Asia & Pacific ITU Regional Training on
Planning Internet of Things (IoT) Networks
Bandung, Indonesia 2018

Session 8: Planning for IoT Networks:

Threats, Issues and Challenges

25-28 September 2018
Bandung, Indonesia

Dr. Nizar Ben Neji
ITU Expert
University of Carthage
nizar.benneji@fsb.rnu.tn

Content

1. **Digital Security Evolution**
2. **Security Threats, Constraints and Concerns in IoT**
3. **Classes and Vectors of attacks**

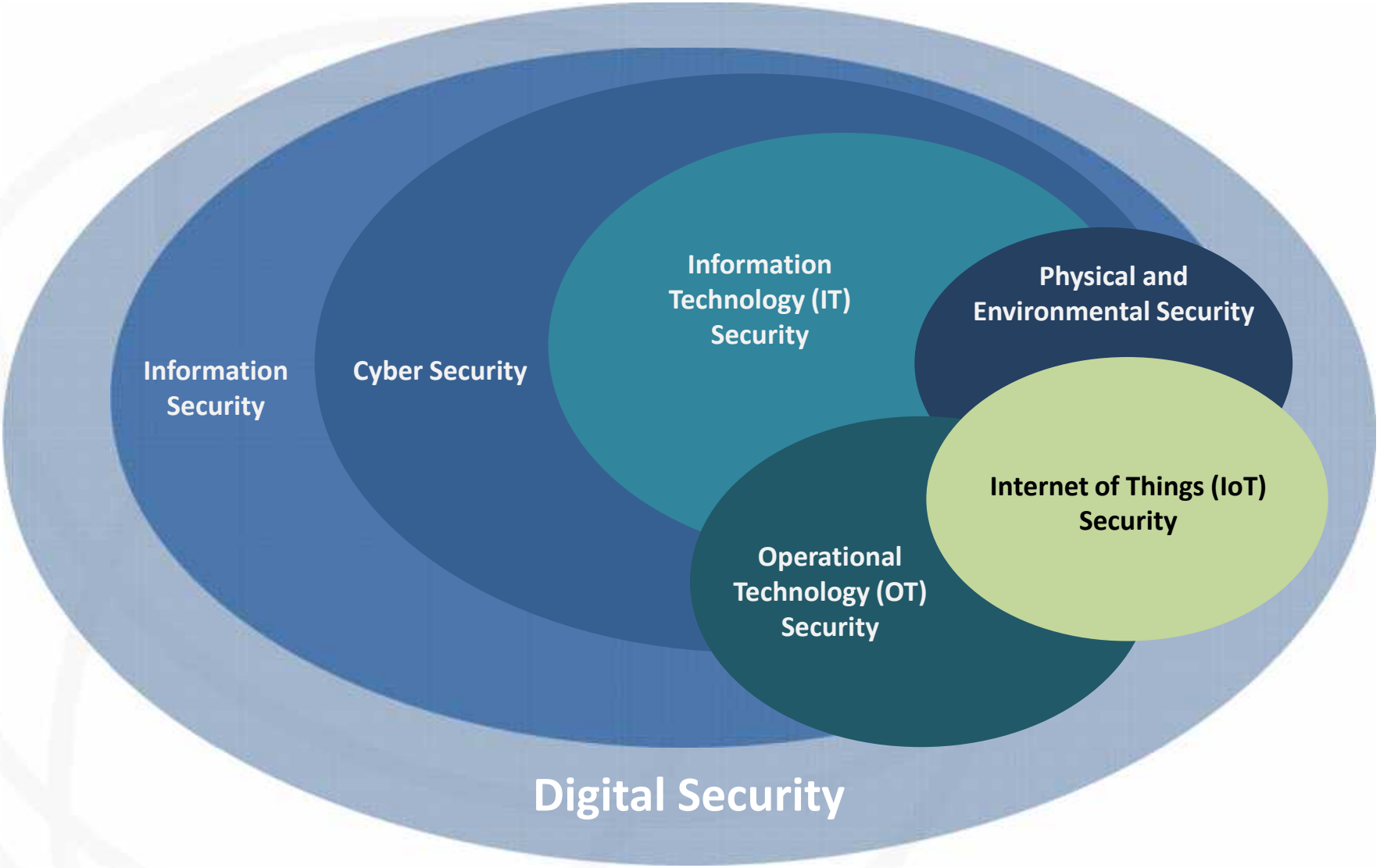
1

Digital Security Evolution

1. Digital Security Evolution
2. Protection Against Cybercriminality
3. Security Objects and Objectives
   - Authentication (Multifactor authentication, AAA, SSO, OTP, ...)
   - Confidentiality and privacy (Encryption, Anonymization, ...)
   - Data integrity over its entire life-cycle (Hashing, Digital signature, Electronic Proofs, Time Stamping, ...)
   - Non-repudiation of creating, approving, sending and receiving documents
   - High availability (Data replication, Failover, Load balancing, ...)
   - Traceability and history of electronic acts and actors
   - Privacy and protection of personal data
   - Building Trust
   - …

Evolution of Security

Digital Security



Digital Security

Terminology

- **Digital security** has evolved to be all-encompassing, since it addresses technology, data or information, physical and environmental security, privacy and safety.
- **Data security** means protection of digital data from corruption and from any destructive forces.
- **Information security** is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information regardless of the form the data may take (e.g., electronic, physical).
- **Cybersecurity** consists of technologies, processes and controls that are designed to protect from the unauthorised exploitation of systems, networks and technologies.

Digital Security

Terminology

- **Information technology security** includes hosts, networks, and application security: physical and logical protection.
- **Computer security** means protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. It includes mobile, server, desktop and cloud systems.
- **Network security** consists of the policies and practices adopted to prevent and monitor unauthorized network access, misuse, modification, or denial of any network resources.
- **Operational security** or procedural security (administration, management and use) means protecting security objects from the illegal actions of unauthorized users and from the unwanted actions of the authorized users.

