



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

Security and Privacy Grand Challenges for the Internet of Things

PRESENTER: GLENN A. FINK

CONTRIBUTORS: DIMITRI V. ZARZHITSKY, THOMAS E. CARROLL, AND ETHAN D. FARQUHAR

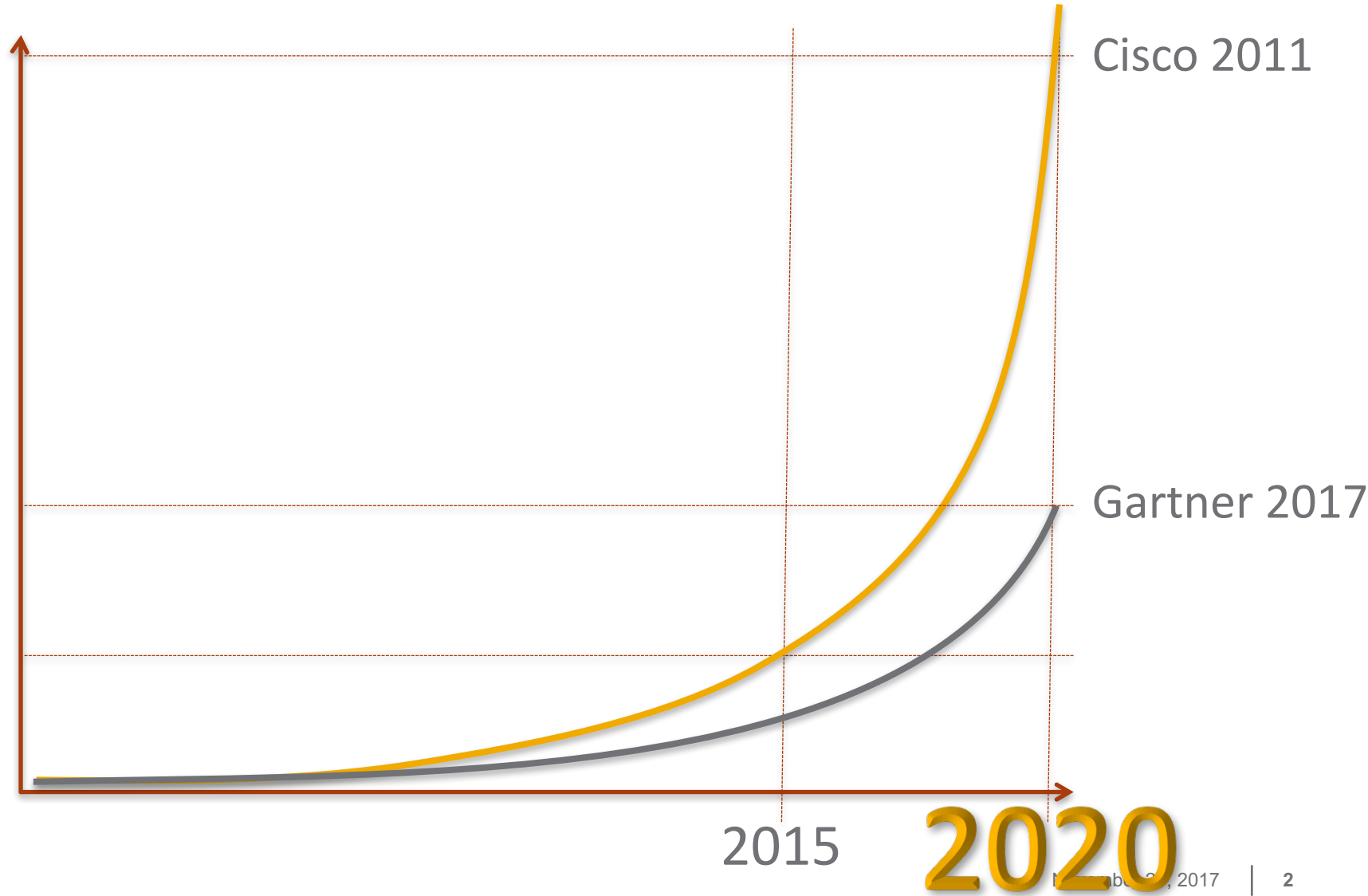
National Security Directorate
Pacific Northwest National Laboratory

