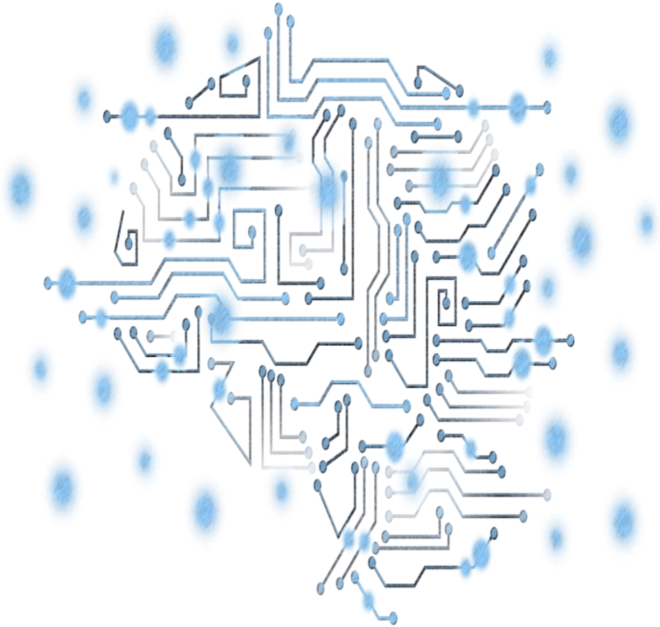
IoT: Cybersecurity

Outline

- Introduction
- Overview of IoT and Cybersecurity
- IoT Cybersecurity Ecosystem
- IoT Threat Landscape
- Supply Chain Security
- Securing IoT Networks

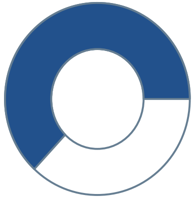
Introduction

- IoT (the Internet of Things) is the concept of connecting objects and devices of all types over the internet.
- Increasingly more objects and systems in our lives are becoming embedded with network connectivity and computing power in order to communicate with similarly connected devices or machines
- Cybercriminals are constantly searching for vulnerabilities in business networks, home computers, and now IoT devices for opportunities to steal information, and take control of computer systems remotely.
- One approach to this problem is how to secure the devices themselves.
- Applying tamper-evident and tamper-proof precautions to these devices will harden these endpoints and stop potential.
- In addition to securing individual IoT devices, organizations also need to ensure that their IoT networks are secure.
- Access control mechanisms and strong user authentication can help to ensure that only authorized users are able to gain access to the IoT framework.



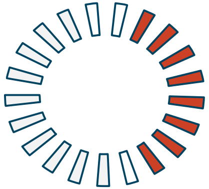
Overview of IoT and Cybersecurity

600% Increase in IOT attack between **2016 - 2017**



61% of IoT adopters have experienced security related incidence in the past

Gartner predicts that by the year 2020, over 25% of enterprise attacks will involve IoT



35% of business do not have cybersecurity expert in their team

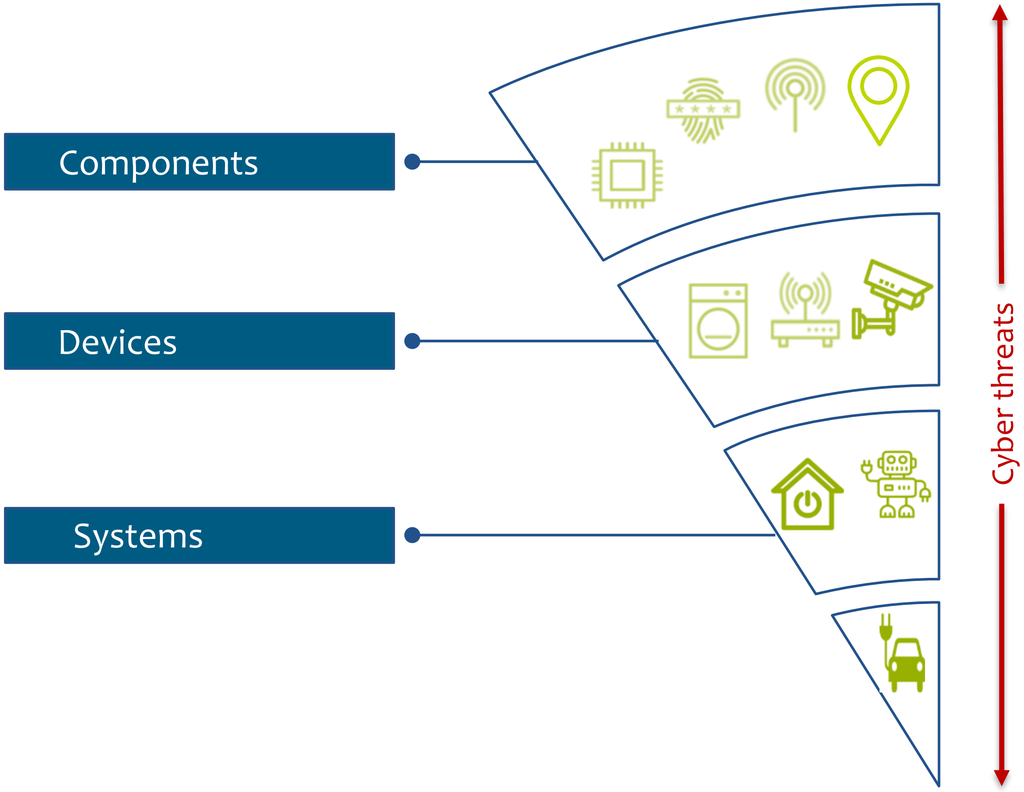
$3.1 Billion In 2021 Worldwide IOT security spending.

