BITS Pilani

Pilani Campus

# Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

BITS Pilani

Pilani Campus

## <SSCSZG570 , Cloud, IoT and Enterprise Security>

# Lecture No. 7: IoT Security – An Overview

**Source Disclaimer**: Content for some of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

# What we shall cover?

01 Context: IoT and its Verticals

02 Need for IoT Security

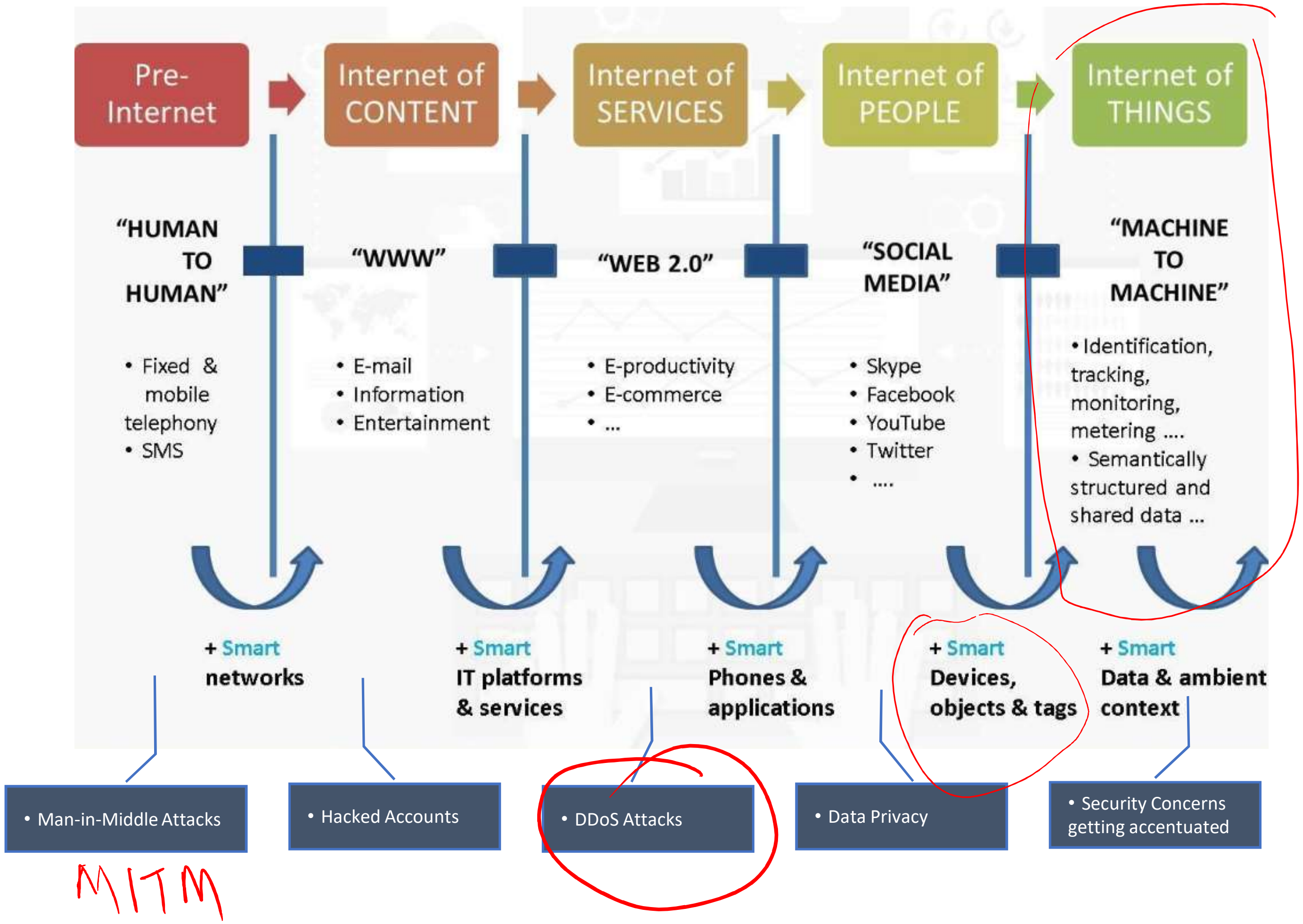
03 The Changing IoT Landscape and What it means for IoT Security

04 Security Practices for the IoT World

# RECAP:

# The Evolving Internet…. And the Evolving Security Concerns!

Image Source: https://twitter.com/GrowUrStartup/status/968870972471341057



- Man-in-Middle Attacks
- Hacked Accounts
- DDoS Attacks
- Data Privacy
- Security Concerns getting accentuated

MITM

# IoT is Everywhere

**HEALTH** BODY

- Patient care
- Patient surveillance
- Elderly monitoring
- Fall detection
- Remote diagnostic Equipment monitoring
- Hospital hygiene
- Bio wearables
- Food sensors

**HOME** CONSUMER

- Thermostats
- Lighting
- Remote control appliances
- Detection (intrusion /smoke)
- Energy / water monitoring
- Infotainment
- Pet feeding

**TRANSPORT** MOBILITY

- Smart car
- Traffic routing
- Telematics
- Package monitoring
- Smart parking
- Insurance adjustments
- Supply chain
- Shipping
- Public transport
- Airlines
- Trains

**CITIES** URBAN PLANNING

- Smart lighting
- Waste management
- Maintenance
- Surveillance
- Signage
- Utilities / Smart grid
- Emergency services

**INDUSTRY** INFRASTRUCTURE

- Heat, ventilation and air conditioning
- Security
- Smart lighting
- Transit
- Emergency alerts
- Structural integrity
- Occupancy
- Energy credits

Image Source: https://www.slideshare.net/akabhay/internet-of-things-the-battle-for-your-home-commute-and-life

