Better Buildings Residential Network Peer Exchange Call Series:

This Year I'm Grateful for… Cybersecurity

November 8, 2018

Agenda and Ground Rules

- Agenda Review and Ground Rules
- Opening Poll
- Residential Network Overview and Upcoming Call Schedule
- Featured Speakers:
  - **Glenn Fink**, Pacific Northwest National Laboratory
  - **Kara Saul Rinaldi**, Home Performance Coalition
  - **Danish Saleem,** National Renewable Energy Laboratory
- Open Discussion
- Closing Poll and Announcements

Ground Rules:

1. **Sales of services and commercial messages are not appropriate** during Peer Exchange Calls.
2. Calls are a safe place for discussion; **please do not attribute information to individuals** on the call.

The views expressed by speakers are their own, and do not reflect those of the Dept. of Energy.

Better Buildings Residential Network

Join the Network

Member Benefits:

- Recognition in media and publications
- Speaking opportunities
- Updates on latest trends
- Voluntary member initiatives
- Solution Center guided tours

Commitment:

- Members only need to provide *one number*: their organization's number of residential energy upgrades per year

Upcoming calls:

- December 13th: All I Want for the Holidays Is…

Peer Exchange Call summaries are posted on the Better Buildings website a few weeks after the call

For more information or to join, for no cost, email bbresidentialnetwork@ee.doe.gov, or go to energy.gov/eere/bbrn & click Join

Glenn Fink
Pacific Northwest National Laboratory

U.S. DEPARTMENT OF ENERGY

Pacific Northwest
NATIONAL LABORATORY

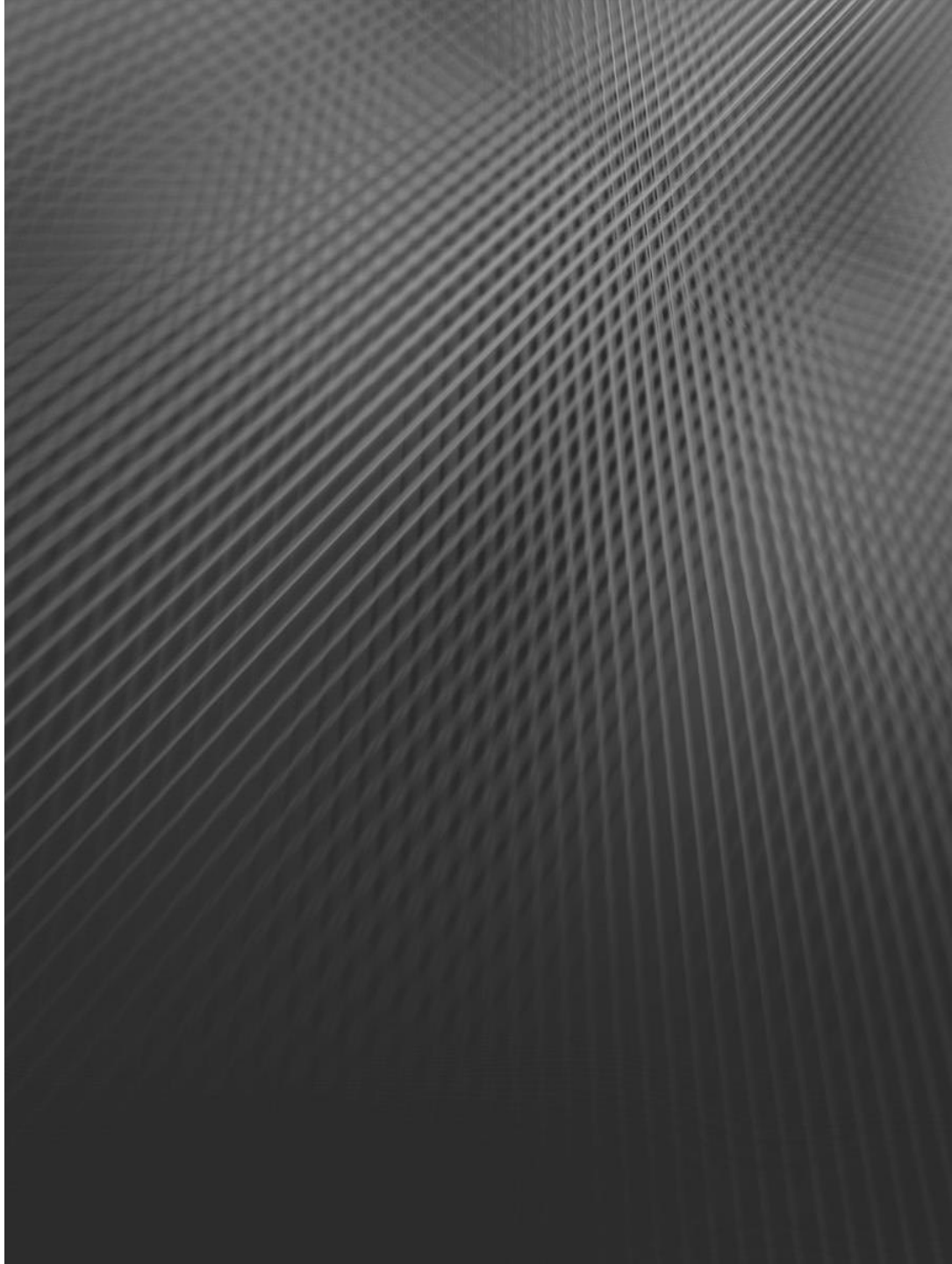
Internet of Things: A Security and Privacy Perspective

