mechanisms to provide the security specified in the security policy.

Protection Provided by Mechanisms

Protection Provided by General Mechanisms Against Basic Attacks

	Over the Air Encryption	Identity Authentication	Secure Identification	Cloaking	Information Assurance
Eavesdropping	Good	None	Some	None	None
Snooping	Good	Good	Good	Good	None
Modification	Good	Good	Some	Some	Some
Tracking	None	None	Good	Some	None
Tracing	None	None	Good	Some	None
Replay	Good	Good	Good	Some	None
Counterfeit	Good	Good	Good	Good	Some
Spoofing	Good	Good	Good	Good	Some

*This table is a general guideline of the protection provided by each of the named general mechanisms. The general mechanisms defined here may be the combination of multiple fundamental mechanisms, e.g., under information assurance data integrity may be provided with SHA-256 and an X.509 certificate may provide data origin authentication (i.e., non-repudiation). The general mechanisms defined here may be implemented in multiple ways. For example, Identity Authentication may be implemented with a password. It may also be implemented with a symmetric key cipher. Mechanism usage and implementation determine the actual protection achieved with each of these general mechanisms.

Mechanism Implementation

- A general mechanism may be implemented in many different ways with **base mechanisms**.
- A base mechanism is a mechanism such as a password or symmetric key cipher that may be utilized to provide specific functionality, e.g., Tag Identity Authentication
- Each base mechanism has its **own security level**.
- Ensure that the chosen base mechanism provides the minimum security level required in the policy.

Protection Provided by Identity Authentication Mechanisms

Protection Provided by Identity Authentication Mechanisms in Doing Tag Authentication

	Password	Symmetric Key Cipher	Asymmetric Cipher
Eavesdropping	None	None	None
Snooping	Good	Good	Good
Modification	Good	Good	Good
Tracking	None	None	None
Tracing	None	None	None
Replay	None	Good	Good
Counterfeit*	Some	Good	Good
Spoofing*	Some	Good	Good

*A password must be sent in the clear from an Interrogator to a Tag. Any password sent and overheard by an Attacker (Eavesdropping) may be Replayed, Counterfeited, and Spoofed. Any conversations utilizing a symmetric key cipher or an asymmetric cipher that are captured by an Attacker (Eavesdropping) may be replayed; however, the authentication protocols for these ciphers utilize a random number generated by the Interrogator and the Tag so that each identity authentication communication sequence is unique (or with an expected repetition cycle that is sufficiently long). This protects them against Replay, Counterfeit, and Spoofing attacks.

Levels of Security

I.	No Security	The tag is not protected from cyber threats and can be read, written, and locked by anyone with understanding of the protocol.
II.	16-bit Security	The tag is protected through a 16-bit random secret. A brute force air interface guessing attack reveals the secret in two hours.
III.	32-bit Security	The tag is protected through a 32-bit random secret. A brute force air interface guessing attack will expose the secret in two weeks.
IV.	64-bit Security	The tag is protected through a 64-bit random secret. A brute force air interface guessing attack will expose the secret in 64 billion years.
V.	80-bit Security	The tag is protected through a 80-bit random secret or equivalent cipher strength, e.g., RSA with a 1024-bit key.
VI.	128-bit Security	The tag is protected through a 128-bit random secret or equivalent cipher strength.
VII.	Best Security	The tag is stored in a secure bank vault and cannot be read from the outside world. It is very secure, yet also unusable.

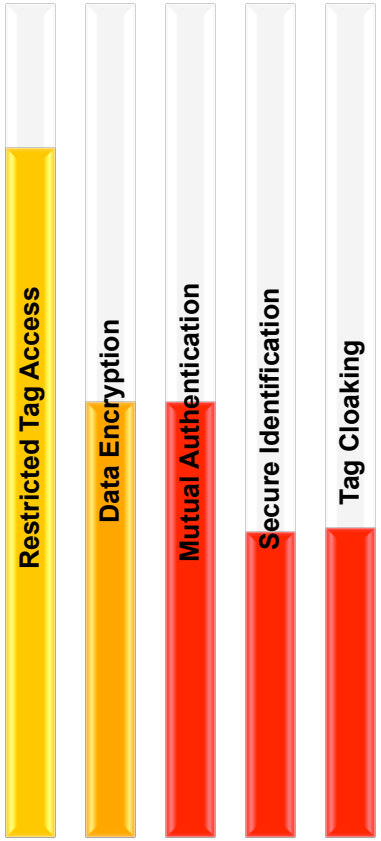
*Air interface times are expected times assuming EPCglobal Gen2 air interface is the only mechanism that an attacker may use with an unauthorized reader attempting to guess the secret. The limiting factor here is the time required for communication over the air interface. Other attack scenarios may have significantly shorter expected times to compromise the secret. Operational vulnerabilities may degrade the security level, for example by sending a password over an unencrypted channel the password is compromised by an eavesdropper.