SCADA

N/W

PLC

Sensors

R

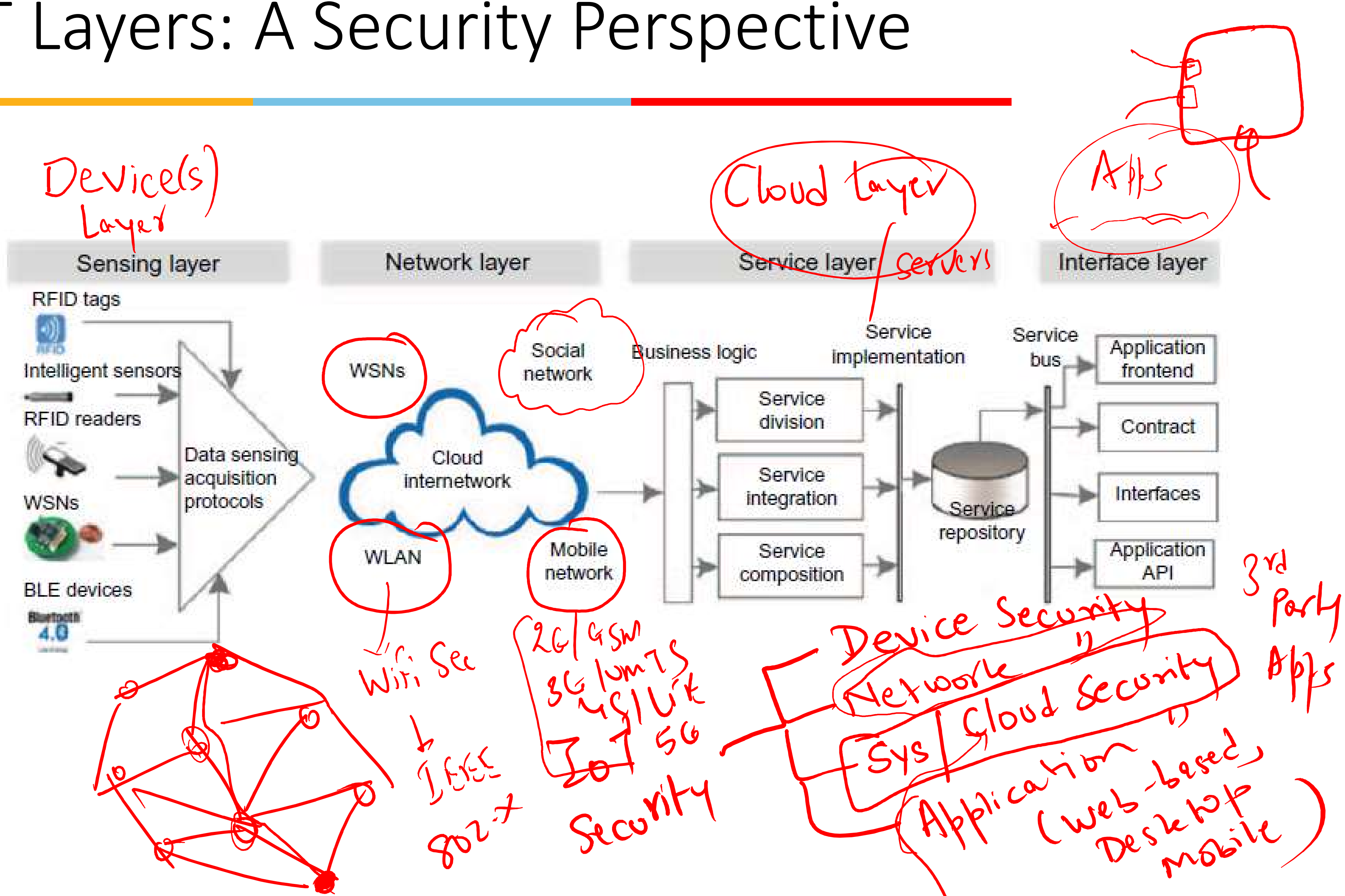
Actuators

Cntrl

TCU
SIM

AMI
=
IIoT

# IoT Layers: A Security Perspective



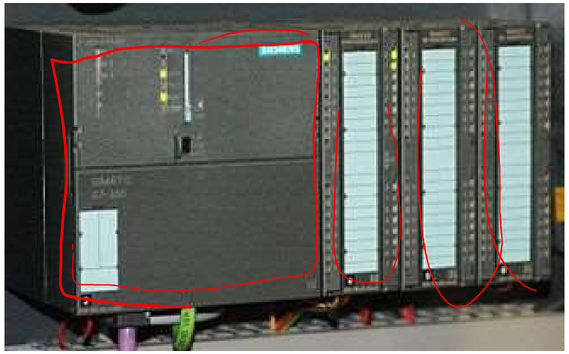
Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

# The Stuxnet Attack!

IIoT

Industry 4.0

- Discovered in 2010
- Targeted Attack (Microsoft Windows OS → Siemens Step 7 software)
- Compromised Iranian PLCs, causing fast spinning centrifuges to tear themselves apart
- Ruined almost one-fifth of Iran's Nuclear Centrifuges
- Overall, infected 200,000 computers, 1000 machines



Siemens Simatic S7-300 PLC CPU with three I/O modules attached

| Affected Country | Share of infected computers |
|---|---|
| Iran | 58.85% |
| Indonesia | 18.22% |
| India | 8.31% |
| Azerbaijan | 2.57% |
| United States | 1.56% |
| Pakistan | 1.28% |
| Other countries | 9.2% |

PLCs

1100pm

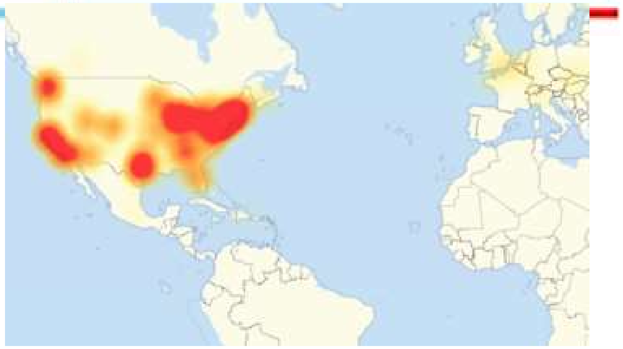
URL | FQDN → IP Addr

172.16.8.5

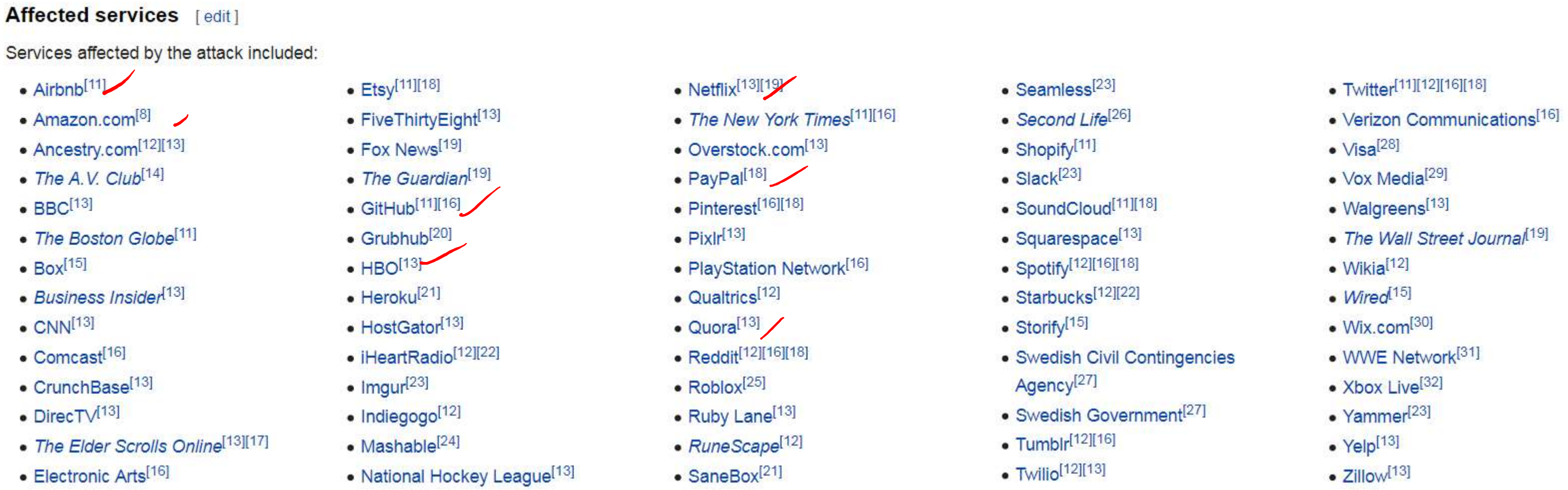
# How Safe Are IoT Devices?

- **The 2016 Dyn DNS Service DDoS Attack**
- Orchestrated via IoT devices like printers, IP cameras, home gateways etc
- Tens of millions of remotely controlled IoT devices used in attack
- IoT devices were infected by the Mirai malware
- With an estimated load of 1.2 terabits per second, the attack is, according to experts, the largest DDoS on record

Source: http://downdetector.com/status/level3



Map of areas most affected by attack, 16:45 UTC, 21 October 2016.



**Affected services** [ edit ]

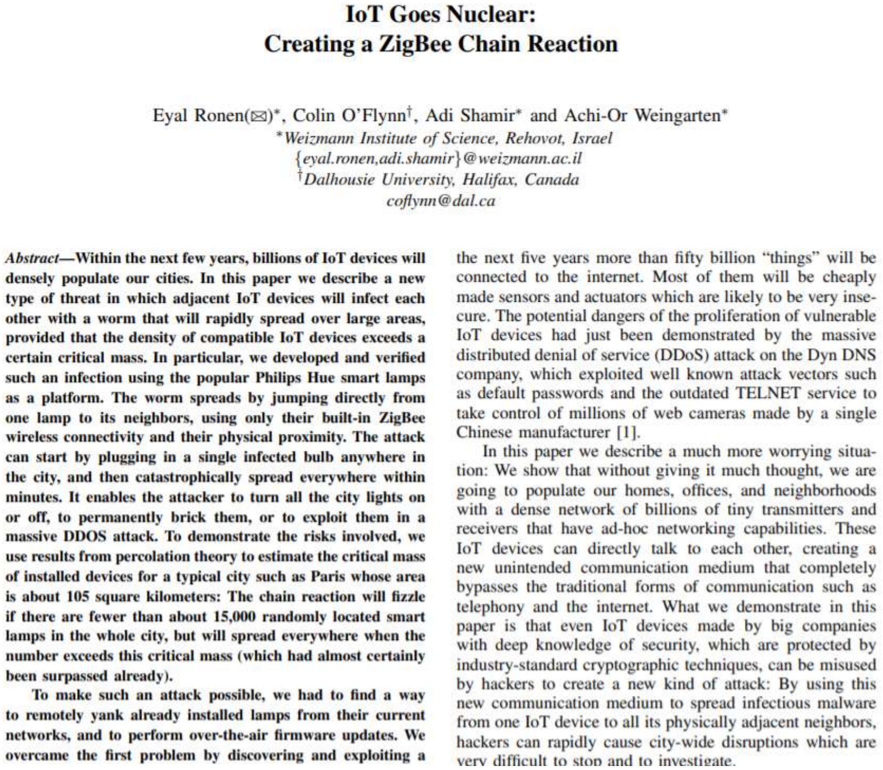
Services affected by the attack included:

- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

Source: Wikipedia

# How Safe Are IoT Devices?

RSA



## IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*
*Weizmann Institute of Science, Rehovot, Israel
{eyal.ronen,adi.shamir}@weizmann.ac.il
†Dalhousie University, Halifax, Canada
coflynn@dal.ca

***Abstract*—Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will rapidly spread over large areas, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes. It enables the attacker to turn all the city lights on or off, to permanently brick them, or to exploit them in a massive DDOS attack. To demonstrate the risks involved, we use results from percolation theory to estimate the critical mass of installed devices for a typical city such as Paris whose area is about 105 square kilometers: The chain reaction will fizzle if there are fewer than about 15,000 randomly located smart lamps in the whole city, but will spread everywhere when the number exceeds this critical mass (which had almost certainly been surpassed already).**

**To make such an attack possible, we had to find a way to remotely yank already installed lamps from their current networks, and to perform over-the-air firmware updates. We overcome the first problem by discovering and exploiting a**

the next five years more than fifty billion "things" will be connected to the internet. Most of them will be cheaply made sensors and actuators which are likely to be very insecure. The potential dangers of the proliferation of vulnerable IoT devices had just been demonstrated by the massive distributed denial of service (DDoS) attack on the Dyn DNS company, which exploited well known attack vectors such as default passwords and the outdated TELNET service to take control of millions of web cameras made by a single Chinese manufacturer [1].

In this paper we describe a much more worrying situation: We show that without giving it much thought, we are going to populate our homes, offices, and neighborhoods with a dense network of billions of tiny transmitters and receivers that have ad-hoc networking capabilities. These IoT devices can directly talk to each other, creating a new unintended communication medium that completely bypasses the traditional forms of communication such as telephony and the internet. What we demonstrate in this paper is that even IoT devices made by big companies with deep knowledge of security, which are protected by industry-standard cryptographic techniques, can be misused by hackers to create a new kind of attack: By using this new communication medium to spread infectious malware from one IoT device to all its physically adjacent neighbors, hackers can rapidly cause city-wide disruptions which are very difficult to stop and to investigate.

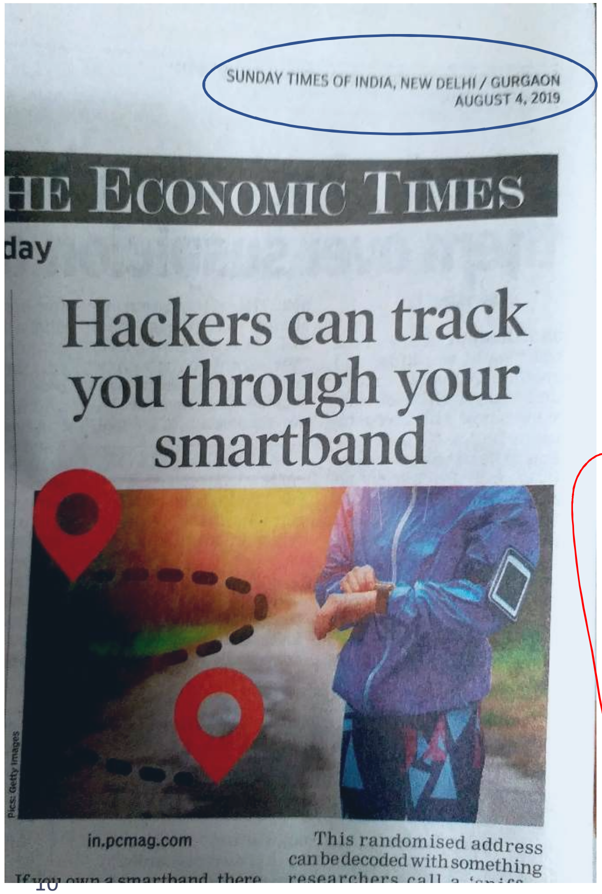
E. Ronen, A. Shamir, A. Weingarten and C. O'Flynn, *"IoT Goes Nuclear: Creating a ZigBee Chain Reaction*," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 195-212.
doi: 10.1109/SP.2017.14

In the same period as the Dyn Attack, researchers uncovered a flaw in the radio protocol Zigbee.

- Demonstrated using an aerial drone to target a set of smart Philips light bulbs in an office tower
- Infected the bulbs with a virus that let the attackers to turn the lights on and off flashing an "SOS" message in Morse code
- This malware was also able to spread like a pathogen among the devices neighbors.

# How Safe Are IoT Devices?

https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/amp/



SUNDAY TIMES OF INDIA, NEW DELHI / GURGAON
AUGUST 4, 2019

HE ECONOMIC TIMES

day

Hackers can track you through your smartband

Pics: Getty Images

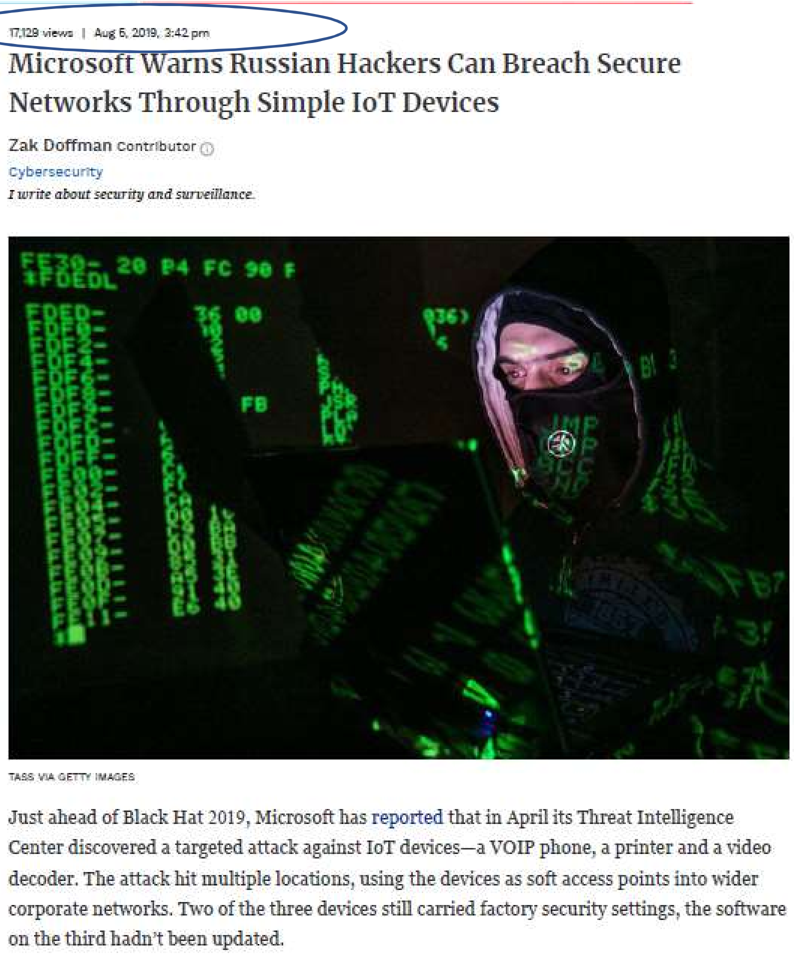
in.pcmag.com

This randomised address can be decoded with something researchers call a 'unifo

If you own a smartband, there

- Findings from a group of researchers in Boston University
- Location Tracking by exploiting a Bluetooth Vulnerability
- Pose issues related to
  - Personal Security
  - Stalking
  - Abuse

- Findings from Microsoft Threat Intelligence Center in April 2019
- Discovered a targeted attack against IoT devices—a VOIP phone, a printer and a video decoder
- Attack hit multiple locations, using the devices as soft access points into wider corporate networks