PRESENTER: GLENN A. FINK

National Security Directorate
Pacific Northwest National Laboratory

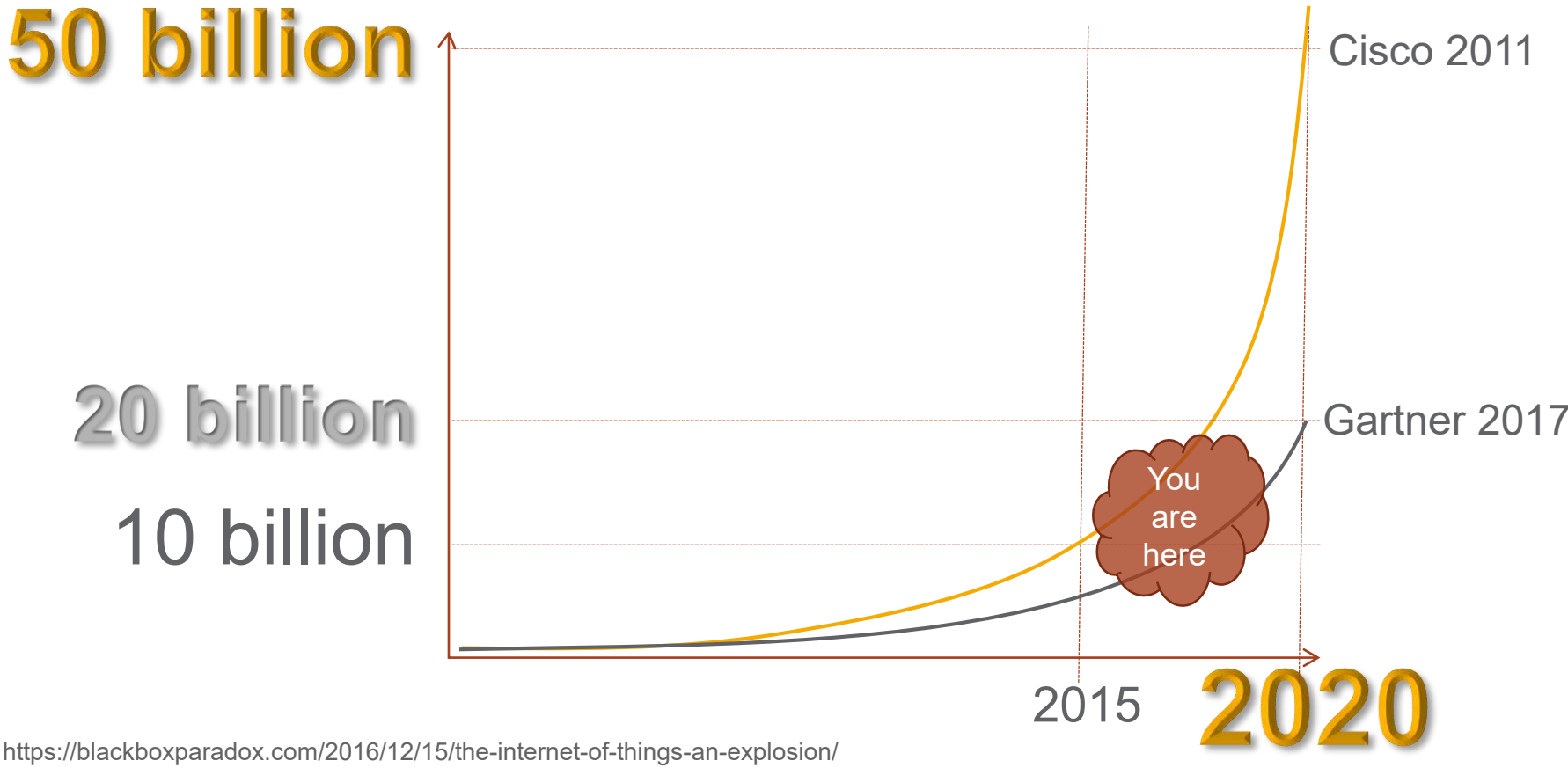
November 2018

PNNL-SA-110917



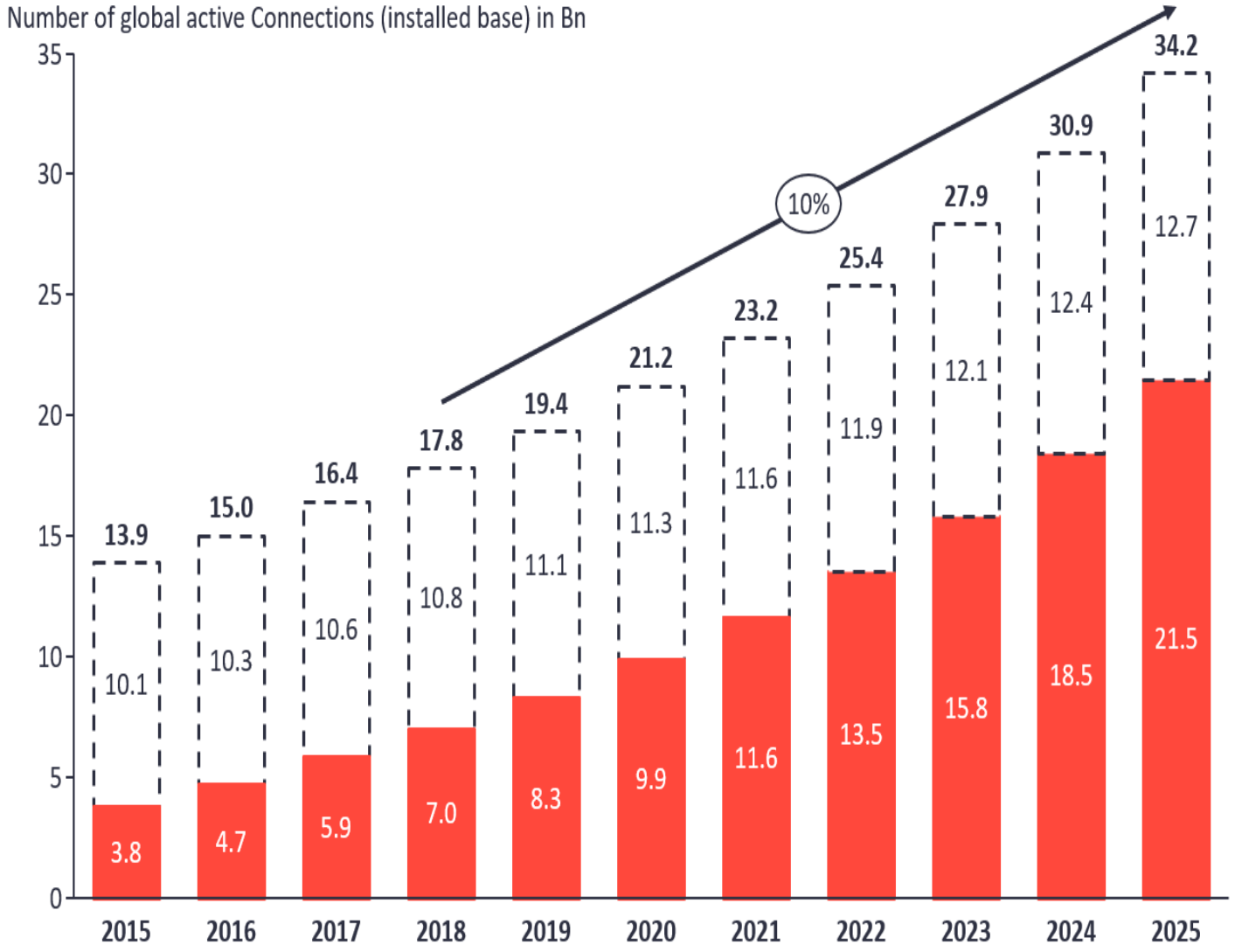
Pacific Northwest NATIONAL LABORATORY

IoT Predictions for 2020



https://blackboxparadox.com/2016/12/15/the-internet-of-things-an-explosion/

Total number of active device connections worldwide



Estimates vary depending on how you measure it:

Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones

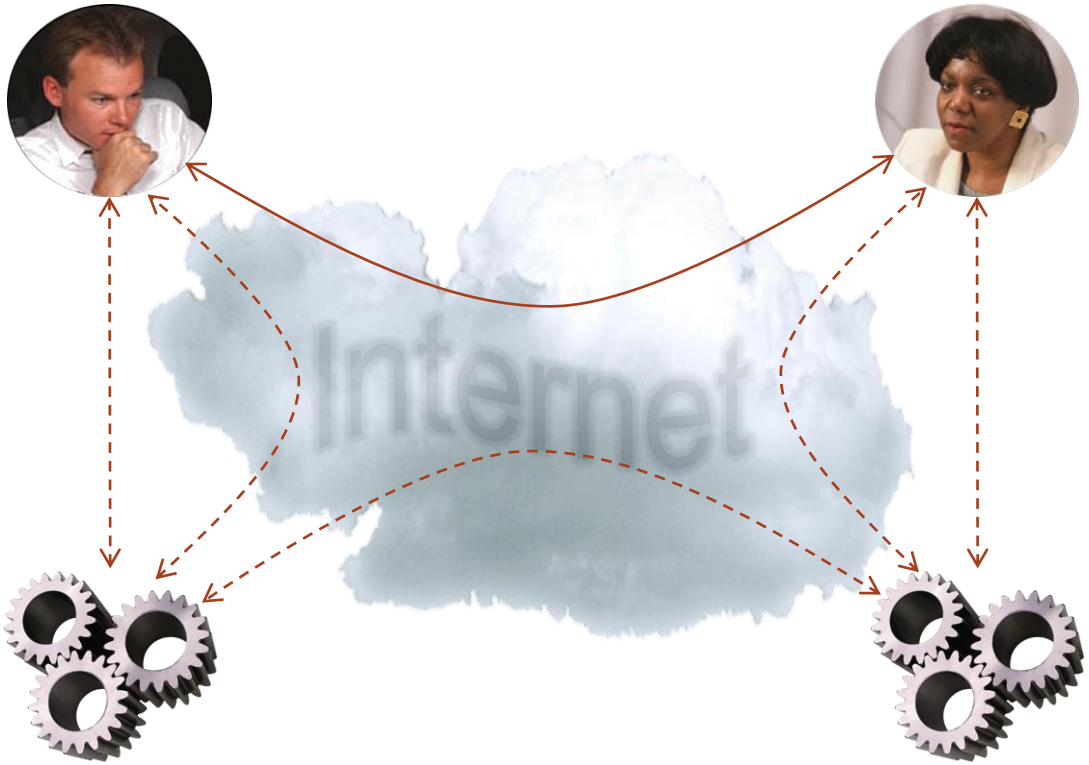
IoT includes all consumer and B2B connected devices

Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Source: IoT Analytics Research 2018

Pacific Northwest
NATIONAL LABORATORY

IoT takes people out of the loop



Pacific Northwest
NATIONAL LABORATORY

The Vision of IoT: "Connect everything to everything"

- "A radical evolution of the current Internet into a network of interconnected *objects* that…harvests information from the environment,…interacts with the physical world, [and]… provide[s] services for information transfer, analytics, applications, and communications."
  —J. Gubbi, University of Melbourne, Australia
- "The opportunity is to bring industrial systems and devices online to deliver data that can be analysed at scale by giant, scalable computing resources [realizing] the central premise of the IoT global data revolution [of] delivering increased efficiency and improvements to the bottom line."
  —Nick Sacke, head of IoT and products at Comms365
- "We build our computer (systems) the way we build our cities: over time, without a plan, on top of ruins." —Ellen Ullman, programmer, author, NPR commentator
- "Interconnectedness makes big programs eventually crumble under their own weight." —Simon Peyton Jones, Microsoft Research, London