Cyber-Awareness Month, October 2017

50 billion

20 billion

10 billion

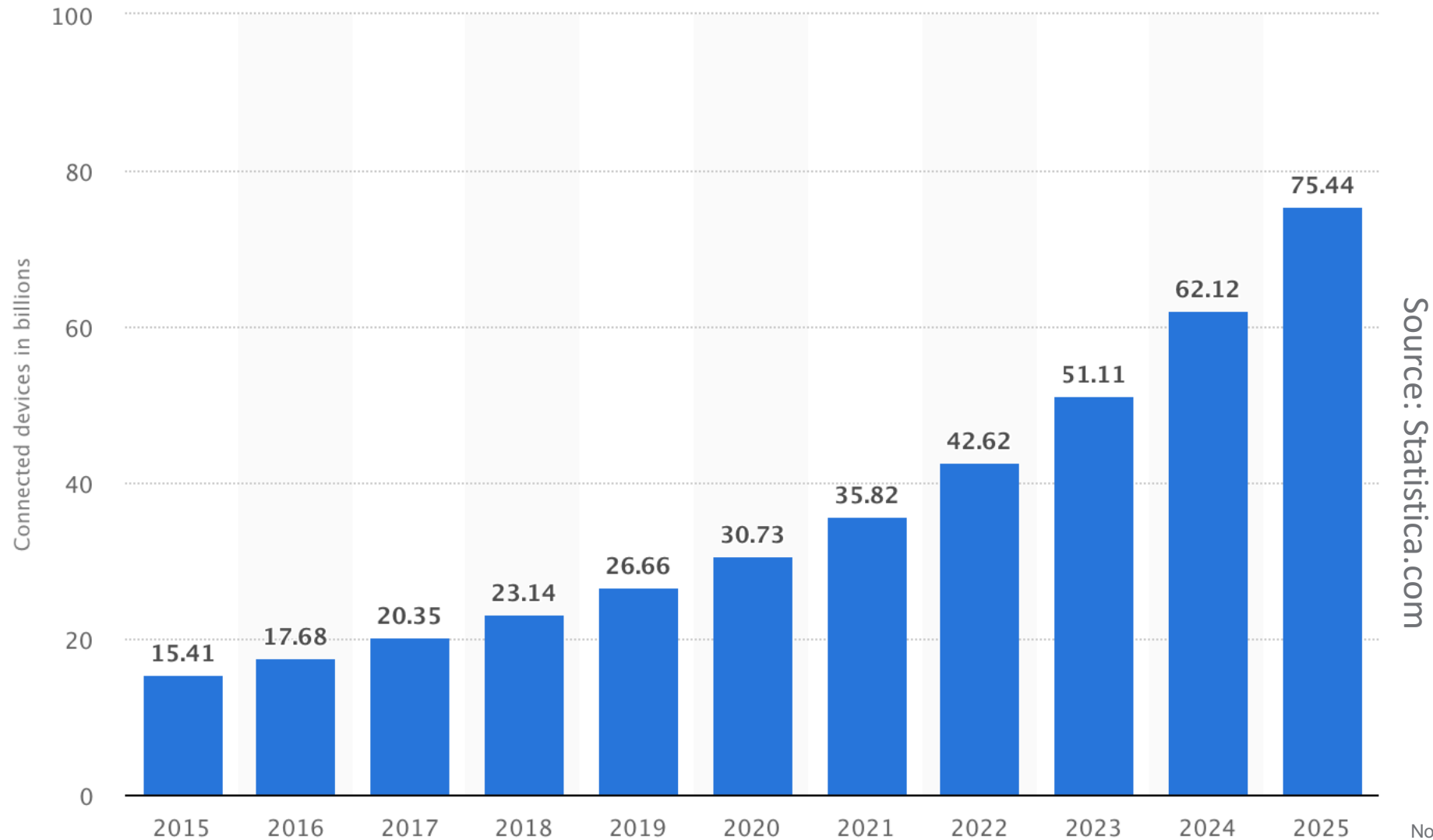


Connected devices installed base worldwide from 2015 to 2025 (in billions)



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

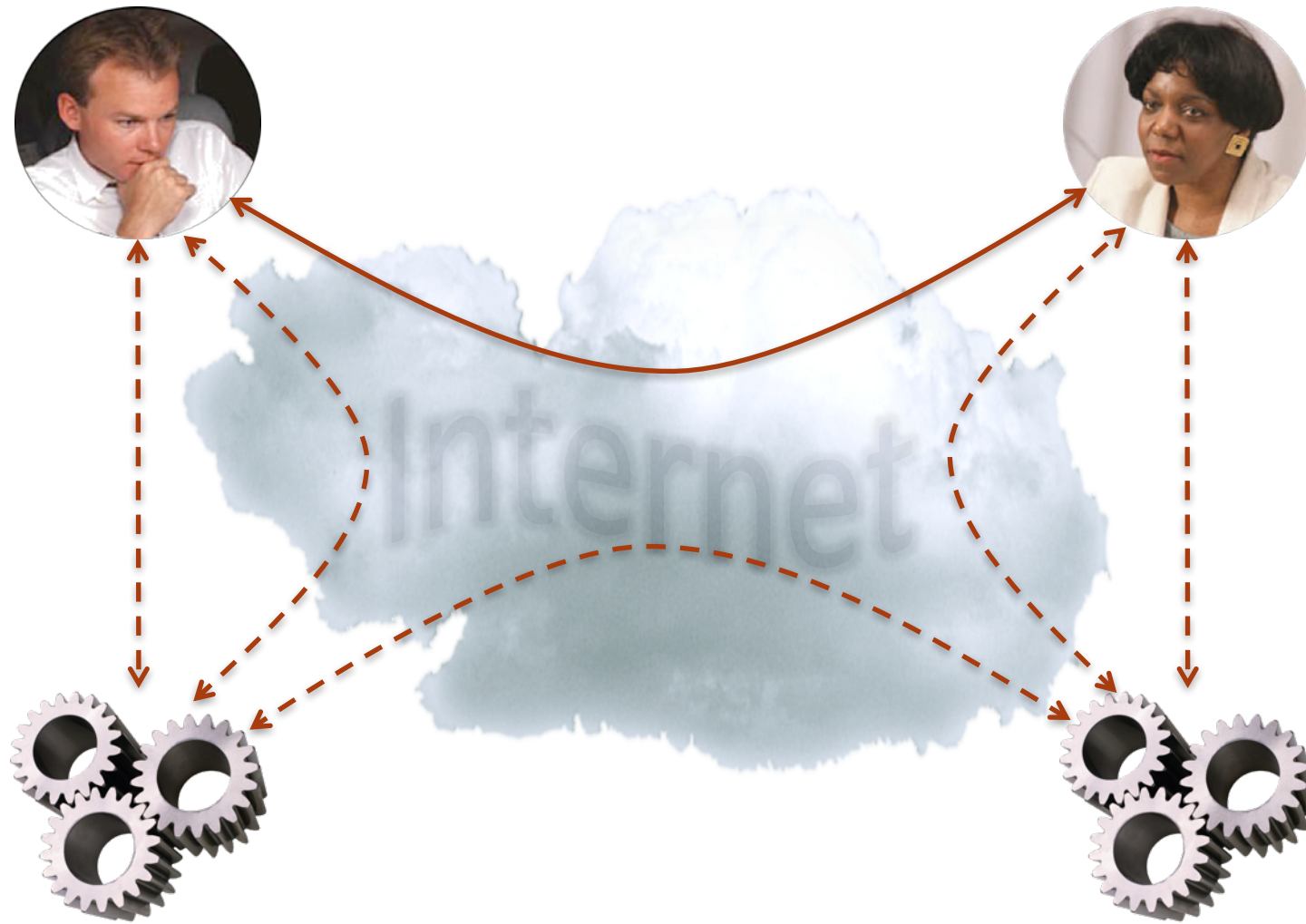


IoT takes people out of the loop



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965





Messages we (unintentionally) send



I buy clothes at
Neimann
Markups



You make my
pulse rate and
blood pressure
increase



Would you like to
download my
contacts via
Bluetooth?



