RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

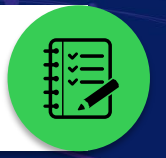
SESSION ID: CMI-W08

Trends and Best Practices in IoT Security

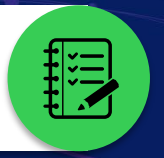
Srinivas Bhattiprolu, CISM, CCSP

Senior Director- Solutions and Services
Nokia Software
@srbhatti5

RSAConference2019
Asia Pacific & Japan

- Importance of IoT and key trends 
- Security Challenges in IoT 
- Possible attacks on the IoT systems 
- Best practices in mitigating these challenges & Case studies 
- Conclusions 

RSAConference2019
Asia Pacific & Japan

- Importance of IoT and key trends 
- Security Challenges in IoT 
- Possible attacks on the IoT systems 
- Best practices in mitigating these challenges & Case studies 
- Conclusions 

Future: New opportunities, New business models and huge potential

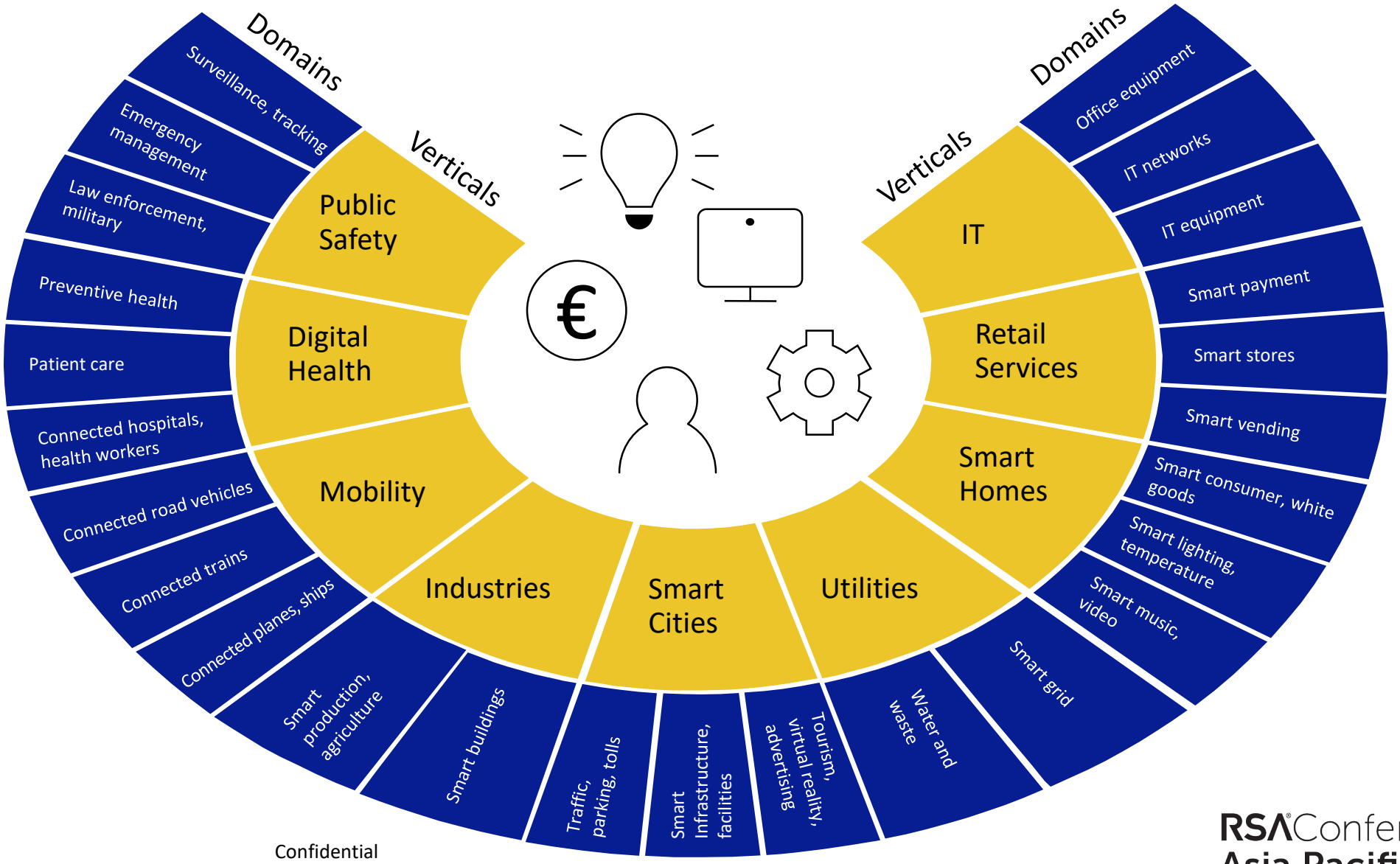
- Automotive
- Health
- Events & tourism
- Industry 4.0
- Mega cities
- Homes & buildings

…of fatalities in car accidents are due to human error and slow reaction **90%**	…of 355 billion gallons of water used daily is wasted due to leakages **20%**	…deaths by non communicable diseases expected in 2030 **52 million**
……productivity gains expected by connected cyber physical systems **26%**	…estimated energy waste in buildings due to inefficient and outdated HVAC systems **50%**	…additional economic benefits by leveraging Smart City applications **50 billion €**