Messages we (unintentionally) send

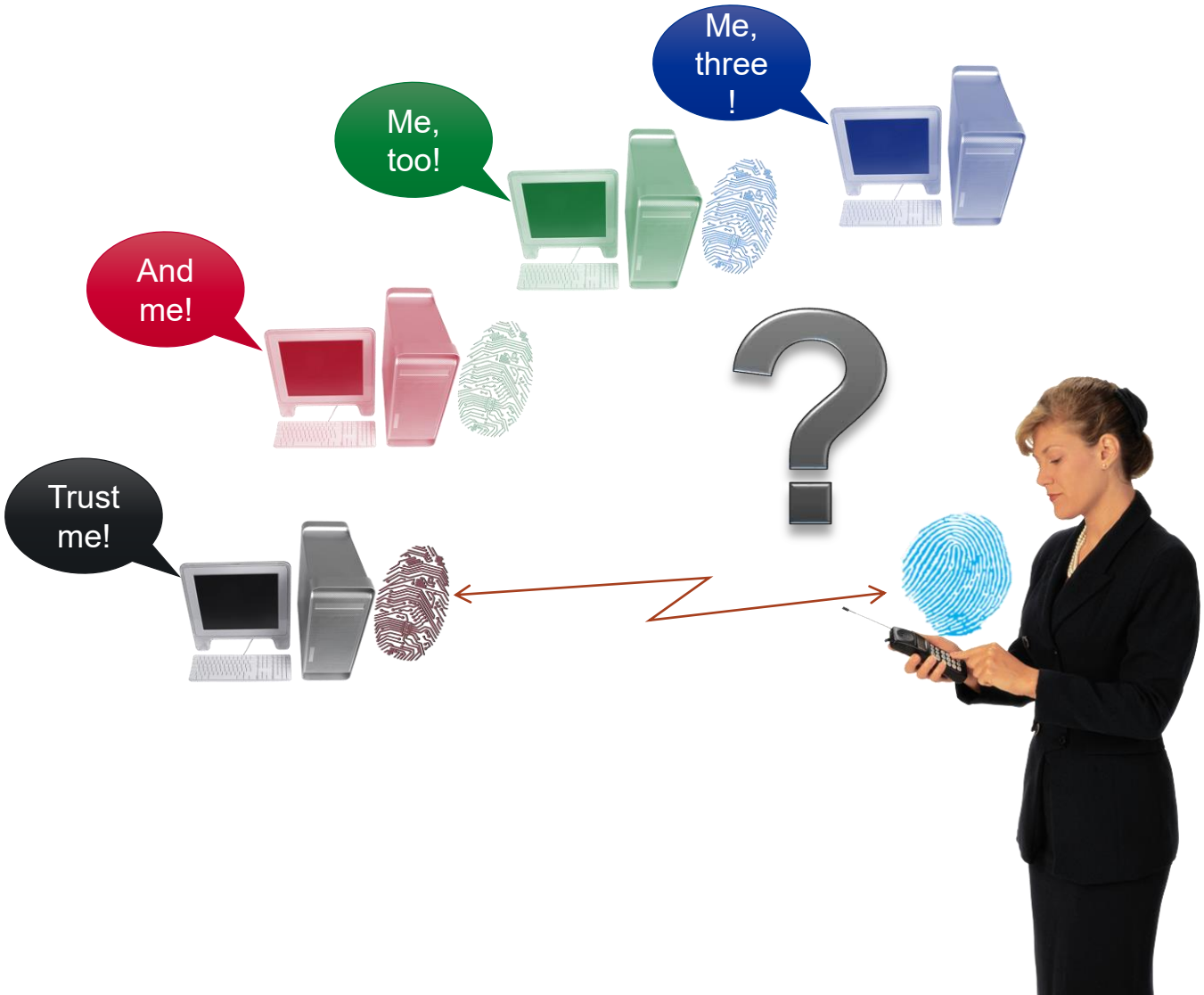
Pacific Northwest
NATIONAL LABORATORY

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

https://imgs.xkcd.com/comics/listening.png

Pacific Northwest
NATIONAL LABORATORY

Multiplying devices redefines identity



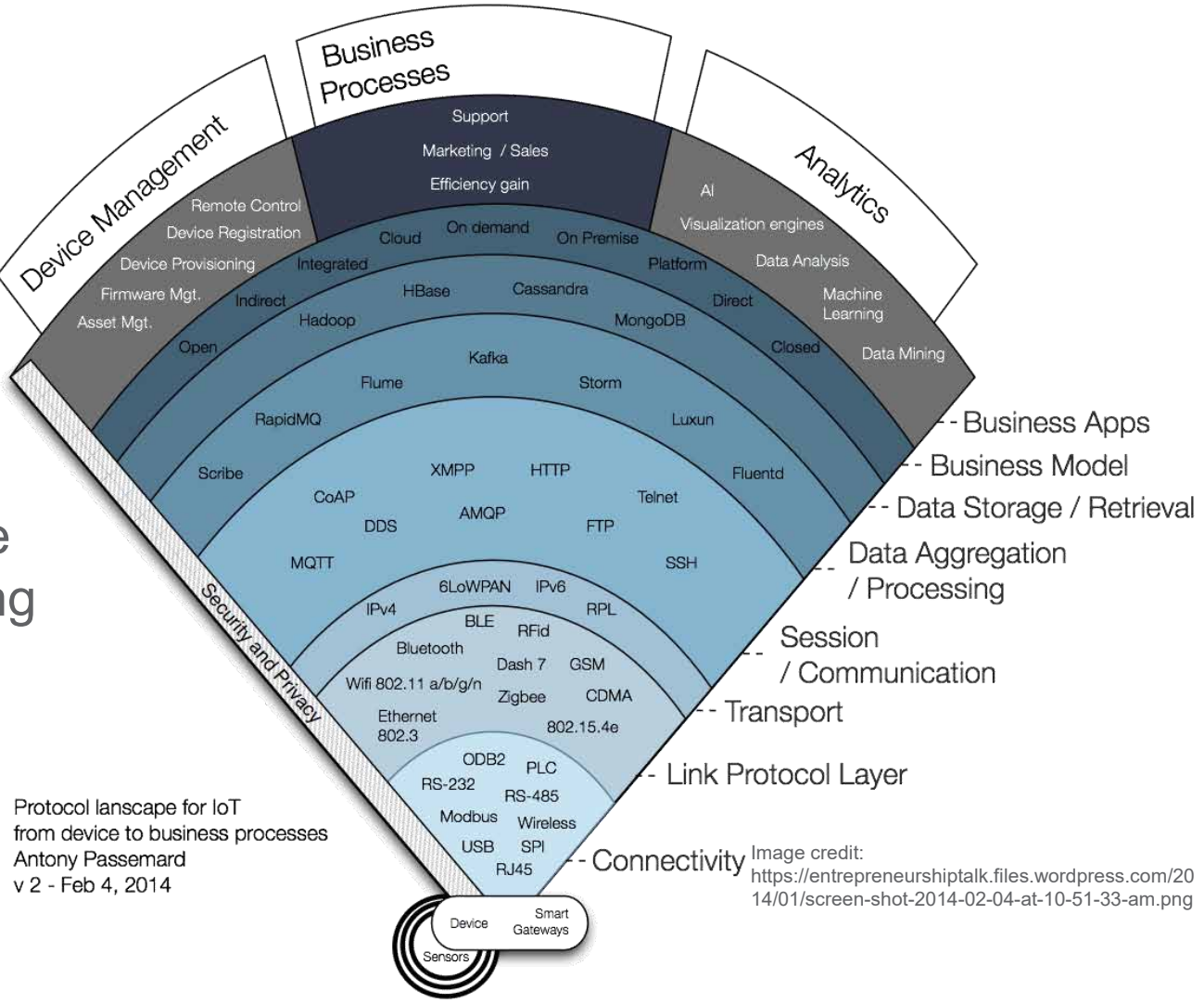
Pacific Northwest
NATIONAL LABORATORY

More devices worsens identity confusion

Pacific Northwest
NATIONAL LABORATORY

There are thousands of IoT networking protocols and the number is growing

This is a chart from 2014

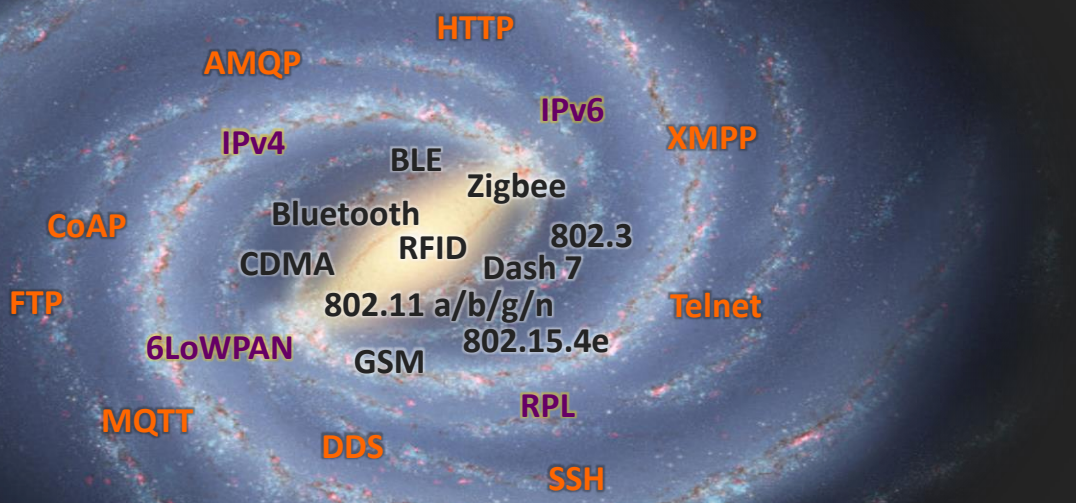


Protocol lanscape for IoT
from device to business processes
Antony Passemard
v 2 - Feb 4, 2014

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

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by **Battelle** *Since 1965*

A galaxy of semi-interoperable microprotocol implementations…



Pacific Northwest
NATIONAL LABORATORY

Are these two TCP state diagrams compatible?