Messages we (unintentionally) send



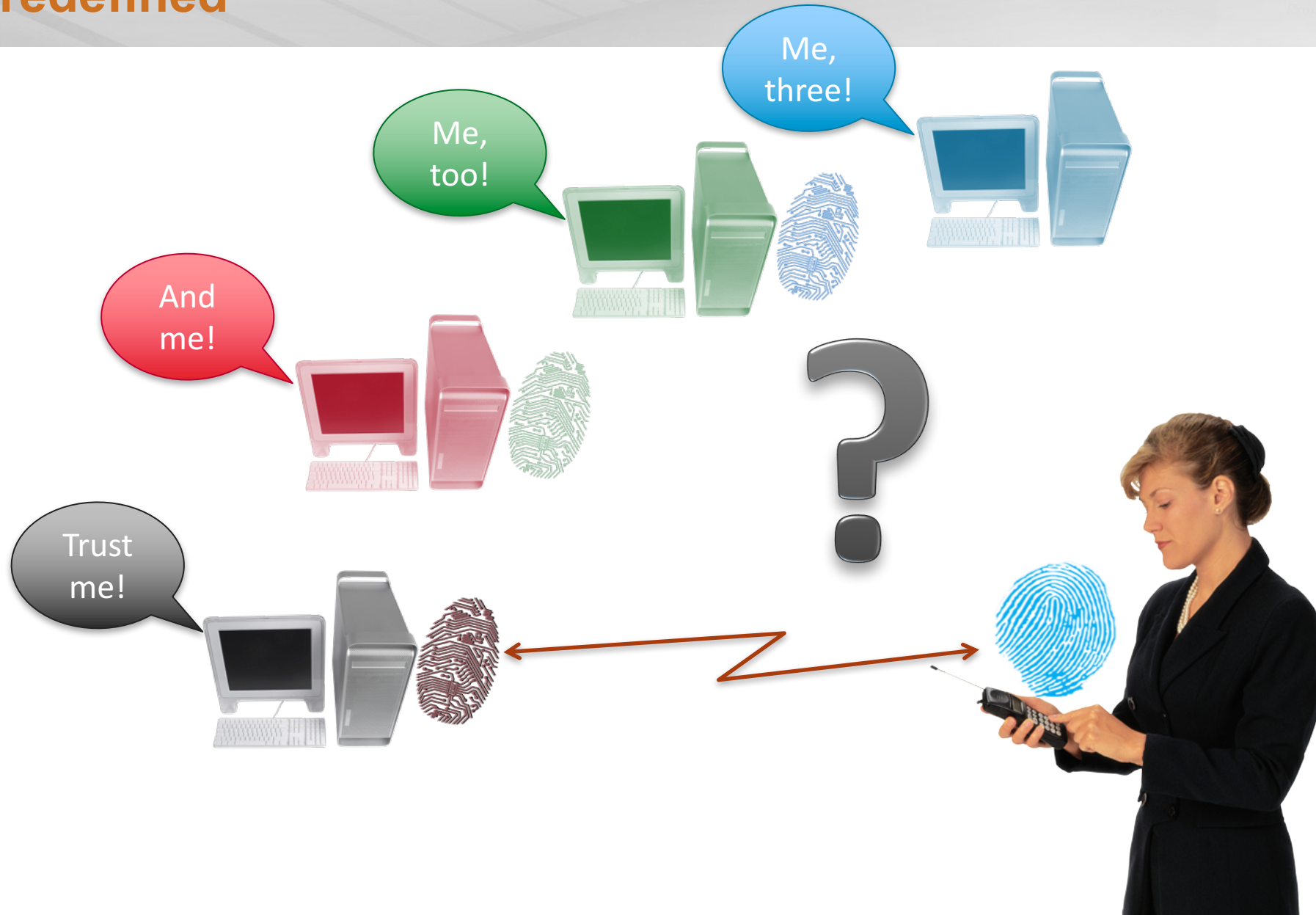
WHEN VISITING A NEW HOUSE, IT'S GOOD TO CHECK WHETHER THEY HAVE AN ALWAYS-ON DEVICE TRANSMITTING YOUR CONVERSATIONS SOMEWHERE.

