How to Identify Cyber Threats and Risks in any IoT Architecture

Ayman KHALIL

Managing Partner & COO

@H3XI0T

linkedin.com/in/khalilayman

RED ALERT LABS
IoT Security

Aviation Cybersecurity & IoT Context

ICAO Cyber Security and Resilience Symposium

As the aviation ecosystem becomes **more connected** and global aviation continues to experience **regular attacks** on several fronts, **Cyber Security** became a **key challenge** for the **aviation industry**.

Acknowledging the urgency and importance of protecting civil aviation's critical infrastructure, information and communication technology systems and data against **cyber threats**, ICAO MID Office is organizing the Cyber Security and Resilience Symposium

The objective of the Cyber Security and Resilience Symposium is to empower the aviation industry with **prevention measures to mitigate** the exploitation of **critical information system** and fostering a cyber-security culture that promotes a **resilient and secure cyberspace**.

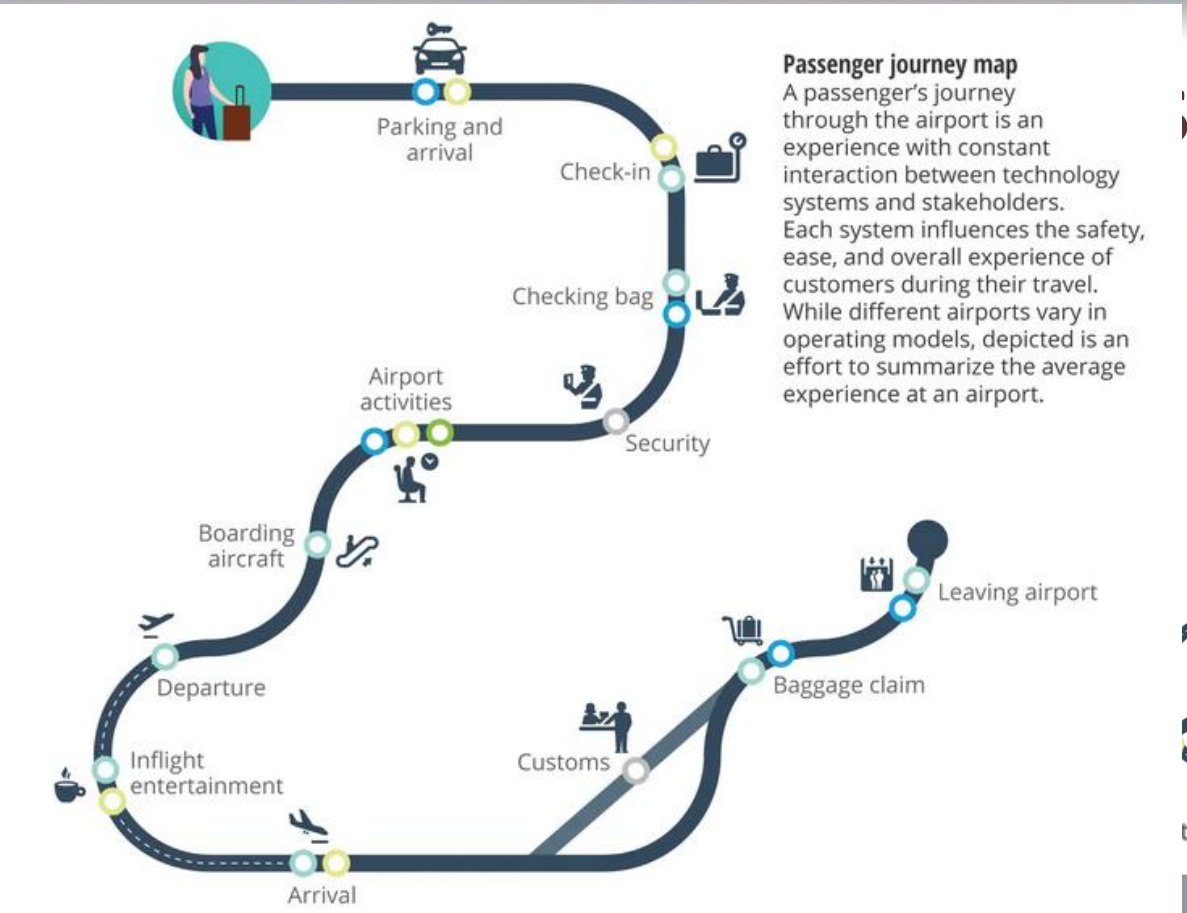
IoT (Internet of Things)

The Internet of Things, or **IoT**,

- is a **system** of interrelated computing **devices**, **mechanical** and **digital** machines,
- ability to **monitor** and **transfer data** over a **network**
- **without** requiring human-to-human or human-to-computer **interaction**.