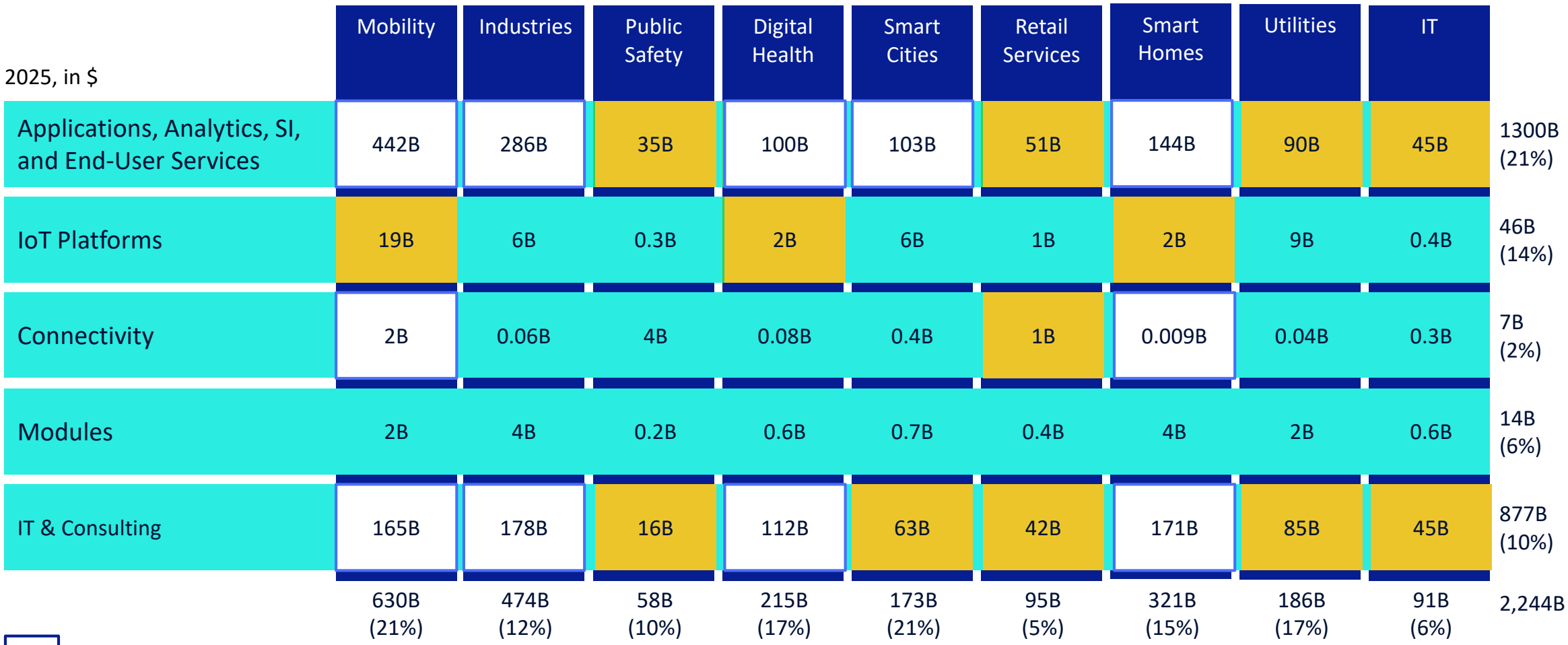
Over 70% of organizations do not generate service revenues from their IoT solutions

There are 500 CSPs around the world but only 31 have a real IoT offering.

IoT Has a Transformational Impact across Vertical Sectors

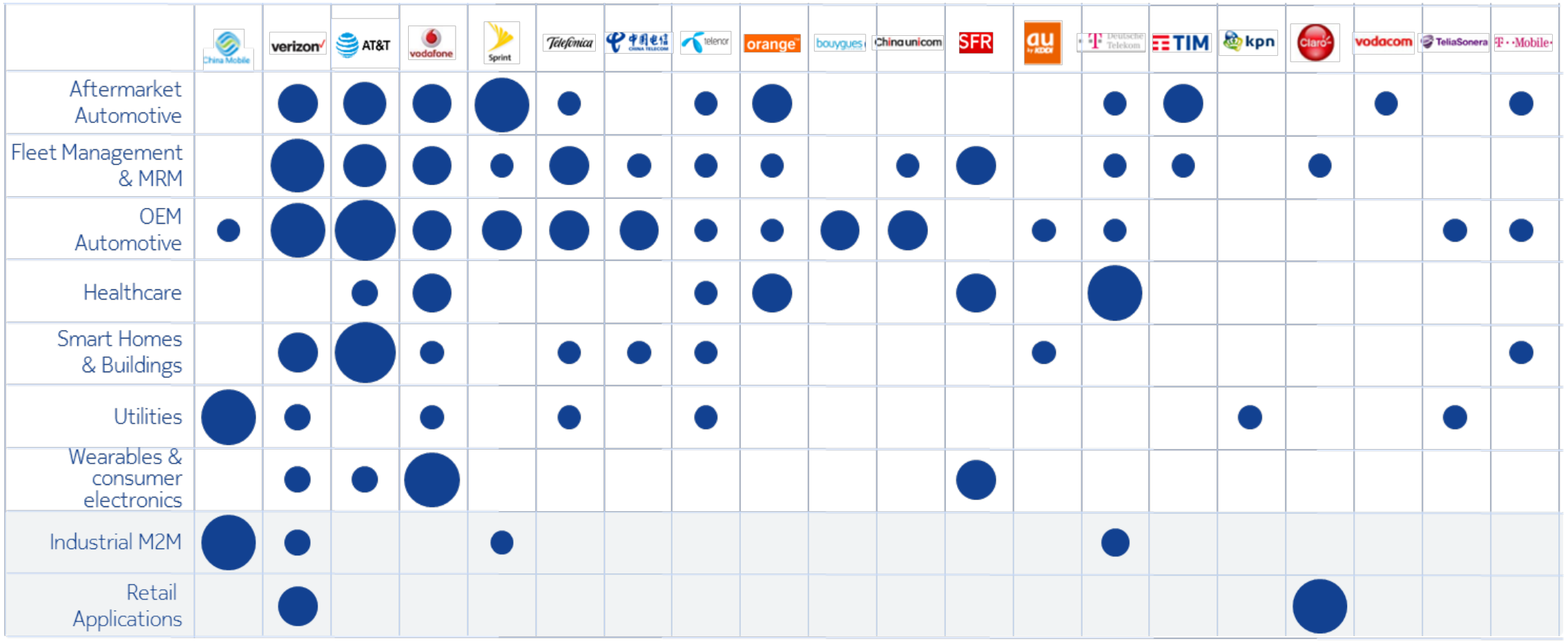


The IoT Opportunity Is Large And Growing



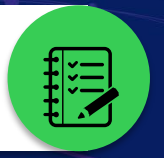
Source: Machina Research 2016, Nokia Corporate Strategy
2016-2025 CAGR

Value exploration by CSPs: current use cases



Bell Labs Consulting Analysis of IoT connections data (Source: Berg Insights, June 2017)

RSAConference2019
Asia Pacific & Japan

- Importance of IoT and key trends 
- Security Challenges in IoT 
- Possible attacks on the IoT systems 
- Best practices in mitigating these challenges & Case studies 
- Conclusions 

Security and privacy are fundamental elements to expand the human possibilities of the connected world

What is the cost of a Security breach?