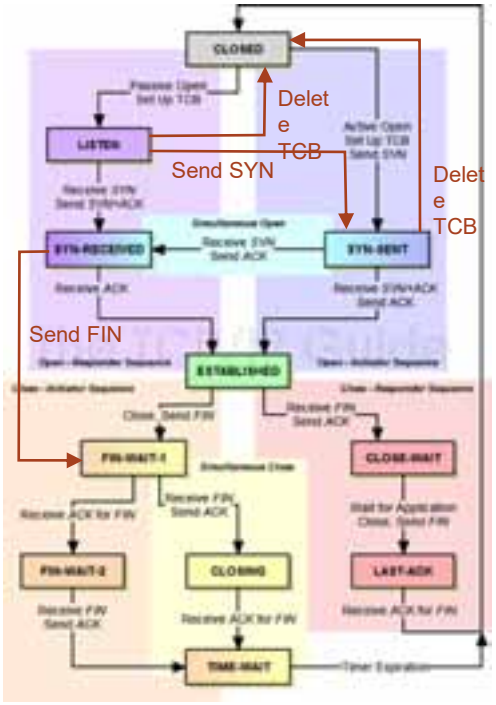


Image credit: https://www.tcpipguide.com

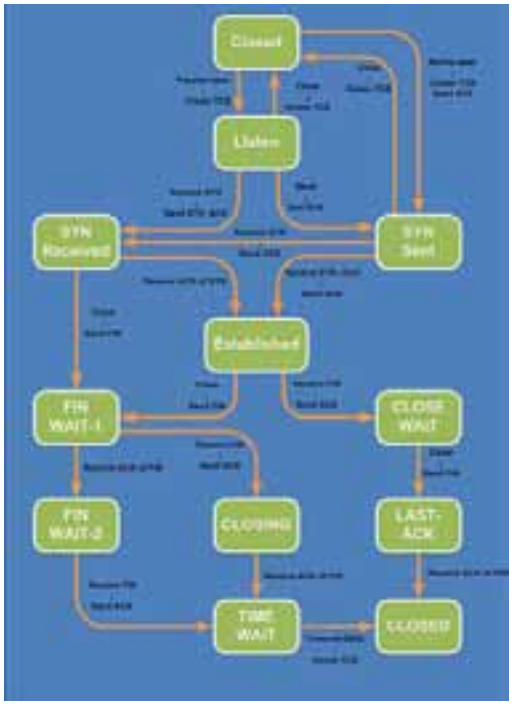
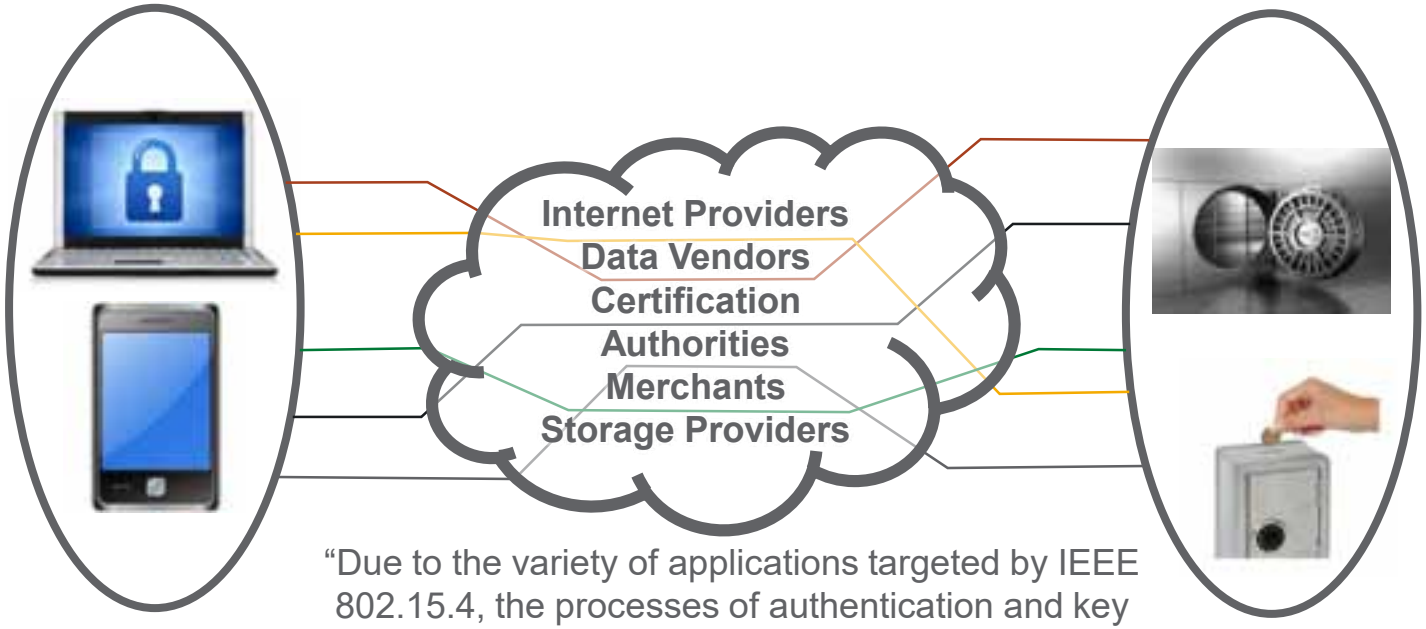


Image credit: https://bluehawk.monmouth.edu

Pacific Northwest
NATIONAL LABORATORY

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)

Pacific Northwest
NATIONAL LABORATORY

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

Pacific Northwest NATIONAL LABORATORY

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

COMPROMISED

F
OF OUR
DIGITAL

Our lives have become a digital patchwork of products and services

Privacy: A social landscape

Background art from: https://cdn-images-1.medium.com/max/2000/1*wdkAlW0wdTn4TayTBiUiAg.gif

Pacific Northwest
NATIONAL LABORATORY

Security:
Cyber crime: Money

Pacific Northwest
NATIONAL LABORATORY

IoT and Cyber crime: Money

Pacific Northwest
NATIONAL LABORATORY

IoT and Cyber crime: Property

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

Forgotten devices in the home

- How many months before support is discontinued?
- How long before the novelty wears off and the owner discards the app?
- But how long will these devices stay connected and hackable?
- Do they convey to the next owners?

Phillips Hue smart bulbs lighting system

GE connected range

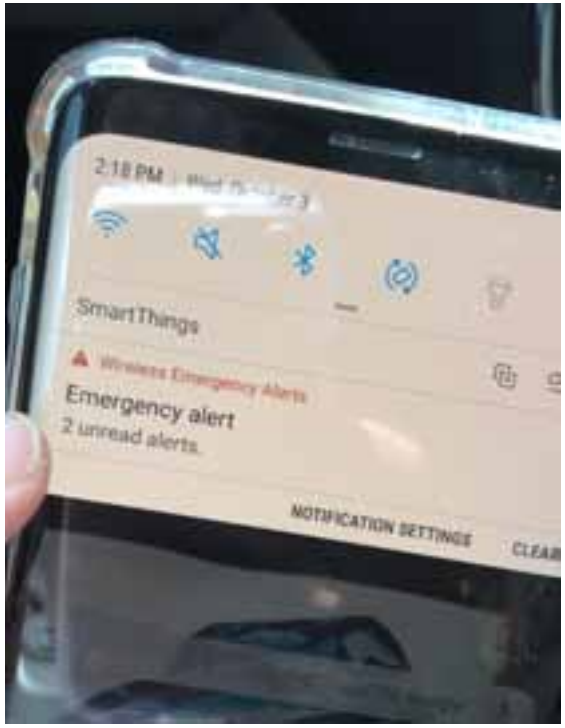
Master Flow 1450 CFM Smart Power Gable Mount Attic Fan, available at home depot

https://www.businessinsider.de/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=UK&IR=T

Pacific Northwest
NATIONAL LABORATORY

Security:
Cellular Devices

https://twitter.com/i/moments/1047552607231692802



It wasn't just US cell phone users that received a text alerting them about a “test of the National Emergency Alert System.”

- Do your devices get Presidential Alerts?
- Do they need them?
- What happens to them when they receive them?
- What else could they receive that way?