17,129 views | Aug 5, 2019, 3:42 pm

Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices

Zak Doffman Contributor

Cybersecurity

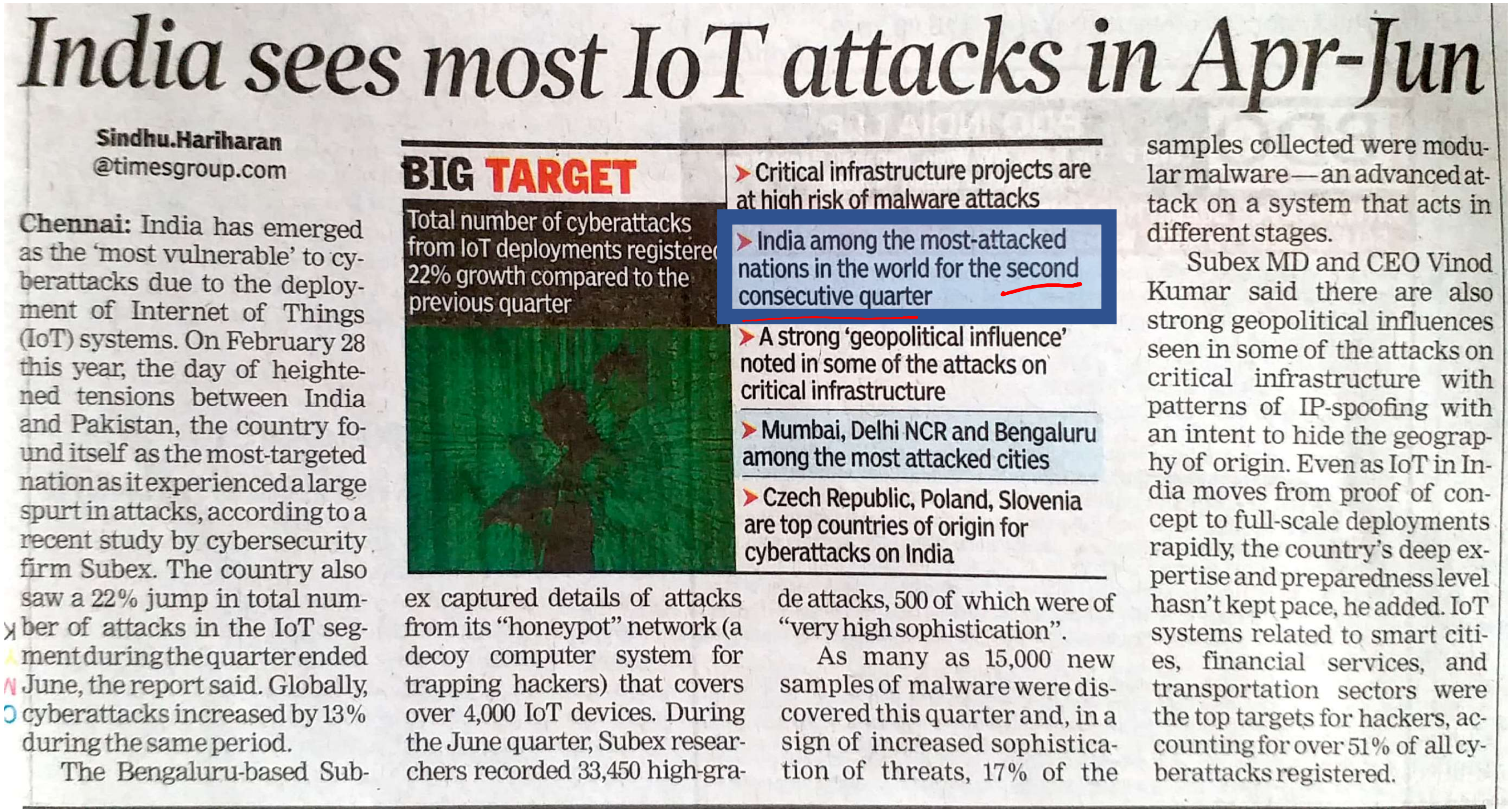
*I write about security and surveillance.*

TASS VIA GETTY IMAGES

Just ahead of Black Hat 2019, Microsoft has reported that in April its Threat Intelligence Center discovered a targeted attack against IoT devices—a VOIP phone, a printer and a video decoder. The attack hit multiple locations, using the devices as soft access points into wider corporate networks. Two of the three devices still carried factory security settings, the software on the third hadn't been updated.

# How Safe Are IoT Devices?

**August 13, 2019** Times of India



## India sees most IoT attacks in Apr-Jun

Sindhu.Hariharan
@timesgroup.com

**BIG TARGET**

Total number of cyberattacks from IoT deployments registered 22% growth compared to the previous quarter

- Critical infrastructure projects are at high risk of malware attacks
- India among the most-attacked nations in the world for the second consecutive quarter
- A strong 'geopolitical influence' noted in some of the attacks on critical infrastructure
- Mumbai, Delhi NCR and Bengaluru among the most attacked cities
- Czech Republic, Poland, Slovenia are top countries of origin for cyberattacks on India

**Chennai:** India has emerged as the 'most vulnerable' to cyberattacks due to the deployment of Internet of Things (IoT) systems. On February 28 this year, the day of heightened tensions between India and Pakistan, the country found itself as the most-targeted nation as it experienced a large spurt in attacks, according to a recent study by cybersecurity firm Subex. The country also saw a 22% jump in total number of attacks in the IoT segment during the quarter ended June, the report said. Globally, cyberattacks increased by 13% during the same period.

The Bengaluru-based Subex captured details of attacks from its "honeypot" network (a decoy computer system for trapping hackers) that covers over 4,000 IoT devices. During the June quarter, Subex researchers recorded 33,450 high-grade attacks, 500 of which were of "very high sophistication".

As many as 15,000 new samples of malware were discovered this quarter, and in a sign of increased sophistication of threats, 17% of the samples collected were modular malware—an advanced attack on a system that acts in different stages.

Subex MD and CEO Vinod Kumar said there are also strong geopolitical influences seen in some of the attacks on critical infrastructure with patterns of IP-spoofing with an intent to hide the geography of origin. Even as IoT in India moves from proof of concept to full-scale deployments rapidly, the country's deep expertise and preparedness level hasn't kept pace, he added. IoT systems related to smart cities, financial services, and transportation sectors were the top targets for hackers, accounting for over 51% of all cyberattacks registered.

# Recent, back home....

Tuesday, March 02, 2021

Hindustan Times

FIRST VOICE. LAST WORD.

Over 5mn sign up on Day 1 as vaccine drive enters Phase 2

Modi begins next leg with Covaxin shot, urges others to get vaccinated

NOT APP BUT SITE: CO-WIN MIX-UP AFFECTS MANY

Residents wary amid spate of crime in city

BODY OF DALIT GIRL, 17, FOUND IN ALIGARH FIELD

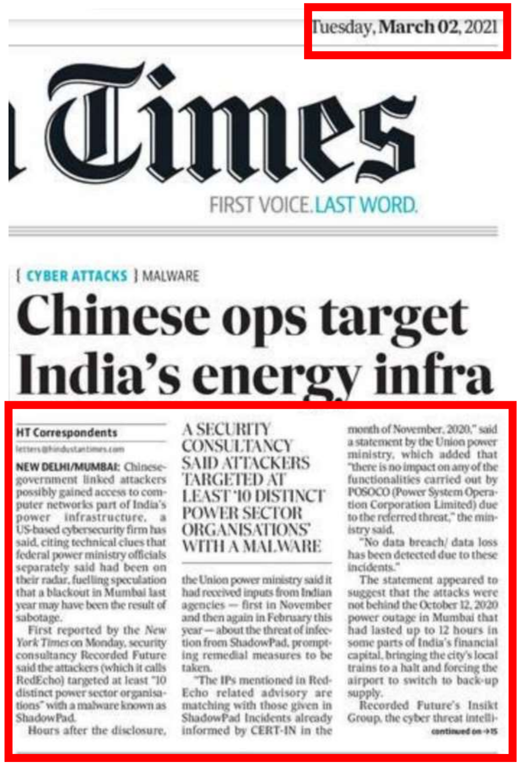
project still stuck, another begins at choked Ashram

WILL YOU MARRY HER, SC ASKS RAPE CASE ACCUSED

URBAN JOBLESS RATE BELOW 7% FOR FIRST TIME IN 2 YRS

Global rise in food prices benefits Indian farmers but domestic inflation could hit recovery: Experts

COVID-19 VACCINATION
One year of Covid-19
Tracking the virus
KAMA AYURVEDA
THE PROMISE OF BRINGADI
CLINICALLY PROVEN* TO REDUCE HAIRFALL
HELPS PREVENT SCALP INFECTIONS
BOOSTS LUSH HAIR GROWTH



Tuesday, March 02, 2021

Times

FIRST VOICE. LAST WORD.

