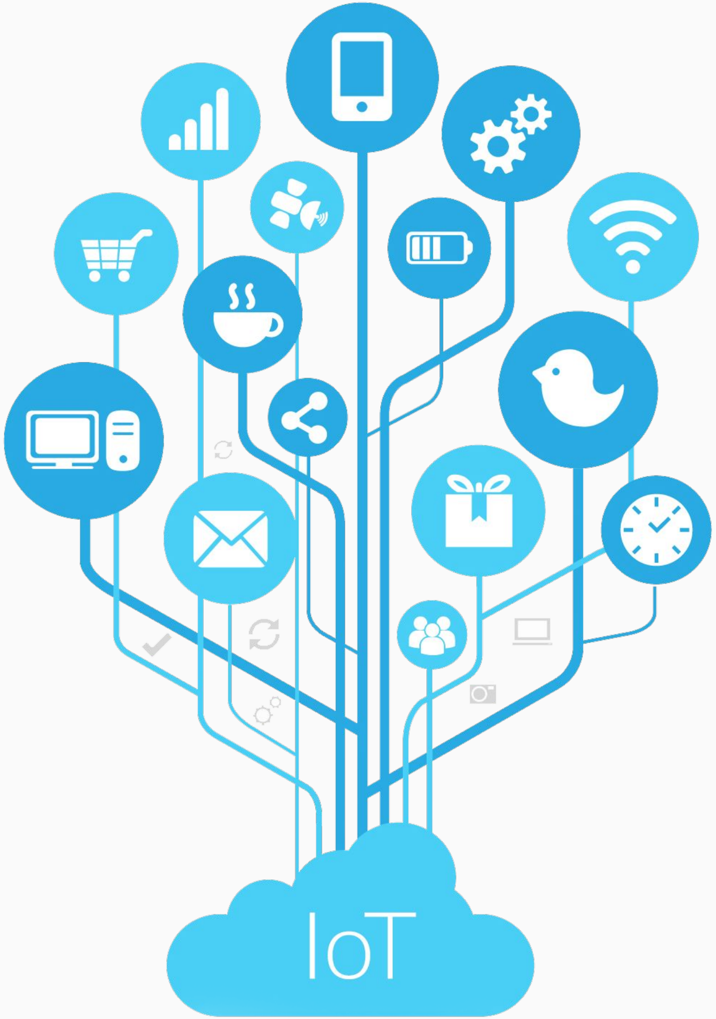
Diogo Ferreira *76504*
Luís Leira *76514*

