

CABLE-TEC EXPO® 2017

SCTE • ISBE

# THE NEXT BIG...

DEAL  
CONNECTION  
INNOVATION  
TECHNOLOGY  
LEADER  
NETWORK



DENVER, CO  
OCTOBER 17-20



IOT SECURITY: IS IT REALLY A RISK?

SCTE · ISBE

# Adapting Proven Technology to Counter IoT Threats

Petr Peterka  
Chief Technology Officer  
Verimatrix



DENVER, CO  
OCTOBER 17-20

# THEY TELL US IOT WILL BE BIG!

## Registered Vehicles with IoT Application by Region

World Market, Forecast: 2013 - 2030



**Machina Research: Consumer IoT will reach \$700 billion in annual revenue by 2022.**

Navio, a tech-focused research firm, has published a new report on the state of the IoT market, which is expected to grow at a CAGR of 31.72 percent from 2014-2022.

And given that IBM says that there are more than 9 billion connected devices operating today, and that those devices will generate 2.5 quintillion bytes of new data every day, which is expected to be increasingly difficult to manage, monitor and maintain, which will increase the cost of ownership of smart devices, the “Industrial Internet” has the potential to add \$10 to \$15 trillion (with a “T”) to global GDP over the next 20 years, and Cisco predicts that the number of smart devices will top 7 billion in 2022, up from 1.1 billion in 2013.

**Navigant Research: The worldwide smart device market will reach 1.1 billion in 2022.**

## More connectivity, more threats

New types of devices with low resources and large scale, enabling sustained DDoS attacks

### Massive DDoS Attack Against Dyn DNS Service Knocks Popular Sites Offline

Friday, October 21, 2016 Swati Khandelwal

[G+](#) 138 [Like](#) 20K [Share](#) 18.3K [Tweet](#) 3271 [in Share](#) 266 [Share](#) 22.2K



## More critical national infrastructure

A complex interconnected set of devices vulnerable to malware and DDoS attacks

TECHNOLOGY NEWS | Wed Jan 18, 2017 | 6:22am EST

### Ukraine's power outage was a cyber attack: Ukrenergo



Dispatchers are seen inside the control room of Ukraine's National power company Ukrenergo in Kiev, Ukraine, October 13, 2016. REUTERS/Valentyn Ogirenko

## Attack Types

Research

Hacktivist

Economic exploits

Terrorism and cyber warfare



## Four Levels of Threats



Nuisance level



Threats to business and brand



Threats to life



Threats to national security and critical infrastructure

## Light Bulb Attach

Fail: Insecure network joining

Threat: Control light remotely

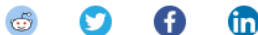
Security

81

### IoT worm can hack Philips Hue lightbulbs, spread across cities

Easy chain reaction hack would spread across Paris, boffins say

10 Nov 2016 at 06:02, Darren Pauli



Researchers have developed a proof-of-concept worm they say can rip through Philips Hue lightbulbs across entire cities – causing the insecure web-connected globes to flick on and off.

The software nasty, detailed in a paper titled *IoT Goes Nuclear: Creating a ZigBee Chain Reaction* [PDF], exploits hardcoded symmetric encryption keys to control devices over Zigbee wireless networks. This allows the malware to compromise a single light globe from up to 400 metres away.

[https://www.theregister.co.uk/2016/11/10/iot\\_worm\\_can\\_hack\\_philips\\_hue\\_lightbulbs\\_spread\\_across\\_cities/](https://www.theregister.co.uk/2016/11/10/iot_worm_can_hack_philips_hue_lightbulbs_spread_across_cities/)

## Smart Fridge Attack

Fail: Verifying validity of SSL certificate

Threat: Neighbor stealing Gmail credentials



[http://www.theregister.co.uk/2015/08/24/smart\\_fridge\\_security\\_fubar/](http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/)

## Connected TV Attack

Fail: Verify validity of SSL certificate

Threat: Impact on privacy



<http://arstechnica.com/security/2015/11/man-in-the-middle-attack-on-vizio-tvs-coughs-up-owners-viewing-habits>

