Industry Panel: IF06

Time: 10:30- 12:30 pm

Date: February 06, 2018

IEEE World Forum on Internet of Things

IOT Security: Issues and Challenges for Mass Market Deployment

Session Chair and Moderator:

Subir Das, PhD

Vencore Labs, NJ, USA

sdas@Vencorelabs.com

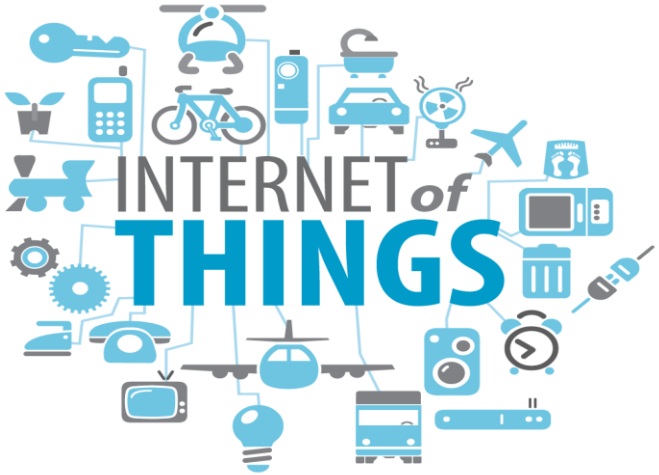
Session Plan

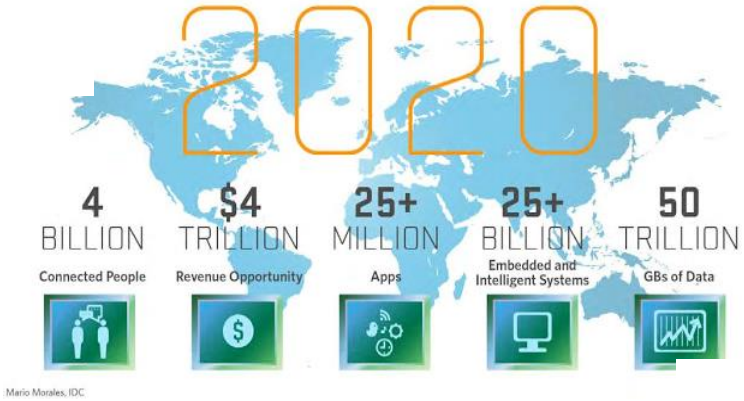
- Introduction to the Panel and Panelists- 25 mins
- Presentation by Panelists –60 mins (20 mins each)
- Moderated Discussions including Q & A – 35 mins

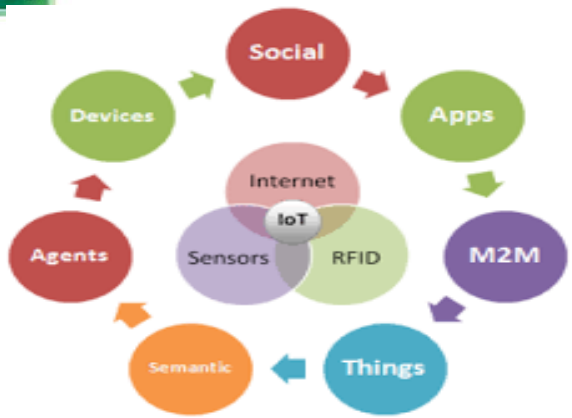
Distinguished Panelists

- Dr. Subir Das (Moderator) – Chief Scientist, Vencore Labs, USA
- Mr. Anand Rajan – Senior Director, Emerging Security Lab, Intel Corporation, USA
- Mr. Asad Haque – Lead Security Architect, Comcast, USA
- Dr. Lily Chen – Manager, Cryptographic Technology Group, NIST, USA