IoT network monitoring in a vulnerable environment

Técnicas de Perceção de Redes

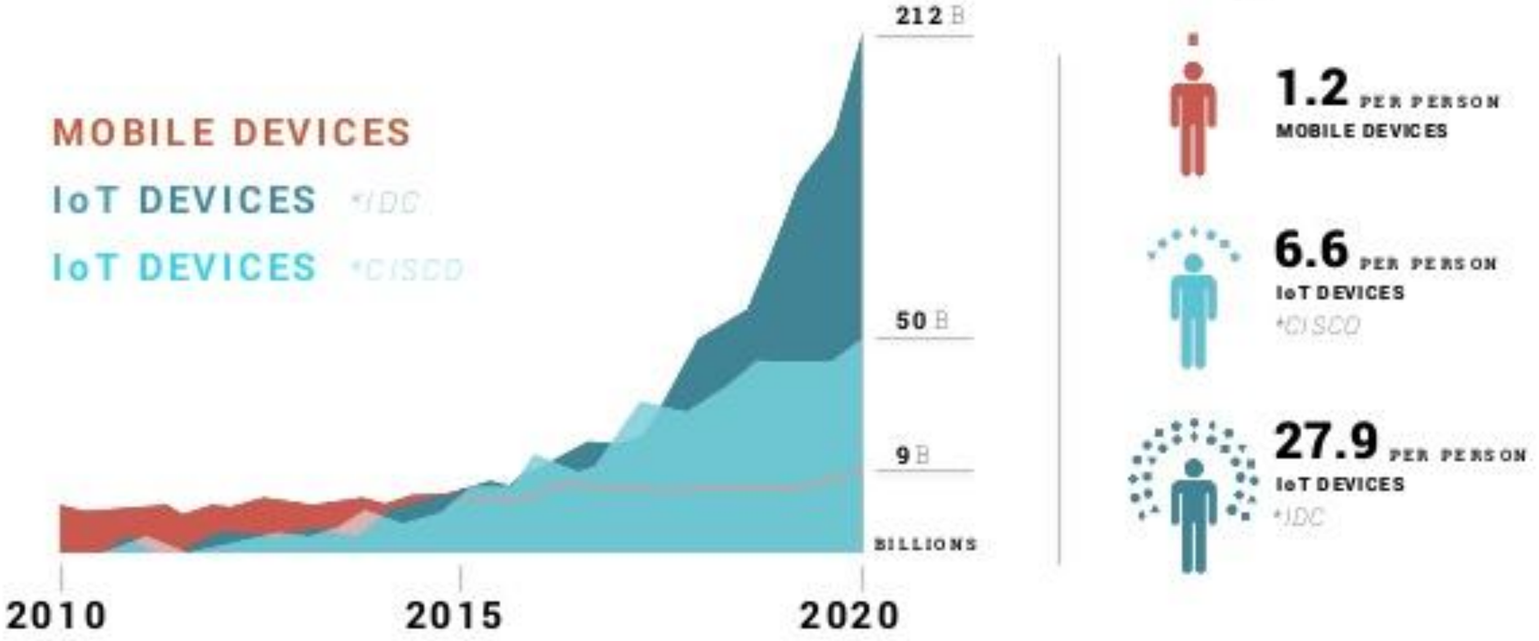
What is IoT?



Business intelligence platform

- Detects attacks on IoT networks
- Designed for large-scale companies to monitor network attacks on their devices

212BB Connected Devices by 2020



Why is this a problem?

The Internet of Things: The security crisis of 2018?

Information age, 2017

DDoS attacks increased 91% in 2017 thanks to IoT

In Q3 2017, organizations faced an average of 237 DDoS attack attempts per month. And with DDoS-for-hire services, criminals can now attack and attempt to take down a company for less than $100.

Tech Republic, 2017

Z-Wave Downgrade Attack Left Over 100 Million IoT Devices Open to Hackers

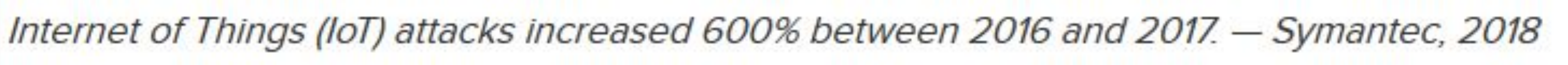
The Hacker News, March 2018

Why is this a problem?

IoT attacks are getting worse -- and no one's listening

There's a running joke regarding connected gadgets and the internet of things: "The 'S' in IoT stands for security."