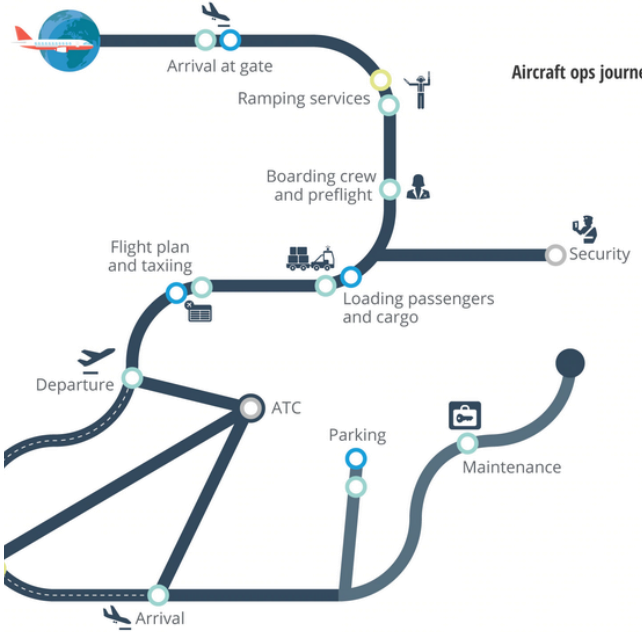
An **IoT Device** is a “Thing”,

- A **Hardware**
- A **Software**
- **Sensors** which detect and/or measure events in its operational environment and send the information to other components
- **Actuators** which are output units that execute decisions based on previously processed information



Passenger journey map
A passenger's journey through the airport is an experience with constant interaction between technology systems and stakeholders. Each system influences the safety, ease, and overall experience of customers during their travel. While different airports vary in operating models, depicted is an effort to summarize the average experience at an airport.

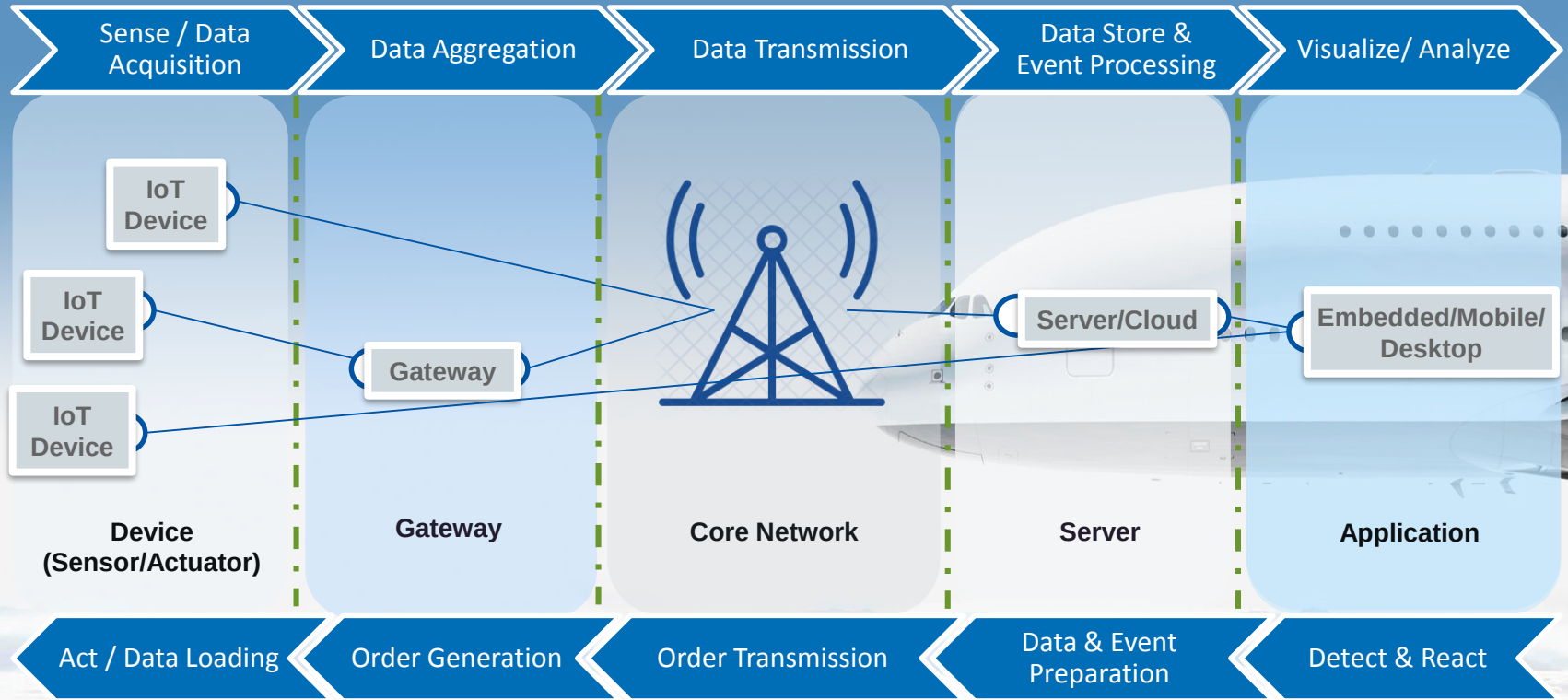
Smart Airports?