Identity redefined



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965





More devices worsens identity confusion



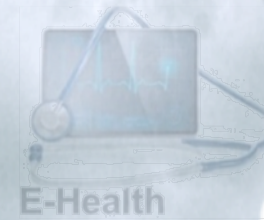
Automotive



Mobile Computing



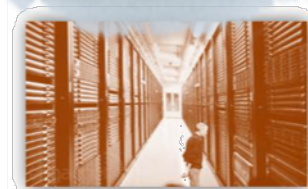
Consumer



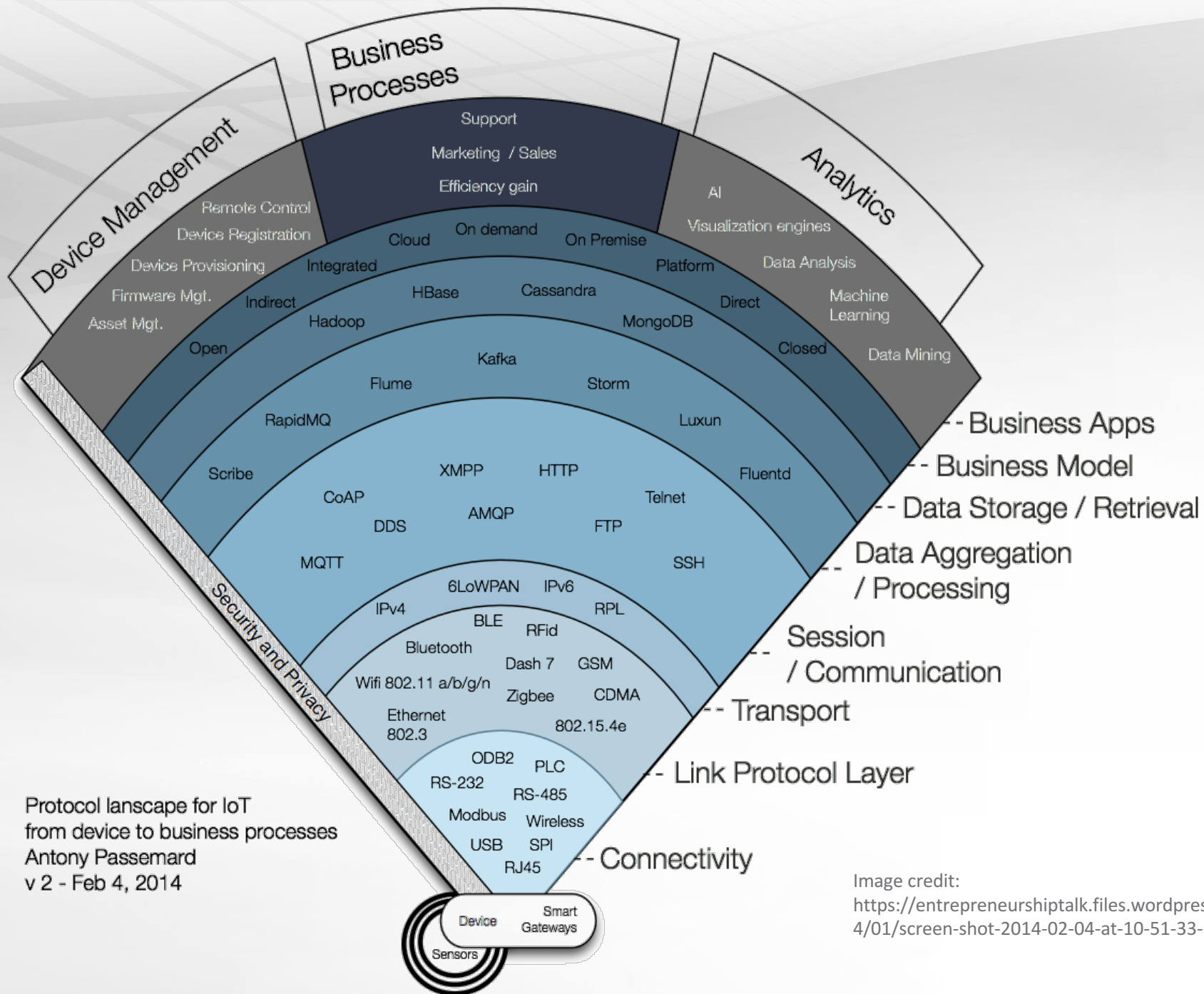
E-Health



Industrial



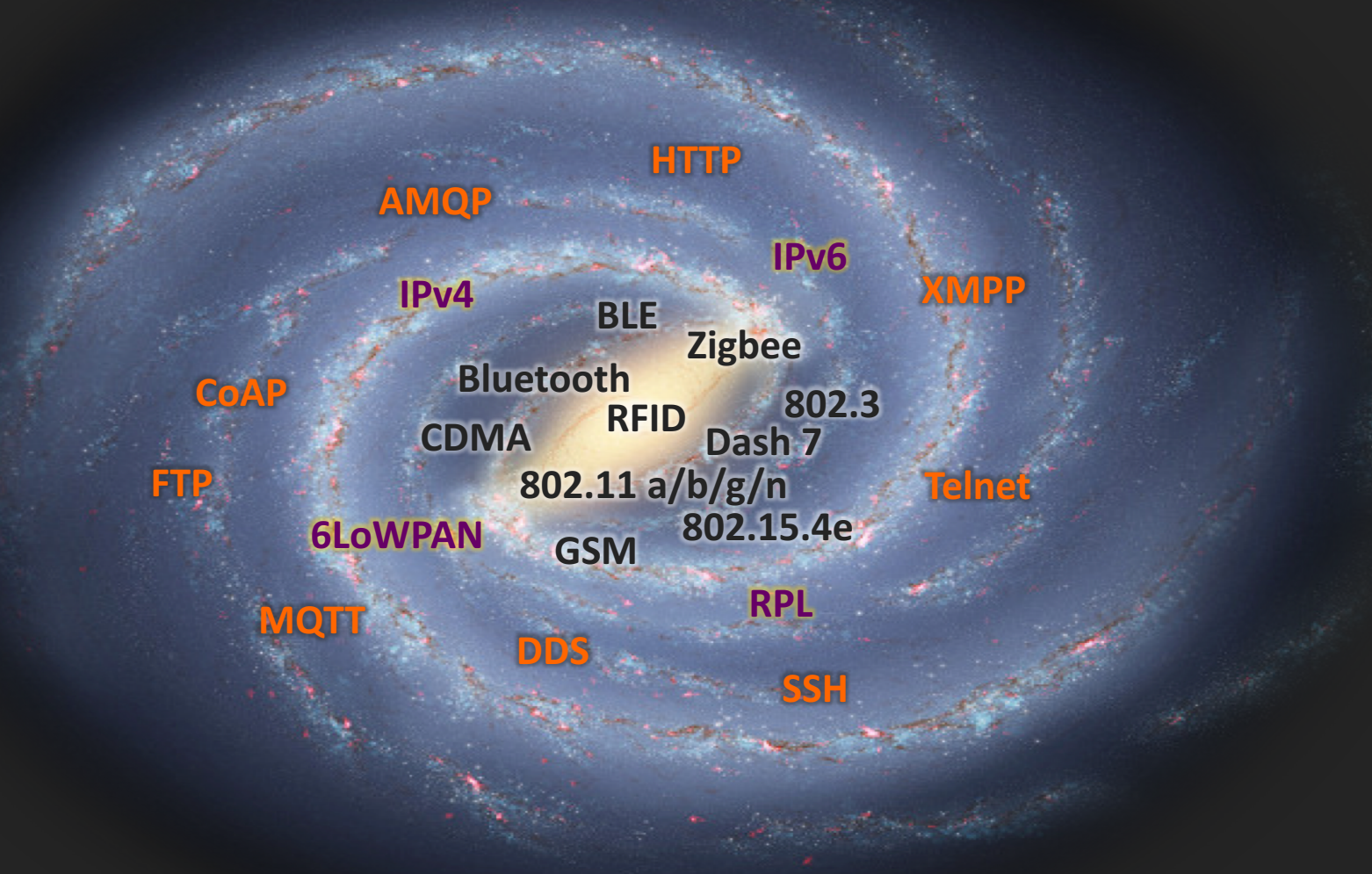
Communications



Protocol landscape for IoT from device to business processes
Antony Passemard
v 2 - Feb 4, 2014

Image credit:
<https://entrepreneurshiptalk.files.wordpress.com/2014/01/screen-shot-2014-02-04-at-10-51-33-am.png>

A galaxy of semi-interoperable microprotocol implementations...





Consider: Are these two TCP state diagrams compatible?