Cost of cybercrime in 2018 in the Asia Pacific Region (est at $600B globally)

$171B

Average annualized cost of cybersecurity (USD)

$11.7M

Percentage increase in cost of cybersecurity in a year

22.7 %

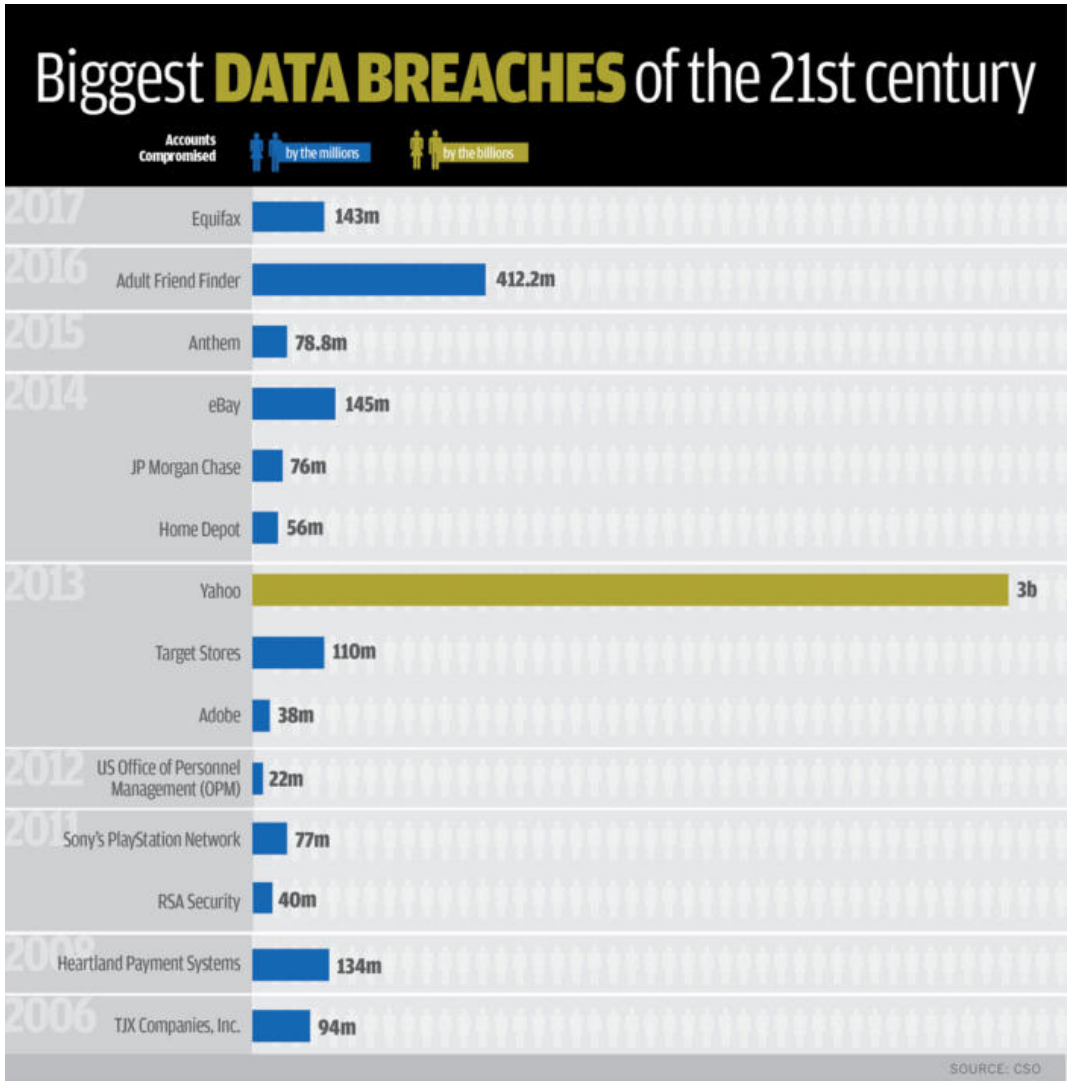
Average number of security breaches each year

130

Percentage increase in average annual number of security breaches

27.4 %

Source: https://www.accenture.com/sg-en/insight-cost-of-cybercrime-2017; www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.htm



SourceThe 18 biggest data breaches of the 21st century Dec 2018

IoT Security Challenges- A perspective

Long IoT Device Lifetime

High effort to update devices in the field.
Outdated security mechanisms needed for legacy devices.

Encryption power decreases over lifetime!

→ Cracking of encryption in 5-10 years possible!

Anti-Malware support seldom available for 10+ years

→ Small quantities might not get any support!

Signaling Storms

There will be many IoT devices.
Normal IoT device signaling footprint will often be low.

Malware could increase device activity drastically

→ **Networks can overload**

→ **Battery drain**

Networks are not overprovisioned to cater for unexpected high loads

Roaming devices could jump between networks

→ **Affects visited network and roaming interfaces**

When a network goes down or locks out devices, they seek for connectivity

Badly maintained IoT devices

How many users really care as long as it works?

Who updates traffic-light?

