IoT Security: Threats, Challenges, and Safeguards

Joseph Bugeja
ABOUT ME

✓ Phd student in Computer Science

✓ Main research themes: security, privacy, and Internet of Things

✓ Lic in Computer Science, MSc in Information Security, BSc in Computer Science and AI

✓ 14 years working in the software industry
MY PREVIOUS PROFESSIONAL INFORMATION SECURITY DUTIES

- Business Continuity
- Risk Management
- Incident Management
- Policy
- Software Development Lifecycle
- Organization
- Access Control
- Asset Management
- Comms & Ops Management
- HR Security
- Compliance
- Physical & Environmental

Joseph Bugeja

IoT Security
Joseph Bugeja

IoT Security

Source: https://edu.mah.se/sv/Course/DA351A
AGENDA

Introduction

Challenges in Securing IoT

Countermeasures

The Internet of Things

Attacks and Malicious Threat Agents

Joseph Bugeja

IoT Security
Introduction
A WHILE AGO AND STILL

Fences

Seals

Signatures

Locks

Joseph Bugeja
THE LANDSCAPE AROUND US HAS EVOLVED

Internet

Smart speakers

Wearables

Websites

Drones

How can we secure these things?
✅ 73,000 private video cameras leaking live footage (2014)

But now cameras are getting tinier, more powerful, and portable allowing them to be embedded in ‘unexpected’ devices.
Smart devices may jeopardize your security and privacy

“A hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees”

“Hackers could steal personal information and turn the microphone of the doll into a surveillance device”

“After hearing the anchor’s comment, their own devices also tried to order pricey dollhouses”
A plain-clothed police officer quickly identifies and locks in on a wanted suspect in a crowded square through the 5G glasses’ facial recognition function.

Chinese police test gait-recognition technology from AI start-up Watrix that identifies people based on how they walk

- Known as gait recognition, the technology works by analysing thousands of metrics about a person’s walk and storing them in a database
- Software can identify a person from 50 metres away – even if they have their face covered or back to camera

The Pentagon has a laser that can identify people from a distance—by their heartbeat

The Jetson prototype can pick up on a unique cardiac signature from 200 meters away, even through clothes.
The Internet of Things
THE EVOLUTION OF NETWORKING

1. Network

2. The Internet

Joseph Bugeja

IoT Security
THE EVOLUTION OF NETWORKING

3. Mobile-Internet

4. Mobiles + People + PCs

Joseph Bugeja

IoT Security
THE INTERNET OF THINGS

5. Internet of Things

Interconnected Objects

Joseph Bugeja

IoT Security
THE INCREASE IN THE DEPLOYMENT OF IOT DEVICES

Global Connected and IoT Device Installed Base Forecast

DIFFERENT APPLICATIONS OF IOT

Joseph Bugeja

IoT Security
BASIC REQUIREMENTS FOR AN IOT SOLUTION

1. Unique Address
2. Sensing & actuating
3. Ability to Communicate
4. Notification & Control
IOT IN SMART HOMES

- Improves energy efficiency, security/safety, entertainment, and healthcare support.
- Remote management of Internet-connected devices such as doors, refrigerators, TVs, etc.
- Data related with home, power, telecoms, gas and water can be sent automatically to utility companies and to other service providers for other reasons.
A smart connected home leverages IoT technologies to improve the quality and efficiency of life to the residents.
THE SMART CONNECTED HOME CHARACTERISTICS

- Perimeter in the cloud(s)
- Wireless & cellular technologies
- Physical and digital access
DIGITAL CHATTER INSIDE THE HOME

The Joy of Tech

FATTYPANTS IS KIDDING HIMSELF IF HE THINKS HE’S EATING LESS THAN 2000 CALORIES A DAY!

AT LEAST YOU GET USED! I NEVER DO! ALL HE EATS IS TAKE-OUT!

I REFUSE TO PICK UP THIS FRENCH FRY. LAZYBONES CAN DO IT HIMSELF!