Digital Security

Terminology

- **Physical security** is the protection of the IT infrastructure from physical actions and events that could cause serious loss. It includes protection from flood, fire, natural disasters, theft, burglary, vandalism and terrorism.
- **IoT security** is the protection of the connected environment (smart cities, smart buildings, connected cars, …) and it consists of the security practices, policies and techniques deployed to protect the interactions between things, people and between people and things. It includes but not limited to the following:
  - IoT Cloud security
  - IoT Gateway security
  - Mobile Device security
  - Light Weight security
  - …

Digital Security

Objects / Objectives

- In the Internet of Things, we need to protect a set of **elements**:
  - Data and information
  - Things and infrastructure
  - Applications and services
  - Systems and machines
  - Networks
  - Processes
  - Businesses (reputation, financial loss, ..)
  - Human (personal data, life, ..)
- Against the **security threats** that can be:
  - Accidental
  - Intentional
- To guarantee a set of **security objectives**:
  - Authentication
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Availability
  - Traceability
  - Privacy
  - Trust
  - …

Digital Security

Security objectives

- **Authentication** means being sure of the identity of the entity (human or machine) with which the transaction or the communication is being conducted.
- **Confidentiality** means protecting data from illegal access and from disclosure to unauthorized parties.
- **Integrity** means guaranteeing that data has not been altered since it was created, transmitted or stored.
- **Non-repudiation** means preventing a corresponding entity from denying its involvement in an electronic transaction
- **High-availability** means that a system needs to be accessible and usable 24/7 or just upon demand by an authorized entity

Digital Security

Security objectives

- **Traceability** means the ability to trace and identify all stages and events that led to a particular point in a system or process.
- **Privacy** means personal information needs to be collected, processed (used), protected, stored and destroyed legally and fairly.
- **Trust** means giving assurance that the trusted part will act as expected and not in way to cause harm to the system.
- …