Pacific Northwest
NATIONAL LABORATORY

Security:
Medical Devices

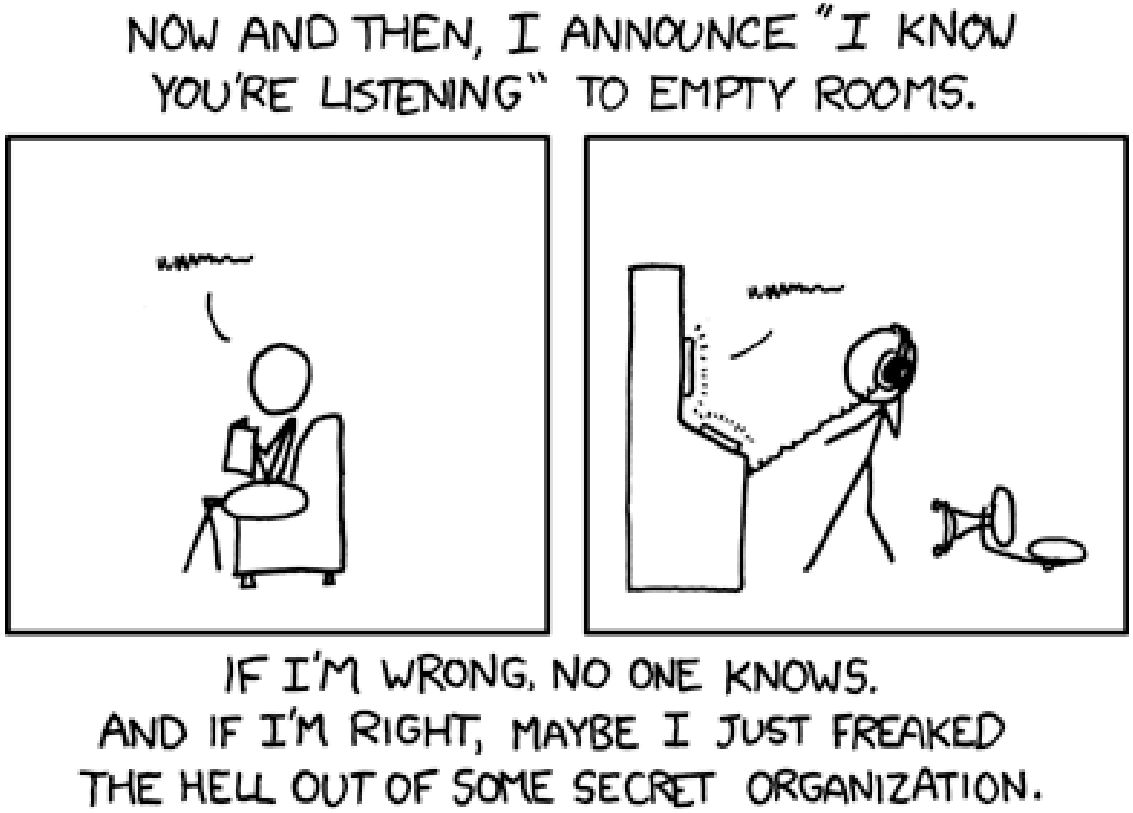
FDA's concerns about cybersecurity vulnerabilities include:

- 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


The Register
Biting the hand that feeds IT
Security
Hackers could turn your smar
into a bomb and blow your fam
smithereens – new claim
And before that, pwn your IoT gadgets via po
supply gear
By Darren Pauli 4 Jan 2017 at 08:03
154
SHARE
WIRED
LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM
MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE
iness.ca
gy meets business
ternet of Things lead to the
ll Things?
Catherine Acz
Publishe
Could Hacking Your Fridge, Car, and Printer Really Be a Thing? Examining IoT for 2017
TNW
About 90%
TV Signals
By Catalin Cimpanu
ars TECHNICA
Billions of devices imperiled by new clickless Bluetooth attack
HackRead
olphins inspire ultr onic attac
at pwn smartphones, cars and
ssistants
Katie Morley, CONSUMER AFFAIRS EDITOR
News
By Robert McMillan
Sept. 13, 2017 5:30 a.m. ET
to hackers
Vulnerable Smartphones, IoT Devices: 400%
rease in infection rate
THE WALL STREET JOURNAL.
Latest Weapon: Cyber Extortion
shed light on this growing threat as extortionists seek
net of Th
Report: AI, IoT, Secu
Threats Will
Internet's Fu
By Rhea Kelly 09/20/17
ZDNet
VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE
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
By Roger A. Grimes
TechRepublic
Researchers use $5 speaker to
smartphones, automobiles
Cybersecurity researchers from the University of Michigan
backdoor access into systems.
'Bear-ly' Innocent: Kids' Voice Recordings Leaked in Creepy IoT Teddy Hack
28.02.2017 (updated 18:13 28.02.2017)
Get short URL
0 435 8 5
of web-con
exposing 8
n.
led toys called CloudPets have been
d voice messages left by
Cyber attack could sink cruise ships, Government advice warns
16 Sep 2017, 9:15pm

Pacific Northwest
NATIONAL LABORATORY

So what do we do now?

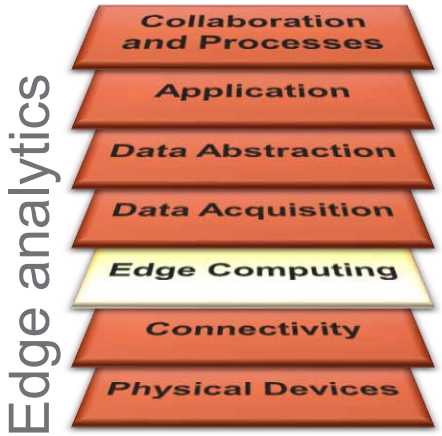


https://xkcd.com/525/

Pacific Northwest NATIONAL LABORATORY

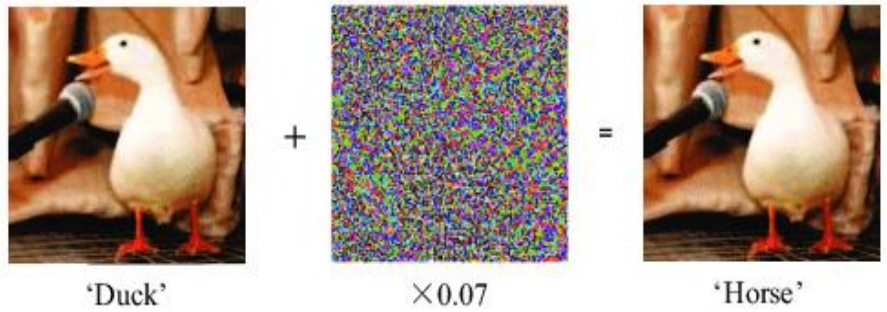
Research Challenges:
Scientific and Technical

Bandwidth



Identity vs. Anonymity vs. Pseudonymity

Adversarial machine learning



https://www.researchgate.net/publication/324055823_An_Overview_of_Vulnerabilities_of_Voice_Controlled_Systems

Research Challenges:
Social and Legal

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Legal:
- Minimal required safe configurations
- Rate/capability limiting
- Liability
- Data sovereignty

- Standards: crucial for "Future proofing" operations
- Must adapt to innovation trends and ensure interoperability
- Must be consolidated

- Theory: protocol stacks that enforce "laws" of data management

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

Pacific Northwest NATIONAL LABORATORY

End-user Challenges:
What should consumers do?

Think before you connect!

- It all boils down to applying basic cyber hygiene:
  - If you don't need a device, consider not using it…especially those passive listeners:
    - ✓ Alexa, Smart TV, voice-activated anything…
  - See if the device is useful without an internet connection or using that of another device
  - Always change the default device passwords
    - ✓ Consider an alternative device if you cannot change it
  - Keep a master list of devices and passwords, change them from time to time
  - Consider keeping all your devices on a separate wireless network from your personal computing resources

Image credit: https://cdn-images-1.medium.com/max/2000/1*wdkAlW0wdTn4TayTBiUiAg.gif

Key Takeaways: Glenn Fink

- Our lives have become a digital patchwork of connected products, devices and services – all transmitting information
- Security for these devices is varied and optional; many will implement the bare minimum set of such features necessary
- What can we do as individuals? Think before you connect – is this device necessary? Also practice good “cyber hygiene.”

Kara Saul Rinaldi
AnnDyl Policy Group

U.S. DEPARTMENT OF
ENERGY

“This Year I’m Grateful for… Cybersecurity”

BBRN Webinar

November 8, 2018

Kara Saul Rinaldi, President & CEO AnnDyl Policy Group

Vice President of Government Affairs, Home Performance Coalition

Who is the Home Performance Coalition?

- National research, policy, and conference organization.
- Work with stakeholders to address challenging issues in the residential energy efficiency / home performance industry:
  - Evaluate carbon and energy efficiency policy and recommending methods for utilizing home performance;
  - Seek synergies between weatherization and private sector programs and policies;
  - Support interoperability and reducing program costs through development of national data standards;
  - Work to ensure the value of energy efficient homes is visible in the real estate transaction;
  - Find intersections between smart grid and device technologies and home performance;
  - Reforming cost-effectiveness screening practices; and
  - Educate policymakers, advocating for legislation and regulations that reduce residential energy consumption.

AnnDyl Policy Group / Home Performance Coalition

What is at Stake?

- What is the data that we are discussing and what can it tell about you?
- Energy User Data
  - Directly from the meter, in intervals, energy usage signatures and patterns.
- Beneficial Use?
- Malicious Use?