59

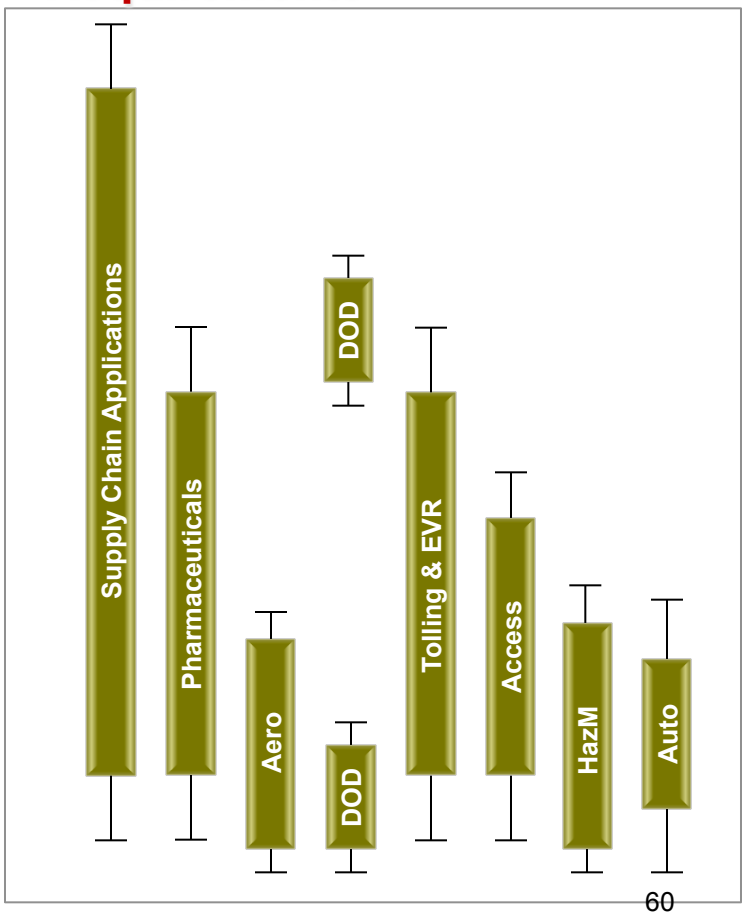
Recommended Levels of Security

Security Level	
I.	No Security
II.	16-bit Security
III.	32-bit Security
IV.	64-bit Security
V.	80-bit Security
VI.	128-bit Security
VII.	Best Security

Mechanisms



Application Security Requirements



Networks Change Everything

- **Metcalf's Law**: The value of a network grows as the square of the number of devices on that network.

- The benefit of a device is amplified by data network connectivity
  - services may be provided that the device alone could not provide.

The IoT Edge is Networked

- The IoT edge device is
  - Networked (often wireless)
    - Full-time connectivity
    - Occasional connectivity
  - Resource constrained
    - Power
    - Computation
    - Size
  - Typically mobile