$6 Trillion By 2021 Annual total damage caused by cybercrime

By 2025 it is predicted that there will be an estimated **75 billion** internet connected devices globally

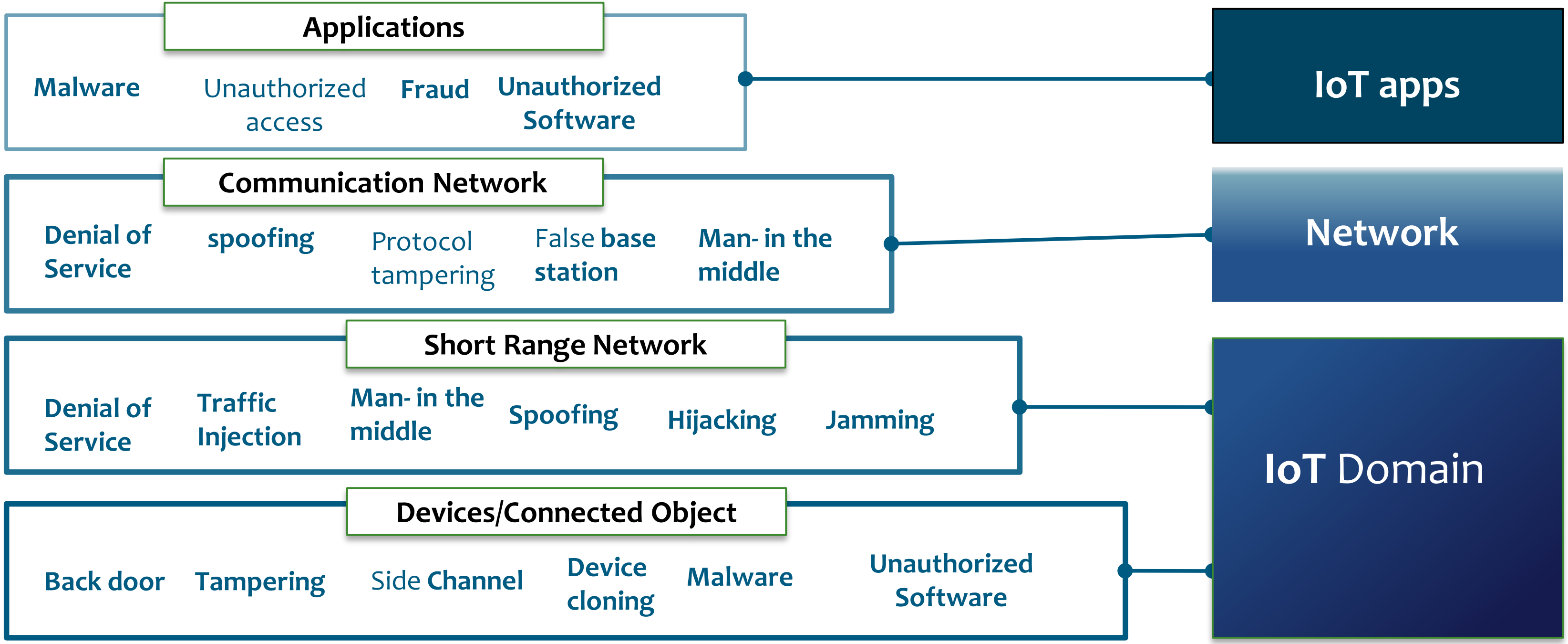
IOT Cybersecurity Ecosystem

- An IoT system is made up of various connected devices – which in turn comprise a number of integrated components – as well as a management, control and processing infrastructure.
- Devices can be subverted into performing incorrect actions or sending inaccurate data. When the device in question is a vehicle or a power plant, such activity can potentially threaten human safety.
- Connected devices may be a threat to a network if vulnerabilities along the IoT ecosystem are not adequately addressed.
- IoT risk extends beyond your own organization. connected devices can be used as part of a greater attack on other entities



IOT Security Ecosystem

IOT Threat Landscape



Applications

Malware

Unauthorized access

Fraud

Unauthorized Software

IoT apps

Communication Network

Denial of Service

spoofing

Protocol tampering

False base station