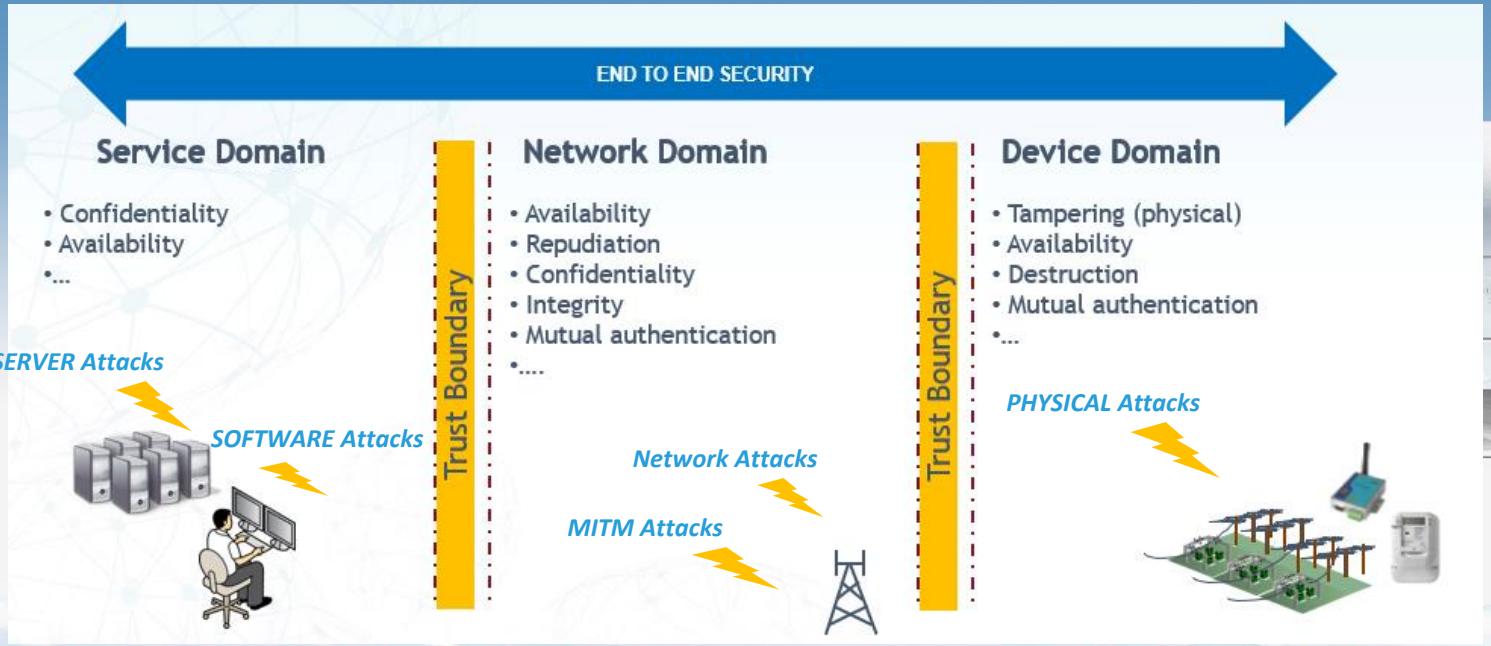
Aircraft ops journey map

tte

Typical IoT Infrastructure



IoT Threats


END TO END SECURITY
Service Domain
• Confidentiality
• Availability
•...
Trust Boundary
Network Domain
• Availability
• Repudiation
• Confidentiality
• Integrity
• Mutual authentication
•....
Trust Boundary
Device Domain
• Tampering (physical)
• Availability
• Destruction
• Mutual authentication
•...
SERVER Attacks
SOFTWARE Attacks
Network Attacks
MITM Attacks
PHYSICAL Attacks

Why Is It Hard To Secure?

Complex, distributed systems

- Many languages, Operation Systems, and networks
- Specialized hardware

Developing applications is hard