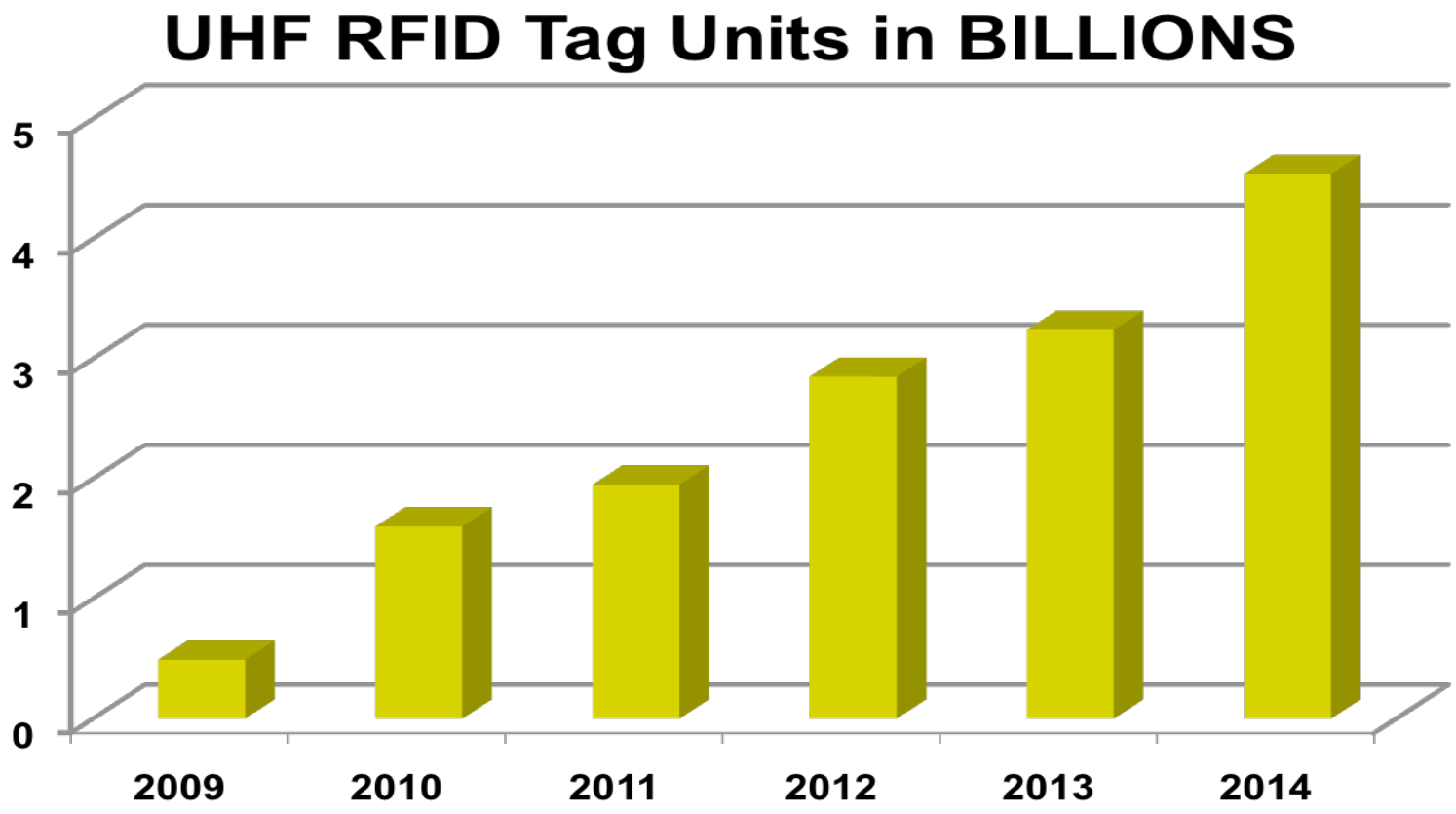
No Device is an Island

- Every networked device is an entry point into your network (DATA ATTACKS!)
- No device is to be fully trusted by any other
- Every device is a city state to be protected

Security Must be Designed into Every Device and the Network From the Beginning and From the Lowest Layers on Up

A CLOSER LOOK AT PASSIVE UHF RFID SYSTEMS

Today: Passive UHF Market is Growing 35% Year-on-Year



Source: VDC Research Group

Number of Tags Shipped

Passive UHF (millions)

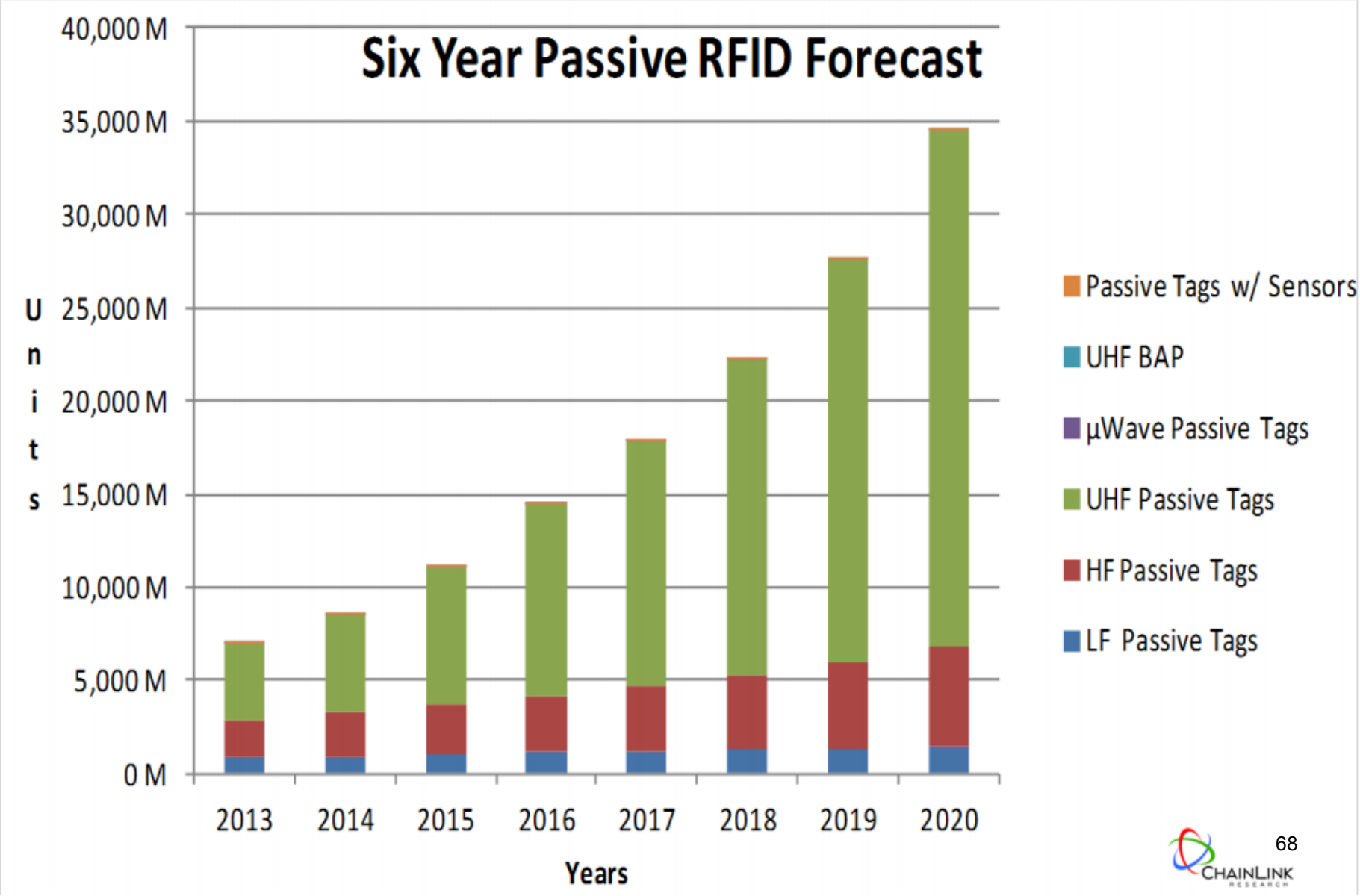
Application	2012	2013
Retail apparel, shoes	1675	2250
Retail items other	20	25
Logistics, roll cages conveyances	100	125
Asset management/ inventory	400	500
Medical/health care	15	18
Air baggage and cargo	70	72
Access Control/ticketing	1.2	1.5
Embedded	0.1	0.1
People	20	22
Other	50	65
Total	**2351.3**	**3078.6**