## Connected Car Attack

Fail: No segmentation

Fail: No OTA update

Threat: Losing control in a driving car



<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

## Insulin Pump Vulnerability

Fail: Unencrypted Communications  
(plaintext commands)

Threat: Taking control of insulin delivery on  
the pump

<http://nypost.com/2016/12/29/yes-pacemakers-can-get-hacked>

## Other Examples

Pacemaker

Blood pressure monitors

<https://www.cyberscoop.com/johnson-and-johnson-insulin-pumps-hacked/>

## Johnson & Johnson warns insulin pumps can be hacked





## Vulnerabilities

- Nuclear installation
- Energy grids
- Water supply networks
- Communication services
- Transport systems
- Hospitals

## Cyber Attack on New York Dam Highlights the Dark Side of the Internet of Things

By [John Bonazzo](#) - 03/10/16 6:00pm



What would happen if U.S. infrastructure could be controlled through a computer screen? (Photo: Roslan Rahman/Getty Images)

The Obama administration will announce within the next week that a [2013 cyber attack](#) against a New York dam was perpetrated by Iranian hackers. The Department of Justice has prepared an indictment against those responsible,

[according to CNN.](#)

<http://observer.com/2016/03/cyber-attack-on-new-york-dam-highlights-the-dark-side-of-the-internet-of-things/>



IoT is not new



False idea that IoT needs completely security rethink



IoT security challenges can be met by existing technologies



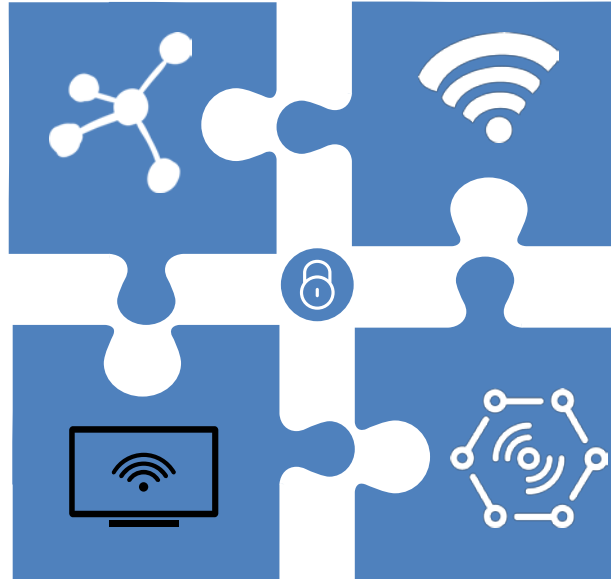
Connected security is now achievable on low powered IoT devices