Cyber criminality

Prediction and statistics

- Experts are predicting that cybercrime will cost businesses **6 trillion dollars** annually by 2021
- Millions of cyber crimes but few are prosecuted and adjudicated
- **556 Million** victims per year, **1.5 Million** victims per day and **1.8 victims** per second
- Top 3 countries victim of cybercrimes:
  - 92% Russia
  - 84% China
  - 80% South Africa
- Cyber crime goes mobile: **2/3 of Internet users** are using mobile devices and **31%** of victims are mobile users
- **40% of social network users** have fallen victim
- In 2020, 20.8 billion **Internet connected things**: Human more exposed to cyber criminality (Smart TV, Cameras, Intercoms, Locks, Cars, …)

Cyber criminality

Protection of the cyberspace

- **Cybercrime** is defined as a crime in which
  - A machine or a system is the object of the crime or target (hacking, software piracy, cyber vandalism, …)
  - A machine or a system is used as a tool or weapon to commit an offense (Cyber terrorism, Cyber defamation, cyber harassment, …)
- Protection against cybercrime activity needs:
  - IT mechanisms (hardware and software security solutions)
  - non IT mechanisms (regulation texts, policies, procedures, training, …)
- Protection of the cyberspace needs at first level:
  - Regulation texts (Laws, Decrees, Ministerial orders, …)
  - National Security Strategies
  - Security Policies (Information System, Network Security, Password, Privacy, …)
  - Technical and Management Procedures
  - Trainings (awareness, academic, recycling, …)
  - …

Cyber criminality

Stack of rules

2

Security Threats and Concerns in IoT

1. Security Vulnerability
2. Security Threat
3. Security Risk
4. Threat Agent and Business Impact
5. Security Assessment Guidelines
6. Security Contraints

Security Vulnerability

Definition

- **A security vulnerability** is a weakness in a product or a system that could allow an attacker to compromise the integrity, the availability, or the confidentiality of that product or that system.
- **The security weakness** in the system is generally due to a:
  - **Design** mistake or forgotten scenarios that can be exploited later by an attacker
  - Fault at the **implementation** level introduced by coders
  - Problem introduced at the **hosting** or deployment phase due to obsolete packages, systems not updated or security patches not applied
  - **Mishandling**, **misconfiguration** and any weaknesses introduced later by the end user

Security Vulnerability

OWASP IoT Vulnerabilities (1/4)

- **Username Enumeration:** Ability to collect a set of valid usernames by interacting with the authentication mechanism
- **Weak Passwords:** Ability to set weak account passwords or ability to use pre-programmed default passwords
- **Account Lockout:** Ability to continue sending multiple authentication attempts after failed login attempts
- **Unencrypted Services:** Network services are not properly encrypted to prevent eavesdropping or tampering by attackers
- **Weak Authentication:** Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner
- **Poorly Implemented Encryption:** Encryption is implemented however it is improperly configured or is not being properly updated, e.g. using SSL v2 or SSL v3

Security Vulnerability

OWASP IoT Vulnerabilities (2/4)

- **Update Sent Without Encryption:** Updates are transmitted over the network without using TLS or encrypting the update file itself
- **Update Location Writable:** Storage location for update files is world writable potentially allowing firmware to be modified and distributed to all users
- **Denial of Service:** Service can be attacked in a way that denies access to that service or deny access to the entire device
- **Removal of Storage Media:** Ability to physically remove the storage media from the device
- **No Manual Update Mechanism:** No option to manually force an update check for the device
- **Missing Update Mechanism:** No ability to update device

Security Vulnerability

OWASP IoT Vulnerabilities (3/4)

- **Firmware Version Display and/or Last Update Date:** Current firmware version is not displayed and/or the last update date is not displayed
- **Firmware and storage extraction:** Firmware contains a lot of useful information, like source code and binaries of running services, pre-set passwords, ssh keys etc
- **Manipulating the code execution flow of the device:** With the help of a JTAG adapter and gdb we can modify the execution of firmware in the device and bypass almost all software based security controls. Side channel attacks can also modify the execution flow or can be used to leak interesting information from the device.
- **Insecure 3rd party components:** Out of date versions of openssl, ssh, web servers, etc.