[ CYBER ATTACKS ] MALWARE

## Chinese ops target India's energy infra

HT Correspondents

letters@hindustantimes.com

**NEW DELHI/MUMBAI:** Chinese-government linked attackers possibly gained access to computer networks part of India's power infrastructure, a US-based cybersecurity firm has said, citing technical clues that federal power ministry officials separately said had been on their radar, fuelling speculation that a blackout in Mumbai last year may have been the result of sabotage.

First reported by the *New York Times* on Monday, security consultancy Recorded Future said the attackers (which it calls RedEcho) targeted at least "10 distinct power sector organisations" with a malware known as ShadowPad.

Hours after the disclosure, the Union power ministry said it had received inputs from Indian agencies — first in November and then again in February this year — about the threat of infection from ShadowPad, prompting remedial measures to be taken.

A SECURITY CONSULTANCY SAID ATTACKERS TARGETED AT LEAST '10 DISTINCT POWER SECTOR ORGANISATIONS' WITH A MALWARE

"The IPs mentioned in RedEcho related advisory are matching with those given in ShadowPad Incidents already informed by CERT-IN in the month of November, 2020," said a statement by the Union power ministry, which added that "there is no impact on any of the functionalities carried out by POSOCO (Power System Operation Corporation Limited) due to the referred threat," the ministry said.

"No data breach/ data loss has been detected due to these incidents."

The statement appeared to suggest that the attacks were not behind the October 12, 2020 power outage in Mumbai that had lasted up to 12 hours in some parts of India's financial capital, bringing the city's local trains to a halt and forcing the airport to switch to back-up supply.

Recorded Future's Insikt Group, the cyber threat intelli-

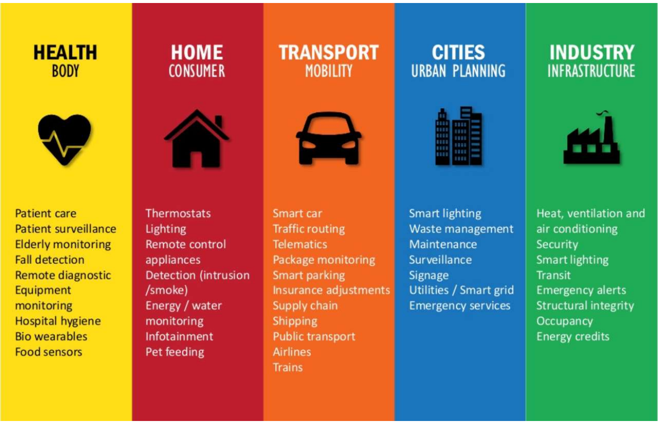
continued on →15

March 02, 2021

- Chinese attackers gained access to computer networks in India's power infrastructure
- Speculation that last year Mumbai power outage may be a result of this sabotage
- Malware known as ShadowPad
- Targeted at least 10 district power sector organizations

# Why IoT Security?

- Rapid Growth of IoT Devices and Solutions
- TTM pressures leading to security compromises
- Robust Security and Data Privacy are key for Businesses to survive
- Data / Information Loss can lead to far reaching consequences



**HEALTH**
BODY

Patient care
Patient surveillance
Elderly monitoring
Fall detection
Remote diagnostic Equipment monitoring
Hospital hygiene
Bio wearables
Food sensors

**HOME**
CONSUMER

Thermostats
Lighting
Remote control appliances
Detection (intrusion /smoke)
Energy / water monitoring
Infotainment
Pet feeding

**TRANSPORT**
MOBILITY

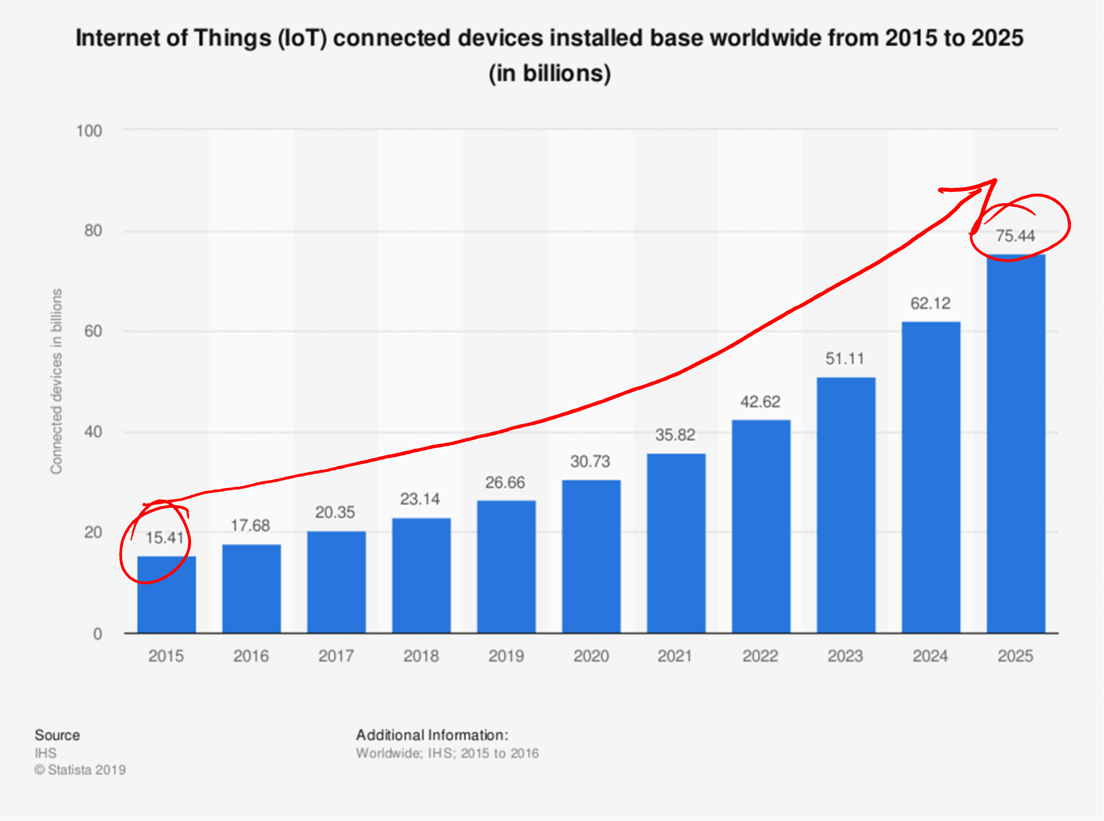
Smart car
Traffic routing
Telematics
Package monitoring
Smart parking
Insurance adjustments
Supply chain
Shipping
Public transport
Airlines
Trains

**CITIES**
URBAN PLANNING

Smart lighting
Waste management
Maintenance
Surveillance
Signage
Utilities / Smart grid
Emergency services

**INDUSTRY**
INFRASTRUCTURE

Heat, ventilation and air conditioning
Security
Smart lighting
Transit
Emergency alerts
Structural integrity
Occupancy
Energy credits

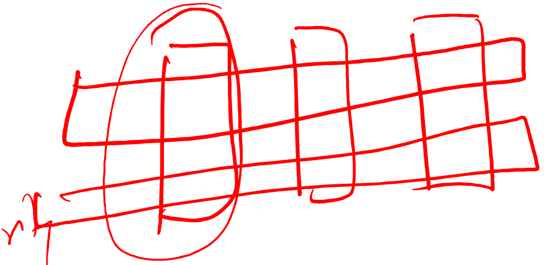


Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

Source
IHS
© Statista 2019

Additional Information:
Worldwide; IHS; 2015 to 2016

Image Source: https://www.slideshare.net/akabhay/internet-of-things-the-battle-for-your-home-commute-and-life



Data security

# IoT Security: Involved Domains

- Device Security
  - ➢ Securing the IoT Device
  - ➢ **Challenges**: Limited System Resources