9.9 billion UHF RFID tags sold thru 2013

Our industry has enabled 9.9 billion connections to everyday items, which roughly equals the number of Ethernet connections to the Internet today

Data Courtesy IDTechEx

Future = Sustained growth



Item Tagging is the Driver

Medical Inventory

Laundry Management

Operational Configuration

Brand Protection

Retail Inventory

Customer Service

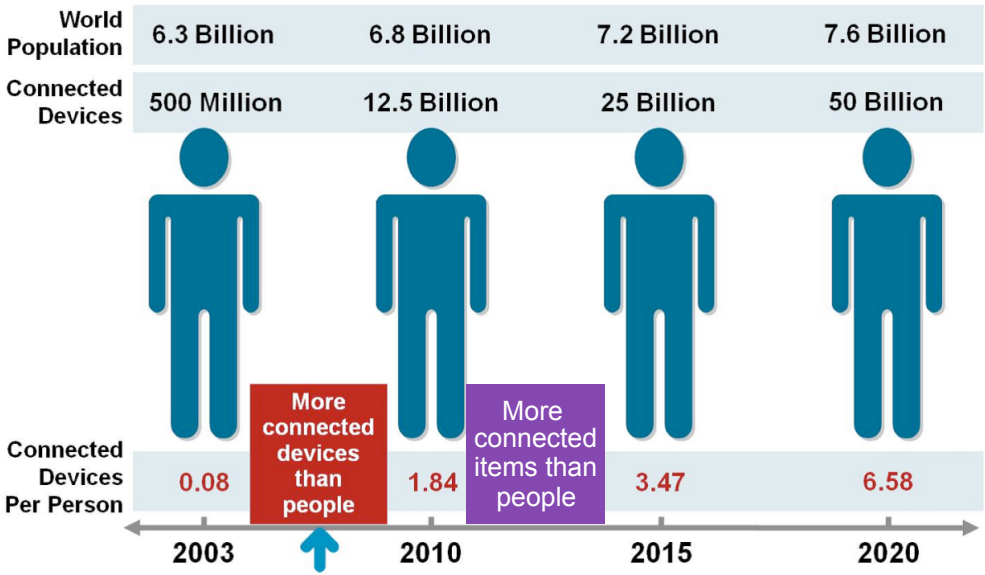
Race Timing

Asset Management

Logistics/Security

Consumer Applications are Next

RAIN = Billions of consumers × trillions of tags

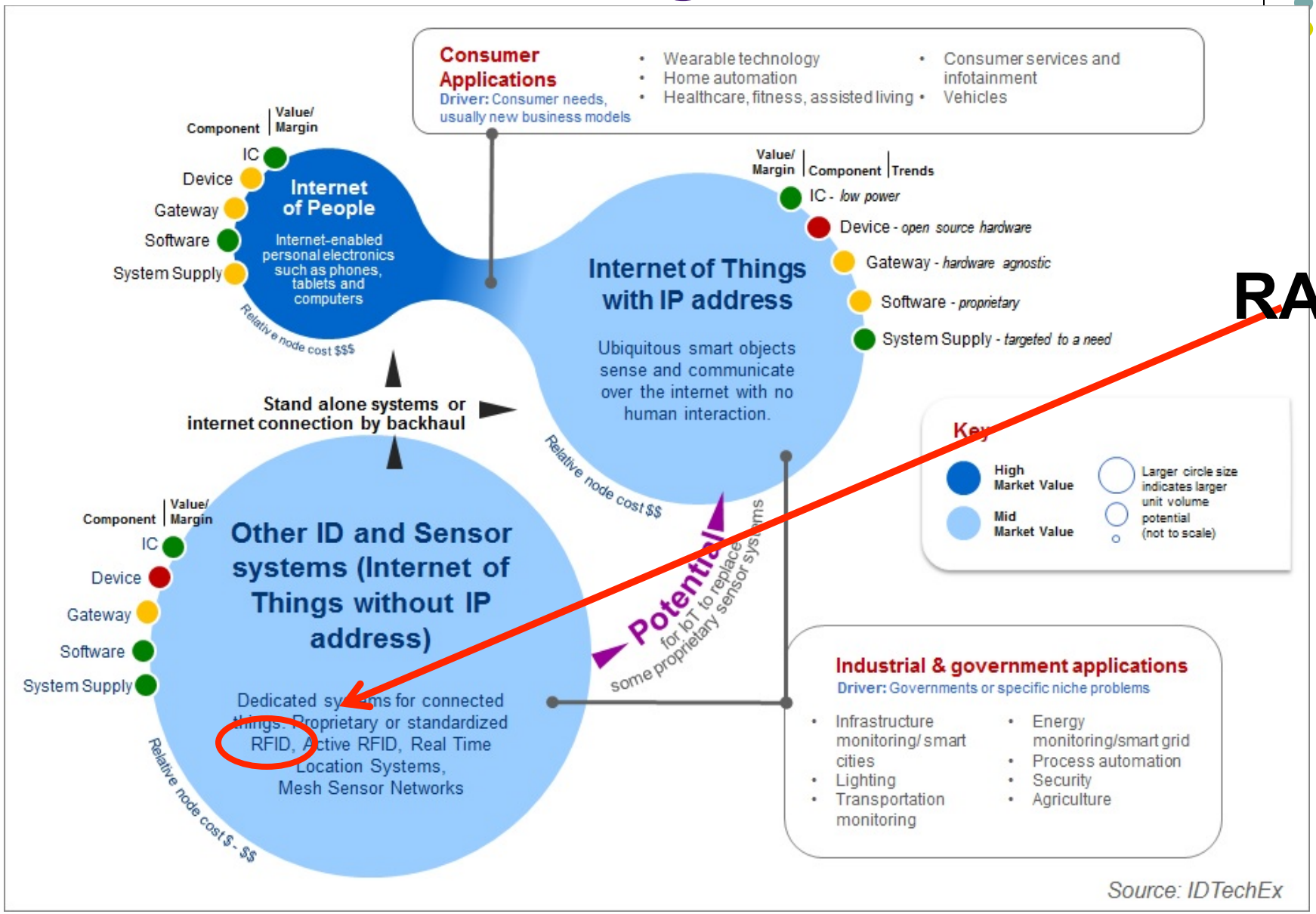


Source: Intel (2012)

RAIN™ RFID

http://www.RAINRFID.org

Internet of Things



RAIN

Potentially Trillions of Tag Reads per Day with basically zero security on the tags

(This is the definition of BIG DATA!)

Big Data can violate your privacy without any one piece of data violating your privacy.

Connecting bits and atoms using RFID promises to create Huge Data.

GEN2 SECURITY FRAMEWORK

Gen2/ISO 18000-63 Standards

Gen2 Today	Definition
Select	Select a population of tags
Inventory	Inventory selected tags; get their EPCs
Access	Read/write/lock tag memory; kill the tag
V2 Enhancements	**Definition**
Anticounterfeiting	Authenticate a tag as genuine
Security	Modify tag information securely
File Management	Create files and assign access privileges
Data Hiding	Hide tag data to protect consumer privacy
Loss Prevention	Use a tag for EAS

In Gen2 V1.2.0

New in Gen2 V2.0.0

Security Framework

- Security framework defined to enable a set of cryptographically secure functionality.