Security Vulnerability

OWASP IoT Vulnerabilities (4/4)

- **Obtaining console access:** By connecting to a serial interface, it is possible to obtain full console access to a device. Usually security measures include custom bootloaders that prevent the attacker from entering single user mode, but that can also be bypassed.

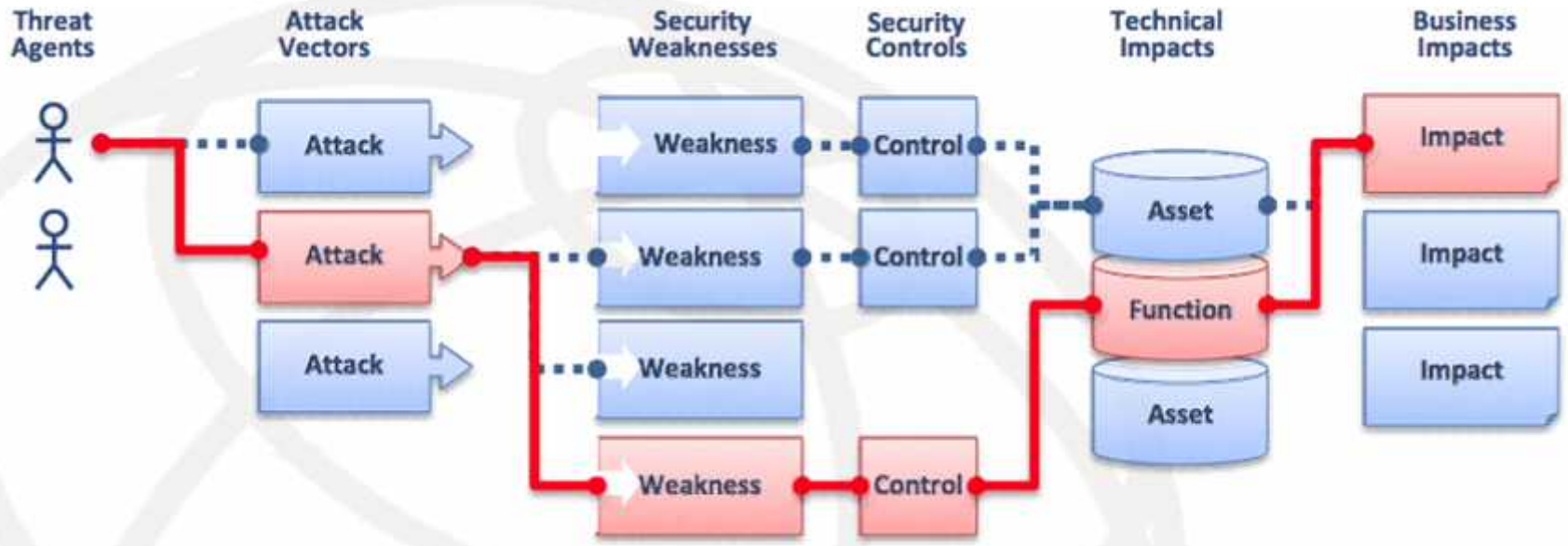
Security Threat

Definition

- A **security a threat** is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm to a system that can be physical or virtual
- Threats can be classified according to their type (accidental, intentional) and origin (internal and external):
  - Natural disaster (earthquake, fire, tornado, …)
  - Loss of essential services (electrical power failure, non-operational telecom access, …)
  - System malfunctioning or technical failures (equipment failure, software failure, system overloaded, …)
  - Human threats (hacking, spying, error in use, abuse of rights, …)
- Vulnerability + Threat ⟶ Security Risk

Threat Agent and Business Impact

OWASP



A **threat agent** through an **attack vector** exploits a **weakness** (vulnerability) of the system and bypass the related **security controls** (Countermeasures) causing a **technical impact** on an IT resource (asset) connected to a **business impact**.