The home is a part of the grid…

Image credit: Unsplash_Jens Kreuter, Unsplash_Naomi Hebert, LG, Philips, Nest, Washington Post

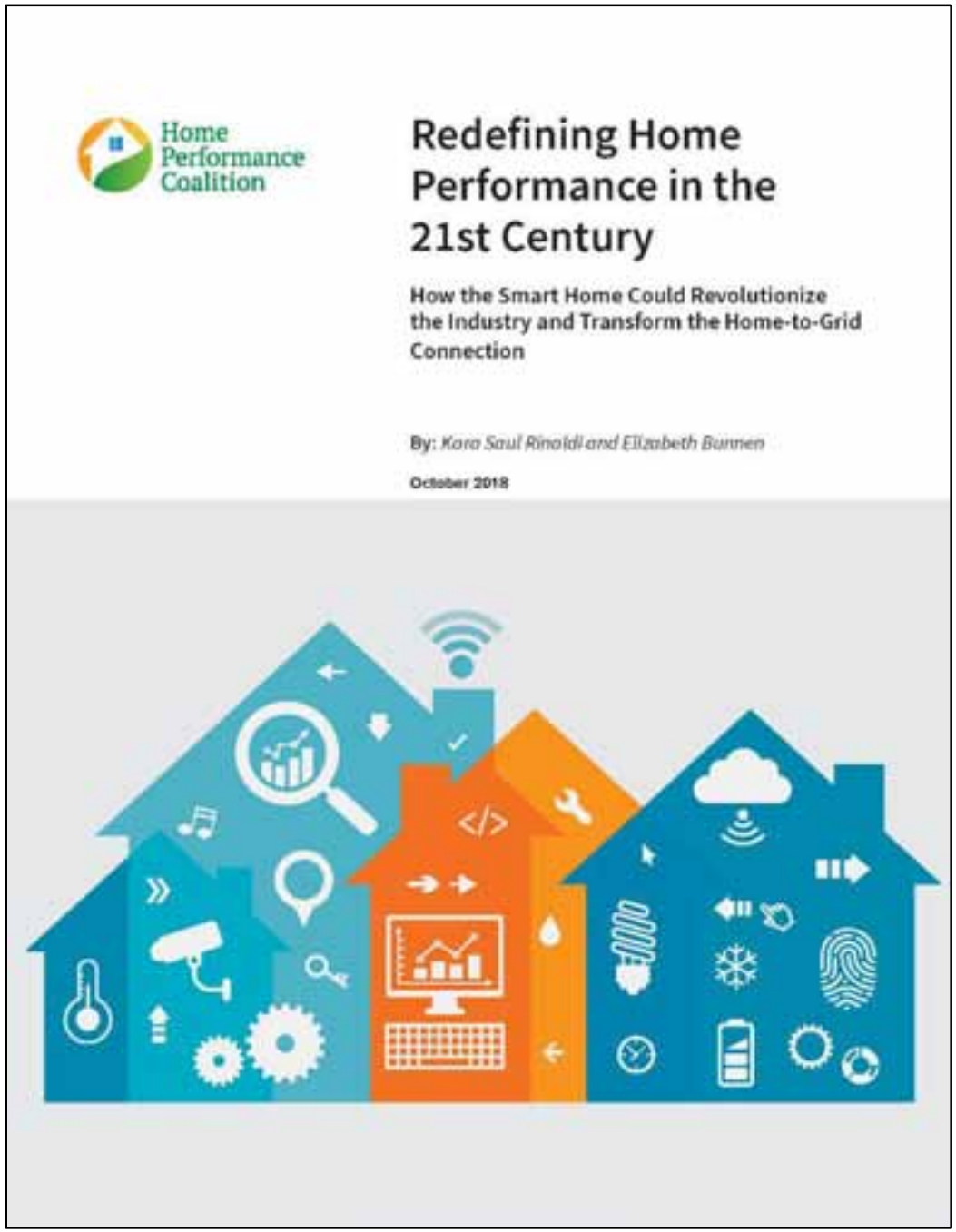
AnnDyl Policy Group / Home Performance Coalition

Whose Data Is it?

- The Customer or The Utility?
- Nations Ahead of the US:
  - Australia, Europe, Switzerland
- Industries Ahead of Energy:
  - Financial Services
  - Healthcare

Not IF the data should be portable but HOW it should be portable?

AnnDyl Policy Group / Home Performance Coalition



http://www.homeperformance.org/sites/default/files/HPC_Smart-Home-Report_201810.pdf

AnnDyl Policy Group / Home Performance Coalition

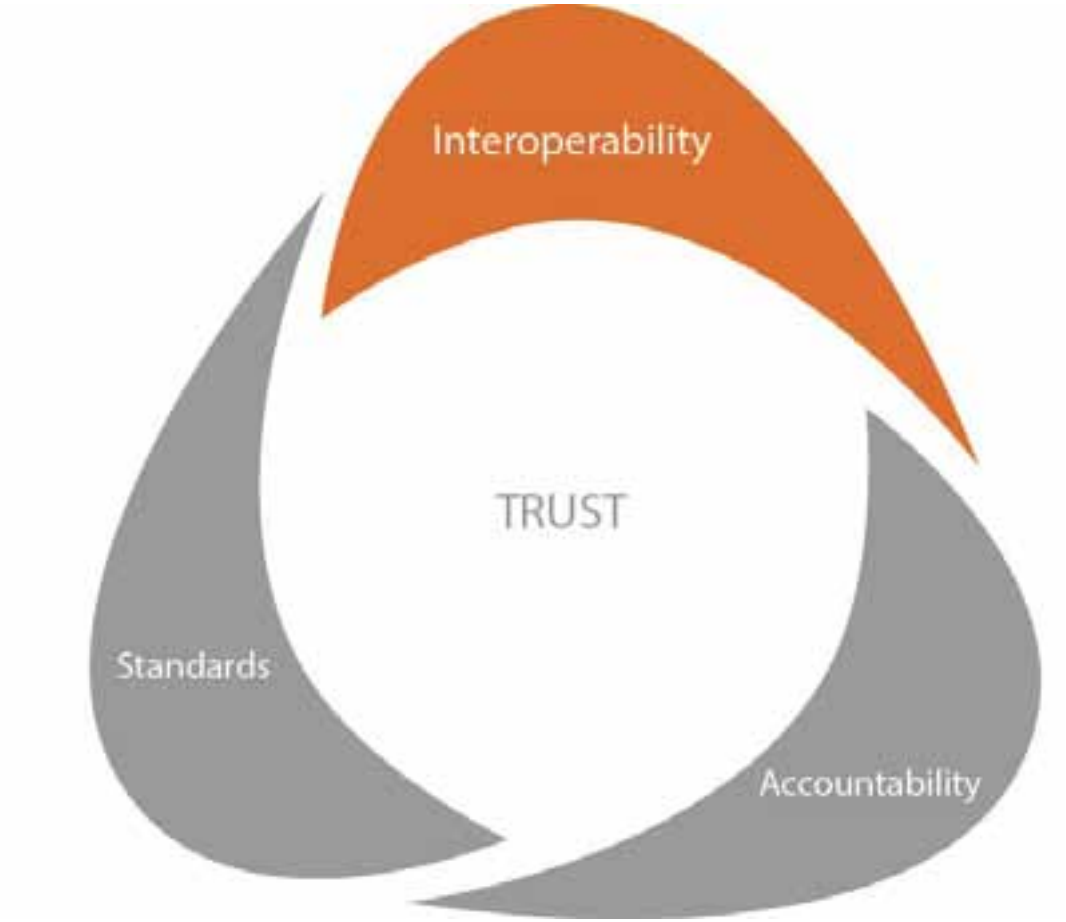
Full Disclosure: Recommendation #5

Improve Data Access Policies and Increase Data Sharing

Image credit: 123RF

AnnDyl Policy Group / Home Performance Coalition

Standards - Interoperability – Accountability



AnnDyl Policy Group / Home Performance Coalition

Data as a Commodity

- Selling Energy (Utility)
- Selling Data (Customer/Utility)
- Ensure User Experience
- 3rd Party Access – security, reliable, efficient

Image credit: 123RF, Shutterstock

AnnDyl Policy Group / Home Performance Coalition

Policy to Advance Utility Data Access

- Access to Consumer Energy Information Act or the E-Access Act (114th – HR1980/S.1044)
- Open Standards for Utility Transfer
- Green Button and Green Button Connect My Data
- HPXML

Image credit: Unsplash_Andy-Feliciotti

AnnDyl Policy Group / Home Performance Coalition

Source: Mission Data http://www.missiondata.io

AnnDyl Policy Group | Home Performance Coalition

Thank you!

Kara Saul Rinaldi

President and CEO – AnnDyl Policy Group, LLC
Vice President of Government Affairs - Home Performance Coalition

kara@anndyl.com

ksaul-rinaldi@homeperformance.org

(202) 276-1773

Key Takeaways: Kara Saul Rinaldi

- With respect to household energy consumption data, the question of “whose is it” has not been clearly settled.
- This data should be made portable; such portability will require improved data access policies and increased data sharing.
- The Access to Consumer Energy Information Act, open standards for utility data transfer, Green Button and HPXML are all initiatives which can help to advance the state of residential energy consumption data.