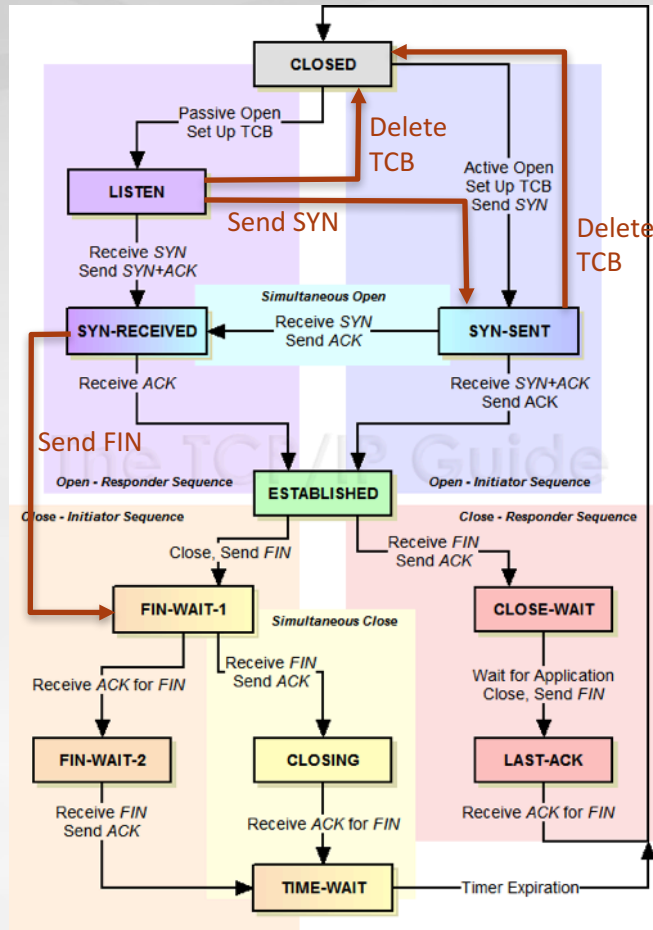


Image credit: <https://www.tcpiptide.com>

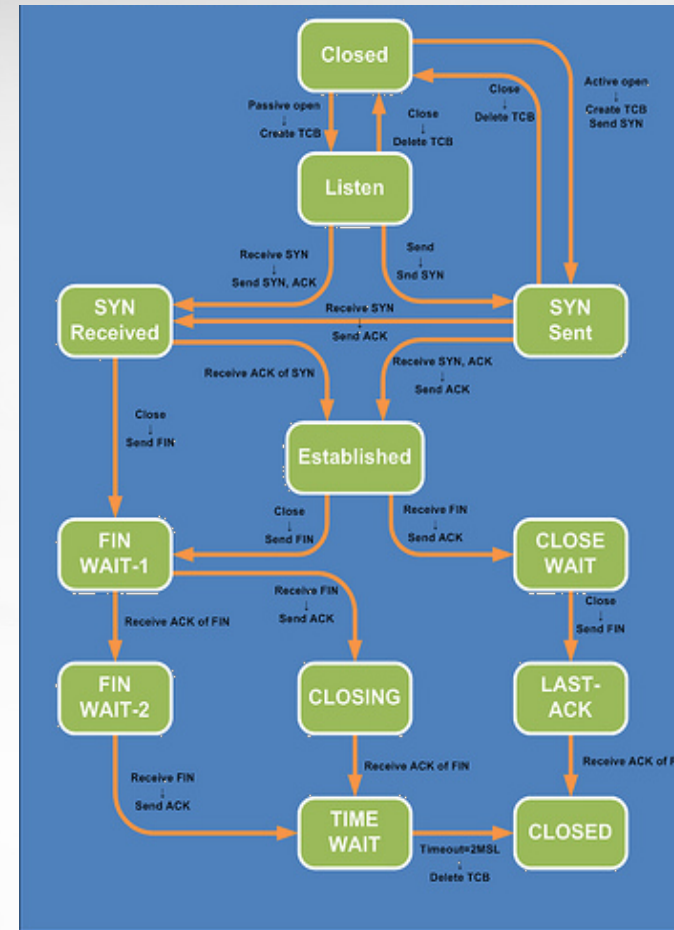
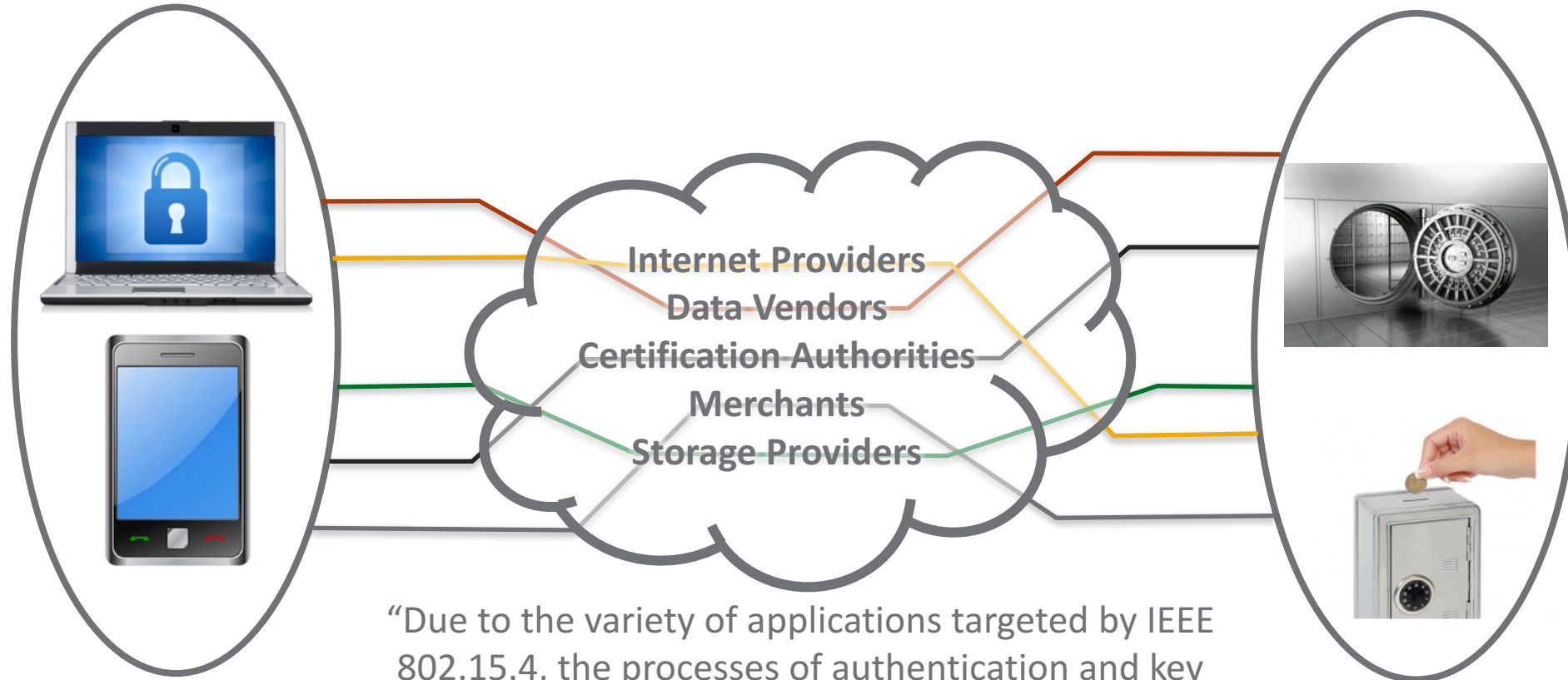


Image credit: <https://bluehawk.monmouth.edu>

Security varied and optional



“Due to the variety of applications targeted by IEEE 802.15.4, the processes of authentication and key exchange are *not defined in the standard.*”