Introduction



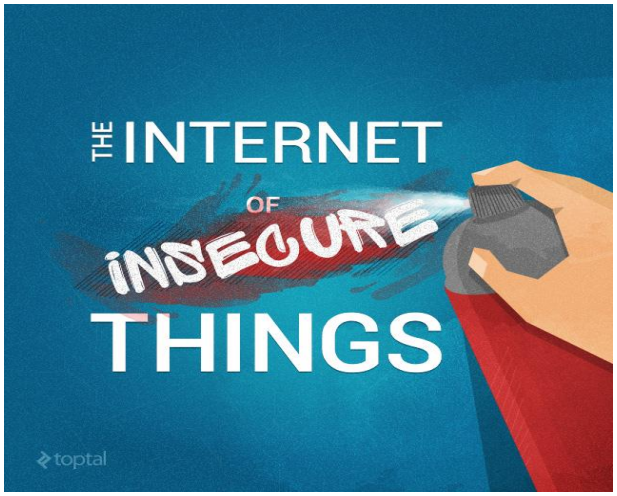




Source: Google Search: what is IoT?

VENCORELABS

Introduction contd..



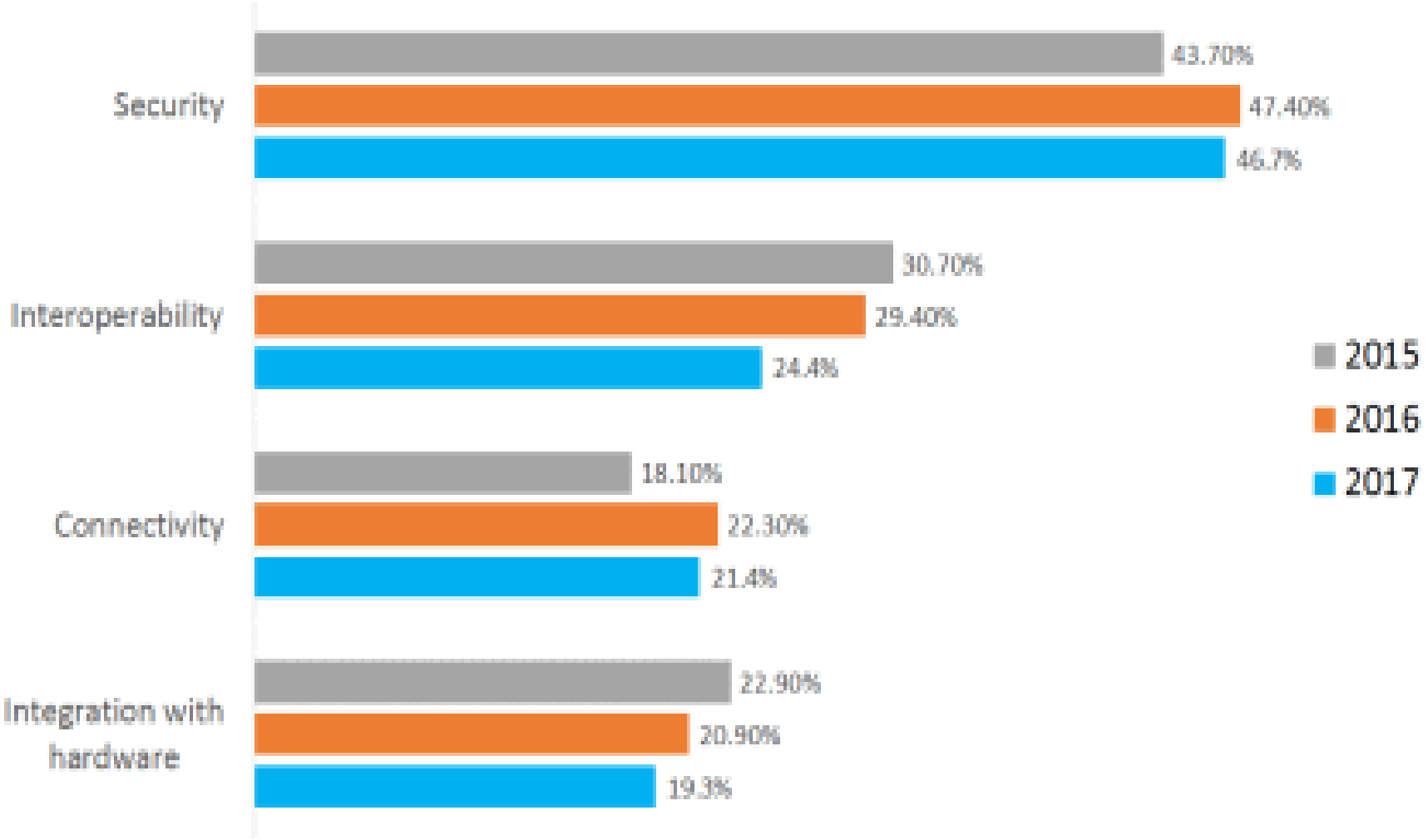
Source: Google: What is IoT security?