Security Assessment Guidelines

Insecure Web Interface

- Assess any web interface to determine if weak passwords are allowed
- Assess the account lockout mechanism
- Assess the web interface for XSS, SQLi and CSRF vulnerabilities and other web application vulnerabilities
- Assess the use of HTTPS to protect transmitted information
- Assess the ability to change the username and password
- Determine if web application firewalls (WAF) are used to protect web interfaces

Insecure Network Services

- Assess the solution to ensure network services don't respond poorly to buffer overflow, fuzzing or denial of service attacks
- Assess the solution to ensure test ports are not present or open

Security Assessment Guidelines

Insufficient Authentication/Authorization

- Assess the solution for the use of strong passwords where authentication is needed
- Assess the solution for multi-user environments and ensure it includes functionality for role separation
- Assess the solution for the possibility of implementing two-factor authentication or more
- Assess password recovery mechanisms
- Assess the solution for the option to require strong passwords
- Assess the solution for the option to force password expiration after a specific period
- Assess the solution for the option to change the default username and password

Security Assessment Guidelines

Lack of Transport Encryption

- Assess the solution to determine the use of encrypted communication between devices and between devices and Internet
- Assess the solution to determine if accepted encryption practices are used and if proprietary protocols are avoided
- Assess the solution to determine if a firewall option is available

Privacy Concerns

- Assess the solution to determine the amount of personal information collected and whether it is encrypted at rest and in transit or no
- Assess the solution to determine whether the gathered data is anonymised or no
- Assess the solution to ensure that the gathered data needed for proper operation of the device is visible to the end users

Security Assessment Guidelines

Insecure Cloud Interface

- Assess the cloud interfaces for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces)
- Assess the cloud-based web interface to ensure it includes at least a two-factor authentication, an account lockout mechanism and disallows weak passwords
- Assess any cloud interfaces for XSS, SQLi and CSRF vulnerabilities and other vulnerabilities
- Assess all cloud interfaces to ensure transport encryption is used
- Assess the cloud interfaces to determine if the option to require strong passwords is available
- Assess the cloud interfaces to determine if the option to force password expiration after a specific period is available
- Assess the cloud interfaces to determine if the option to change the default username and password is available

Security Assessment Guidelines

Insecure Mobile Interface

- Assess the mobile interface to ensure that it includes at least a two-factor authentication, an account lockout mechanism and disallows weak passwords
- Assess the mobile interface to determine if it uses transport encryption
- Assess the mobile interface to determine if the option to require strong passwords is available
- Assess the mobile interface to determine if the option to force password expiration after a specific period is available
- Assess the mobile interface to determine if the option to change the default username and password is available
- Assess the mobile interface to determine the amount of personal information collected

Security Assessment Guidelines

Insufficient Security Configurability

- Assess the solution to determine if password security options (password policy, factors definition, …) are available
- Assess the solution to determine if encryption options (e.g. Enabling AES-256 where AES-128 is the default setting) are available
- Assess the solution to determine if logging for events is available
- Assess the solution to determine if alerts and notifications to the user for security events are available and sent properly

Insecure Software/Firmware

- Assess the device to ensure it includes update capability and can be updated quickly when vulnerabilities are discovered
- Assess the device to ensure it uses encrypted update files and that the files are transmitted using encryption
- Assess the device to ensure that it uses signed files and then validates that file before installation

Security Assessment Guidelines

Poor Physical Security

- Assess the device to ensure it utilizes a minimal number of physical external ports (e.g. USB ports) on the device
- Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port
- Assess the device to determine if it allows for disabling of unused physical ports such as USB
- Assess the device to determine if it includes the ability to limit administrative capabilities to a local interface only (no remote administration)