Cnet, March 2018

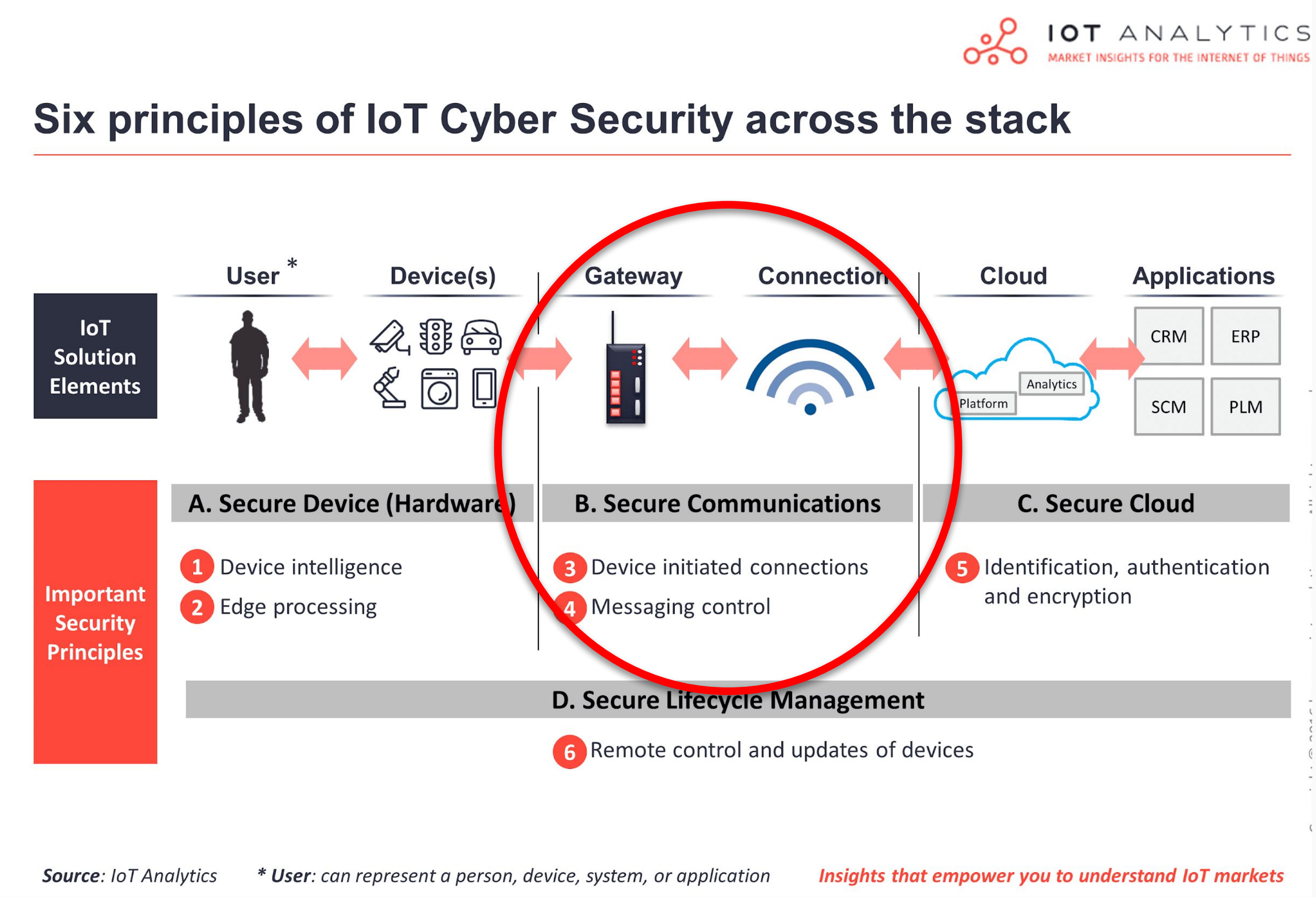


Internet of Things (IoT) attacks increased 600% between 2016 and 2017. — Symantec, 2018

IoT security spending to reach $1.5 billion in 2018

Gartner estimates that worldwide IoT security spending is set to climb this year in light of an escalation in attacks targeting IoT devices.

ZDNet, March 2018



IOT ANALYTICS
MARKET INSIGHTS FOR THE INTERNET OF THINGS

Six principles of IoT Cyber Security across the stack

A. Secure Device (Hardware)

1. Device intelligence
2. Edge processing

B. Secure Communications

3. Device initiated connections
4. Messaging control

C. Secure Cloud

5. Identification, authentication and encryption

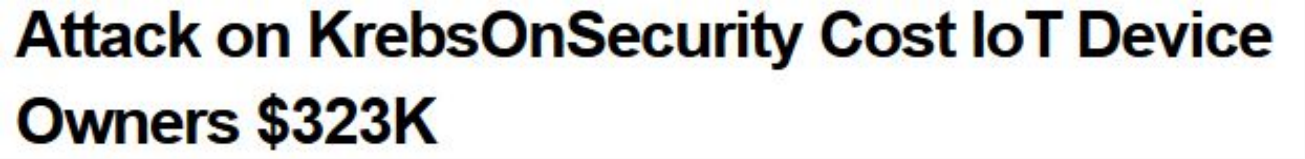
D. Secure Lifecycle Management

6. Remote control and updates of devices

__Source__: IoT Analytics *__* User__: can represent a person, device, system, or application* *__Insights that empower you to understand IoT markets__*