Man- in the middle

Network

Short Range Network

Denial of Service

Traffic Injection

Man- in the middle

Spoofing

Hijacking

Jamming

Devices/Connected Object

Back door

Tampering

Side Channel

Device cloning

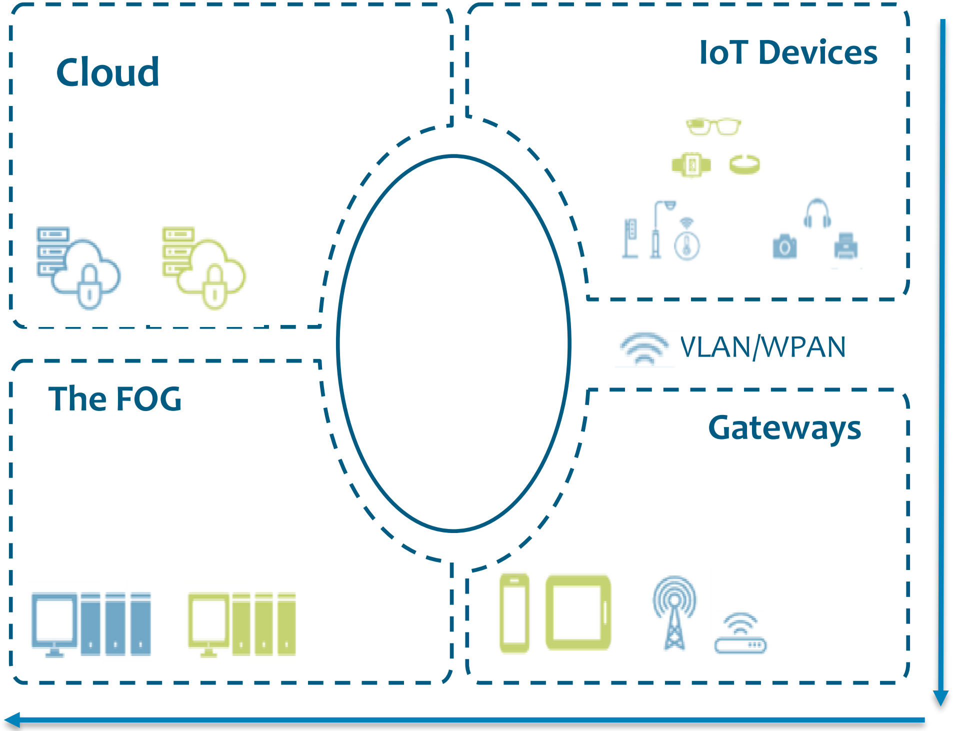
Malware

Unauthorized Software

IoT Domain

Supply chain security

- The security of an IoT system goes beyond protecting each of its constituent devices, management of the supply chain is crucial as the security of a system relies heavily on being able to trust in its various components.
- A single vulnerable device can compromise an entire system. Therefore it is imperative to conduct security assessment of the entire supply chain:
  - By assessing the risks and threats inherent in a given supply chain
  - By carrying out security audits on development and production plans
  - By security-testing solutions that do not hold a recognized security certificate
  - By assessing a system's inherent risks and threats
  - By evaluating the different layers (cloud, fog, remote mobile controllers) and their interface