Power

Computational ability

Storage

- Network Security
  - ➢ Security the network connecting IoT Devices to Backend Systems
  - ➢ **Challenges**: Wider range of devices + communication protocols + standards
- Cloud/ Back-end Systems Security
  - ➢ Securing the backend Applications from attacks
  - ➢ Firewalls, Security Gateways, IDS/IPS
- Mutual Authentication
  - ➢ Device(s) ←→ User(s)
  - ➢ Passwords, PINs, Multi-factor, Digital Certificates

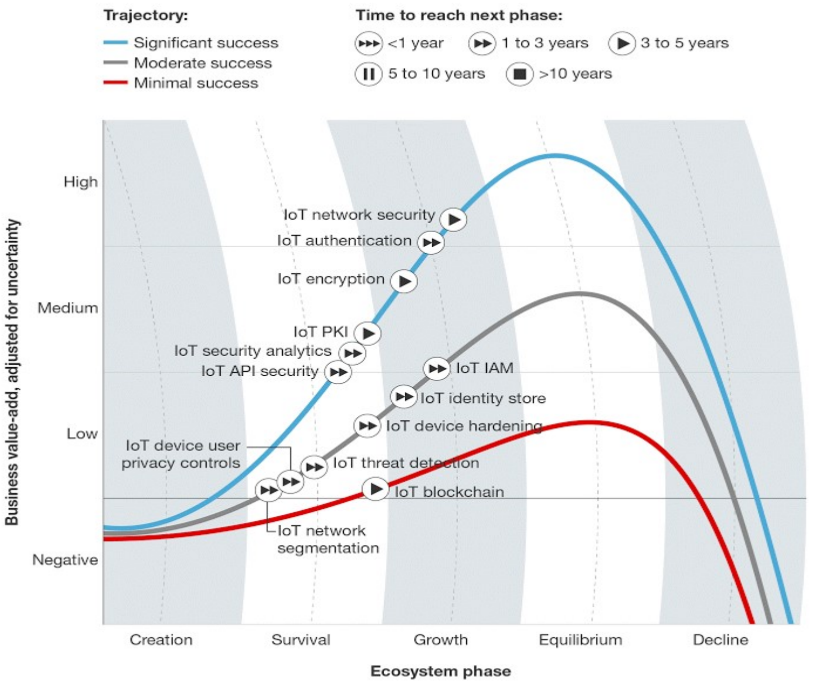
Cloud security

- Encryption
  - ➢ Data Integrity for data at rest and in transit
  - ➢ Strong Key Management Processes

FORRESTER® RESEARCH

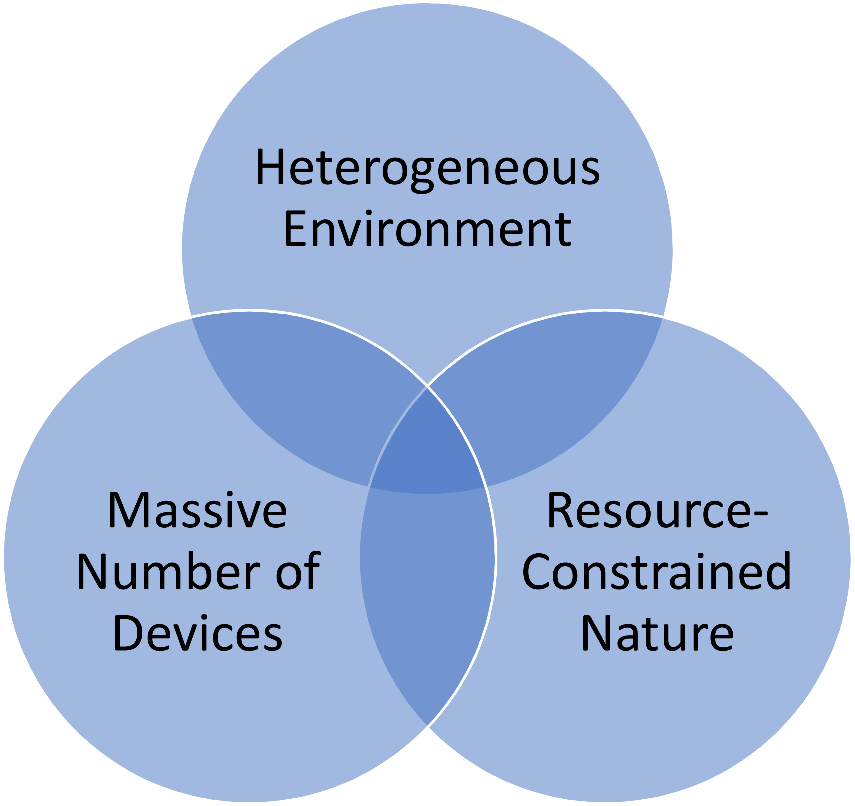
**TechRadar™: Internet Of Things Security, Q1 '17**

*TechRadar™: Internet Of Things Security, Q1 2017*



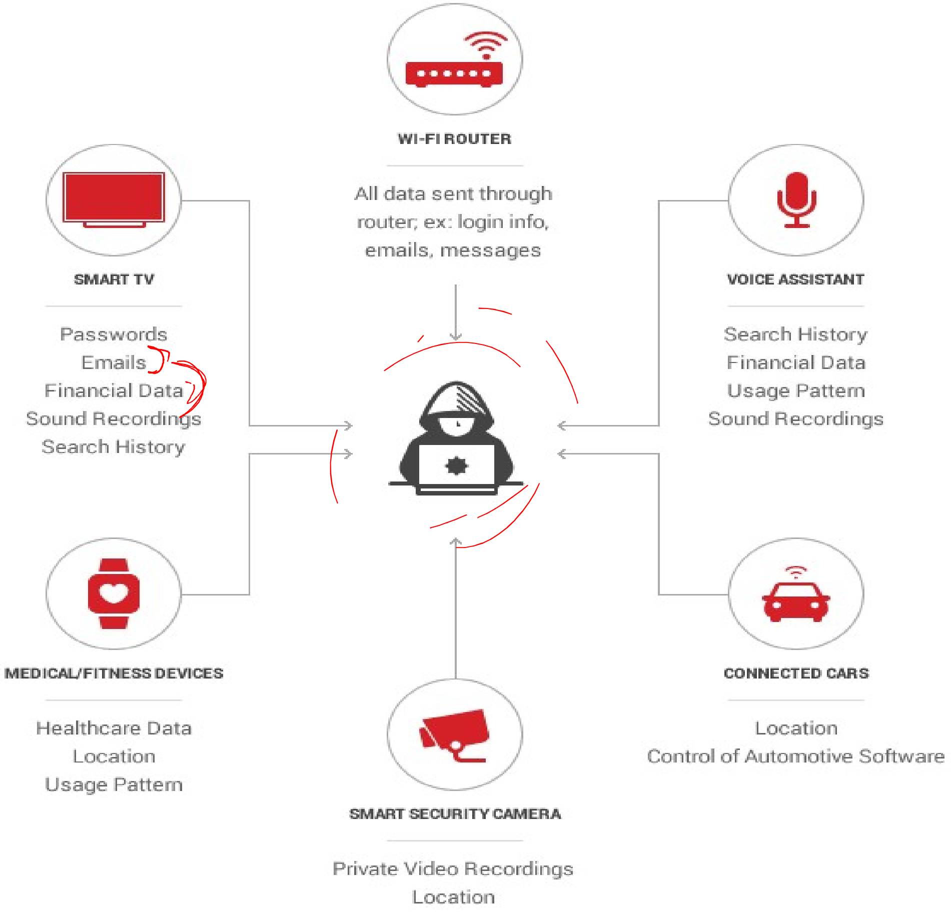
117394 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