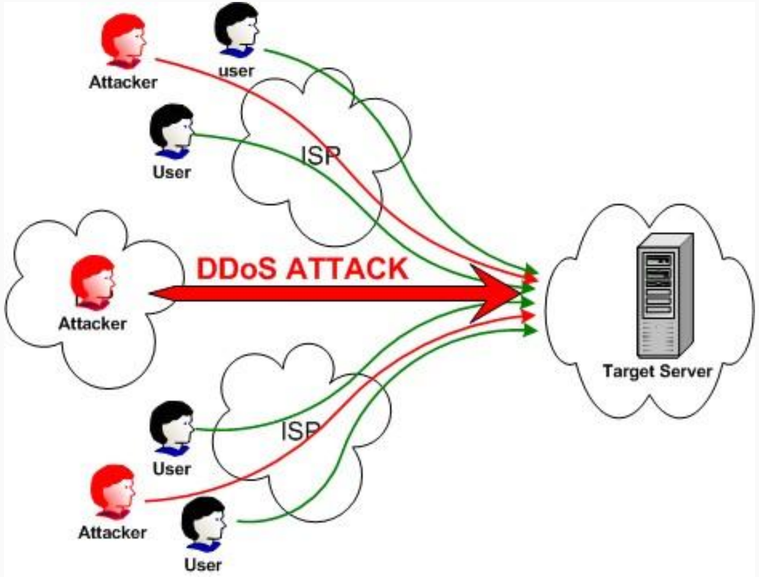
Our product targets three major scenarios

1. DDoS Attack



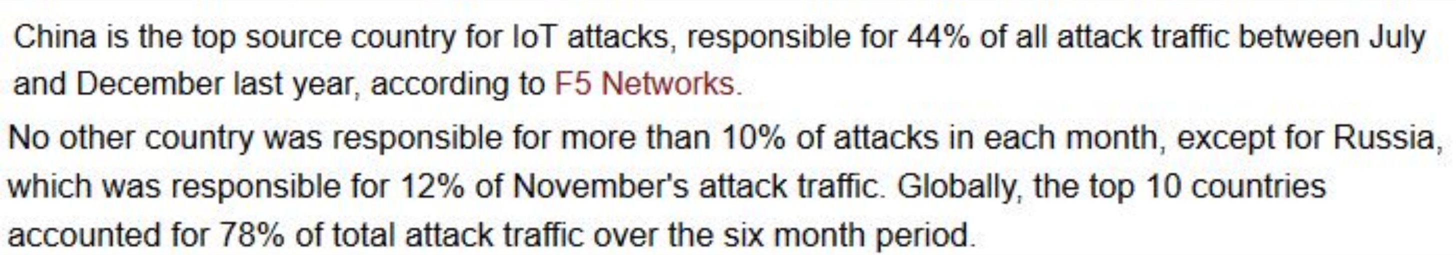
Attack on KrebsOnSecurity Cost IoT Device Owners $323K