VENCORELABS

Attacks that are Keeping the CSOs Awake

- Stuxnet (2010-2014)
  - Targeted industrial programmable logic controller
  - Affected Iran's uranium enrichment facility, as reported (2010-2014)
- Mirai botnet (2016)
  - Infected older routers and IP cameras and then flooded DNs provider Dyn with a DDoS attack that took down major sites (2016)
- Cold in Finland (2016)
  - Cybercriminals shut down the heating of two buildings in Finnish city by launching DDoS attack was launched to keep heating controllers keep rebooting
- BrickerBot (2017): DDoS attack to kill the device
- The Botnet Barrage (2017)
  - An unnamed university's 5000 devices were attacked by breaking weak passwords and then slowed the network connectivity

Where are the Concerns in IoT?

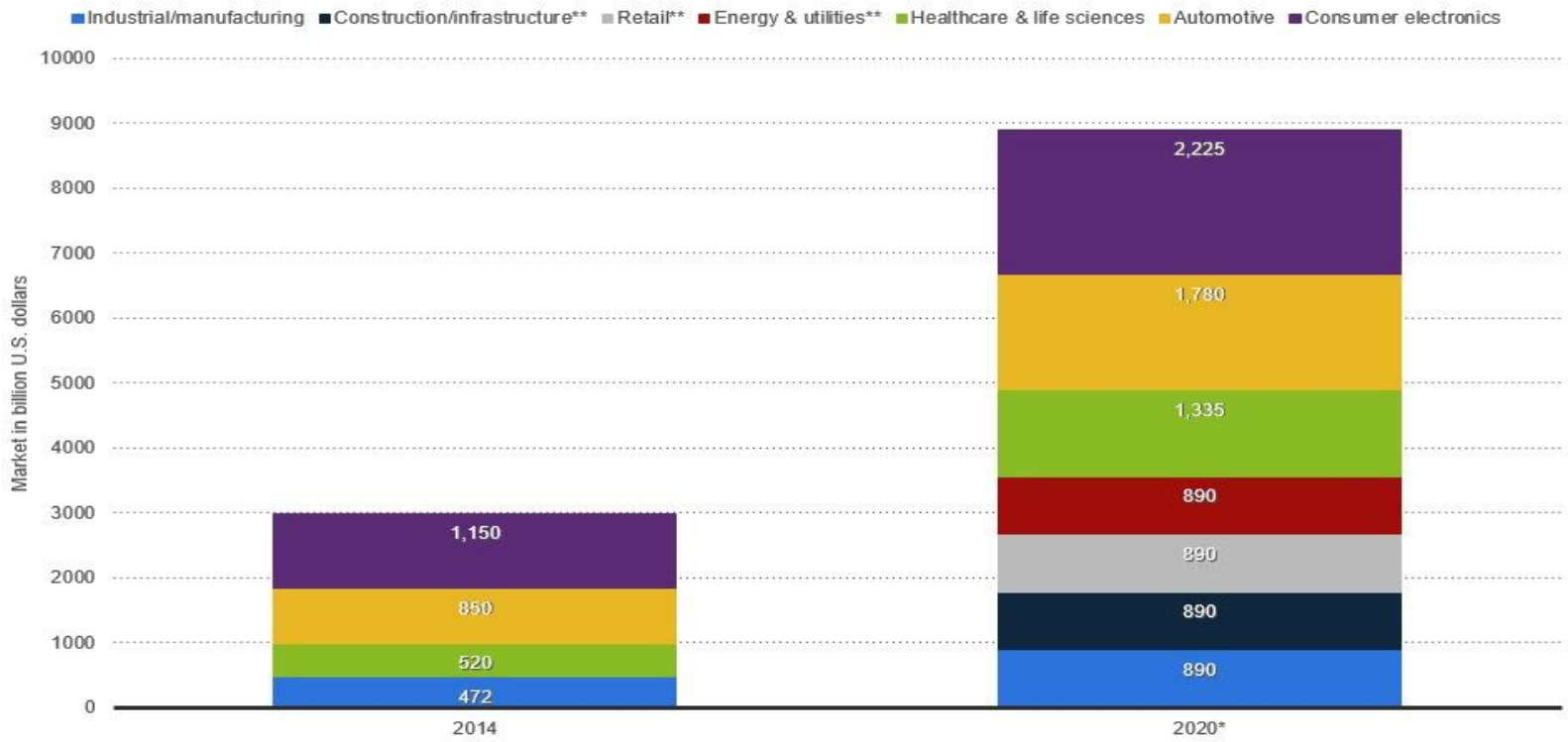


Source: IoT Developer Survey

VENCORELABS

Market Trends

Size of the Internet of Things market worldwide in 2014 and 2020, by industry (in billion U.S. dollars)

