IoT Security

Marmara El Masri
Nicolas Jaramillo
Zachary Matthews

What is the Internet of Things?

Internet of Things - the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

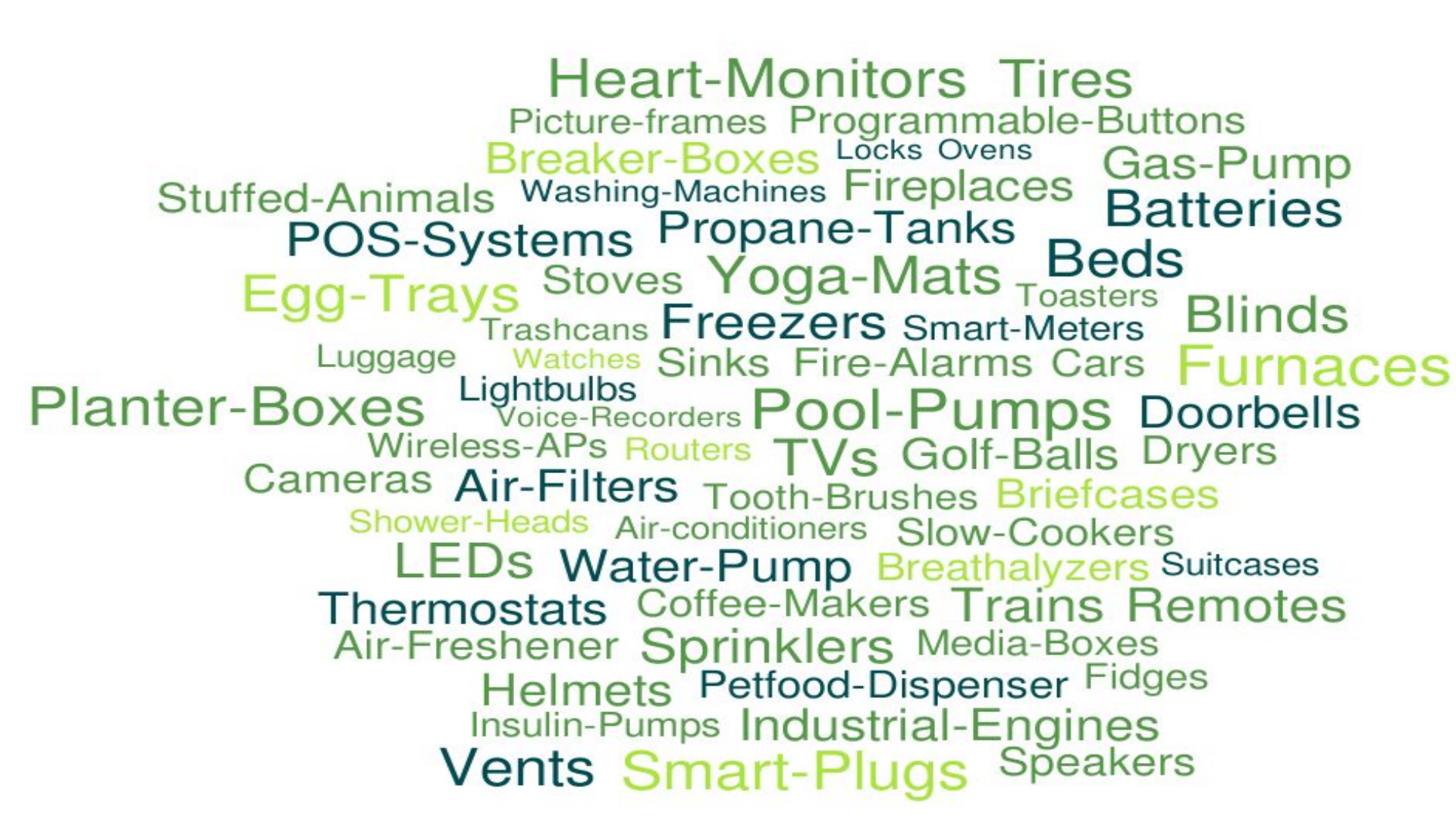
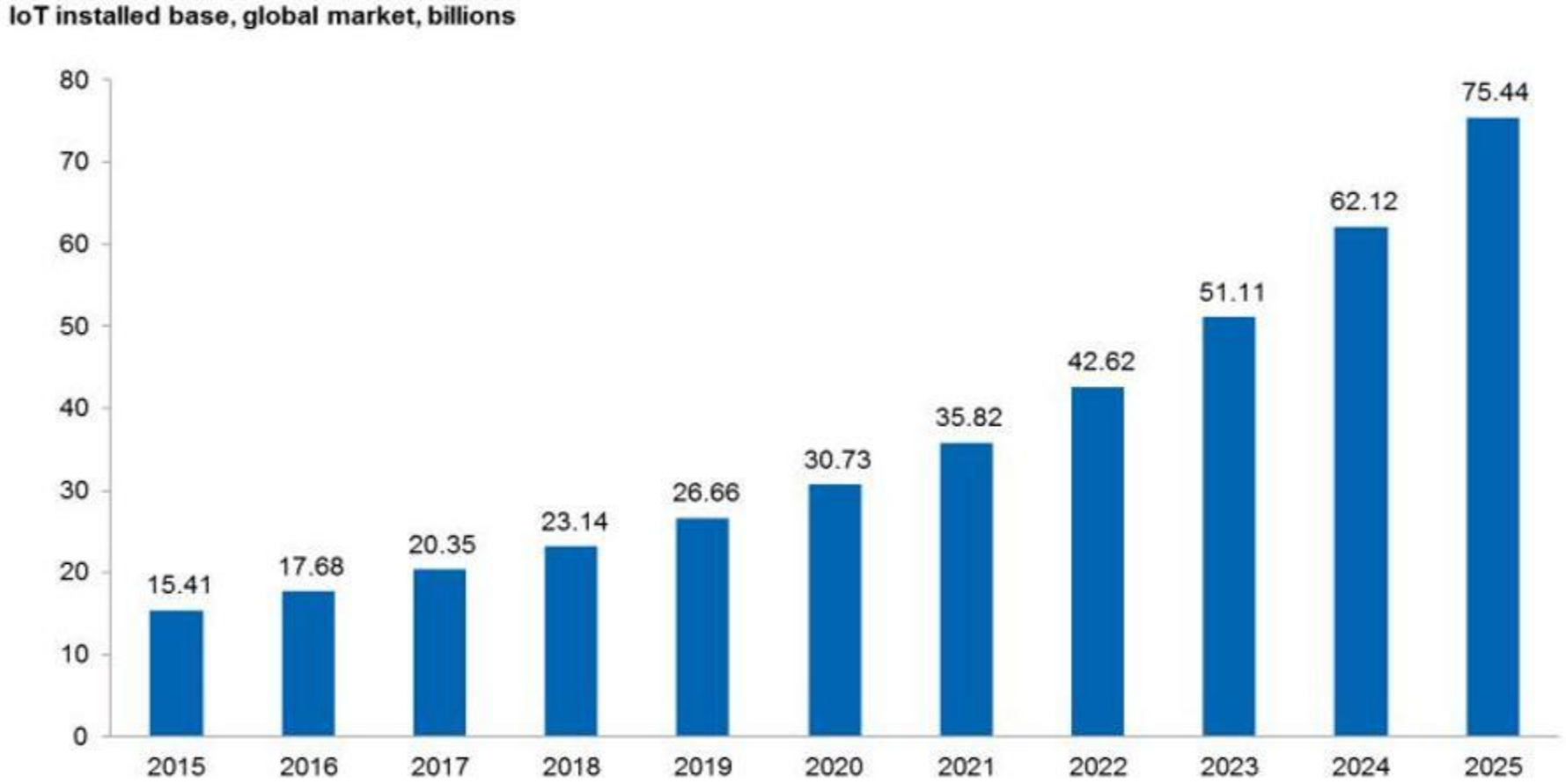

