



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

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



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 7: IoT Security – An Overview

What we shall cover?

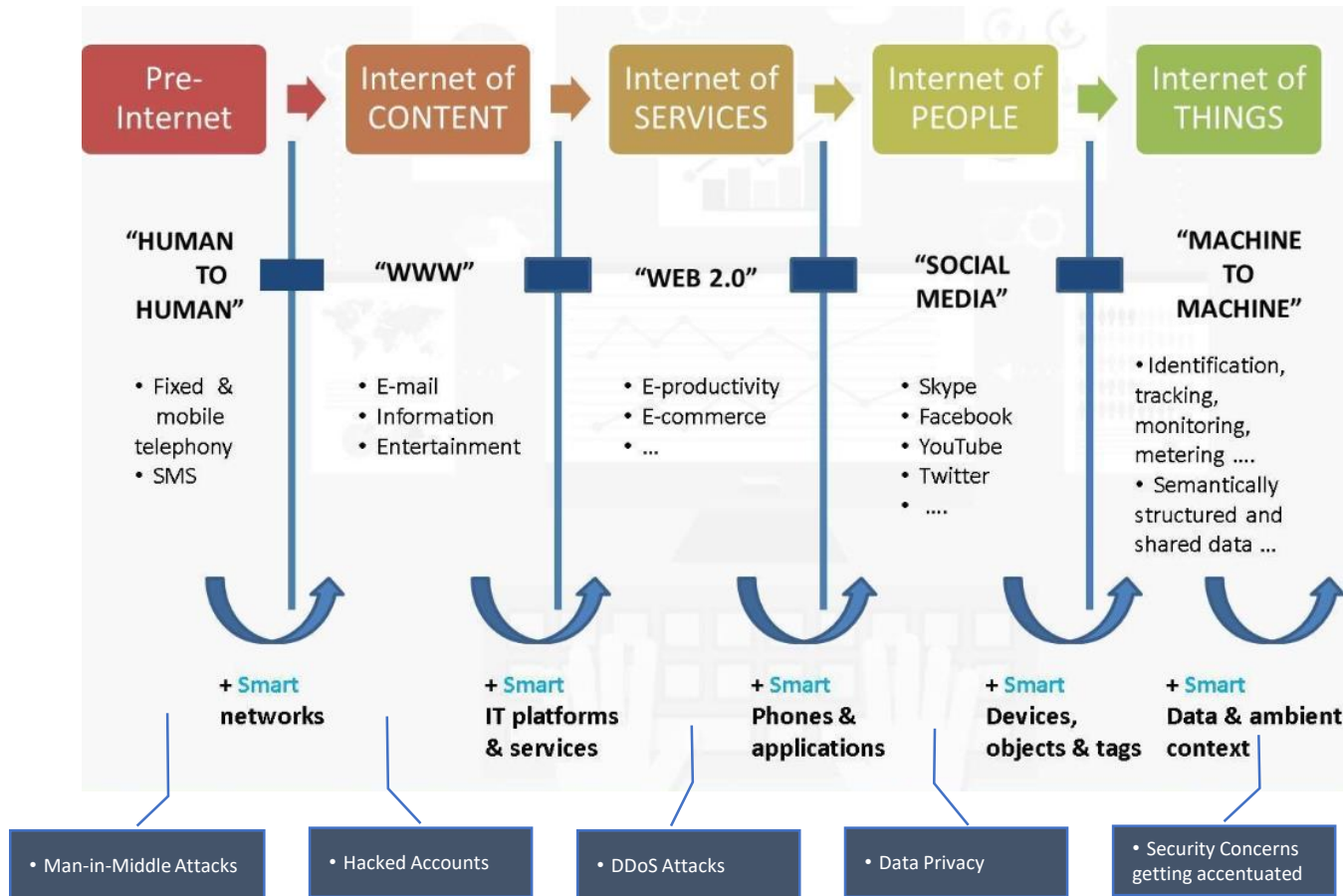
- 01 Context: IoT and its Verticals
- 02 Need for IoT Security
- 03 The Changing IoT Landscape and What it means for IoT Security
- 04 Security Practices for the IoT World