Danish Saleem
National Renewable Energy Laboratory

U.S. DEPARTMENT OF
ENERGY

Cybersecurity Considerations for Connected Smart Home Systems and DERs

Danish Saleem
DER Cybersecurity Standards Lead
National Renewable Energy Laboratory

11/08/2018

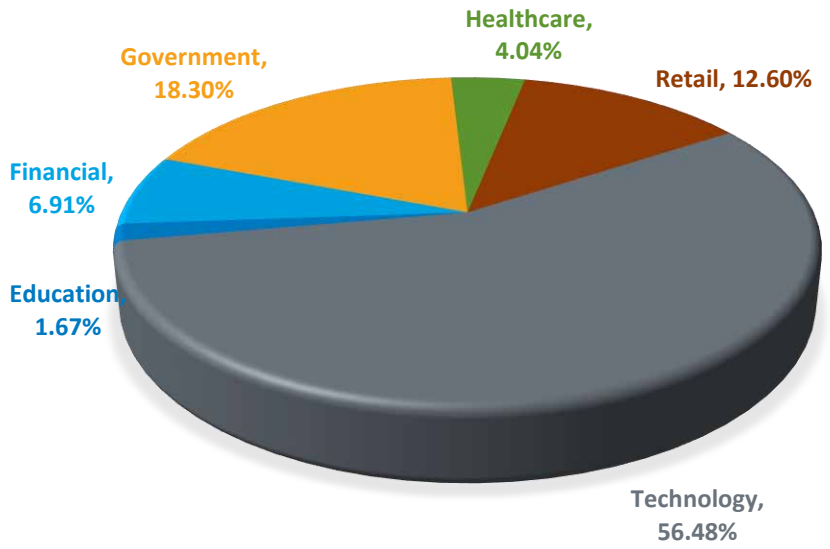
Agenda

1. Background
2. Common vulnerabilities and attacks
3. Common types of cyber-attacks
4. Case studies: Vulnerabilities in home automation system and buildings
5. Recommendations: Six Cybersecurity principles
6. Best practices and recommended areas for research
7. NREL's cybersecurity focus

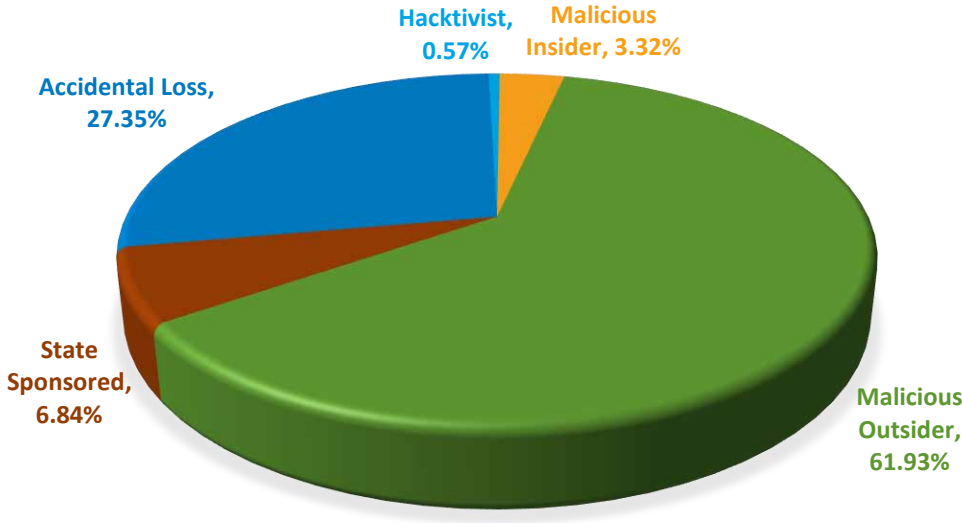
- New voice assistants
- Internet connected video monitors

- Lack of situational awareness
- DERs connected to home

RECORDS LOST/STOLEN BY INDUSTRY



RECORDS LOST/STOLEN BY SOURCE



Background

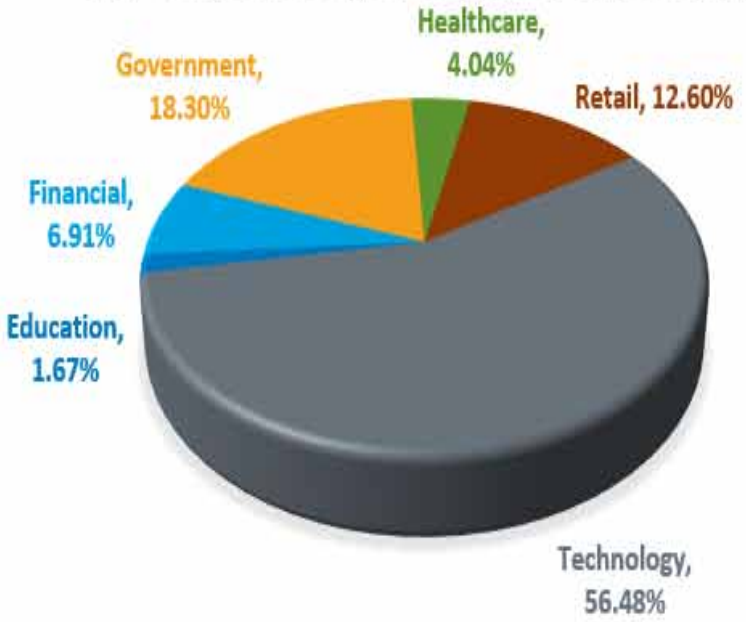
What is Residential Internet of Things (IoT)

Why there is a need to secure residential applications

- New voice assistants
- Internet connected video monitors
- Lack of situational awareness
- DERs connected to home

Data lost or stolen so far

RECORDS LOST/STOLEN BY INDUSTRY



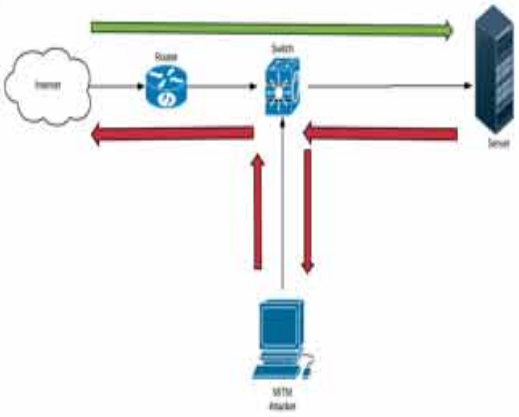
RECORDS LOST/STOLEN BY SOURCE

Common Vulnerabilities in Residential IoT

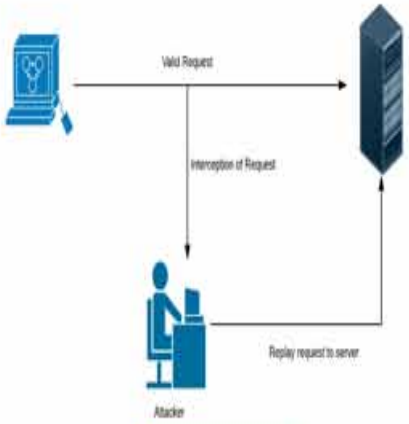
	Vulnerabilities	Examples/Hacks
1	Poor product design	Researchers at University of Michigan demonstrated successful hack that opened electronic locks, changed system pre-sets and remotely trigger a false fire alarm. [1]
2	Inadequate authentication procedures	Nine separate vulnerabilities were identified in a recently introduced indoor and outdoor lighting system.
3	Non-secure communication protocols	25% of smart home devices were compromised in less than three hours
4	Use of open source software and/or limited software patching	Internet-connected baby monitors. Researchers found only one model was secure (out of 9 different models of baby monitors) from a potential cyberattack. [4]
5	Lack of understanding of equipment/device	12 out of 16 different bluetooth-enabled smart locks had insufficient security and were susceptible to cyberattack. [5]

Common Types of Cyber-Attacks

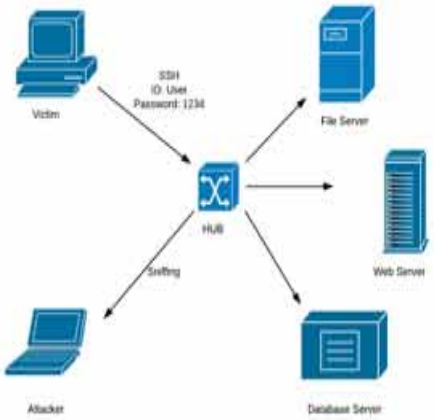
TYPES OF ATTACKS
Man in the middle
Replay/Masquerade
Eavesdropping
Certificates spoofing
Denial of Service
Wireless
Least privilege violation



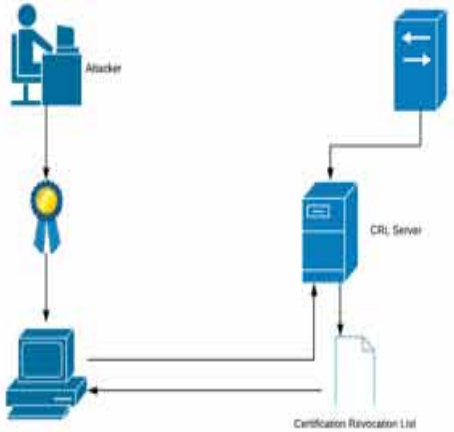
Man In The Middle (MITM)



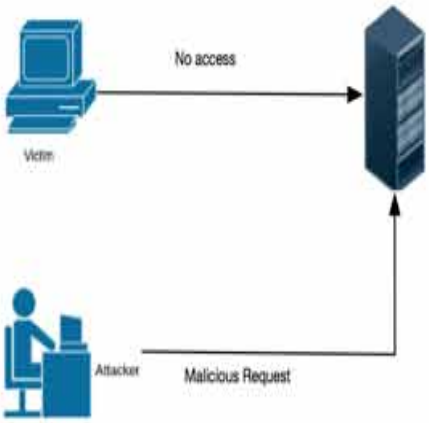
Replay



Eavesdropping



Spoofing Through Certificates



Denial of Service (DoS)