6LoWPAN Security Analysis (emphasis mine)



Security varied and optional

“In response to cost and power consumption considerations, these devices will typically implement the minimum set of features necessary.” RFC 7428



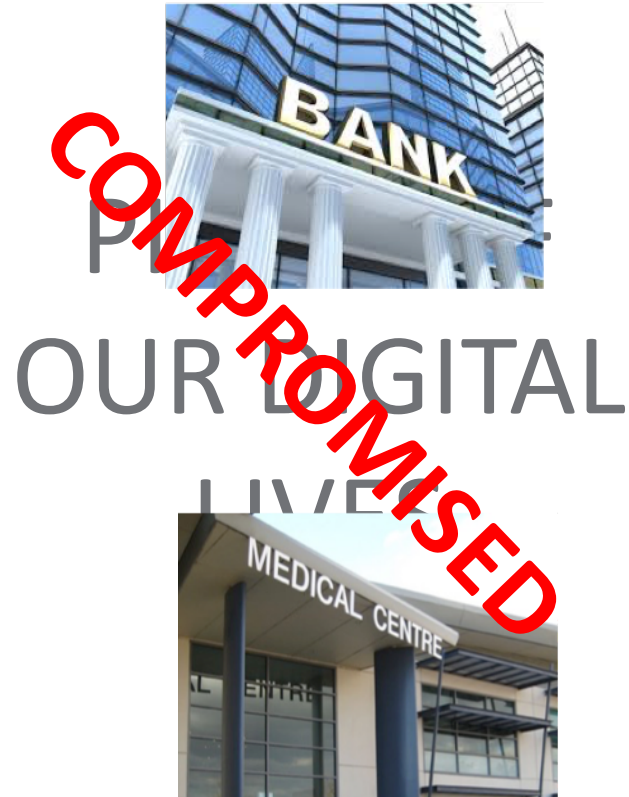
(in)Security: Who chooses which level of security to implement?