RECAP:

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



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

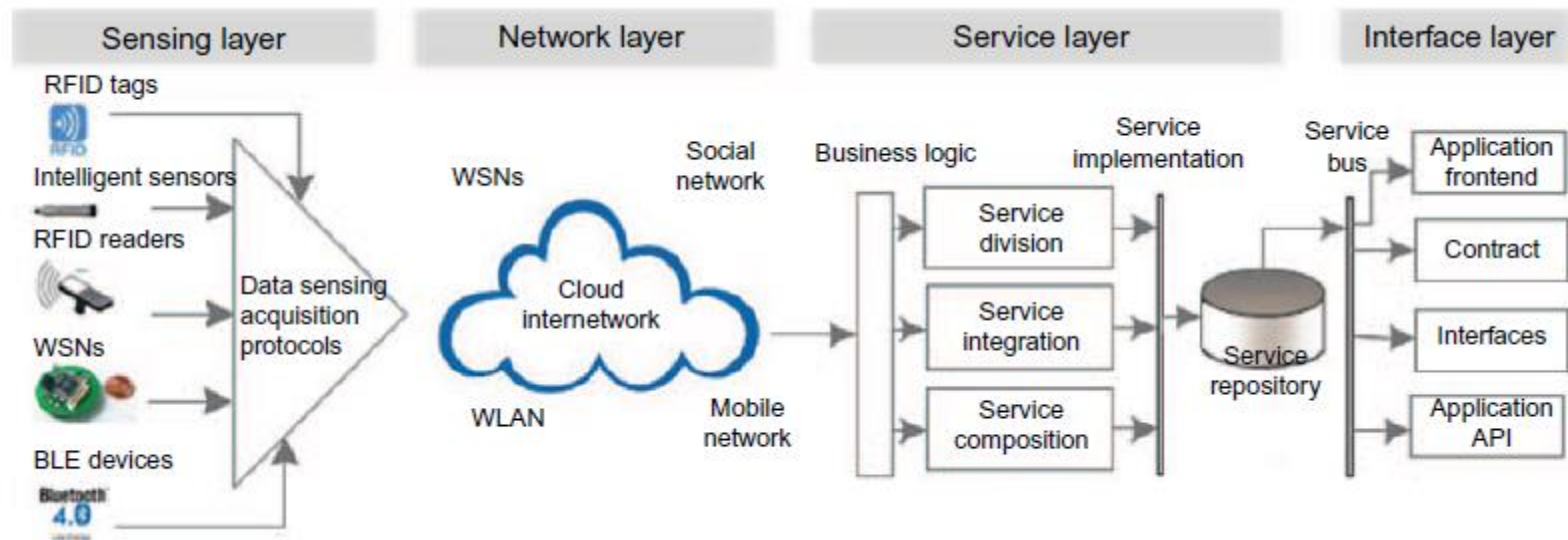


IoT is Everywhere



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

IoT Layers: A Security Perspective

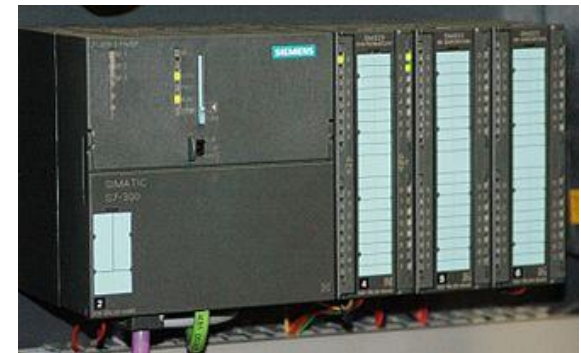


Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



The Stuxnet Attack!