→ **Vulnerable devices can be hijacked by attackers**

Nobody will care about it as long as the traffic flows, no accident happens,…

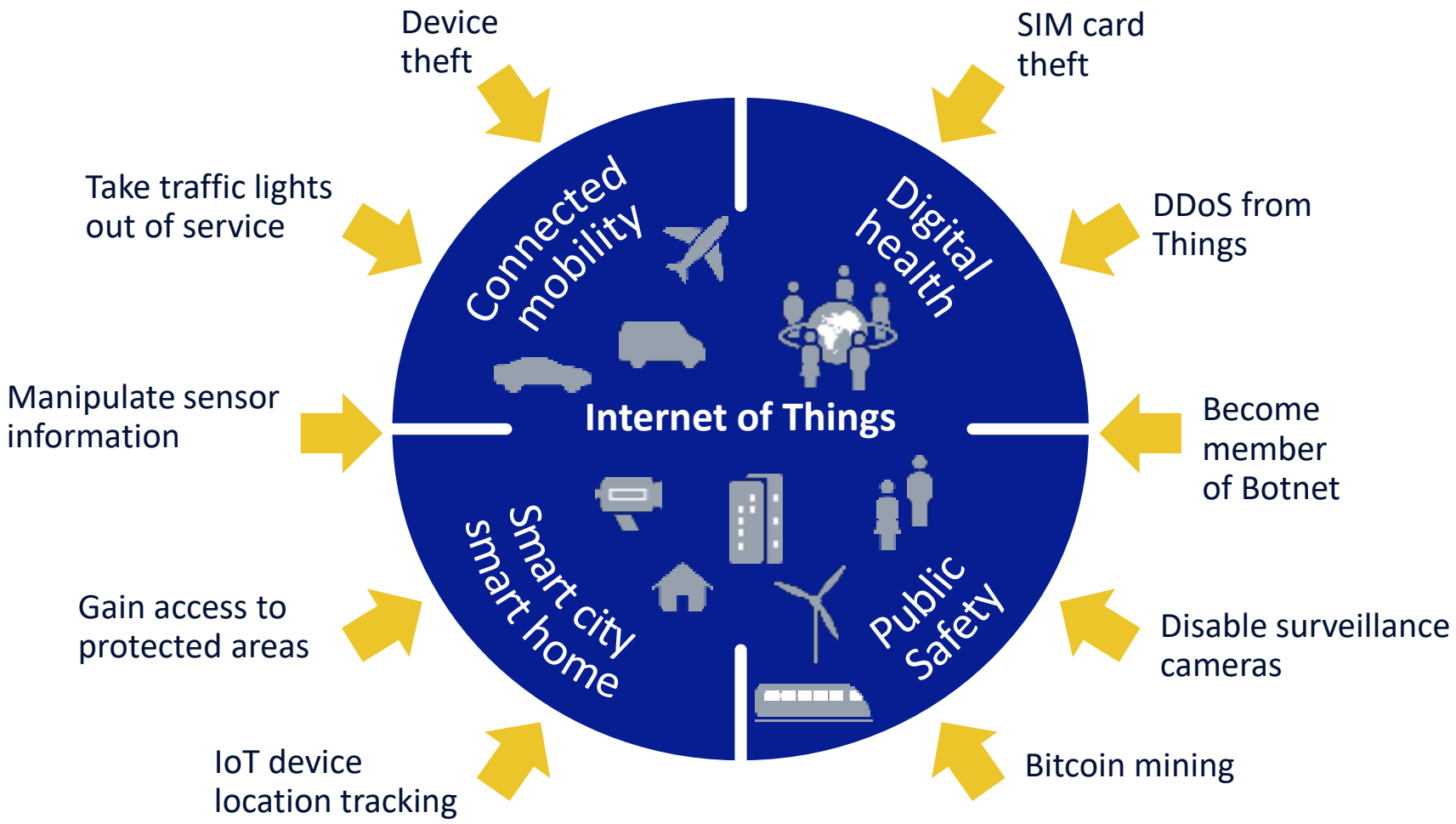
Garage-openers?

→ **Could be sending 1 mio SPAM mails per day since years?**

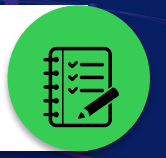
Nobody will care to check as long as the door opens.

Coming with 5G - the Internet of (hacked) Things

Exploding risks for abuse and security breaches



RSAConference2019
Asia Pacific & Japan

- Importance of IoT and key trends 
- Security Challenges in IoT 
- Possible attacks on the IoT systems 
- Best practices in mitigating these challenges & Case studies 
- Conclusions 

What are the threats for the Internet of Things?