Heart-Monitors
Tires
Picture-frames
Programmable-Buttons
Breaker-Boxes
Locks
Ovens
Gas-Pump
Stuffed-Animals
Washing-Machines
Fireplaces
Batteries
POS-Systems
Propane-Tanks
Beds
Egg-Trays
Stoves
Yoga-Mats
Toasters
Blinds
Trashcans
Freezers
Smart-Meters
Luggage
Watches
Sinks
Fire-Alarms
Cars
Furnaces
Planter-Boxes
Lightbulbs
Voice-Recorders
Pool-Pumps
Doorbells
Wireless-APs
Routers
TVs
Golf-Balls
Dryers
Cameras
Air-Filters
Tooth-Brushes
Briefcases
Shower-Heads
Air-conditioners
Slow-Cookers
LEDs
Water-Pump
Breathalyzers
Suitcases
Thermostats
Coffee-Makers
Trains
Remotes
Air-Freshener
Sprinklers
Media-Boxes
Helmets
Petfood-Dispenser
Fidges
Insulin-Pumps
Industrial-Engines
Vents
Smart-Plugs
Speakers

Figure 1. The IoT market will be massive



Source: IHS

So what are the issues with IoT?

There are 3 overarching issues in terms of IoT security:

- Pervasiveness
- Uniqueness
- Ecosystem

Pervasiveness

- IoT devices are everywhere
- IoT devices largely outnumber conventional computing devices

Uniqueness

- IoT devices vary greatly in terms of their design and implementation
- This makes it more likely that one of your devices is vulnerable but also makes maintenance a pain

Ecosystem

- IoT devices typically leverage 3rd party web services to do what they want to do
- Where is your data going and what is being done with it?