# IoT Device Security : Key Focus Area in IoT Security


Heterogeneous Environment
Massive Number of Devices
Resource-Constrained Nature

# Data Privacy Issues with IoT Devices

**Information a malicious hacker can obtain from an IoT device**



WI-FI ROUTER

All data sent through router; ex: login info, emails, messages

SMART TV

Passwords
Emails
Financial Data
Sound Recordings
Search History

VOICE ASSISTANT

Search History
Financial Data
Usage Pattern
Sound Recordings

MEDICAL/FITNESS DEVICES

Healthcare Data
Location
Usage Pattern

CONNECTED CARS

Location
Control of Automotive Software

SMART SECURITY CAMERA

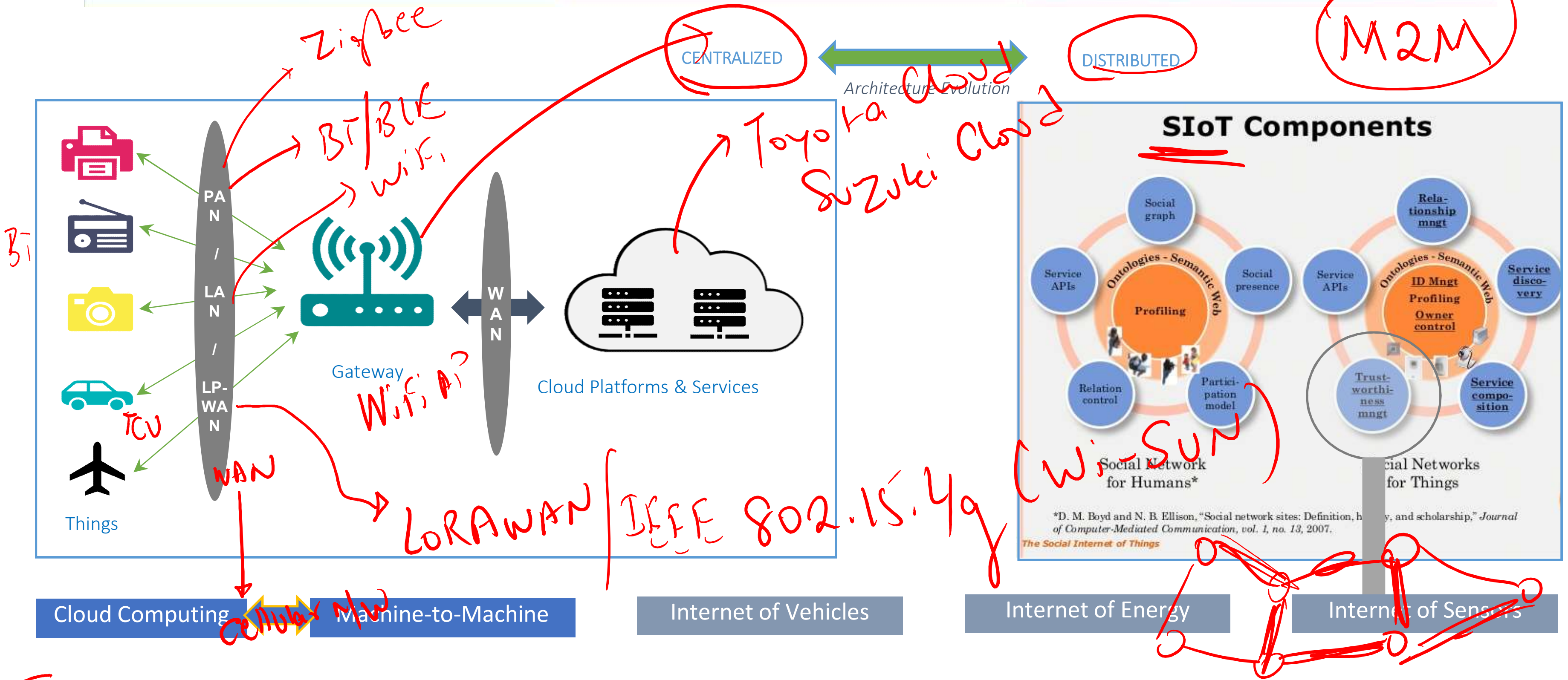
Private Video Recordings
Location

Source: HEIMDAL SECURITY

SCADA

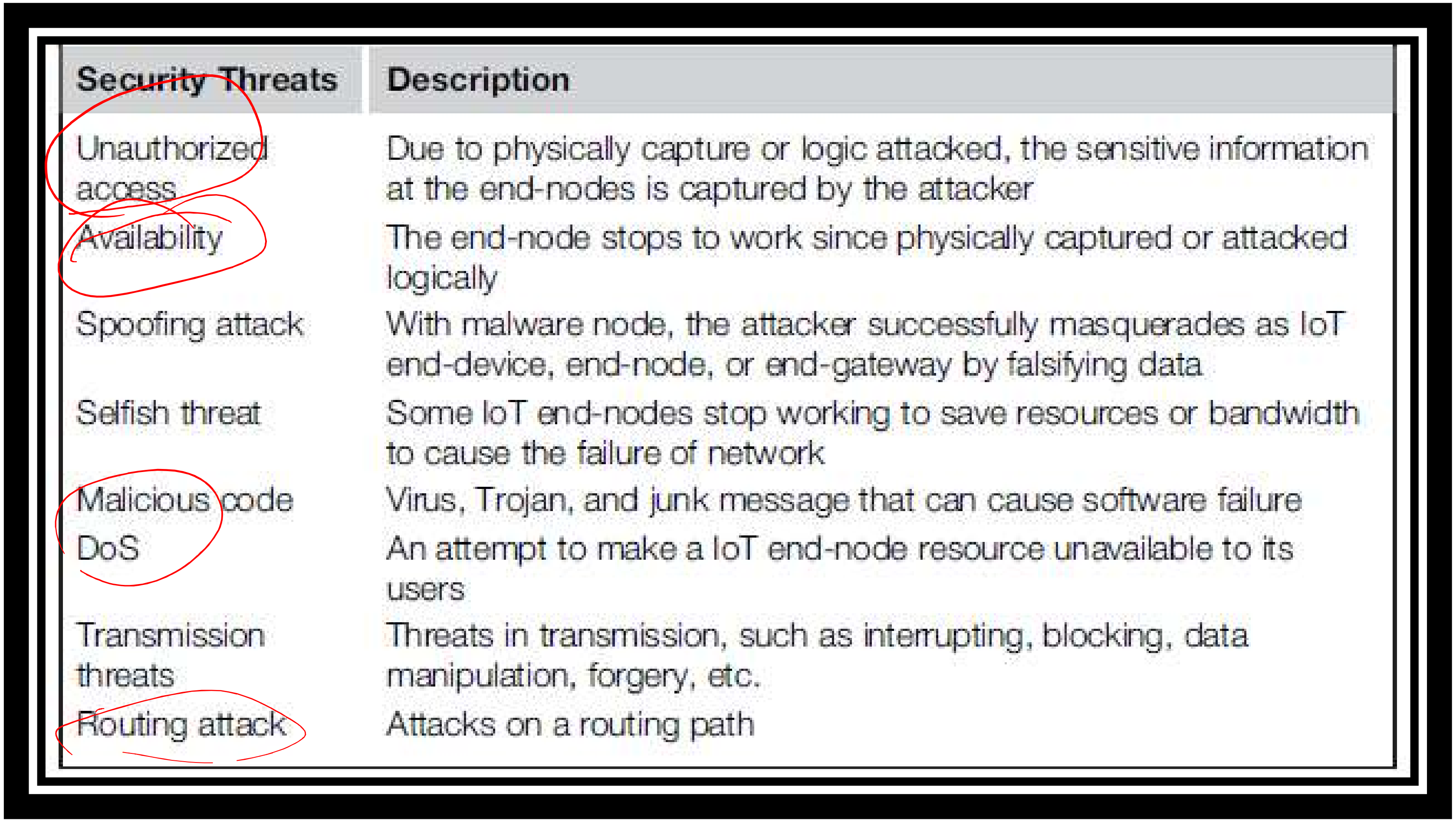
P2P

# IoT Architectures – The Evolving Landscape!



- *"The way to secure the Internet of Things is to allow the self-organizing migration of services away from a central cloud alone and into local infrastructure ecosystems where they can act independently"* - https://www.scmagazineuk.com/doriot-project-secure-internet-things/article/1590701