HE SPENT A FORTUNE ON US SMARTBULBS AND HE ONLY USES THE "WHITE LIGHT" SETTING! *SIGH*

DID YOU SEE WHAT TIME HE GOT IN LAST NIGHT? SCANDALOUS!

HEY GUYS! THE HOUSE SMARTMETER IS TELLING EVERYONE THAT SCAREDY CAT STILL USES A NIGHT LIGHT! HA HA!

DUMMY NEEDS TO TEST ME NOW AND THEN, OR AT LEAST CHECK MY APP!

DON’T BOTHER HIM! THE PREVIOUS SMOKE DETECTOR, HE BEAT TO DEATH WITH A BROOM HANDLE!!

What your Internet of Things is saying about you...

© 2014 Geek Culture
Challenges in Securing IoT
IOT REFERENCE FRAMEWORK

- IoT Services
- Network channels and infrastructure
- IoT Devices

Software apps.

Sensors
Actuators
Connected objects

IoT Gateway

IoT Network

Joseph Bugeja

IoT Security
THE SMART CONNECTED HOME ARCHITECTURE

Note: WAN, LAN, NAN, HAN, PAN, BAN, and WSN correspond to wide area, local area, neighbourhood area, home area, personal area, body area, and wireless sensor networks respectively.
Some Device Level Challenges

- Memory, computing, energy, storage, and throughput constraints
- Lack of keyboard, mouse, and tactile screen
- Easily accessible devices are prone to physical attacks
Some network and service-level challenges

- Use of bridges, hubs or gateways make the design of end-to-end security challenging

- Devices can join/leave the home networks anytime from anywhere

- Some devices are expected to operate for a long time without requiring maintenance
Attacks and Malicious Threat Agents
Information security is generally defined as the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (ISO27001)
INFORMATION SECURITY REQUIREMENTS

- Security requirements in the Information Assurance & Security (IAS) octave

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Definition</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Ensuring that only authorized users access the information</td>
<td>C</td>
</tr>
<tr>
<td>Integrity</td>
<td>Ensuring completeness, accuracy, and absence of unauthorized data manipulation</td>
<td>I</td>
</tr>
<tr>
<td>Availability</td>
<td>Ensuring that all system services are available, when requested by an authorized user</td>
<td>A</td>
</tr>
<tr>
<td>Accountability</td>
<td>An ability of a system to hold users responsible for their actions</td>
<td>AC</td>
</tr>
<tr>
<td>Auditability</td>
<td>An ability of a system to conduct persistent monitoring of all actions</td>
<td>AU</td>
</tr>
<tr>
<td>Trustworthiness</td>
<td>An ability of a system to verify identity and establish trust in a third party</td>
<td>TW</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>An ability of a system to confirm occurrence/non-occurrence of an action</td>
<td>NR</td>
</tr>
<tr>
<td>Privacy</td>
<td>Ensuring that the system obeys privacy policies and enabling individuals to control their personal information</td>
<td>P</td>
</tr>
</tbody>
</table>
Evolution of security threats over time