Security Constraints

Resources Limitation

- Low power requirements are needed since **security is energy consuming**
- Security countermeasures must never degrade in the **absence of connectivity** or in case of **low bandwidth**
- **Absence of physical barrier**: IoT nodes are likely to fall into adversarial hands and attackers can have easily physical access to edge components and can manipulate them, move them to hostile networks, and control their resources
- **Distributed and ad-hoc nature** of the system make security a complicated mission especially face to **heterogeneous systems**

Security Constraints

Large number of connected devices

- The volume of IoT means that every design and security consideration must also take **into account scale** (volume of nodes)
- Security countermeasures must perform well at volume (volume of transactions and data).
- Simple bootstrapping into an ecosystem can create a self denial of service condition
- Huge interconnectedness in IoT architectures complicates traceability and faulty data propagation is not easily detected
- Monitoring is becoming more complex du to the exponential increase in the number of IoT nodes
- Distributed environment and no single points where to implement security policy

Security Constraints

Big Data

- The more the system has data the more valuable it is as target
- **Volume:** Security should consider the vast amounts of data generated by the IoT nodes every second
- **Velocity:** Security should consider the speed at which new data is generated and the speed at which data moves around.
- **Variety:** Security should take into account structured and unstructured data like text, photo, audio and video contents
- **Variability:** Security should consider changing data, model and linkage
- **Value:** Generated value is based on accurate data
- **Veracity:** IoT systems should always verify data from the edge in order to prevent accidental or intentional misinformation and harm the whole system

3

Classes and vectors of attacks

1. Attack vectors and surface
2. Sources of attacks
3. Classification of attacks and attackers
    - Active and passive attacks
    - Physical Attacks
    - Network Attacks
    - Application Attacks
    - Inherited Internet Attacks
    - IoT Specific Attacks

Security Attack

Definition

- Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools.
- **Attack cost** is measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost
- IoT attacks may target
  - IoT sensors
  - IoT devices
  - IoT gateways
  - Home LAN
  - Cloud

Attack Surface

Weak Points

- An attack surface is the some of the different **attack vectors** or weak points that are accessible to a hacker
- Attack surfaces can be divided in to **three categories**
  - Physical attack surface
  - Network attack surface
  - Software attack surface
- **Attack surface analysis** is an assessment of the total number of exploitable vulnerabilities which attackers can take advantage of to compromise authenticity, confidentiality, integrity, privacy or availability of a system

Attack Surface

OWASP IoT Attack Surface Areas (1/6)

Attack Surface	Vulnerability
Ecosystem Access Control	• Implicit trust between components • Enrollment security • Decommissioning system • Lost access procedures
Device Memory	• Cleartext usernames • Cleartext passwords • Third-party credentials • Encryption keys
Device Physical Interfaces	• Firmware extraction • User CLI • Admin CLI • Privilege escalation • Reset to insecure state • Removal of storage media

Attack Surface

OWASP IoT Attack Surface Areas (2/6)

Attack Surface	Vulnerability
Device Web Interface	• SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Weak passwords • Account lockout • Known default credentials
Device Firmware	• Hardcoded credentials • Sensitive information disclosure • Sensitive URL disclosure • Encryption keys • Firmware version display and/or last update date
Local Data Storage	• Unencrypted data • Data encrypted with discovered keys • Lack of data integrity checks

Attack Surface

OWASP IoT Attack Surface Areas (3/6)

Attack Surface	Vulnerability
Administrative Interface	• SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Weak passwords • Account lockout • Known default credentials • Security/encryption options • Logging options • Two-factor authentication • Inability to wipe device
Third-party Backend APIs	• Unencrypted PII sent • Encrypted PII sent • Device information leaked • Location leaked

Attack Surface

OWASP IoT Attack Surface Areas (4/6)

Attack Surface	Vulnerability
Cloud Web Interface	• SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Weak passwords • Account lockout • Known default credentials • Transport encryption • Insecure password recovery mechanism • Two-factor authentication
Update Mechanism	• Update sent without encryption • Updates not signed • Update location writable • Update verification • Malicious update • Missing update mechanism • No manual update mechanism