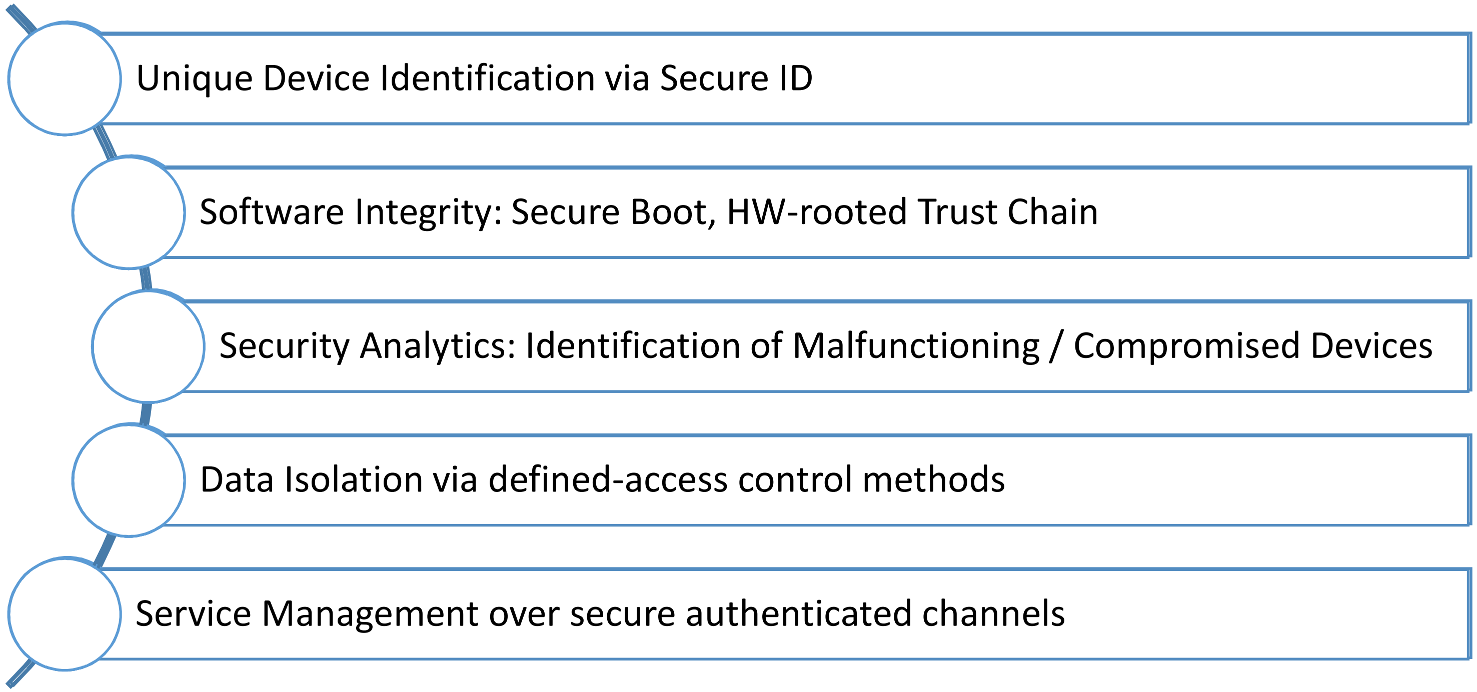
# Vulnerabilities with IoT Devices



| Security Threats | Description |
|---|---|
| Unauthorized access | Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker |
| Availability | The end-node stops to work since physically captured or attacked logically |
| Spoofing attack | With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data |
| Selfish threat | Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network |
| Malicious code | Virus, Trojan, and junk message that can cause software failure |
| DoS | An attempt to make a IoT end-node resource unavailable to its users |
| Transmission threats | Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc. |
| Routing attack | Attacks on a routing path |

Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

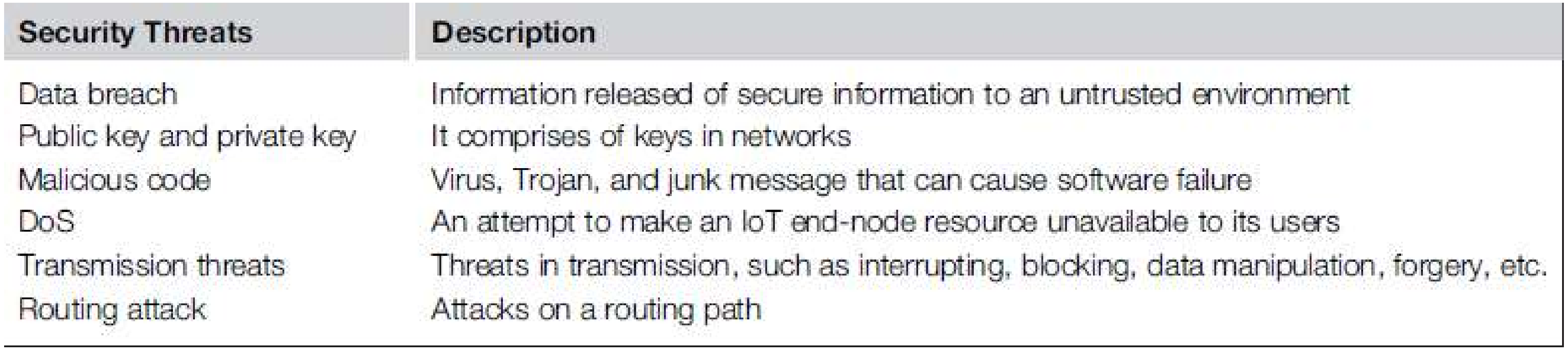
# IoT Device Security



- Unique Device Identification via Secure ID
- Software Integrity: Secure Boot, HW-rooted Trust Chain
- Security Analytics: Identification of Malfunctioning / Compromised Devices
- Data Isolation via defined-access control methods
- Service Management over secure authenticated channels

Case Study: AWS IoT and AWS IoT Device Defender

# Vulnerabilities with IoT Networks



| Security Threats | Description |
|---|---|
| Data breach | Information released of secure information to an untrusted environment |
| Public key and private key | It comprises of keys in networks |
| Malicious code | Virus, Trojan, and junk message that can cause software failure |
| DoS | An attempt to make an IoT end-node resource unavailable to its users |
| Transmission threats | Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc. |
| Routing attack | Attacks on a routing path |

Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

# Guidelines for Secure System Engineering

- Forrester Research: “***There is no single, magic security bullet that can easily fix all IoT security issues***”

- IoT Security Foundation
  - Establishing Principles for Internet of Things Security

*» Does the data need to be private?*

*» Does the data need to be trusted?*

*» Is the safe and/or timely arrival of data important?*

*» Is it necessary to restrict access to or control of the device?*

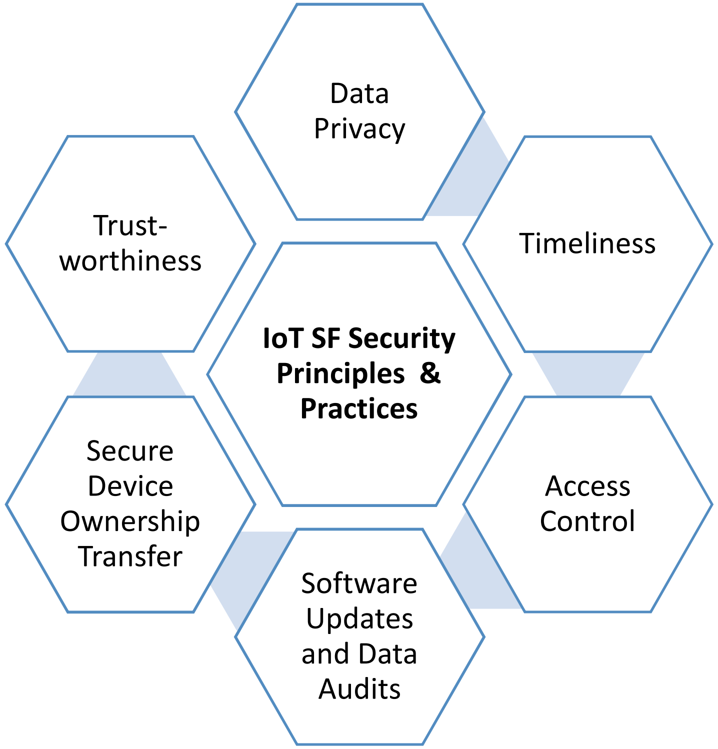
*» Is it necessary to update the software on the device?*

*» Will ownership of the device need to be managed or transferred in a secure manner?*

*» Does the data need to be audited?*

- Do not re-invent the wheel – rely on reusing existing cyber security principles and practices

*“the underlying principles that inform good security practices are well established and quite stable”* – IoT SF


Data Privacy
Trust-worthiness
Timeliness
IoT SF Security Principles & Practices
Secure Device Ownership Transfer
Access Control
Software Updates and Data Audits