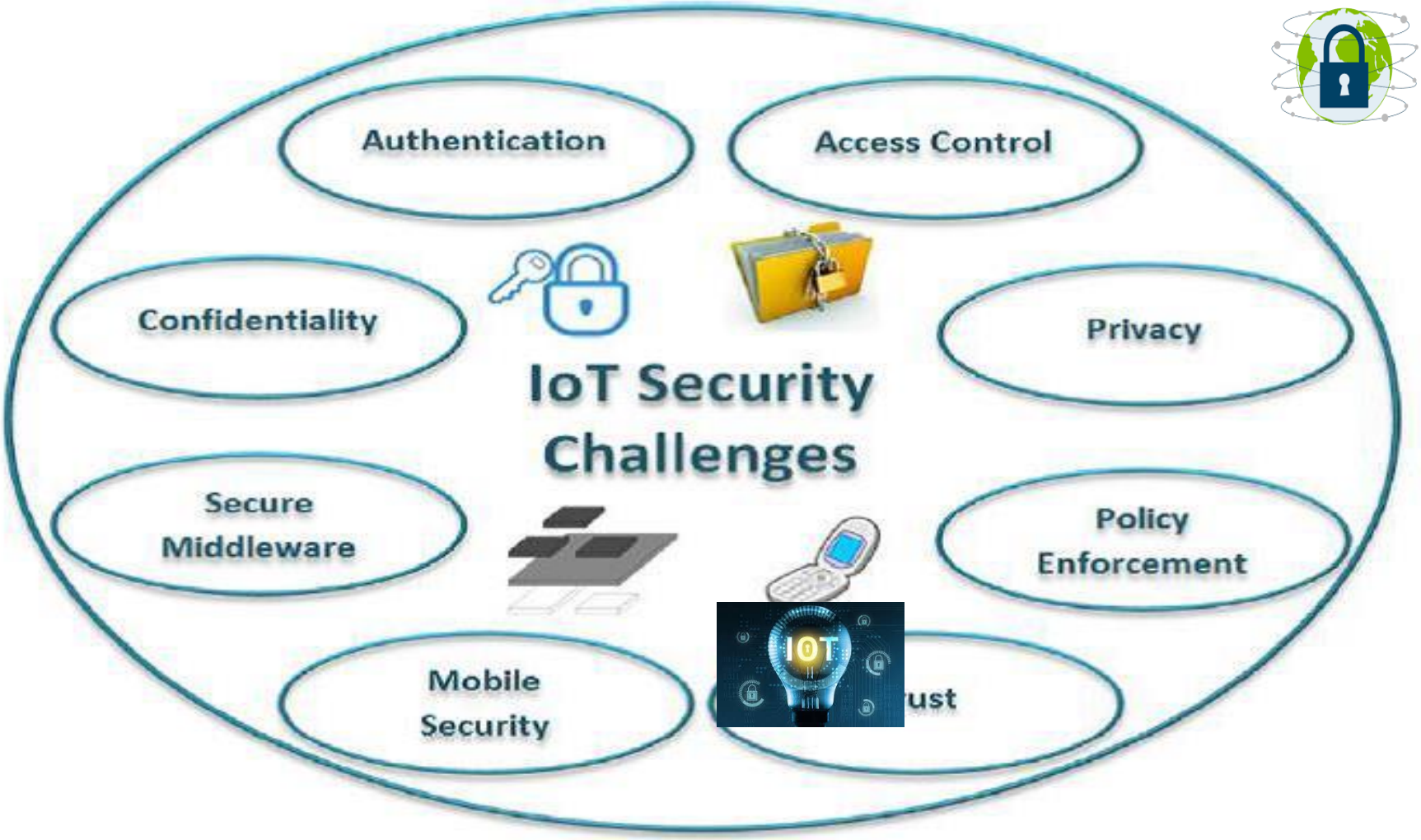


statista

Source: Forbes 2017 Roundup

VENCORELABS

Where are the Challenges?