Service disruption

- Disable surveillance cameras
- Take traffic lights out of service

Sabotage and destruction of system

- SIM card theft
- Device theft

Steal very personal information

- Location tracking
- Sensitive data theft: healthcare, payment info

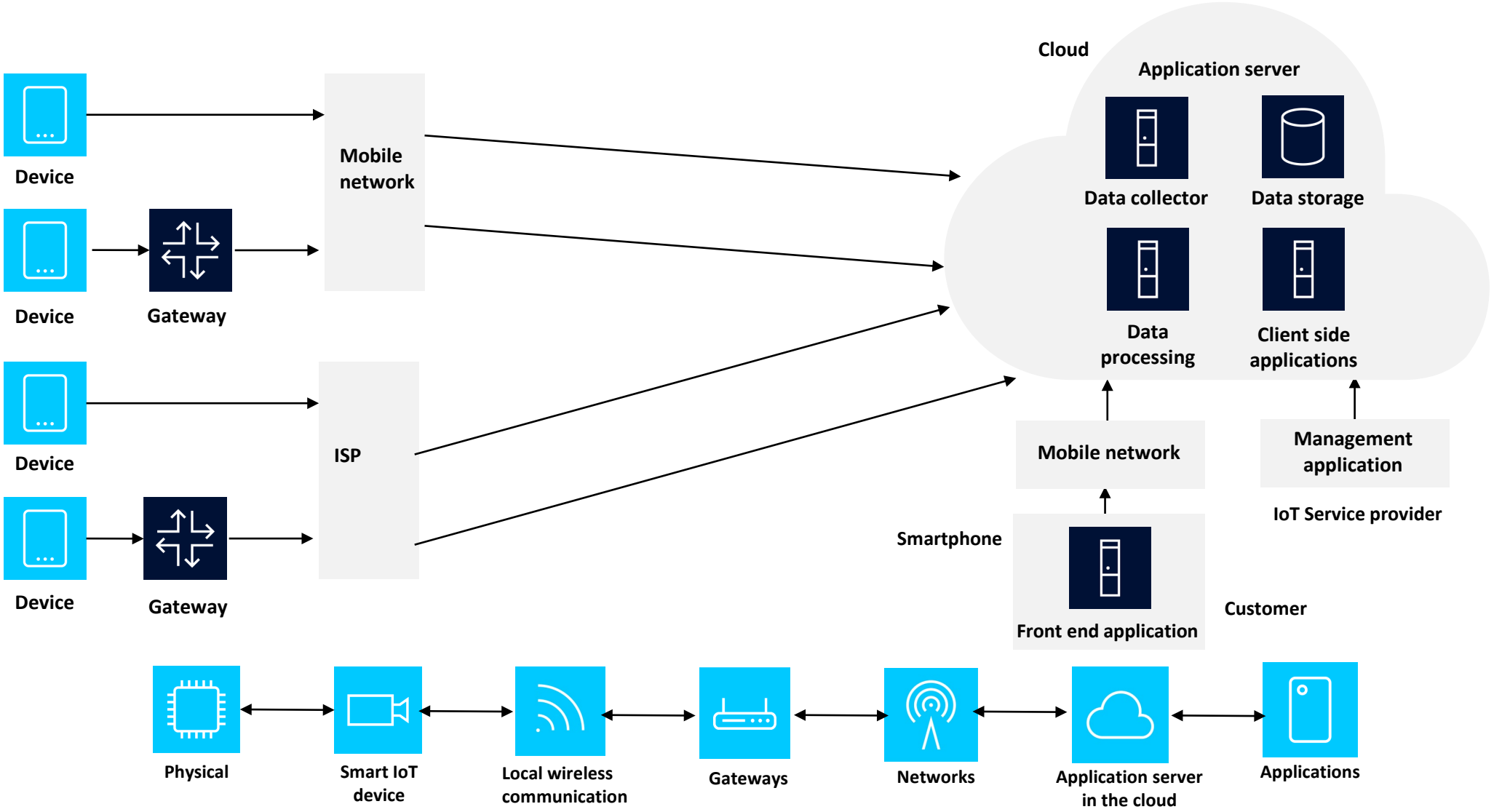
Manipulate system

- Modify sensor information
- Gain access to protected areas (e.g. car brakes)

"Things" leveraged as part of bigger attacks

- Become member of BotNet
- Generate e-mail spam
- Perform DDoS from Things
- Perform bitcoin mining
- Perform click fraud

IoT eco system and threats at different levels



IoT eco system and threats at different levels

- Orphaned devices, can be tampered easily
- Physical tampering of the components possible

Physical

- Simplistic implementation of various stacks
- Improper exception handling and input validation
- Excessive and direct exposure to internet

Smart IoT Device

- Use of non IP protocols that are less secure
- Local data link are less secure & lack protection
- Hijack firmware upgrades

Local wireless Communication

- Gateways will form a conduit to devices
- Deficiencies in software libraries

Gateways

- Transport corruption,
- Transport disruption and snooping attacks
- Data poisoning attacks

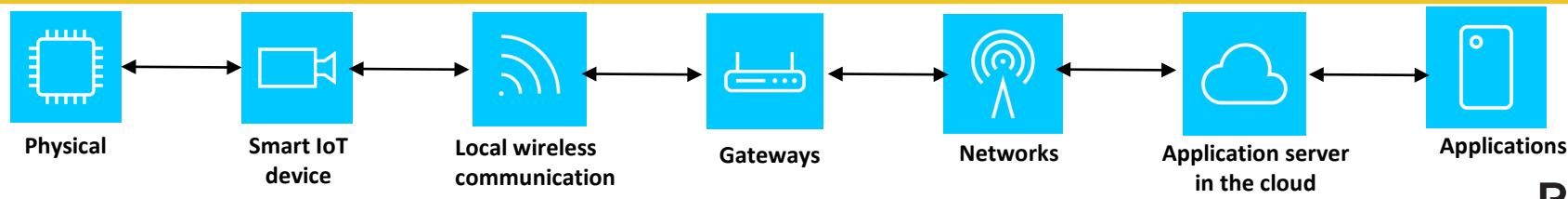
Networks

- Central point of vulnerability
- Potential for Masquerading

Application server in the cloud

- APIs offer hacking opportunities
- Vulnerabilities in middleware
- Steal the credentials of the applications

- Users installing the devices and applications themselves
- Use of default passwords
- Specific device vulnerabilities



IoT eco system and attacks at different levels

- Physical attacks
- Access to the MMUs

Physical

- Identity, secure tokens and passwords
- Command injection vulnerability
- Enlist devices as DDoS botnets

Smart IoT Device

- Spoofing
- Man in the Middle
- Takeover
- Command injection

Local wireless Communication

- Gateway identity, secure tokens and passwords
- Gateway certificates and keys.
- Credential compromise attacks

Gateways

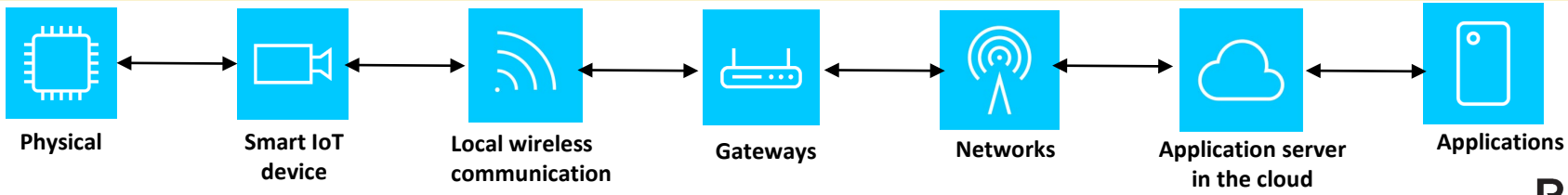
- Sending un encrypted data over internet
- Packet sniffing
- Rogue device sending fake data

Networks

- DoS, Snooping and probing
- Takeover attacks

Application server in the cloud

- Data Manipulation
- Resources access
- Repurpose the identity



IoT attack example: MIRAI Bot

A new breed of very high volume DDoS

More than 1.2 Million Mirai-infected devices on the Internet, with over 166,000 devices active right now.

WHAT

DDOS Attack

Password hacking

Mirai uses Internet of Things (IoT) devices like routers, digital video records (DVRs), and webcams/security cameras, enslaving vast numbers of these devices into a botnet, which is then used to conduct DDoS attacks.