- Requirements loosely defined by end users (mostly retailers).
- Basic Framework Functionality:
  - Tag Authentication
  - Interrogator Authentication
  - Authenticated Communication Channel
  - Encrypted Communication Channel
  - In-field Key Modification

Security Framework Commands

- **Challenge** – Broadcast command. Wrapper for "Message" sent to CryptoSuite for Authentication
- **Authenticate** – Singulated command. Wrapper for "Message" sent to CryptoSuite for Authentication
- **SecureComm** – Singulated command. Wrapper for encrypted (maybe authenticated) standard command.
- **AuthComm** – Singulated command. Wrapper for authenticated standard command.
- **KeyUpdate** – Singulated command. Change key.

Security Framework Tag Response (Delayed Response)

- **Delayed Response** – (Optional – Reader selected) Tags do not have to meet T1 timing
- **ReadBuffer** – Singulated command. Read the result from a security command

Additional Functionality

- "Untraceable" command – Allows portions of UID and other memory to be hidden
  - Does not prevent traceability, simply hides memory
  - Susceptible to "constellation attacks"
  - Interrogators will have difficulty with more than one "Untraceable" tag in the field (eg reports one tag when more than one tag has same UID)
  - Requires secondary channel to identify tag to determine correct key (or password) to use
- File Management – Allows for a standardized file structure to exist within User Memory
  - Access control can be performed on a per-file basis
  - Allows simple separation of data based upon files