Panel will Address and Discuss the Technologies and Challenges

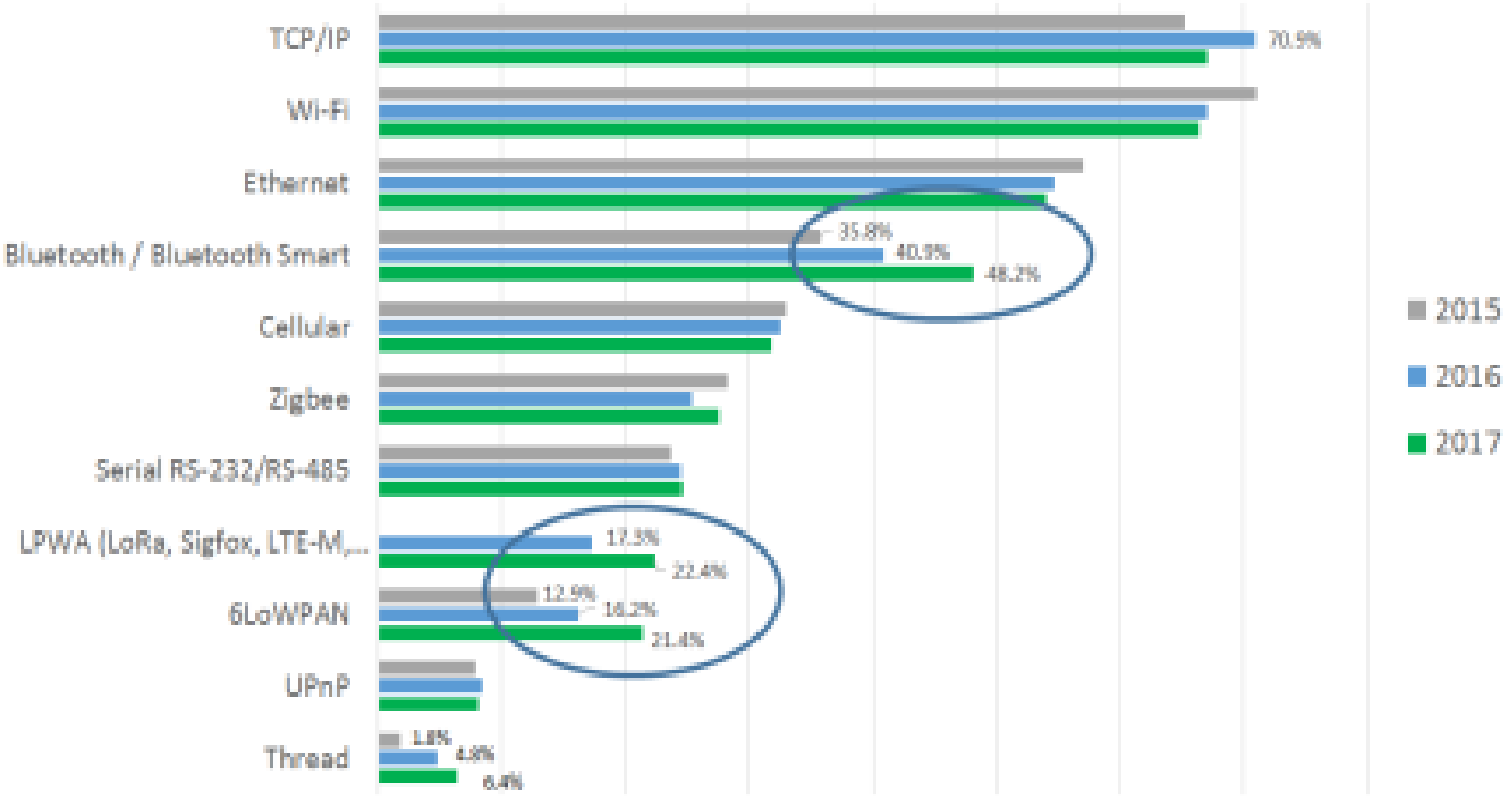
VENCORELABS

Why is it Difficult?

- Due to low cost and smaller memory foot-print, IoT devices have less security functionalities and knobs
- Lack of software updates exposes discovered weaknesses
- Many builders of IoT devices use the software from third party vendors without having much software security knowledge
  - In addition, lack of vendor support for repairing it
- Connected devices are easy to access via Internet due to weak access control mechanism
  - Some IoT device manufacturers put hidden access mechanisms
  - Proliferation of attack software over the Internet becomes easy
- Many IoT devices have wireless communication with no privacy
  - Wireless attack tools are becoming much more inexpensive

Not to mention, default credentials are hardcoded in many devices!

Technology/ Standards Trends



Source: IoT Developer Survey

VENCORELABS

What are the Design Principles?

- Build the security in, DO NOT add it later
- Try to keep security techniques simple but secure
- Use Standards as much as possible

VENCORELABS

What are the Design Rules ?

- Encrypt sensitive data in transit and data at rest
- Use standards-vetted cryptographic algorithms/ implementations
- Identity and access control management must be in place
- Understand the threat model of the use case
- Provision device identity, register user
- Authenticate the device/user and create the relationship
- Get authorization when necessary
- Ensure only necessary communication ports are open

What the Community should do?

- Product developers should
  - Have a red team audit the devices prior to commercial release
  - Force a credential change at the point of setup. (i.e., Devices will not work unless the default credentials are modified)
  - Require https if there's web access
  - Remove unneeded functionality
- End users should
  - Evaluate if the devices you are bringing into your network really need to be smart
  - Segment your network. If you do want IoT devices in your home or business, separate them from networks that contain sensitive information
  - Change the default credentials

What can we Assume/Predict?

- Given all the challenges, no single solution or Standards would fit for all
  - Heterogeneity will be a fact of life
  - Cost of the devices will be a key factor for adding stronger security and access controls
    - There will be always devices with no security!
- Attackers will make every attempt to attack or compromise the IoT devices
  - Some devices will have either inherent weakness or not have the latest security updates
- Common users will never know the vulnerabilities before they are being exploited

Can Early detection make the difference?