- 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



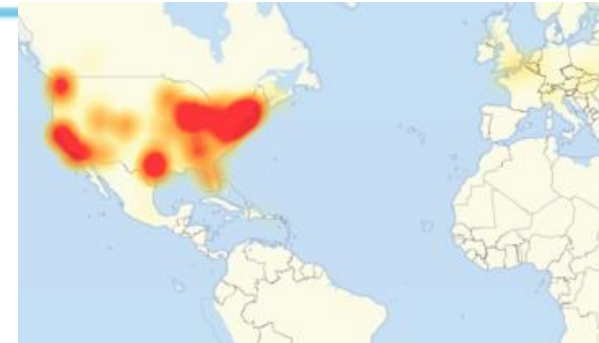
Siemens Simatic S7-300 PLC CPU with three I/O modules attached

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%

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

Source: [Wikipedia](#)



How Safe Are IoT Devices?

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

{[@weizmann.ac.il](mailto:eyal.ronen,adi.shamir)}

[†]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 overcame 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/>

17,129 views | Aug 6, 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.

- 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



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.

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

THE ECONOMIC TIMES

day

Hackers can track you through your smartband



in.pcmag.com

This randomised address can be decoded with something researchers call a decoder



How Safe Are IoT Devices?

August 13, 2019 Times of India

India sees most IoT attacks in Apr-Jun

Sindhu.Hariharan
@timesgroup.com

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 Sub-

BIG TARGET

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



ex 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-gra-

➤ 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

de 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....



March 02, 2021

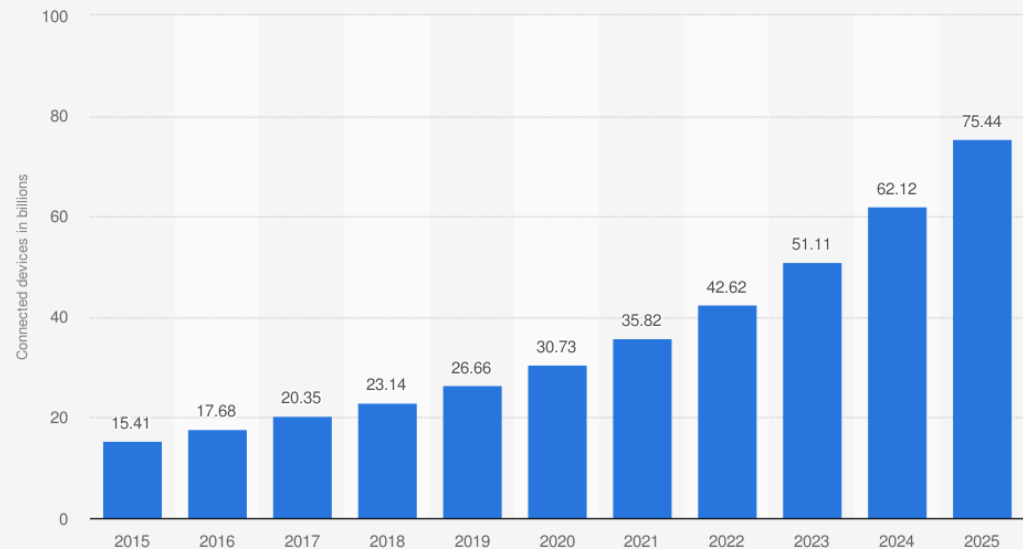
- Chinese attackers gained access to computer networks in India's power infrastructure
- Speculation that last year Mumbai power outage may be a result of this sabotage
- Malware known as ShadowPad
- Targeted at least 10 district power sector organizations

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	HOME CONSUMER	TRANSPORT MOBILITY	CITIES URBAN PLANNING	INDUSTRY INFRASTRUCTURE
				
Patient care Patient surveillance Elderly monitoring Fall detection Remote diagnostic Equipment monitoring Hospital hygiene Bio wearables Food sensors	Thermostats Lighting Remote control appliances Detection (intrusion /smoke) Energy / water monitoring Infotainment Pet feeding	Smart car Traffic routing Telematics Package monitoring Smart parking Insurance adjustments Supply chain Shipping Public transport Airlines Trains	Smart lighting Waste management Maintenance Surveillance Signage Utilities / Smart grid Emergency services	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