ISO Status

Proposal Stage	Preparatory Stage	Committee Stage	Enquiry Stage	Approval Stage	Publication Stage
18000-63 v2		First CD			
29167-10 (AES-CBC)				First DIS	
29167-11 (PRESENT-80)					First FDIS
29167-12 (ECC)				First DIS	
29167-13 (Grain-128A)				First DIS	
29167-14 (AES-OFB)				First DIS	
29167-15 (XOR)		First CD*			
29167-16 (ECDSA+ECDH)				First DIS	
29167-17 (CryptoGPS)				First DIS	
29167-19 (Ramon+AES)		First CD			

29167 Crypto Protocols

	Security Services Provided					Authentication commands Supported	
	TA	IA	MA	AM	SM	A	C
29167-10 (AES-CBC)	✚	✖	✖	✖	✖	✚	▭
29167-11 (PRESENT-80)	✚	✖	✖	✖	✖	▭	✚
29167-12 (ECC)	✚	✖	✖	✖	✖	✚	✚
29167-13 (Grain-128A)	✚	▭	✚	✚	▭	✚	✚
29167-14 (AES-OFB)	✚	▭	✚	✖	✚	✚	▭
29167-15 (XOR)	✚	✚	✚	✖	▭	✚	✖
Target is 18000-4 mode 3 Active Tag							
29167-17 (CryptoGPS)	✚	✖	✖	✖	✖	✚	▭
29167-19 (Ramon+AES)	✚	✖	✚	✖	✚	✚	✖

✚ Supported Service

▭ Optional Service

✖ Not Supported

TA = Tag Authentication
IA = Interrogator Authentication
MA = Mutual Authentication
AM = Authenticated Messaging
SM = Secure Messaging
A = Authenticate Command
C = Challenge Command

Gen2 Identification

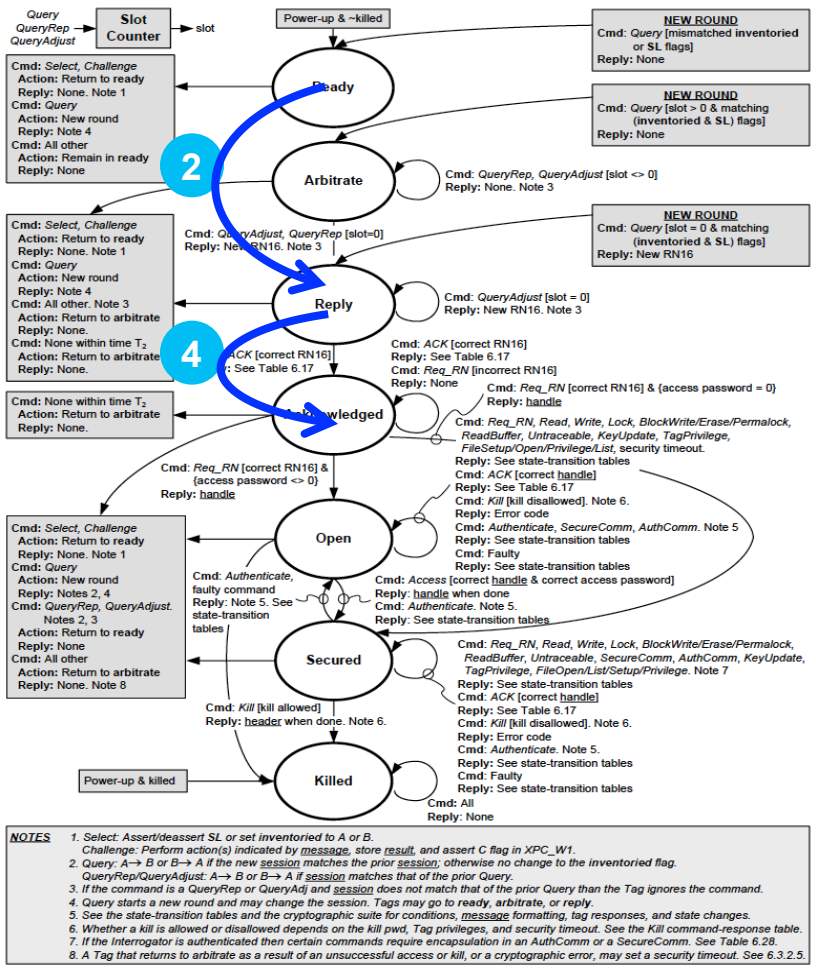
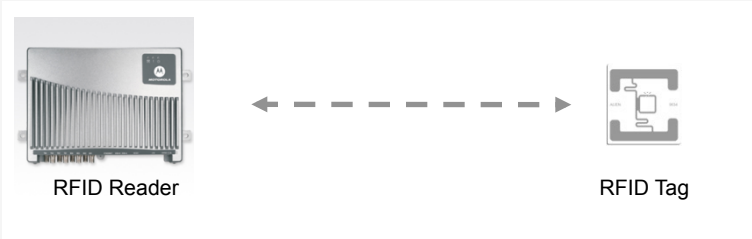