Other IoT issues of note

- Low barrier to entry in terms of production
- Security is expensive and difficult to implement
- Devices run many unnecessary services
- It is very common for Iot devices to have outward facing admin panels

Case Studies

The Internet of Fails in action!

- White Hat
  - Jeep Cherokee hack
- Black Hat
  - 2016 Dyn cyberattack

Jeep Cherokee hack

- Researchers Charlie Miller and Chris Valasek

- Accomplished via Wi-Fi connection
  - Get the year and month of the jeep's manufactured date
  - Brings the search space to 7 million combinations
  - Brute force can be accomplished within an hour
  - Key space can be reduced furthermore
    - Date is based on default system plus a few seconds during which the head unit boots up
    - January 01 2013 00.00 GMT becomes January 01 2013 00.32 GMT

Jeep Cherokee Continued

- First hack
  - Control the music player
  - Track the car with its GPS

- Second hack
  - grants access to CAN bus
    - Steering wheel
    - Transmission
    - Braking System, not to mention dull things like windscreen wiper, air conditioner, door locks and so on

- Chrysler Recalls 1.4M Vehicles for Bug Fix

2016 Dyn cyberattack

- New World Hackers
- Type of attack
  - Massive DDoS attacks
- Companies affected
  - Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, the Playstation network, and many more

2016 Dyn cyberattack

- Hackers relied on Mirai
  - Malware that automatically finds Internet of Things devices to infect and turn into a botnet
- Botnet mainly consisted of routers and surveillance cameras
- 1.2 Tbps range (1,200 gigabits) per second
- Report is up to 100,000 malicious endpoints
- Masked TCP and UDP traffic over port 53

Moving forward

Addressing these issues & preventing them from happening

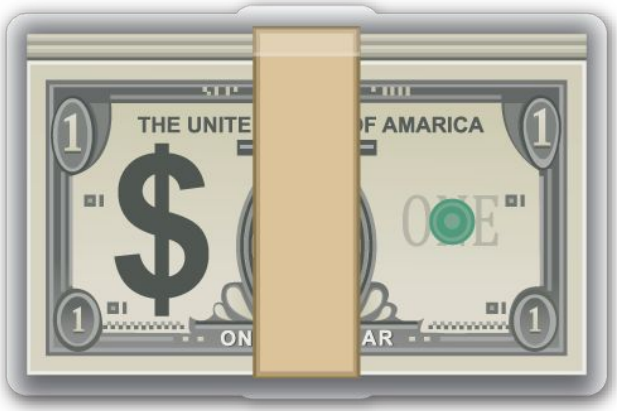
Consequences of negligence

Some of the malicious ways compromised IoT devices could be used:

- Means of conducting a DDoS attack
- Spying on users & stealing sensitive information
- Remotely controlling device -- derailing from intended purpose

Challenges

- Common security techniques are too heavy for IoT devices
- Tradeoff: specific, lighter software or general, more versatile protection?
- Companies maintaining competitive advantage
- Coordinating/integrating with other IoT devices



Ways to make it stop -- Producer

- Don’t hardcode passwords or symmetric encryption keys in firmware
- Use end-to-end encryption -- TLS (SSL) paired with AES
- Utilize token-based authentication
- Track metadata & monitor status of device
- Provide user friendly interface for updates + setup

Ways to make it stop -- Consumer

- Keep firewall and anti-virus software up to date
- Change default passwords
- Watch out for social engineering tactics

Questions

Question 1

Which one of these answers is **NOT** a major security concern for IoT devices?

a) They enlarge the attack surface of an organization

b) IoT devices run unnecessary services like telnet

c) **IoT devices have wireless capabilities**

d) IoT devices typically use inexpensive, low computing power hardware

Question 2

What type of attack was used in the 2016 Dyn Cyberattack?

a) DoS

b) DDoS

c) Trojan Horse

d) Spoofing

Question 3

Which of the following is false?

a) **SSL encryption is sufficient for protecting IoT devices**

b) There is no need for IoT devices to have extensive firewall and anti-virus protection (similar to a laptop's, for example)

c) The producer can contribute to protecting their IoT device

d) Keeping your system up to date is a way of protecting your IoT device

References

- http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things
- https://www.pubnub.com/static/papers/IoT_Security_Whitepaper_Final.pdf
- https://www.slideshare.net/duosecurity/internet-of-fails-where-iot-has-gone-wrong-and-how-were-making-it-right
- https://www.youtube.com/watch?v=WHdU4LutBGU
- https://www.youtube.com/watch?v=5cWck_xcH64
- https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/
- https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/
- http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/
- https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
- https://www.ihs.com/Info/0416/internet-of-things.html

Thank you!

Any questions?