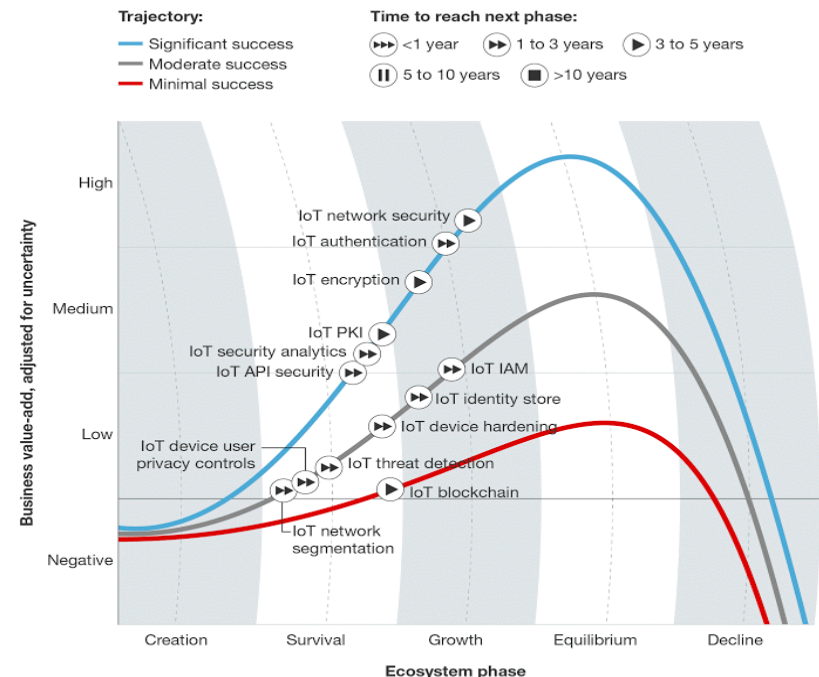
IoT Security: Involved Domains

- Device Security
 - Securing the IoT Device
 - **Challenges:** Limited System Resources
- 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
- Encryption
 - Data Integrity for data at rest and in transit
 - Strong Key Management Processes

FORRESTER RESEARCH

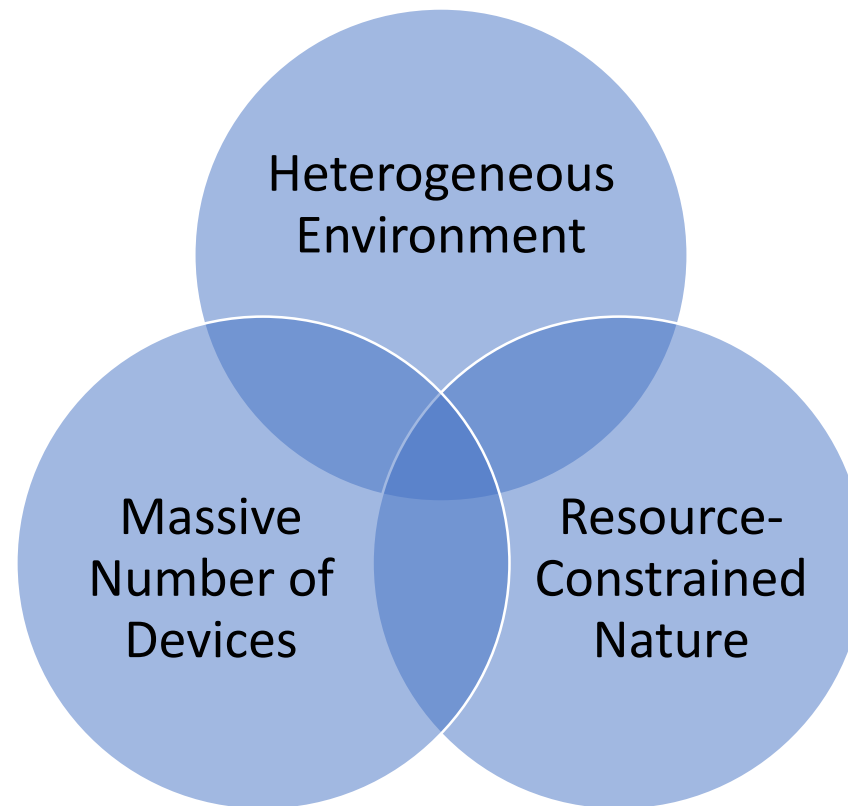
TechRadar™: Internet Of Things Security, Q1 '17