KrebsOnSecurity, May 2018



TheDroidGuy, 2013

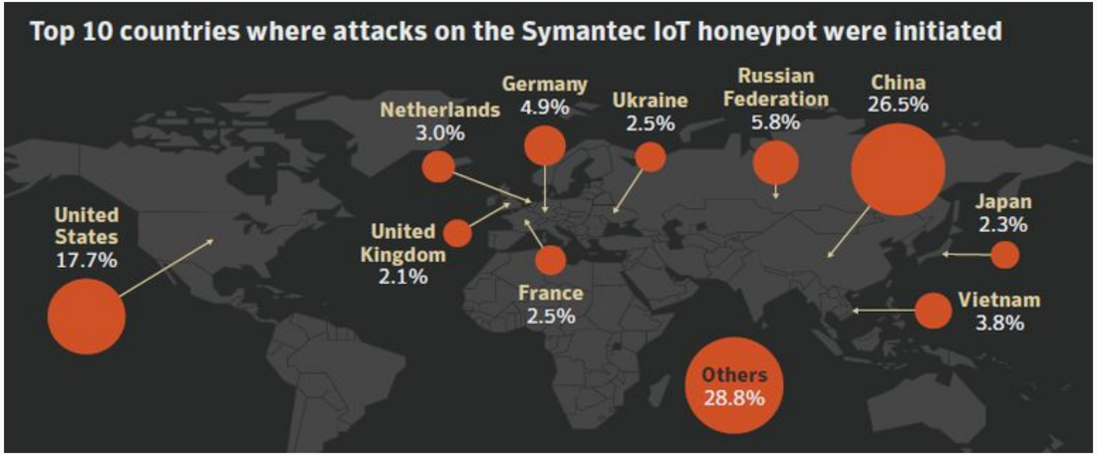
2. Sending private data to attacker



China is the top source country for IoT attacks, responsible for 44% of all attack traffic between July and December last year, according to F5 Networks.

No other country was responsible for more than 10% of attacks in each month, except for Russia, which was responsible for 12% of November's attack traffic. Globally, the top 10 countries accounted for 78% of total attack traffic over the six month period.