Figure 6.21: Tag state diagram

Standard EPC Gen 2 Protocol



1 Select →

2 Query →

← RN16 3

4 ACK →

← EPCID (PC || EPC || CRC) 5

AES OFB Mode

- AES OFB (Output Feedback) mode generates a key stream (O1, O2, O3, …) based upon the AES cipher.
- Initialization Vector (IV) is a 128-bit number

$O1 = E_K(IV)$

$O2 = E_K(O1)$

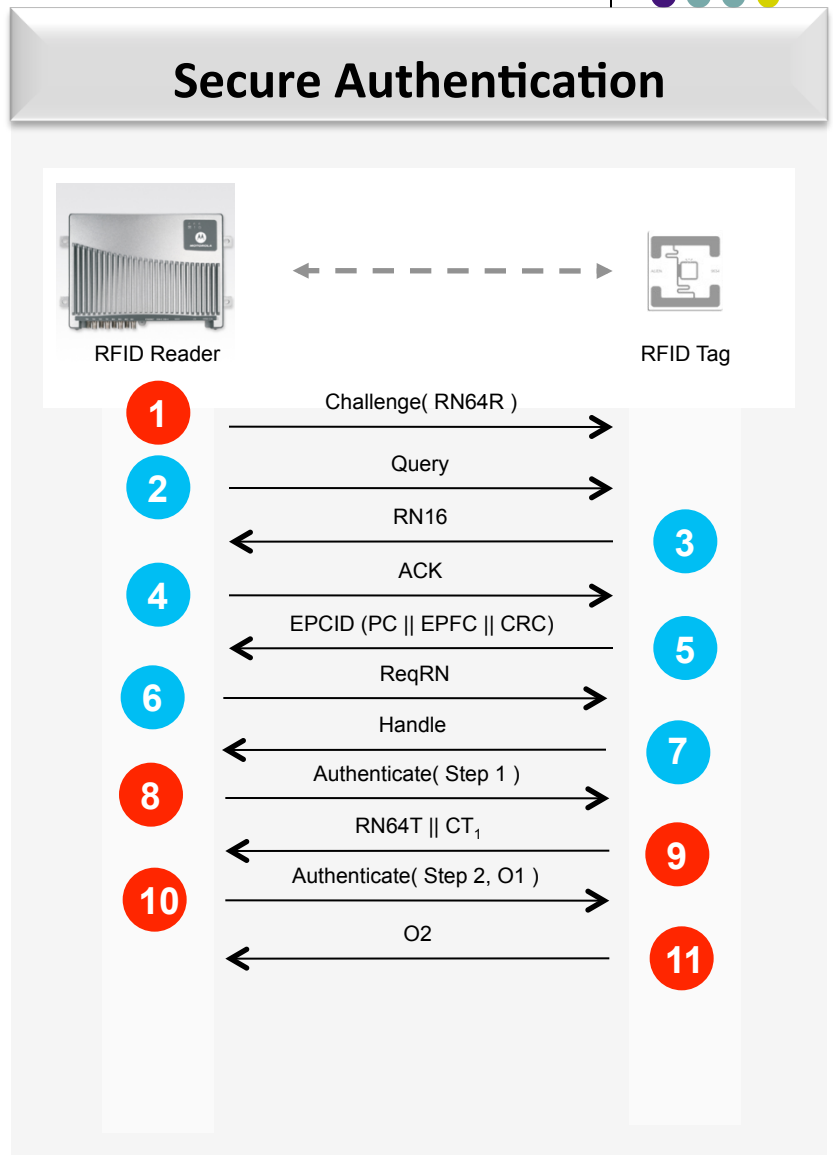
Etc.

CT1 = PT1 XOR O1

CT2 = PT2 XOR O2

Gen2 AES OFB Mutual Authentication

- Challenge
  - Reader sends RN64R
  - Tag generates RN64T
  - Tag computes O1 = E_K(RN64T)
  - Tag computes O2 = E_K(O1)
  - Tag computes CT1 = O1$^{(bits\ 127\text{-}64)}$ XOR RN64R
- Authenticate(Tag Auth)
  - Tag returns RN64T || CT1
- Authenticate(Rdr Auth)
  - Reader sends O1$^{(bits\ 63\text{-}0)}$
  - Tag sends O2