WHEN

(Oct 2016) Largest DDoS attack ever: 1.5Tbps attack against French web hosting provider OHV in which 145,000 hacked webcams were involved

(Oct 2016) Significant DDoS attack causing outage to websites incl. Twitter, GitHub, PayPal, Amazon, Reddit, Netflix, and Spotify,

WHY

The underlying problem is that IoT manufacturers are only designing the devices for functionality and aren't investing in proper security.

Mirai continuously scans the internet for IoT devices and logs into them using the factory default or hard-coded usernames and passwords.

Smart Meters, Health Care systems hacks

PRIVACY AND SECURITY FANATIC

By Ms. Smith | Follow

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Hacking For Privacy: 2 days for amateur hacker to hack smart meter, fake readings

Detailed smart meter data can show what TV shows you watch, scan for copyright-protected DVD movies you watch, and other privacy intrusive details. Yet it takes an amateur hacker only two days to hack a home smart meter and fake the readings -- which could result in a utility bill showing absolutely no power consumption at all.

Network World | Jan 4, 2012 11:59 AM PT

Microsoft | Security

At the Chaos Communication Congress in Germany, 28C3, researchers presented "Smart Hacking For Privacy." After analyzing data collected by a smart meter, these gentlemen were able to determine devices like how many PCs or LCD TVs in a home, what TV program was being watched, and if a DVD movie being played had copyright-protected material. In other words, smart meters do have privacy implications that translate into consumer identification. On the bright side, they showed it takes an amateur hacker only two days to hack a home energy meter and fake the smart meter readings -- which could result in a utility bill showing absolutely no power consumption at all.

RELATED

CIA wants to spy on you through your appliances

Huge 4th Amendment Win for Privacy: Supreme Court Requires Warrant for GPS...

Are smart meters real-time surveillance spies?

Internet

The Reality of "Hacking" Medical Devices

Michael Hatamoto - September 4, 2011 10:14 PM

Print | ShareThis 2 | g+1 1 | 12 comment(s) - last by Meyerstein Con.. on Sep 7 at 5:31 AM

It's possible medical devices face an immediate threat that medical researchers will have to deal with

Modern technology has helped save countless lives, but there is a growing threat that some biotech companies may be ignoring - implanted devices that can be hacked by skilled criminals.

There haven't been specific cases of these devices being compromised, but recent demonstrations at Black Hat -- and an increase in online reports of medical device security issues -- has lawmakers worried about loopholes that must be fixed.

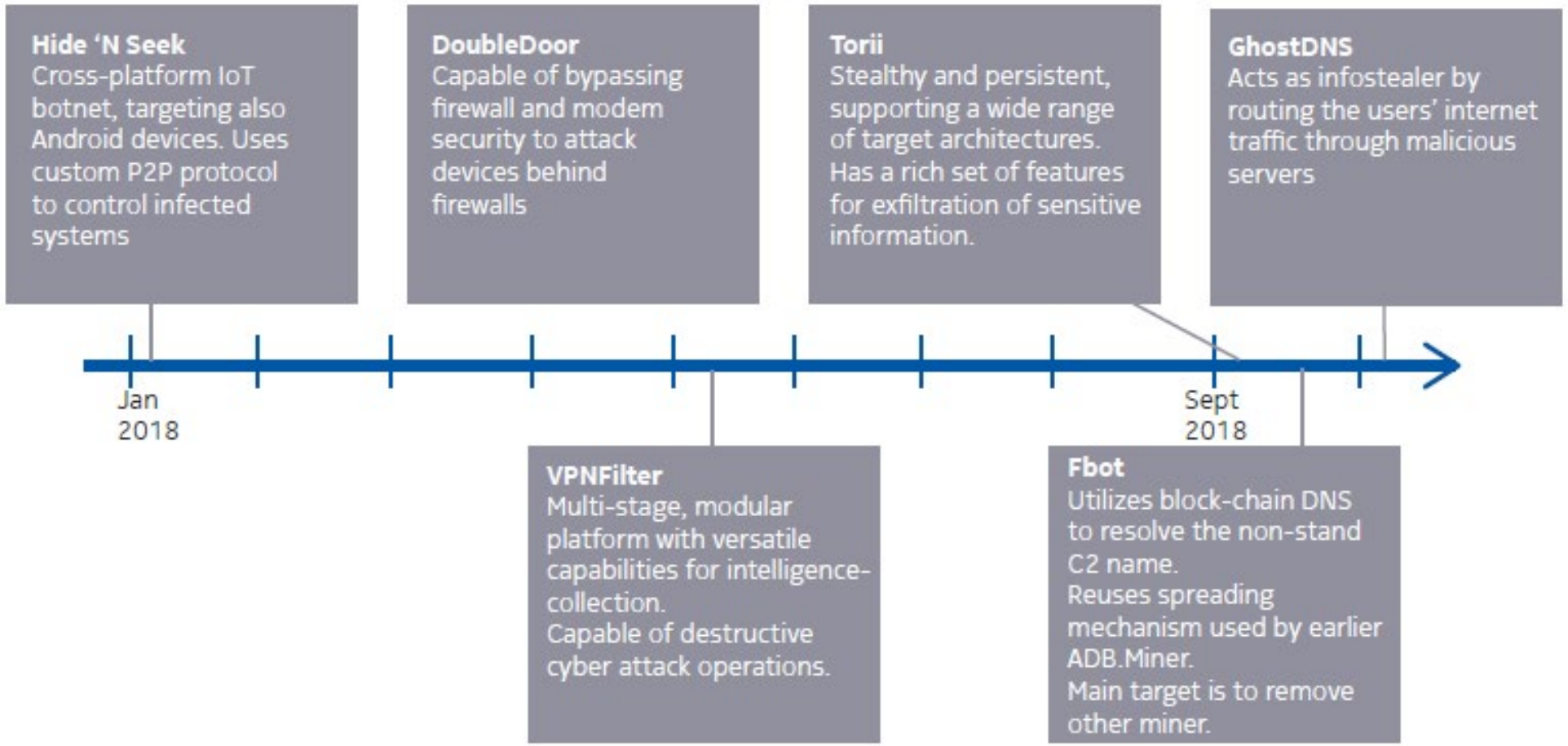
Earlier in the year, a security expert named Jerome Radcliffe hacked his insulin pump's hardware onstage by reverse-engineering the device. He was able to use a small radio frequency transmitter to disable the device, along with controlling how much insulin was pumped using the pump.