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

Our lives have become a digital patchwork of products and services





Privacy: A social landscape

Drones



CCTV



Geo-location



Entertainment



Phones



Smart Home



Wearables



Security: Cyber crime: Money



Security: Cyber crime: Property



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965



Jeep hack by Miller and Valasek, 2015



Tuxedo Touch home security authentication vulnerability, 2015



Vulnerabilities in the AmosConnect communication shipboard platform, 2017



Unsecured security cameras with default passwords, ongoing

PACKAGES
COSTS
INTEGRATION
FRAUD
CYBER

SECURITY
PROTECTION
DEFENSE

SCAMS
RACE
SYSTEMS
REPLACING
ALTERING
LD
DRUG

Security: Medical Devices



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965



Health
**Thousands of 'd
devices exposed**
Hackers make 55,416 log

ge over

g+
in 34
attack that hijacks nearby
patients who rely on them.

A Heart D
By **BARNABY J. FEDER**
Published: March 12, 2008
To the long list of obje
add the human heart.
The threat seems lar
researchers plans to
wireless access to a

- FDA's concerns about cybersecurity vulnerabilities include:
- Malware infections on medical devices themselves
 - Infections of computers, smartphones, and tablets used to access patient data
 - Unsecured or uncontrolled distribution of device keys or passwords
 - Unavailability of security software updates and patches to medical devices

art monitors through
0 COMMENTS
in 0

Security
Hackers could turn your smart meter into a bomb and blow your family to smithereens – new claim
And before that, pwn your IoT gadgets via power supply gear
By Darren Pauli 4 Jan 2017 at 08:03

WIRED
LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM
MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

Business.ca
Technology meets business
Internet of Things lead to the
Catherine Acza
Published

Could Hacking Your Fridge, Car, and Printer Really Be a Thing? Examining IoT for 2017
by ANDREI TIBURCA — 8 months ago

ars TECHNICA
BIZ & IT —
Billions of devices imperiled by new clickless Bluetooth attack
By Catalin Cimpanu

HackRead
exploit works against unpatched devices running Android, Linux, or Windows.
2/2017, 6:00 AM

Dolphins inspire ultrasonic attack that pwn smartphones, cars and assistants

Vulnerable Smartphones, IoT Devices: 400% increase in infection rate

Report: AI, IoT Security Threats Will Be Internet's Future
By Rhea Kelly | 09/20/17

THE WALL STREET JOURNAL.
Latest Weapon: Cyber Extortion

'Fear-ly' Innocent: Kids' Voice Recordings Leaked in Creepy IoT Teddy Hack

TechRepublic.
SECURITY

Researchers use \$5 speaker to tap smartphones, automobiles
Cybersecurity researchers from the University of Michigan backdoor access into systems.

Hackers can gain access to maritime ship data through a built-in backdoor
The proliferation of insecure devices in every facet of our lives will have consequences far beyond the digital realm

Cyber attack could sink cruise ships, Government advice warns
16 Sep 2017, 9:15pm



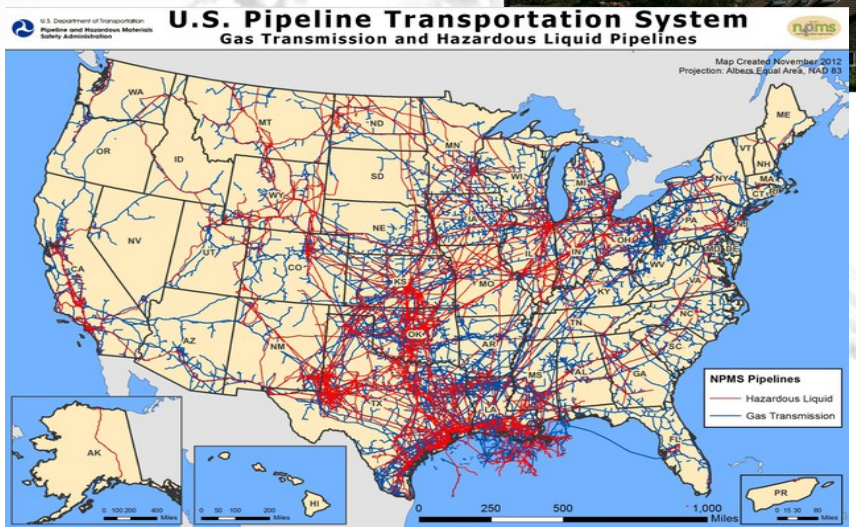
Pacific Northwest NATIONAL LABORATORY
Created by Battelle Since 1965

Security: Cyber warfare



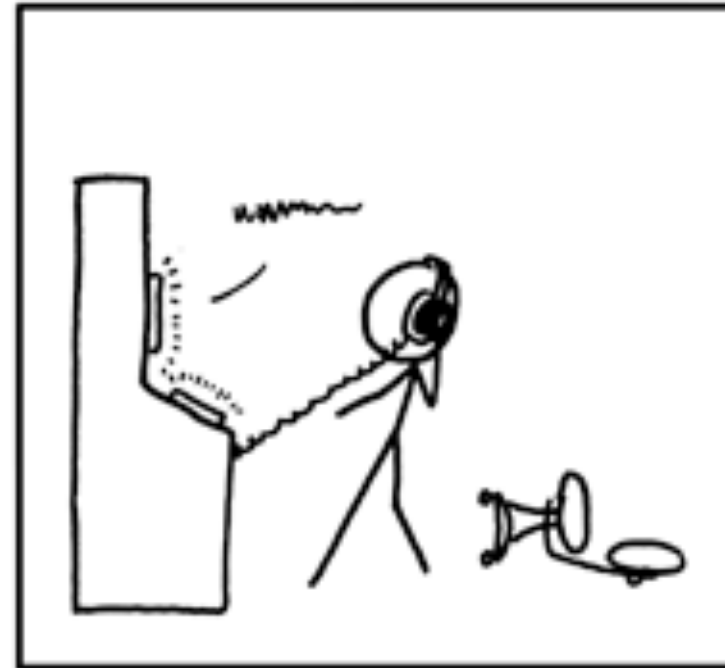
Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965



So what do we do now?