Securing them is even harder

- Enormous attack surface
- Reasoning across hardware, software, languages, devices, etc.
- Many types of threats and attack models
- Valuable data: personal, financial, health, location, presence

No time/money to invest on security + hard ➔ avoid, deal later

Why Is It Hard To Secure?

Longevity: these systems will last for up to 20 years and their security must too.

- Especially for critical infrastructures
- But need to adapt to evolving threats
- Implies “remote” security upgrade capabilities

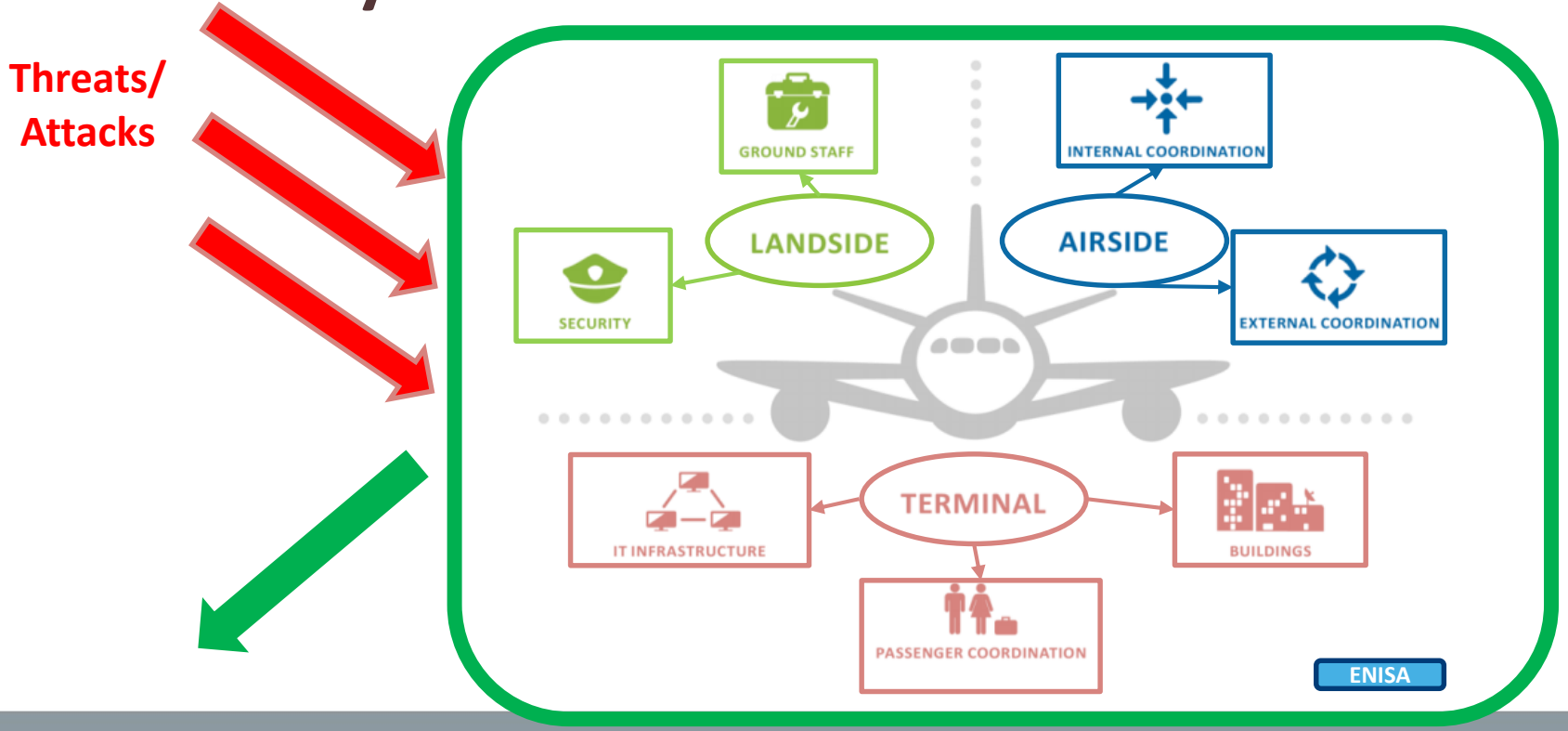
Hardly-reachable: IoT devices are not always close to humans.