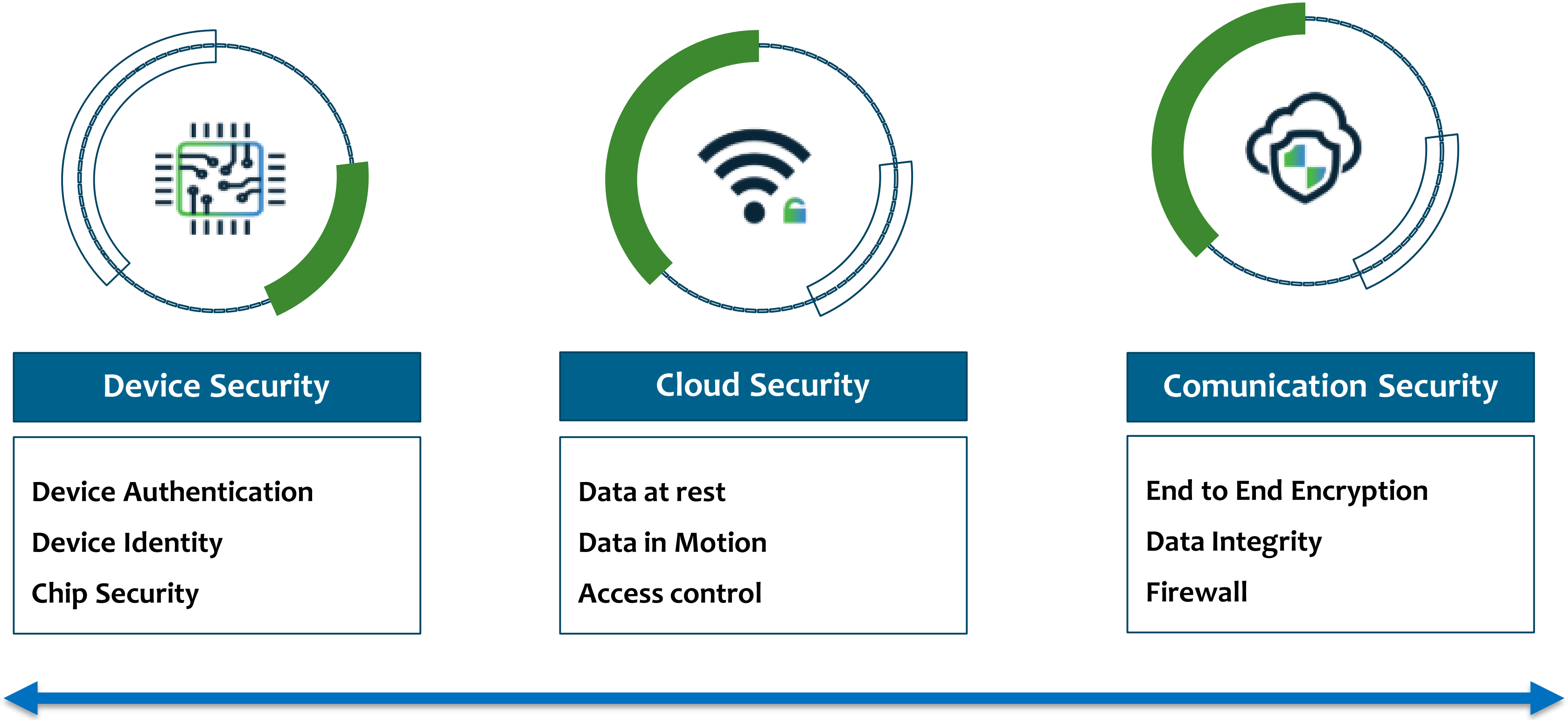


IEEE Standards Activities in the Internet of Things (IoT)

Harmonization and security of IoT: The IEEE 1451-99 is focused on developing a standard for harmonization of Internet of Things (IoT) devices and systems.

This standard defines a method for data sharing, interoperability, and security of messages over a network, where sensors, actuators and other devices can interoperate, regardless of underlying communication technology.

Securing IOT Networks



Device Security

Device Authentication

Device Identity

Chip Security

Cloud Security

Data at rest

Data in Motion

Access control

Comunication Security

End to End Encryption

Data Integrity

Firewall

Security lifecycle management

Application of IOT

Precision Farming and Smart Greenhouses

This is also known as precision agriculture. It is a more controlled and accurate when it comes to raising livestock and growing crops.

Features of precision farming include the adoption of access to high- speed internet, mobile devices, and reliable, low-cost satellites (for imagery and positioning).

Greenhouse farming helps in enhancing the yield of vegetables, fruits, crops, etc. a smart greenhouse can eb designed with IoT which helps monitor and control climate, eliminate the need for manual intervention.

Thank you

ecobank.com

Ecobank
The Pan African Bank