# FOUR KEY ELEMENTS OF IOT SECURITY



Security of the  
Collected Data



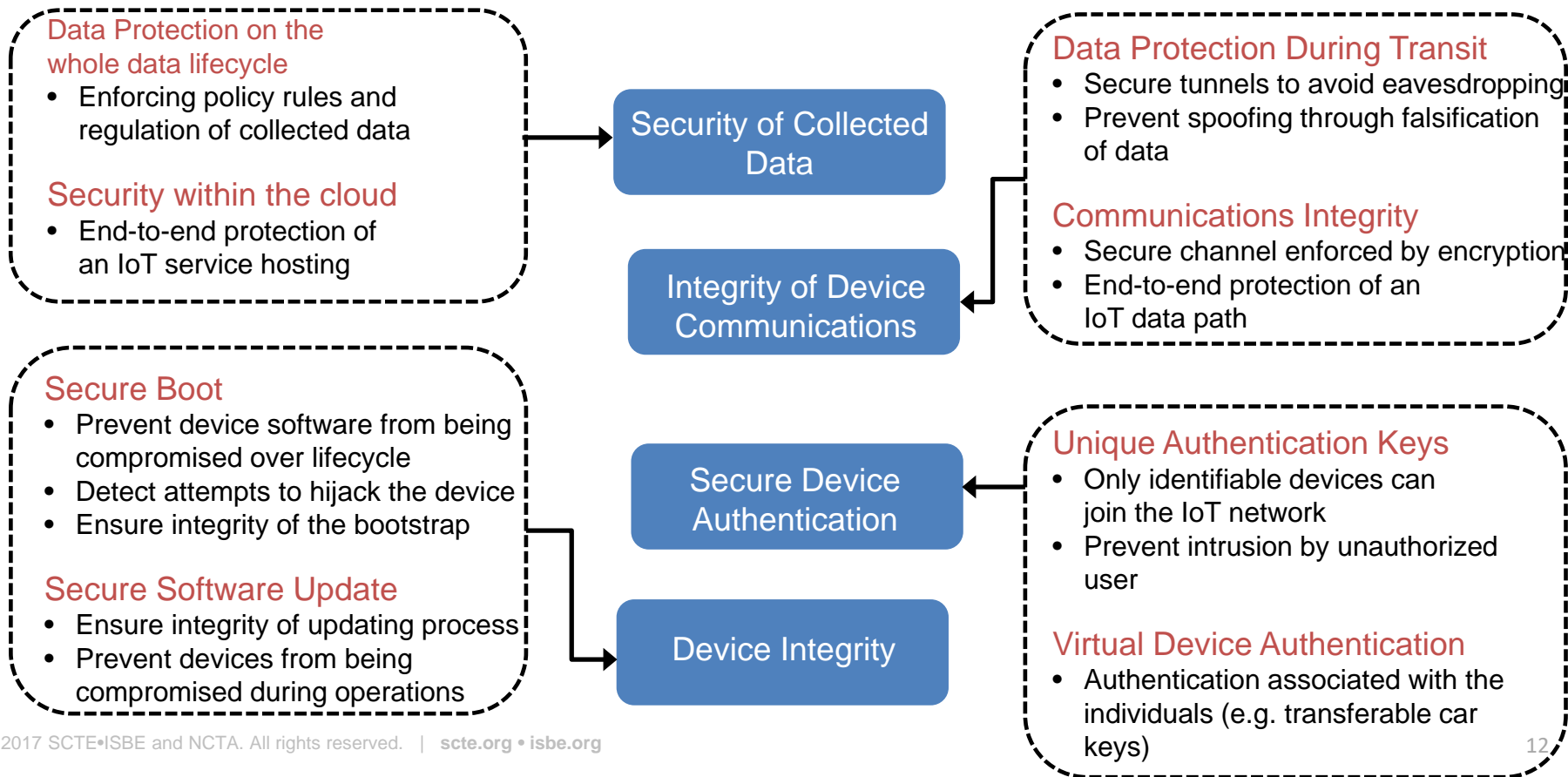
Integrity of Device  
Communications

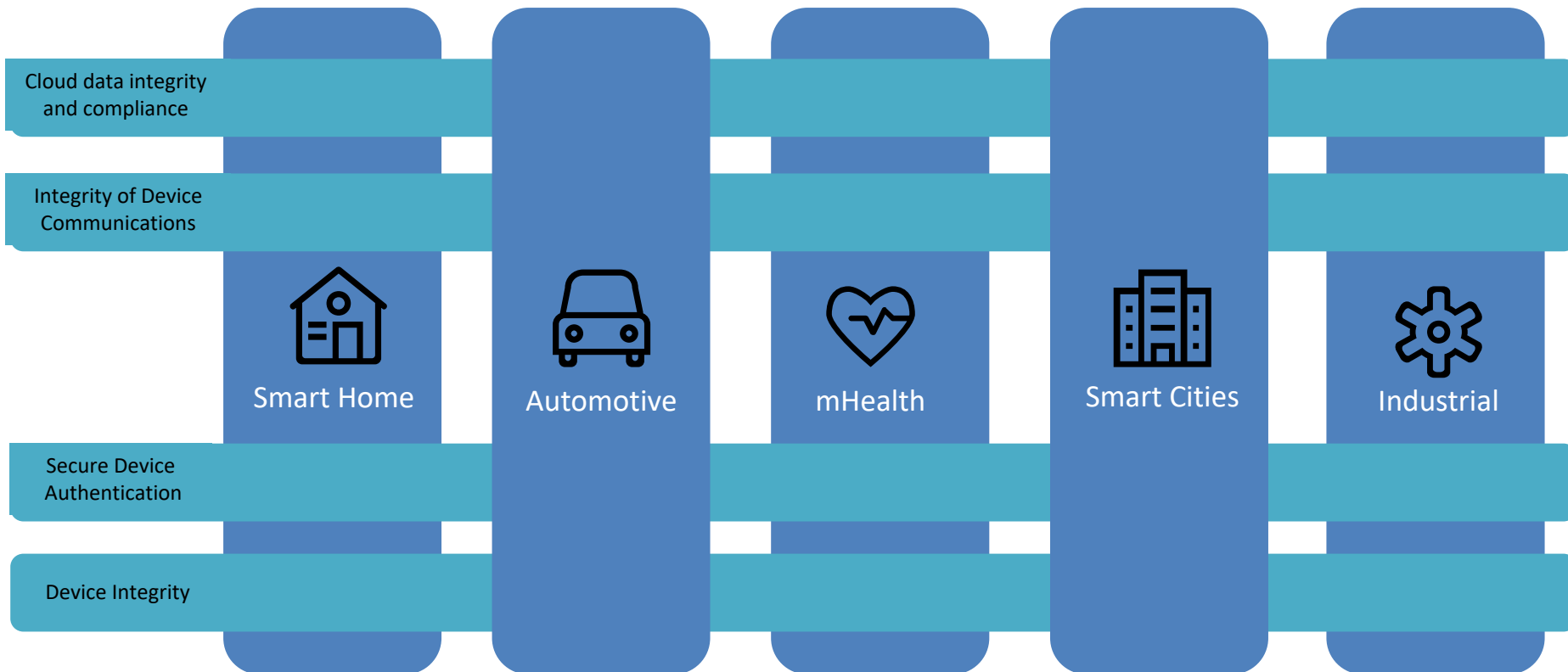


Device Integrity

Device or User  
Authentication







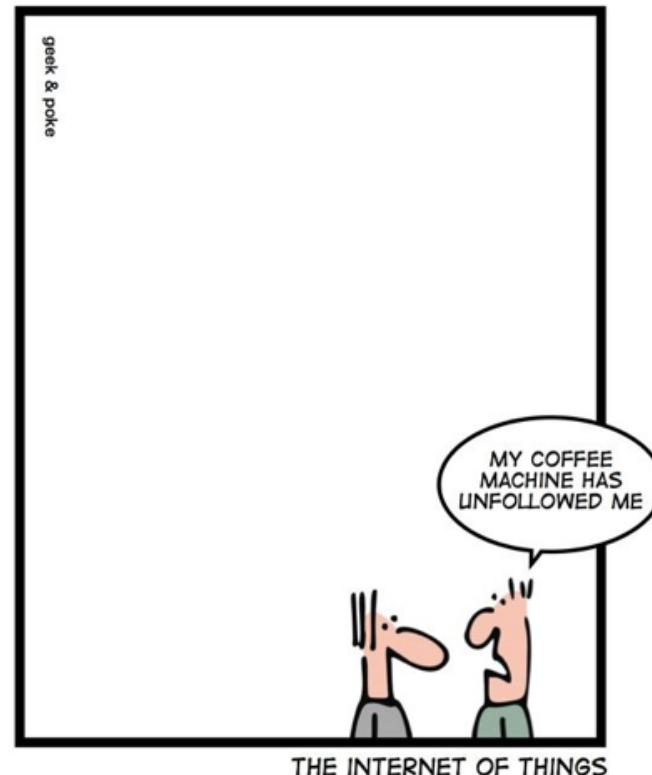
## Not just for Christmas - typical lifetime tasks

- Device credential management
- Secure software update
- Trusted secure IP communications – TCP, UDP, unicast, multicast
- Device threat monitoring
- Threat reporting/aggregation/alerting
- Secure Data repository with regulatory and policy compliance

Few in the industry with a broad, long-term track record

## Summary

- Threat surface of connected systems is extensive
- The security challenge exists over the lifetime of the application
- Look to best combination of innovation and system integrity



SCTE · ISBE

**THANK YOU!**

**Petr Peterka**

ppeterka@verimatrix.com

+1-858-677-7800 x4001



DENVER, CO  
OCTOBER 17-20