- They might be physically exposed to attackers
- User not constantly monitoring activity
- Requires context based privacy configuration

Constrained resources (e.g battery power)

- Limited processing resources
- Sleep mode: communications not always online
- Often with limited bandwidth
- Challenge for revocation and upgradability

Step 1 – Know your environment



Step 2 - Identify Stakeholders

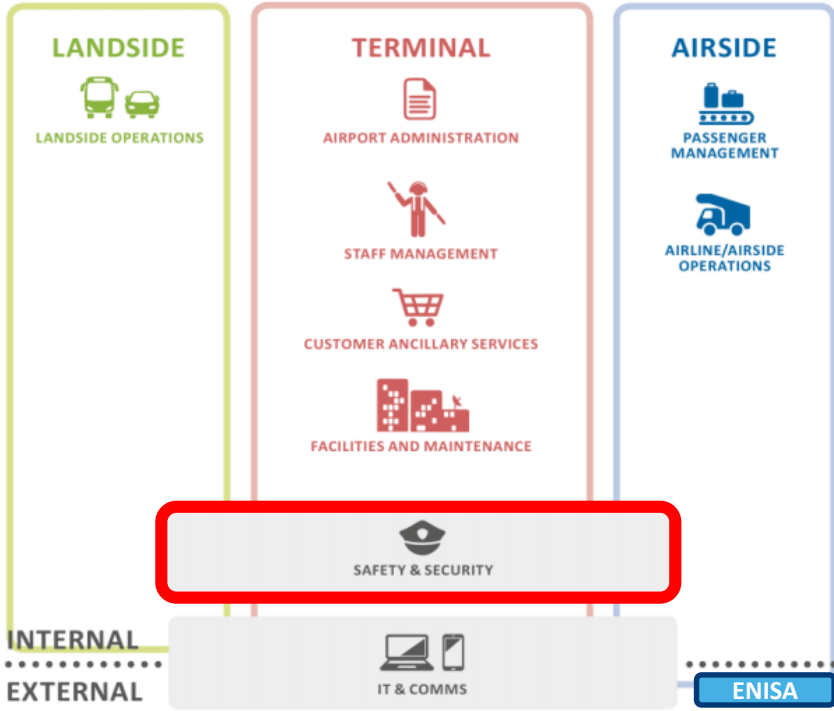
Step 3 & 4 - Identify & Prioritize Your Assets

Most Critical Assets Example:

- Passenger check-in and boarding?
- Baggage handling system?
- Air traffic management (atm), navigational aids…?

Less Critical Assets

- Flight Display System?
- Meteorological information systems?