"My initial reaction was that this was really cool from a technical perspective," Radcliffe said in an interview with the *AP*. "The second reaction was one of maybe sheer terror, to know that there's no security around the devices which are a very active part of keeping me alive."

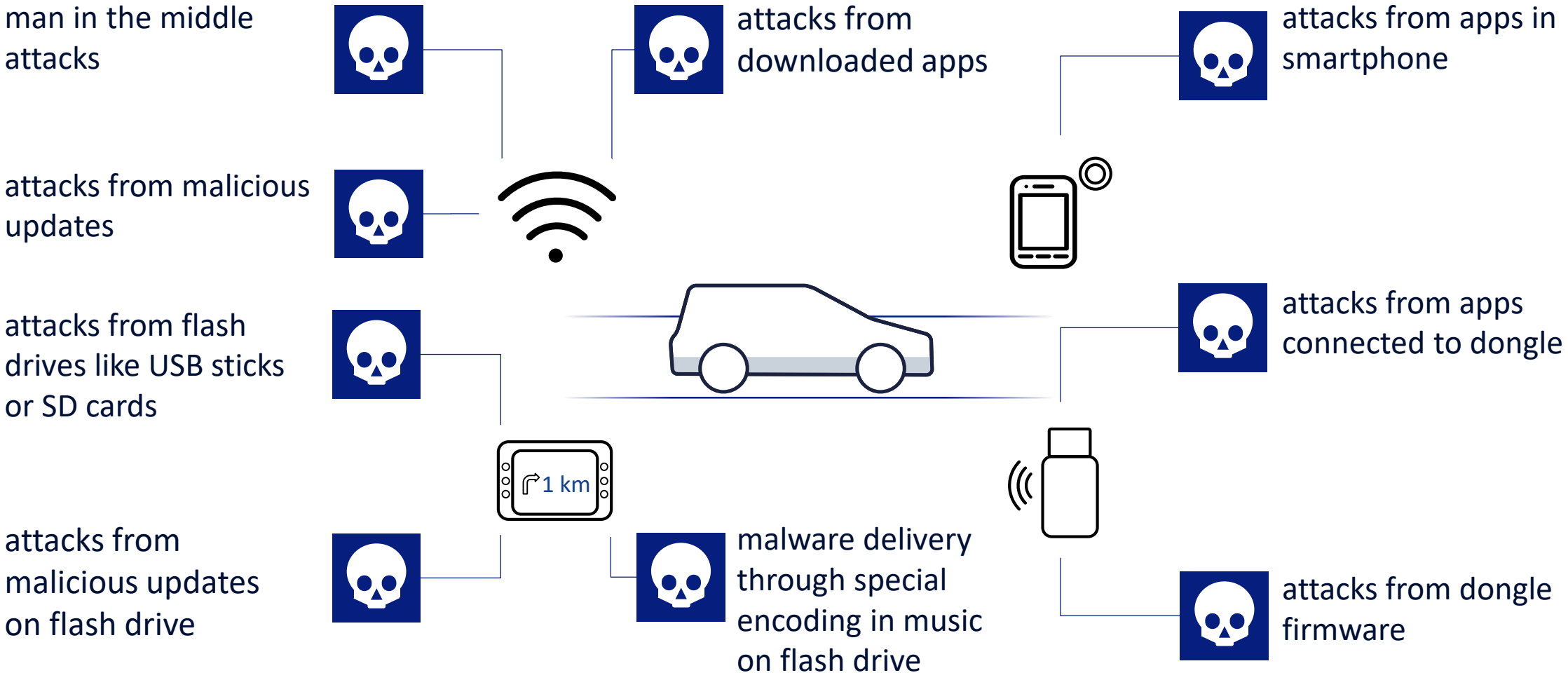
Although it wasn't easy to successfully hack the device, security experts find it alarming that Radcliffe was able to intercept the pump's wireless signals.

Individual hackers likely won't be able to suddenly tamper with these devices anytime soon, but criminals familiar with medical technology could pose a threat if they attack a specific device. Furthermore, Medtronic, one of the biggest medical device suppliers, doubts whether or not Radcliffe and other hackers would be able to tamper with wireless devices in the real world.

IoT Botnet variants



Potential connected cars threats



IoT Security Challenges

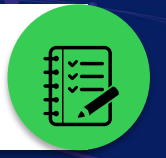
Ecosystem

- Increasing population
- Heterogeneity across IoT
- Homogenous within a specific environment
- Not standardized

Things

- Resource limitations (power, computing, storage, bandwidth)
- Diverse hardware
- Difficult patch management
- Typically not protected by anti-virus
- Long lifetime

RSAConference2019
Asia Pacific & Japan

- Importance of IoT and key trends 
- Security Challenges in IoT 
- Possible attacks on the IoT systems 
- Best practices in mitigating these challenges & Case studies 
- Conclusions 

IoT Security requires a holistic approach

An end to end approach is the need of the hour

Firmware and Software Management

Devices security

Securing the endpoint

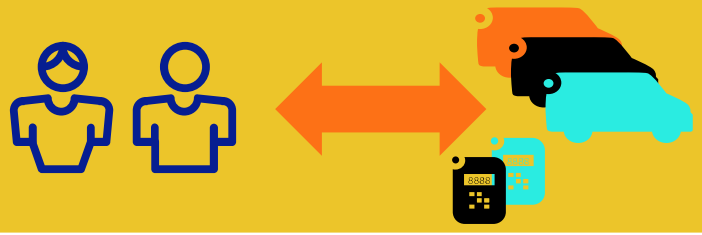
Securing connectivity

Securing the network

Securing applications & backend

platforms and applications

Secure access & management



Recommendations

Hardening

The propagation of malware depends much less on the vulnerabilities associated with the human factor and much more with the hardening of all components of an end-to-end IoT system.

Responsibility

The operator/end user of IoT systems bears a lot of responsibility for the proper setup and configuration of the IoT system

Post infection activity

The post-infection activity will likely not directly affect the owner of the infected IoT devices, as the IoT devices are usually used to launch DDoS attacks against distant targets)

Post Infection impact

For enterprise IoT service providers, however, the effects of post-infection activity are bound to be significant, as the quality of the provided service is affected (degraded service, service interruptions, etc.).