Attack Surface

OWASP IoT Attack Surface Areas (5/6)

Attack Surface	Vulnerability
Mobile Application	• Implicitly trusted by device or cloud • Username enumeration • Account lockout • Known default credentials • Weak passwords • Insecure data storage • Transport encryption • Insecure password recovery mechanism • Two-factor authentication
Ecosystem Communication	• Health checks • Heartbeats • Ecosystem commands • Deprovisioning • Pushing updates

Attack Surface

OWASP IoT Attack Surface Areas (6/6)

Attack Surface	Vulnerability
Vendor Backend APIs	• Inherent trust of cloud or mobile application • Weak authentication • Weak access controls • Injection attacks
Network Traffic	• LAN • LAN to Internet • Short range • Non-standard

Types of Attacks and Attackers

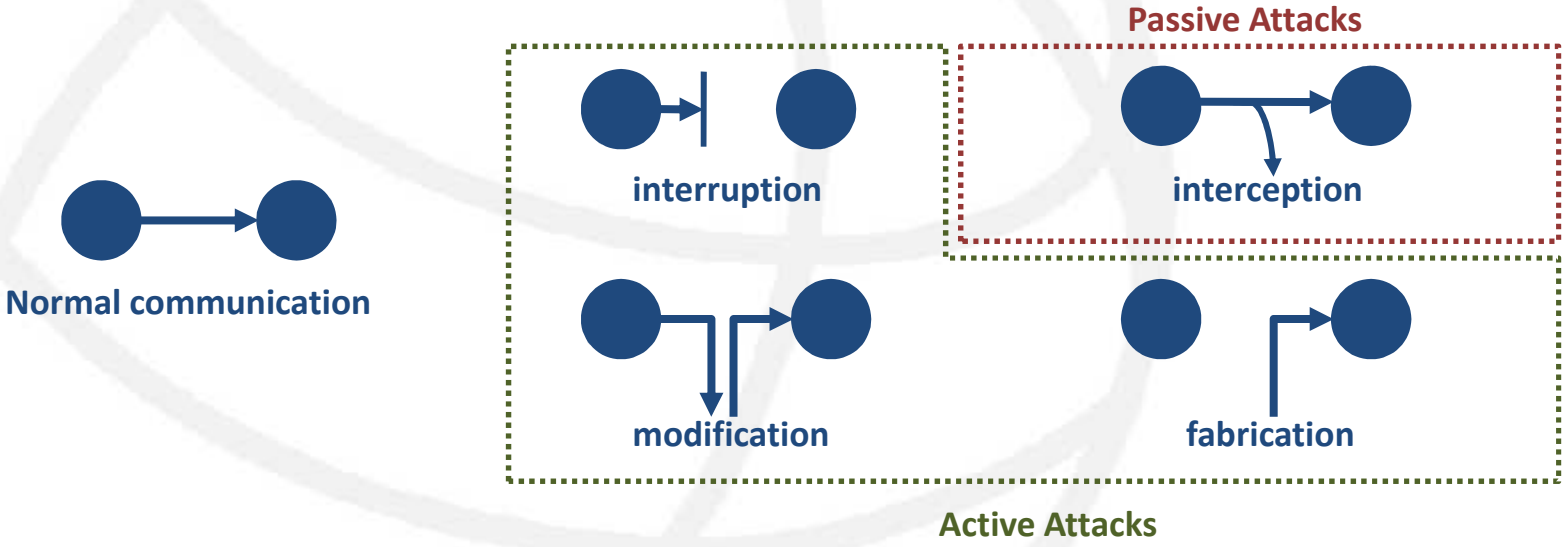
Different Classes

- Active and passive attacks
- Layer classification of attacks:
  - Physical attacks
  - Network attacks
  - Software attacks
- Inherited Internet attacks and IoT specific attacks
- Internal and external attackers
- Individuals, organized groups and intelligence agencies
- 3 types of insider attackers:
  - Malicious: deliberately steals information or sabotages systems
  - Exploited: may be deceived by external parties into providing data or passwords
  - Unintentional: may accidentally delete or modify critical information or unwittingly share sensitive data