Least Privilege Violation

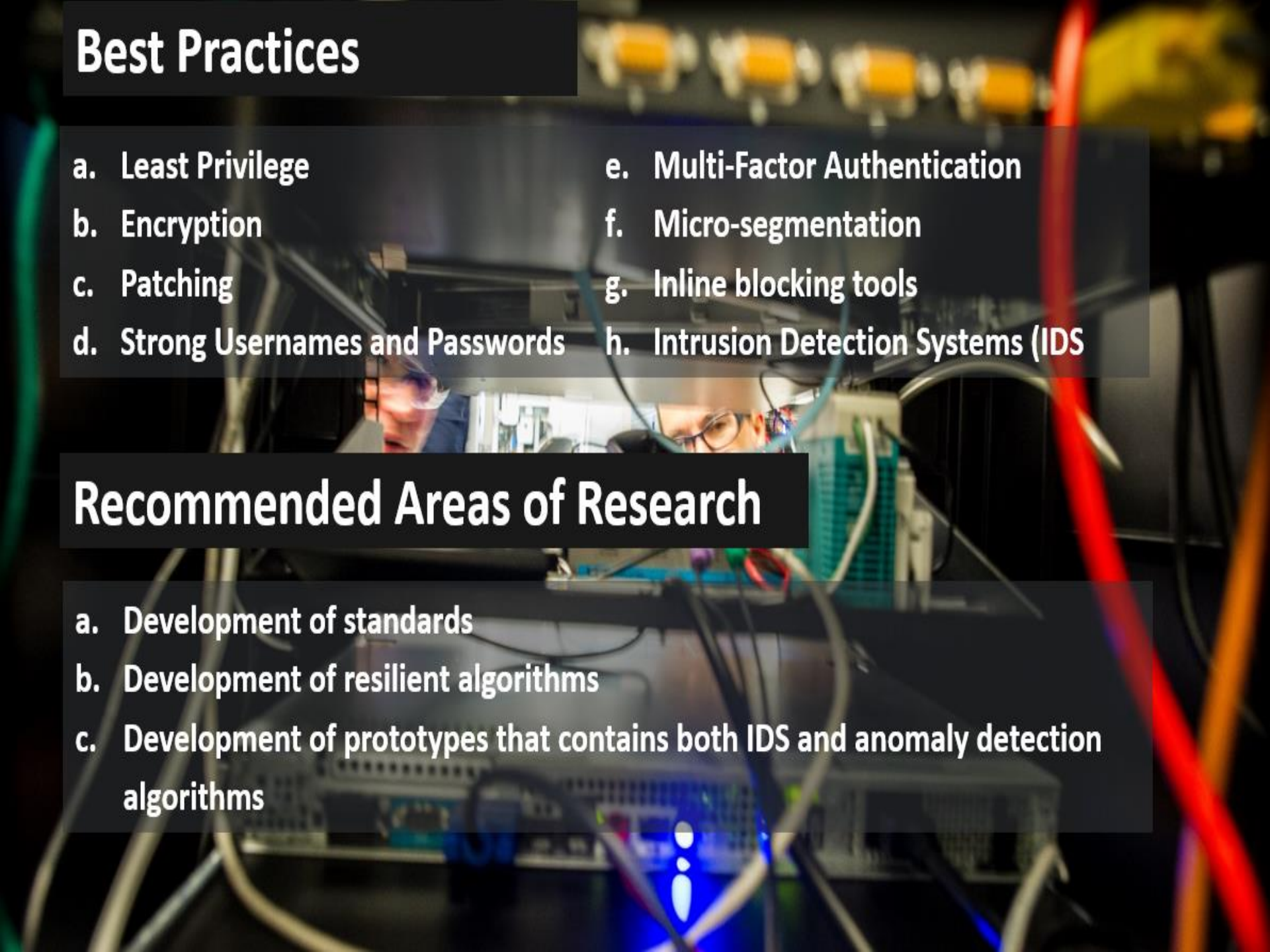
Case Study 1: Home Battery System for Automation

Test Cases	Method of Exploitation	Results
Service disruption via DoS	Denial of service	• DoS appeared to be effective • Application was made inaccessible to user at the time of attack • Application returned to normal state of operation after the attack stopped
Platform operation disruption	Packet capture and spoofing (MiM)	• The encryption used by the application was good enough • No communication between the application and an IoT device could be compromised
Attack software platform from customer LAN	Port scanning Password guessing Vulnerability scans	• Application's web service was found vulnerable. • Sensitive configuration files of the application and the OS were exposed
Software platform data disruption	Escalate privileges	• No authentication within customer LAN • Anyone, with access to the customer LAN, can have the same permissions that the customer have.
Attack communication channel	Physical disconnect of communication DoS on network	• All wireless communications (within the Wi-Fi signal range of the appliance) were disrupted to appliances that were connected to the software • This prevented new data from entering or leaving the appliance. • This attack was performed without any level of access to the customer LAN.

Case Study 2: Buildings

Vulnerability Description	Possible Consequences	Recommended Mitigation
Staff Laptop docking stations	Login IDs, passwords, emails, contacts, hard disk data, banking details etc.	Shut down each USB port from the BIOS and/or use wireless keyboard and connect the key to the inside of the CPU.
SCADA workstations	Full access of system including power and comms controls, badge reader & safety system	a) Enforce screen lock in case of no activity for more than 5 minutes. b) Change keyboard type (wireless) for preventing Key logger kind of attacks
Access to router over LAN or WLAN	Risk of compromising communication network of whole building, scholarly research and information, employee personal information	Setup password recovery
Same password for each door	Loss of reputation, loss of money.	Activate two factor authentication like badge and pin
Loading Dock	Theft or access to all the private and classified information of the affected users.	Designated person to police the activity

Six Cybersecurity Principles for Residential Security



Best Practices

a. Least Privilege
b. Encryption
c. Patching
d. Strong Usernames and Passwords
e. Multi-Factor Authentication
f. Micro-segmentation
g. Inline blocking tools
h. Intrusion Detection Systems (IDS

Recommended Areas of Research

a. Development of standards
b. Development of resilient algorithms
c. Development of prototypes that contains both IDS and anomaly detection algorithms

NREL's Cybersecurity Focus

Cross-cutting projects across industry and the national lab network

- Site security assessments: Developing DER C2M2
- Vendor product cybersecurity evaluations
- Security architectures
- Standards development
- Technology R&D
- Power and cyber co-simulation

DER Cybersecurity Working Group

SECURING DER DEVICES & SERVERS

- **Define standardized procedure for DER and server vulnerability assessments.**
- Leads: Danish Saleem (NREL) and Cedric Carter (MITRE)
- Known equipment vulnerabilities
- Establish certification and auditing procedures
- Maintaining compliance, requirements for patching
- **In process of transferring this to UL STP (likely to become a UL 2900-2-4 standard)**

SECURE NETWORK ARCHITECTURE

- **Create DER control network topology requirements and interface rules.**
- Lead: Candace Suh-Lee (EPRI)
- Perimeter controls
- Segmentation
- Physical security

ACCESS CONTROLS

- **Classify data types, associated ownership, and permissions. Define set of protection mechanisms.**
- Not Started
- Access control lists
- Password control
- Data privacy

COMMUNICATION AND PROTOCOL SECURITY

- **Define requirements and draft language for data-in-transit security rules.**
- Not Started
- Authentication
- Encryption requirements
- Acceptable transport protocols

Security Standards for DER

Cybersecurity Requirements for DERs

Test Cases

Basic Security Controls

1. Role-based access controls
2. Selective encryption
3. Secure firmware updates
4. Network segmentation
5. Intrusion Detection Systems
6. Strong username and password

Advanced Security Controls

1. Transport layer security
2. Session renegotiation
3. Using Message Authentication Code
4. Session resumption
5. Support for multiple certificate authorities
6. Certification Revocation List

Secure Data and Communication of DERs

(Smart Inverters, PV Systems, Wind Turbines, Microgrid Controllers, Production Net Meters, Synchrophasors, Relays)

Certification Procedures for Data and Communication Security of Distributed Energy Resources

Saleem Danish
National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Technical Report
NREL/TP-5D00-71224
April 2018

Contract No. DE-AC36-08GO28308

Thank you

www.nrel.gov

Contact Info:

Danish Saleem
danish.saleem@nrel.gov | 720-404-5912

NREL
Transforming ENERGY

Key Takeaways: Danish Saleem

- Cybersecurity risks run the gamut from compromised hardware to something as simple as poor physical security.
- Behavioral countermeasures are one half of the coin – simply being aware of and applying best practices for each relevant context.
- The other side, technical research to optimize the robustness of technologies, is ongoing now at such organizations as NREL and PNNL. If you have thoughts, share them!

Upcoming Seasonal Messaging Opportunities

Image: City of Sugar Hill

Explore the Residential Program Solution Center

Resources to help improve your program and reach energy efficiency targets:

- Handbooks - explain *why* and *how* to implement specific stages of a program.
- Quick Answers - provide answers and resources for common questions.
- Proven Practices posts - include lessons learned, examples, and helpful tips from successful programs.
- Technology Solutions NEW! - present resources on advanced technologies, **HVAC** & **Heat Pump Water Heaters**, including installation guidance, marketing strategies, & potential savings.

https://rpsc.energy.gov

Thank You!

Follow us to plug into the latest Better Buildings news and updates!

Better Buildings Twitter with #BBResNet

Better Buildings LinkedIn

Office of Energy Effiency and Renewable Energy Facebook

Please send any follow-up questions or future call topic ideas to:
bbresidentialnetwork@ee.doe.gov