Malware propagation

Even if the infection of IoT devices doesn't usually directly affect the owners of the infected devices, it is still essential to detect malware propagation and post-infection activity

End Point Security

End Point security and automated device correction is the key for effective IoT security

Key recommendations for IoT Security

Best Practices

1	**Physically protect IoT Infrastructure**	• The worst security attacks against an IoT infrastructure are launched by gaining physical access to devices
2	**Inventory Control**	• Operators of an IoT system need to keep track of the kinds of IoT devices on their network • This includes the initial configuration of the IoT system and the subsequent monitoring
3	**Keep systems up to date**	• IoT system operators are responsible for ensuring that device operating systems and all device drivers are updated to the latest versions • Much of the overall vulnerability of IoT systems is due to the fact that deployed devices are not actively and timely upgraded and/or patched
4	**Protect Cloud credentials**	• Cloud authentication credentials used for configuring and operating an IoT deployment are the first avenue for malware to gain access and compromise an IoT system
5	**Monitor outbound and lateral IoT traffic**	• It is important to monitor IoT devices for aberrant behaviour in order to automatically identify rogue devices

Best Practices

6	**Protect against malicious activity**	• Agent based protection, signature based protection isn't possible for IoT • Use of ML based protection is the key
7	**Harden devices**	• The devices are hardened by proper configuration and firmware upgrade to the latest version • Not once but continuously
8	**Detect and clean real-time**	• Key is to detect attacks and infections on IoT devices real-time and apply remediation measures • Act on IoT devices in real-time
9	**Segment IoT Traffic**	• It is important to keep the IoT traffic separate from other network segments to limit exposure and the spread of malware. • It is proven that network segmentation and the usage of NAT plays an important role.
10	**Audit frequently**	• Auditing IoT infrastructure for security-related issues is key when responding to security incident

Regulatory requirements across the Globe

Countries must consider IoT specific regulations

IoT Specific standards/regulations

ENISA

- ENISA developed baseline security measures to be adopted by relevant stakeholders.
- The main focus is on IoT resilience and communication, the interoperability with proprietary systems and the reliability of IoT

The IoT Cybersecurity Improvement Act of 2017

- Ensure devices are patchable
- Device vendors to declare no known vulnerabilities
- Requiring each executive agency to inventory all Internet-connected devices in use by the agency
- Specific measures with NIST

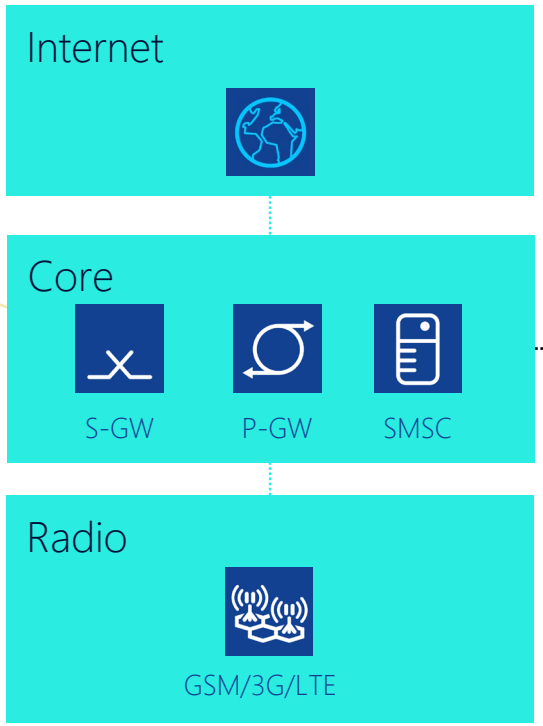
NIST IoT Security guidelines

- Agreement processes
- Organization-project enabling processes
- Technical management processes
- Technical processes

In Asia, gov'ts are legislating new and/or updating cybersecurity laws:

1. Vietnam - new cybersecurity law took effect in Jan 2019
2. Thailand Cybersecurity Code – under review and targeted for legislation in 1H 2019.
3. Singapore – Updated Telecom Act 323 with Cybersecurity Act in 2018, now reviewing IOT cybersecurity guide;
4. Japan - Japan's Parliament passed a bill in Dec 2018 to amend the 2014 Basic Act on Cybersecurity.

Anomalies & malware detection

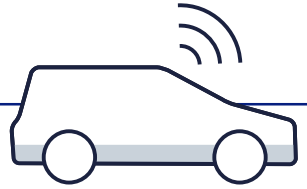


Cluster
pre-defined and self learned traffic profiles for different connected devices (e.g. types of cars, types of ECUs)

Monitor
connected cars for traffic profile compliance

Detect
misbehaving connected cars

Mitigate
by applying automated actions



A few case studies

Illustrative best practices from CSPs who have successfully implemented IoT Security

1 CSP in India

- Dedicated security organization with special focus on IoT security
- Encryption of Data (in motion, at rest and in use)
- Software security controls at multiple levels

2 CSP in Japan

- Standardization activities through rigorous checklists, self audits of new products
- Continuous enrichments of the checklists

3 CSP in MEA

- Employs encryption, firewalls, security protocols, such as TLS and AES, and other mechanisms
- security labs in the run tests on IoT equipment, before certifying these products

4 CSP in APAC

- End-to-end perspective, helping to frame internal processes and discussions with its partners
- Ability to collect, store and use the data in a secure manner

Building the trust in IoT

RSAConference2019
Asia Pacific & Japan

- Importance of IoT and key trends 
- Security Challenges in IoT 
- Possible attacks on the IoT systems 
- Best practices in mitigating these challenges & Case studies 
- Conclusions 

Operators are in a unique position to secure “Things” and end-users

Thousands of device manufacturers, low power, small foot print devices- Standardization is mandatory	Need for a comprehensive and holistic framework
Need for an E2E perspective for IoT Security	Use advanced techniques like AI, analytics to secure IoT solutions
Automated actions against threats is a must	Continuous assessment and analysis, keep the systems updated
CSPs are using Security as brand differentiator in the market	Mitigation mechanisms are becoming intelligent so are threats