Classes of Attacks

Active and Passive attacks

- An **active attack** attempts to alter the system resources or affect their operation, so it may compromise authenticity, integrity or availability
- A **passive attack** attempts to make use of information from the system but does not affect the system resources, so it may compromise confidentiality



Physical Attacks

Hardware and Channel Attacks

- IoT devices deployed in an **unprotected environment** (city streets, forests, car parks, …) easily accessible by attackers
- Target the **hardware** or the **communication channels**
- **Require physical proximity** to the system to get access to the nodes, sensors, collectors, ….
- Physical attacks are mainly:
  - Deploy malicious nodes between legitimate nodes
  - Inject malicious codes to grant access to the IoT system by plugging USB key into the device
  - Extract data, security credentials and source codes or clone the device
  - Physically damage the IoT device to disrupt the availability of the system
  - Conduct a DoS attack by making signal interference on wireless networks
  - Launch sleep deprivation attacks to maximize consumption of energy then shut nodes down
  - Side channel attacks by analysing the physical measurements during computation

Network Attacks

Remote Attacks

- Target the whole **IoT** infrastructure (Nodes, Gateways, Collectors, Cloud, …)
- Attacks can be **conducted remotely** as well as locally and they essentially target network services such as DNS, DHCP and Internet routing
- Network attacks are mainly:
  - Sniffing attacks in order to intercept data and metadata
  - Masquerading or spoofing nodes means that the communicating node is not the claimed one
  - Sinkhole attack by compromising nodes to attract packets from neighboring nodes or to selectively forward, alter or drop traffic, leading to data confidentiality issues, or deny service to the network
  - Routing attacks to alter the traffic flow, to reconfigure the network topology, to create routing loops, to generate false errors or to modify source routes
  - Launch DDoS attacks by overflowing network devices with more requests than they can handle or by exhausting computation or communication resources

Software Attacks

Application Layer

- Software or application layer attacks target software installed in sensors, collectors, gateways and cloud
- Software attack can
  - Help perform reverse engineering,
  - Extract source codes,
  - Compromise and exploit the entire system,
  - Steal sensitive information,
  - Alter stored and transferred data,
  - Deny systems,
  - Compromise or damage nodes.
- Include malware attacks (Virus, Worms, Backdoors, Key loggers, Botnet, Scarewares, Ransomwares, Logic bombs, …)
- Include social engineering attacks and tricking users into providing access or credentials

Inherited Internet Attacks

Examples

- Cryptanalysis attacks attempt to deduce encryption keys (ciphertext-only, chosen-plaintext, adaptive-chosen-plaintext, chosen-ciphertext and adaptive-chosen-ciphertext)
- Phishing, vishing, smishing, pharming and deceiving userswith fake interfaces, nodes and servers
- Software piracy and counterfeiting of programs
- Make a system or a resource unavailable
- Masquerading or spoofing users: the actual sender is not the claimed one
- Malware dissemination (Virus, Worm, Scareware, Ransomware, Trojan, Backdoor, …)
- Tampering documents
- Data leak
- …

IoT Specific Attacks

Examples

- Cross domain attacks since various networks are interconnected (electricity, energy, telecom, computer, …)
- Cross context attacks (personal, professional, social, …)
- Large scale DDoS attacks consisting of a numerous compromised or zombie devices, forming a botnet and sending a flood of traffic to a target server: Zombie devices could be any IoT object such as printers, webcams, baby monitors, residential gateways, …
- Side channel attacks by analyzing physical measurements during computation and the internal state of the physical device during processing

THANK YOU FOR YOUR ATTENTION

Dr. Eng. Nizar Ben Neji
IT Security Trainer, Consultant and Researcher
PhD in Information and Communication Technologies
nizar.benneji@fsb.rnu.tn /(+216) 99 207 377