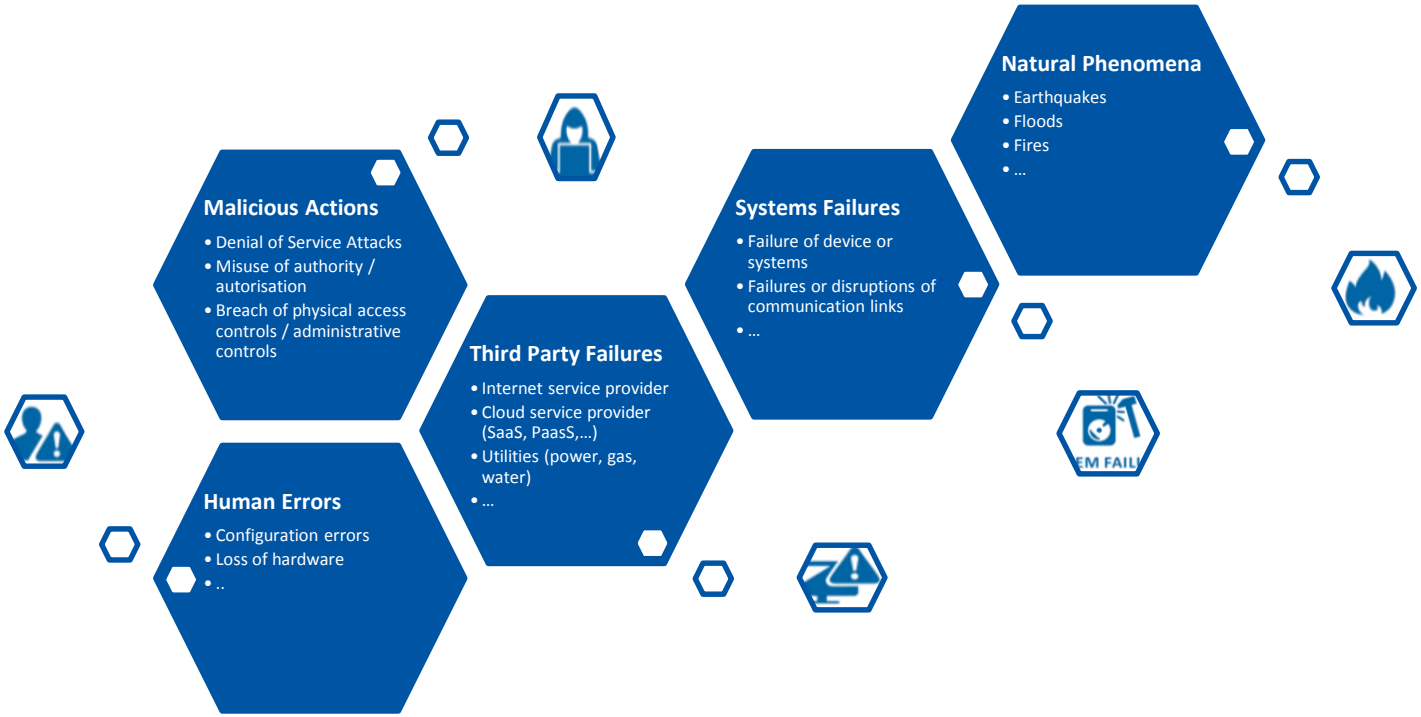


Security & Safety in IoT?

Security & Safety in IoT?

- Security is about preventing the adverse impacts that the environment can have on a system
- Safety is about preventing the adverse impacts a system can have on our environment
- Since IoT systems are intended to affect our environment, security issues often result in safety consequences

Step 5 & 6 - Identify your Threats and Attack scenarios



Step 7 & 8- Evaluate your attacks scenarios & Identify Security Measures

Type of Attacks

- Tampering with airport devices

Asset affected

- Self-service check-in devices, and connected IT Comms,
- Network Security Management

Criticality

- Medium to High

Likelihood

- Medium

Stakeholders involved

- Passengers
- Airline and Airport personnel
- IT Support Services
- Third Party Providers

Recovery Time and Efforts

Attacking check-in devices can compromise the whole chain of entities and processes involved in the e-ticketing system. Often third party providers will be involved in managing part of the service (e.g. local area network). This will require the whole chain to react to the attack by providing the effort needed to detect the flaw, and provide the solution to fix it.

Some Prevention Measures

- Data Encryption
- Disable services, close ports, restrict usage of external
- Intrusion Detection Systems (IDS)

KEY TAKEAWAYS

How to Identify Cyber Threats and Risks in any IoT Architecture

Step 1 – Know your environment

Step 2 - Identify Stakeholders

Step 3 & 4 - Identify & Prioritize Your Assets

Step 5 & 6 - Identify your Threats and Attack scenarios

Step 7 & 8- Evaluate your attacks scenarios & Identify Security Measures

Thank you!

Questions?

Ayman KHALIL
Managing Partner & COO
@H3XI0T
RED ALERT LABS
IoT Security
linkedin.com/in/khalilayman

ICAO

North American Central American and Caribbean (NACC) Office
Mexico City

South American (SAM) Office
Lima

ICAO Headquarters
Montréal

Western and Central African (WACAF) Office
Dakar

European and North Atlantic (EUR/NAT) Office
Paris

Middle East (MID) Office
Cairo

Eastern and Southern African (ESAF) Office
Nairobi

Asia and Pacific (APAC) Sub-office
Beijing

Asia and Pacific (APAC) Office
Bangkok

THANK YOU