Gen2 Identification

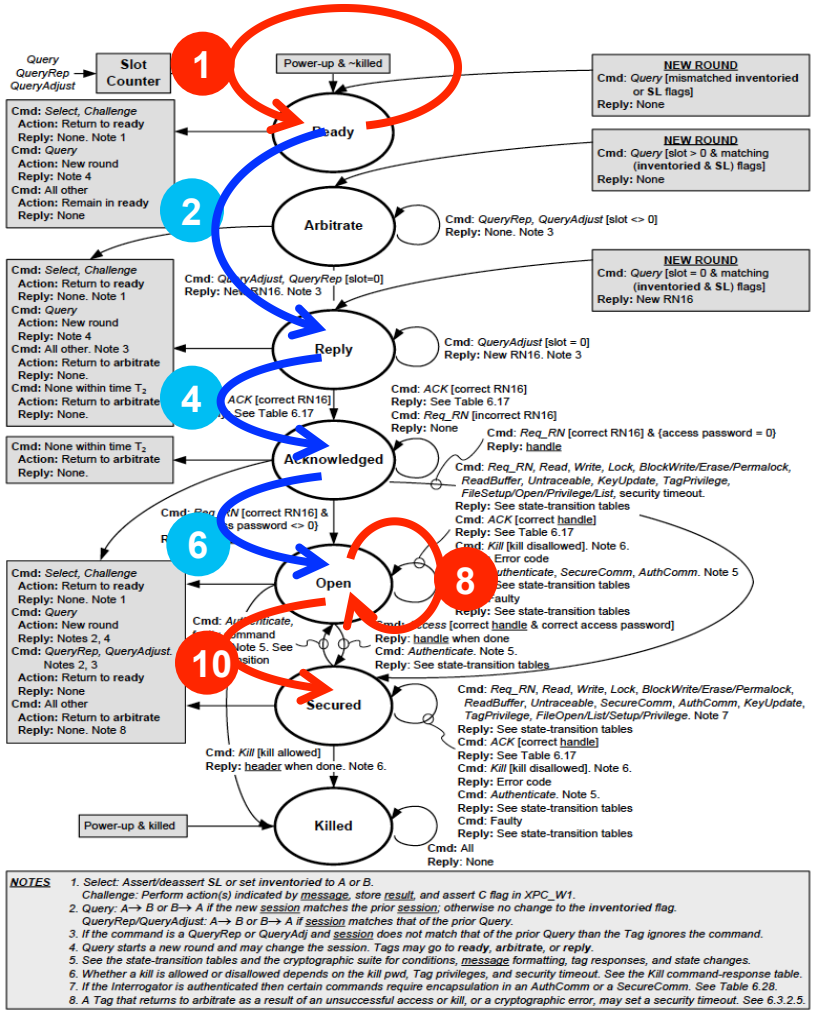
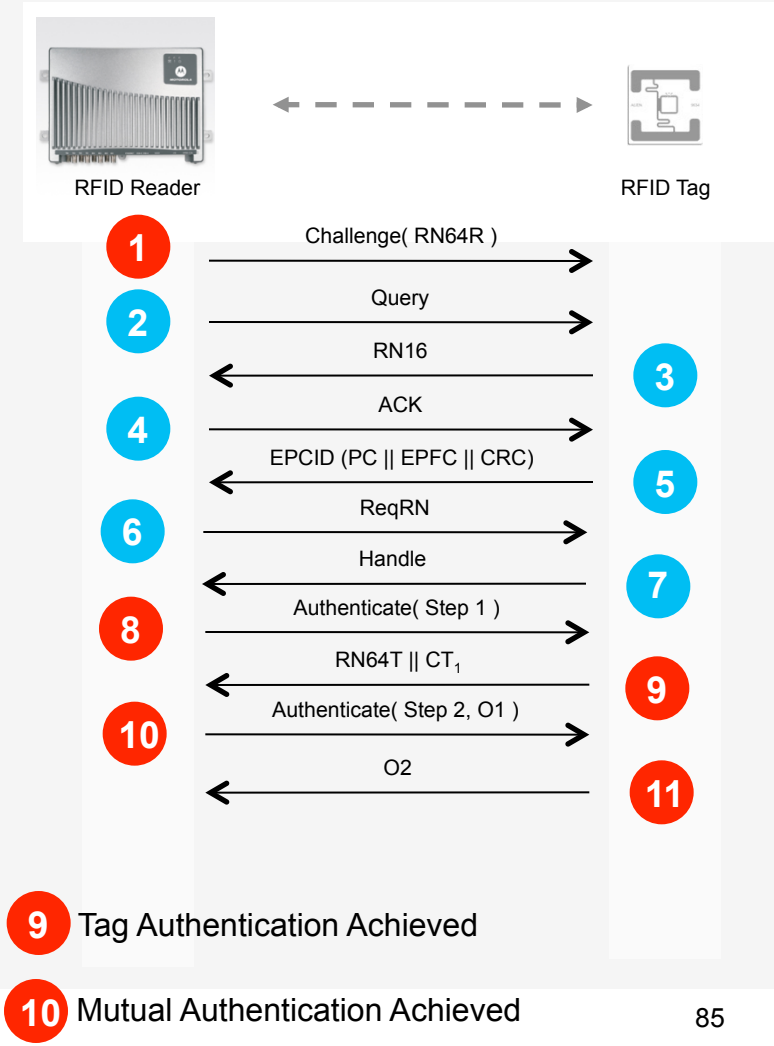


Figure 6.21: Tag state diagram

Secure Authentication



FINAL THOUGHTS

Grand Research Challenge:
Prevent the ubiquitous Internet of Things from becoming a ubiquitous nightmare.

Final Thoughts

- IoT systems already pervade our lives with minimal security
- As we become dependent upon them, particularly for automation, IoT systems must have security built in from the ground up
- IoT devices must utilize physical security mechanisms **and** data security mechanisms
- The adoption of IoT changes everything (again)

The End of a Very Brief Beginning

Daniel W. Engels, PhD

dwe@smu.edu

Lawson
First pants,
THEN
your shoes