NOW AND THEN, I ANNOUNCE "I KNOW YOU'RE LISTENING" TO EMPTY ROOMS.



IF I'M WRONG, NO ONE KNOWS.
AND IF I'M RIGHT, MAYBE I JUST FREAKED
THE HELL OUT OF SOME SECRET ORGANIZATION.

<https://xkcd.com/525/>

Research Challenges: Scientific and Technical



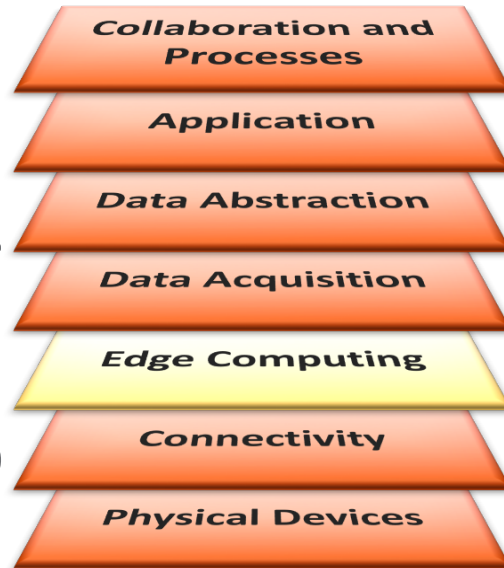
Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

Bandwidth



Edge analytics

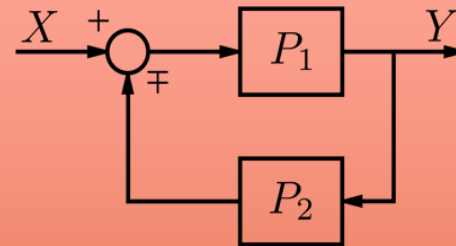


Identity vs. Anonymity vs. Pseudonymity

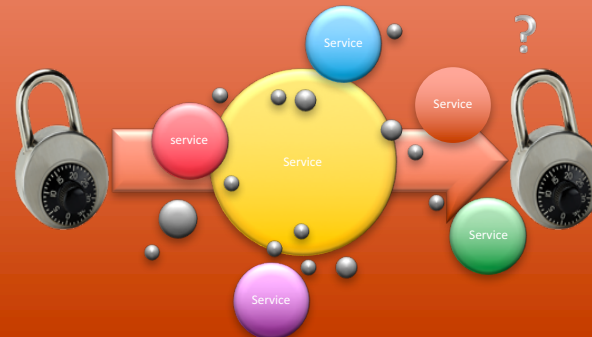


New mathematics:

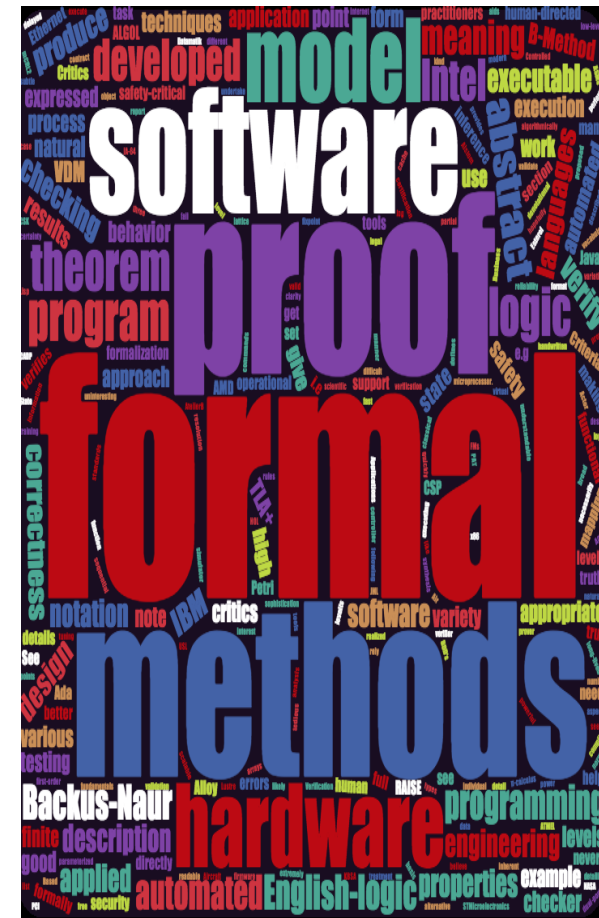
Closed-form security and privacy expressions



Composition of services



Formal methods:



Research Challenges: Social and Legal



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965



- Who owns it?
- Who can access it and for how long?
- Data sovereignty
- Right to be forgotten



- Advanced Digital Rights management
- Reward security/privacy enhancing behaviors
- Gamification of security and privacy



- Theory: protocol stacks that enforce “laws” of data management
- Standards: crucial for “Future proofing” operations
- Must adapt to innovation trends and ensure interoperability
- Must be consolidated



Conclusion:
Which would you prefer to build?



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965



Which would you prefer to be remembered for?



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

Thank you!



GLENN.FINK@PNNL.GOV

Pacific Northwest National Laboratory





Some quotes

- ▶ "We build our computer (systems) the way we build our cities: over time, without a plan, on top of ruins." - Ellen Ullman
- ▶ 'Interconnectedness makes big programs eventually crumble under their own weight.' -- Simon Peyton Jones
- ▶ "A primary cause of complexity is that software vendors uncritically adopt almost any feature that users want."- Niklaus Wirth