TechRadar™: Internet Of Things Security, Q1 2017





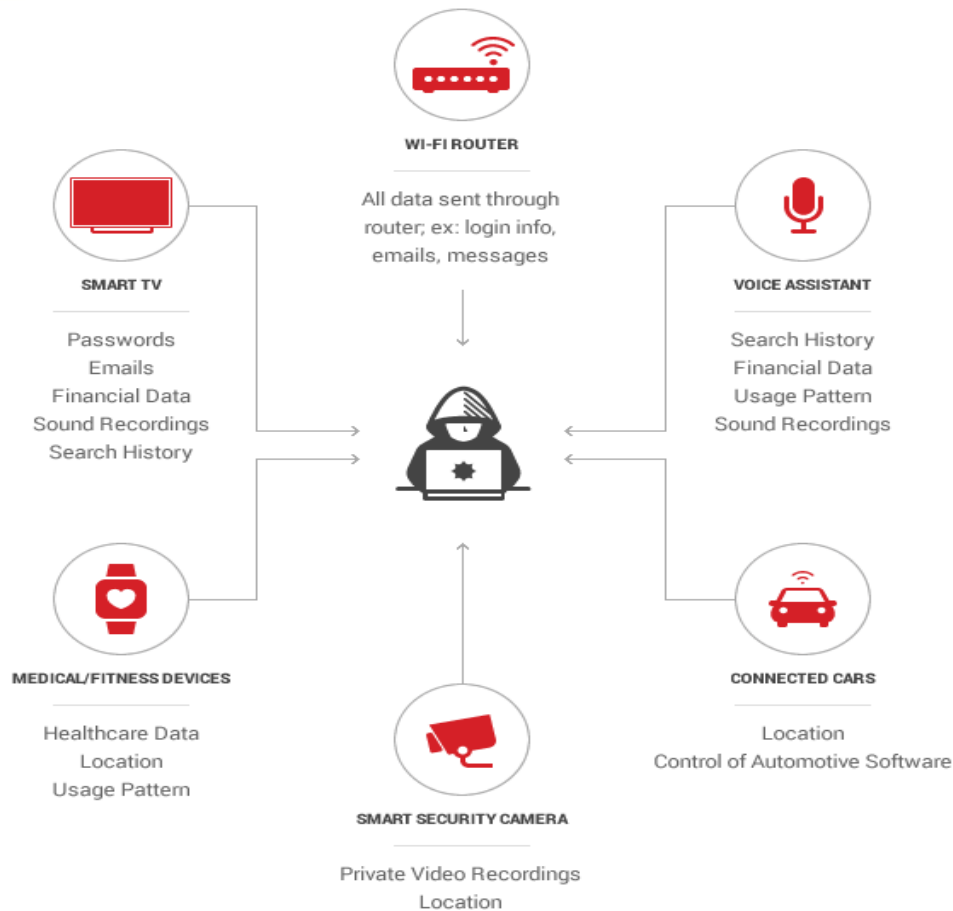
IoT Device Security : Key Focus Area in IoT Security