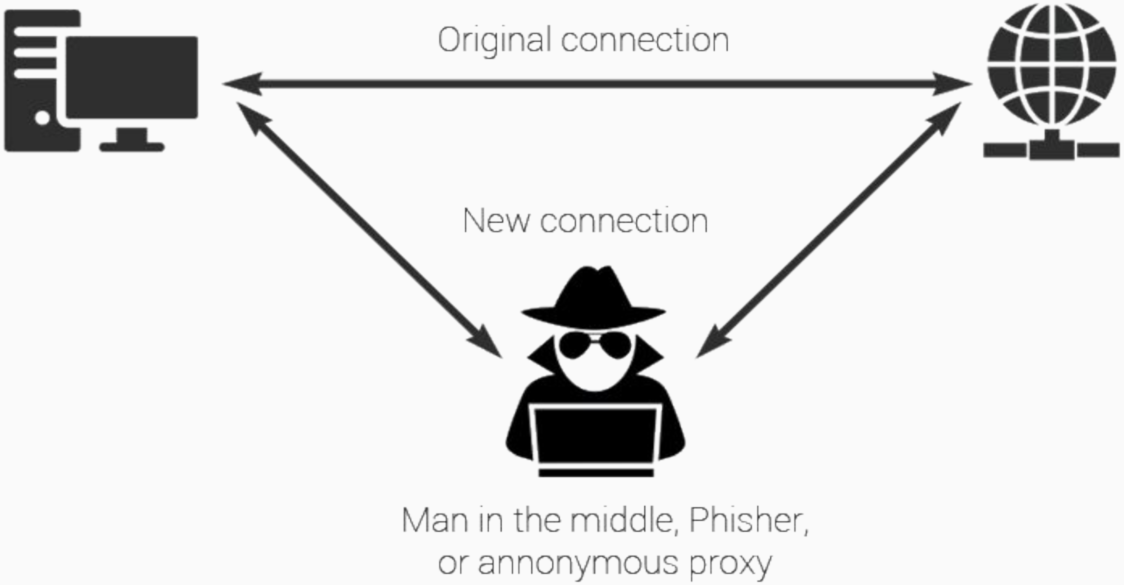
ComputerWorld, March 2018



Top 10 countries where attacks on the Symantec IoT honeypot were initiated

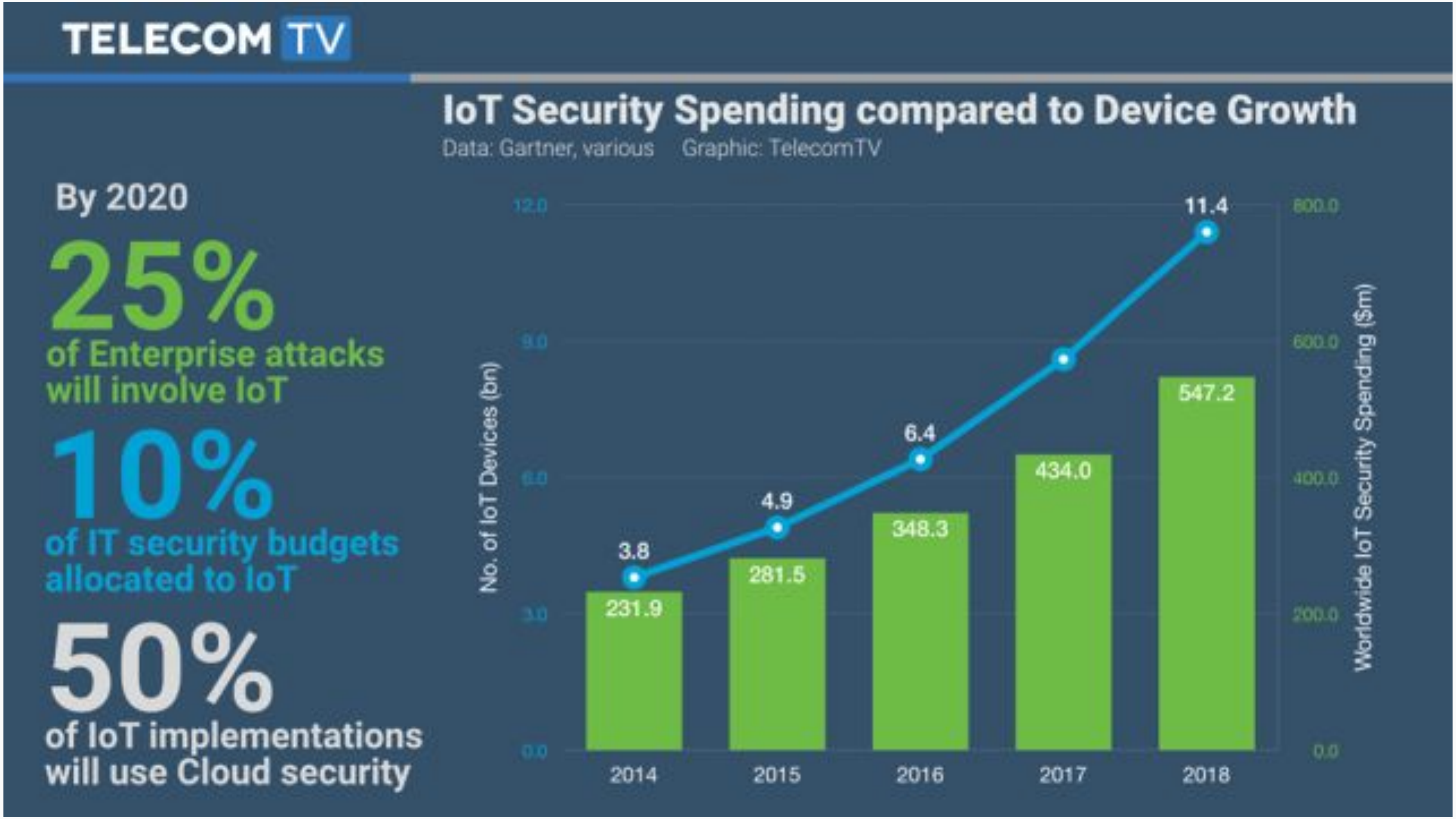
ZDNet, 2017

3. Man-in-the-middle attack



SecureBox, 2017

The market



TELECOM TV

IoT Security Spending compared to Device Growth

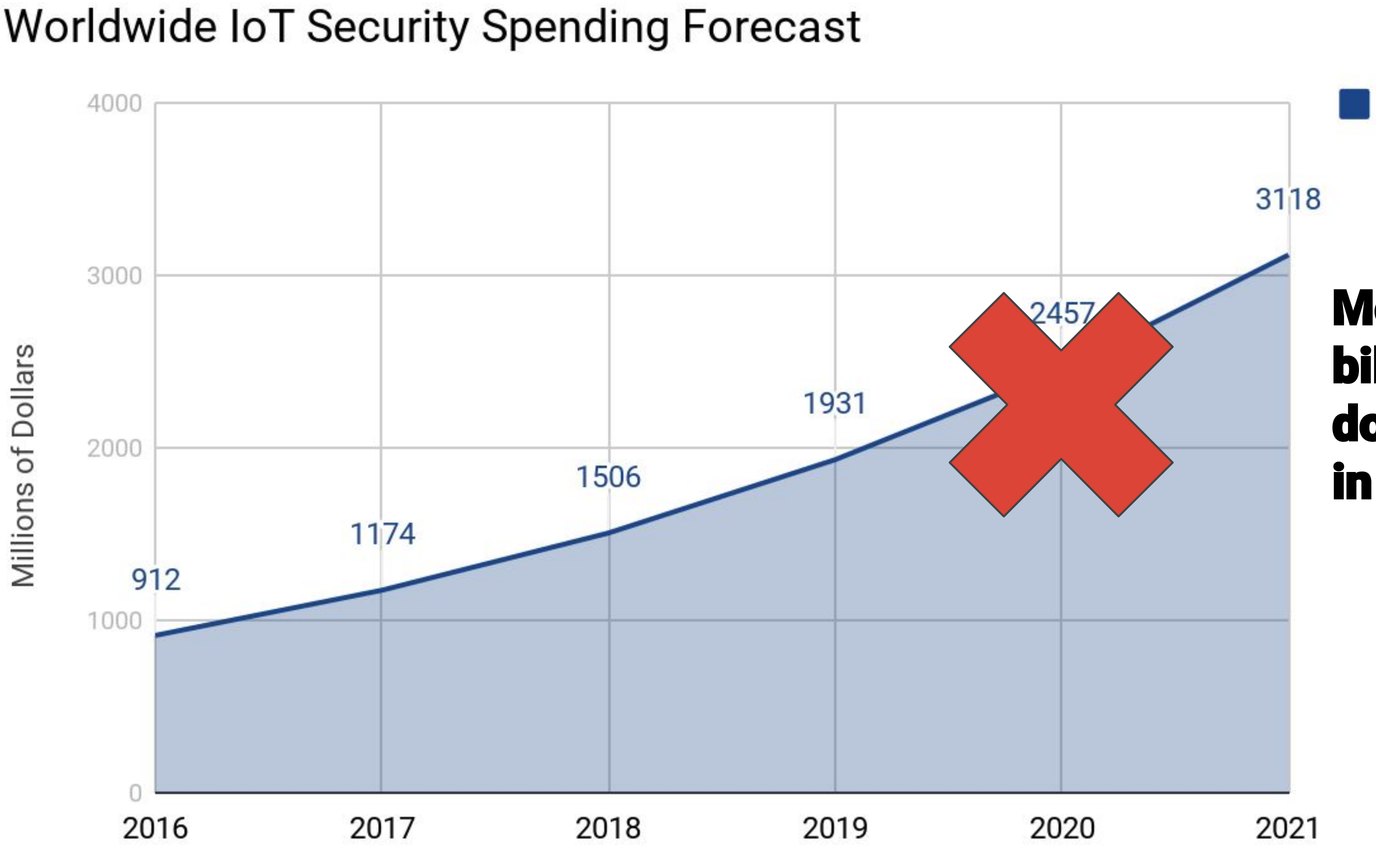
Data: Gartner, various Graphic: TelecomTV

By 2020

25% of Enterprise attacks will involve IoT

10% of IT security budgets allocated to IoT

50% of IoT implementations will use Cloud security



More than 3 billion dollars in 2021!

Gartner, March 2018

Advantages:

- Passive monitoring in the network
- Each monitoring device has low energy consumption and light resource requirements
- Detection of more than 97% of attacks described on previous scenarios

Disadvantages:

- Sensors need to be connected in the same network (e.g. VPN)
- One monitoring device per sensor

Give us a try to stay protected!

Diogo Ferreira *76504*
Luís Leira *76514*

IoT network monitoring in a vulnerable environment

Técnicas de Perceção de Redes