VENCORELABS

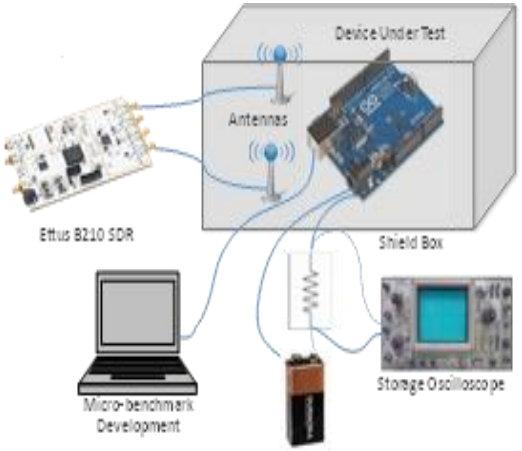
Problems with the Detection

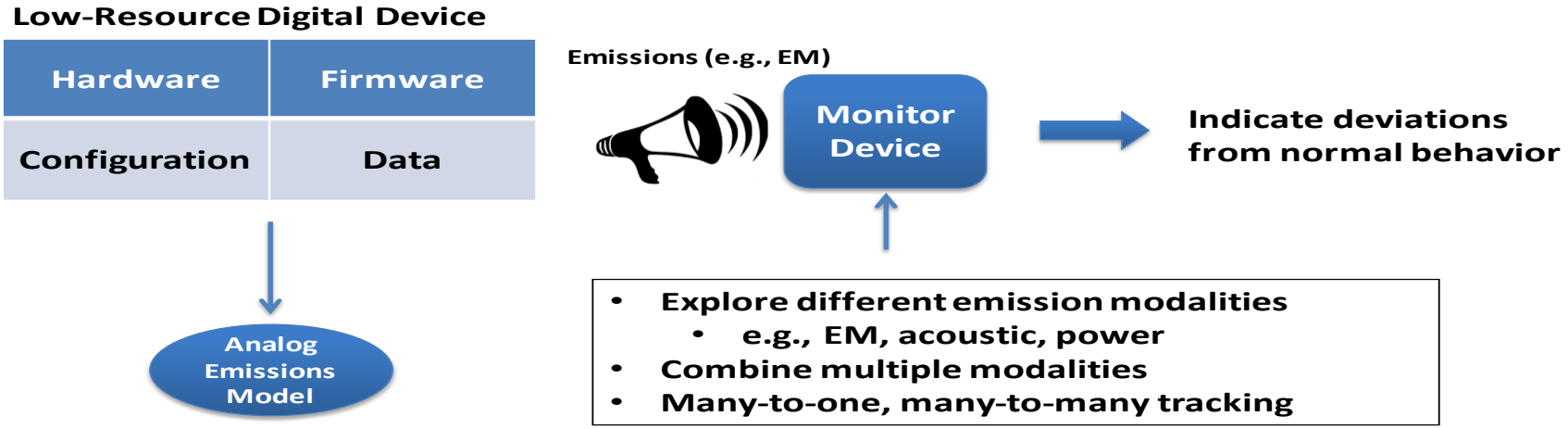
- Many IoT devices have no proper user interface (e.g., display, screen)
- Due to smaller memory foot-prints, it is hard to run the detection software (e.g., anti-malware/virus, scanning software)
- Many IoT devices may not be easily accessible after they are commissioned (e.g., Factory floor, Street light)
  - It may not be even cost effective to perform regular maintenance using traditional IT techniques
- Existing tools and methods are inadequate

Need new ways to detect the vulnerabilities!

An Approach to Dealing with Compromised Devices

- Detect attacks against IoT devices without touching the device
- Run security functions outside the IoT device so that they can be better protected
- Periodic diagnosis, health monitoring





VENCORE LABS

Thank you!