Data Privacy Issues with IoT Devices

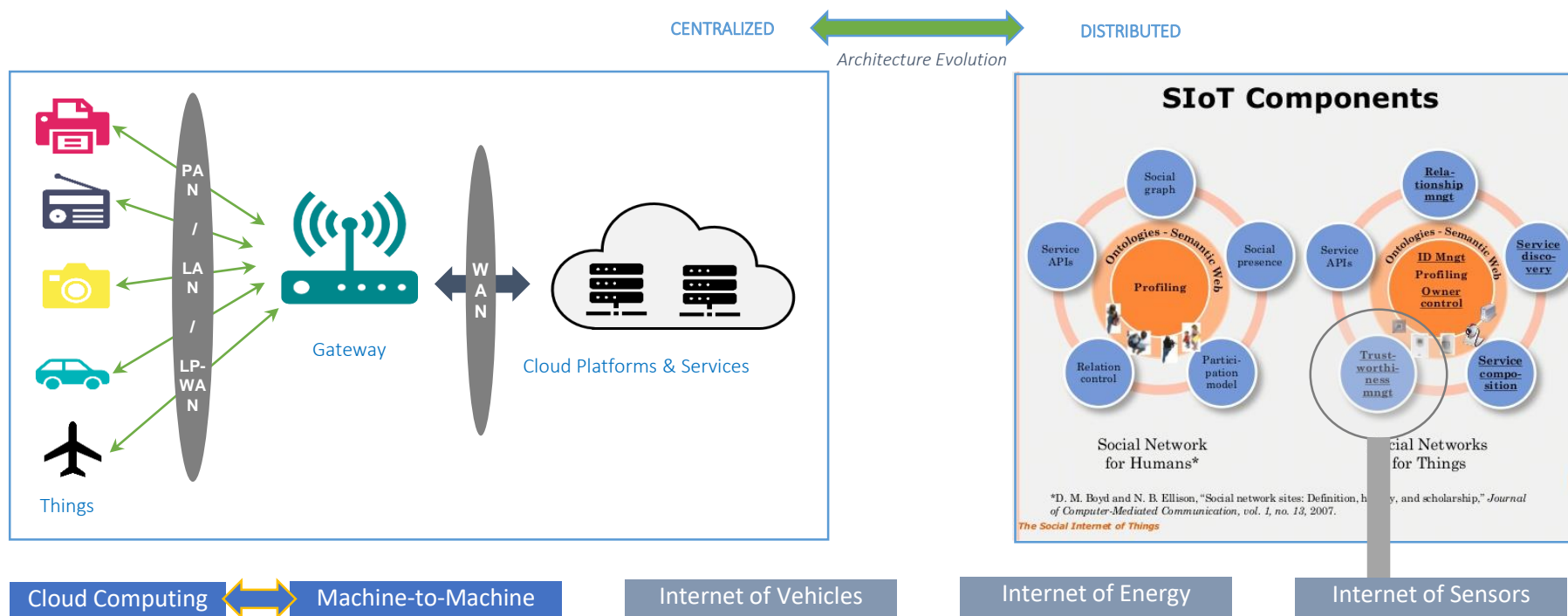
Information a malicious hacker can obtain from an IoT device



Source:



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>

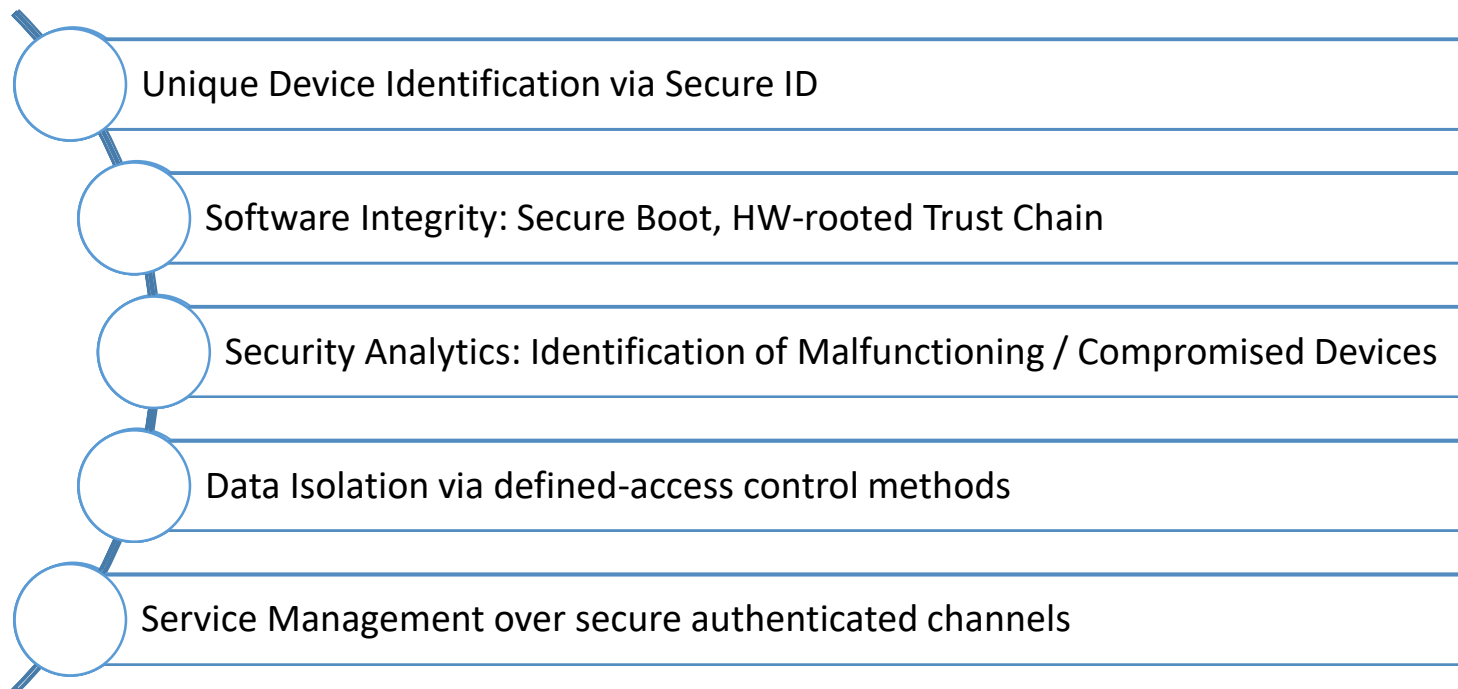
Vulnerabilities with IoT Devices

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



Case Study: AWS IoT and AWS IoT Device Defender

Vulnerabilities with IoT Networks

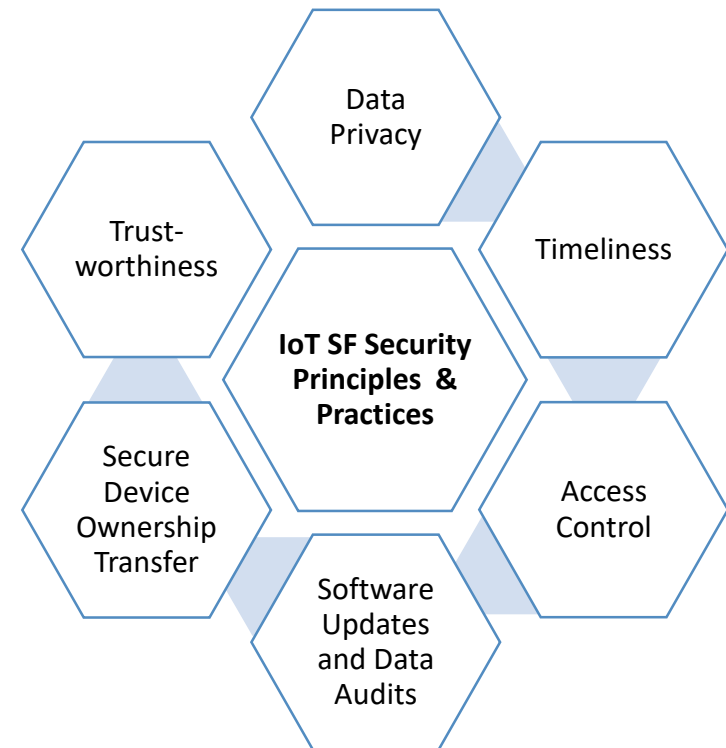
Security Threats	Description
Data breach	Information released of secure information to an untrusted environment
Public key and private key	It comprises of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
DoS	An attempt to make an IoT end-node resource unavailable 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