Joseph Bugeja

IoT Security
## SUMMARY OF IOT SECURITY THREATS

<table>
<thead>
<tr>
<th>Threat</th>
<th>Against</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Trojans</td>
<td>All</td>
</tr>
<tr>
<td>Side-channel attacks</td>
<td>C,AU,NR,P</td>
</tr>
<tr>
<td>DoS</td>
<td>A,AC,AU,NR,P</td>
</tr>
<tr>
<td>Physical attacks</td>
<td>All</td>
</tr>
<tr>
<td>Node replication attacks</td>
<td>All</td>
</tr>
<tr>
<td>Camouflage</td>
<td>All</td>
</tr>
<tr>
<td>Corrupted node</td>
<td>All</td>
</tr>
<tr>
<td>Tracking</td>
<td>P, NR</td>
</tr>
<tr>
<td>Inventorying</td>
<td>P, NR</td>
</tr>
<tr>
<td>Tag cloning</td>
<td>All</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td>All</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>C,NR,P</td>
</tr>
<tr>
<td>Injecting fraudulent packets</td>
<td>P,I,AU,TW,NR</td>
</tr>
<tr>
<td>Routing attacks</td>
<td>C,I,AC,NR,P</td>
</tr>
<tr>
<td>Unauthorized conversation</td>
<td>All</td>
</tr>
<tr>
<td>Malicious injection</td>
<td>All</td>
</tr>
<tr>
<td>Integrity attacks against learning</td>
<td>C,I</td>
</tr>
<tr>
<td>Non-standard frameworks and inadequate testing</td>
<td>All</td>
</tr>
<tr>
<td>Insufficient/Inessential logging</td>
<td>C,AC,NR,P</td>
</tr>
</tbody>
</table>
DOS AS AN EXAMPLE OF AN ATTACK ON DEVICES

Example of an attack: > Denial-of-service

- **Battery draining**: By depleting the battery of a connected device, e.g., a smoke detector, an attacker will be able to disable a fire detection system.

- **Sleep deprivation**: An attacker may attempt to send an undesired set of requests that seem to be legitimate but are not.

- **Outage attacks**: Devices may stop functioning as a result of an unintended error in the manufacturing process, battery draining, sleep deprivation, etc.
- **Black hole**: This attack is launched by using a malicious node, which attracts all the traffic in the network by advertising that it has the shortest path to the destination in the network.

- **Gray hole**: This attack is a variation of Black Hole attack in which the nodes selectively drop some packets.

- **Worm hole**: In this attack, the attacker first records packets at one location in the network and then tunnels them to a different location.

- **Others**: HELLO floods, Sybil, bogus routing information, etc.
Insufficient validation of the input may enable malicious input injection.

An attacker could inject a malicious input that causes the service providers to perform operations on behalf of the attacker.

For example, an attacker may add an unauthorized component that is capable of injecting malicious inputs into the servers. Afterwards, the attacker might be able to steal data, compromise database integrity, or bypass authentication.

Standard database error messages returned by a database may also assist the attacker.
RELATIONSHIP AMONG THE DIFFERENT SECURITY CONCEPTS

- Threat agent
- Threat
- Vulnerability
- Risk
- Asset
- Exposure
- Safeguard

Relationships:
- Threat agent gives rise to threat.
- Threat exploits vulnerability, leading to risk.
- Asset can be damaged by exposure.
- Exposure can be countermeasured by a safeguard.
- Safeguard directly affects asset.
MALICIOUS THREAT AGENTS
JOSEPH BUGEJA
SMART CONNECTED HOMES: CONCEPTS, RISKS, AND CHALLENGES

Joseph Bugeja

IoT Security
“Know your enemy and know yourself and you can fight a thousand battles without disaster”

- Sun Tzu
Threats can come from anywhere, but generally fall under three categories: Human, Non-human, and Nature. Threats can also be deliberate or accidental.
- Threat agent archetypes are collective descriptions of attacks, representing similar risk profiles.

- Intelligent attackers whose motivations drive their objectives.

- Attributes such as skills, access, and resources define their most likely methods.

**Hacker**

- **Motivation:** Curiosity (Low)
- **Objectives:** Try things out, Cause confusion
- **Methods:** Malware, Attack a network or device
MALICIOUS THREAT AGENTS

- Hackers
- Thieves
- Hacktivists
- Competitors & Org. Crime
- Terrorists
- Nation States
Individuals ("hobby hackers") that include malicious persons, script kiddies, and nosy employees of an organization

Viruses, worms, phishing

Primarily motivated by curiosity

Skill-level: Apprentice

Low
THIEVES

- Opportunistic individuals that are associated with stealing mostly for personal financial gain

- System/physical intrusion, DoS, spoofing

- Main motive is monetary gain

- Skill-level: Apprentice

Joseph Bugeja

IoT Security
Hacktivists

- Individuals or members of a larger group that pursue a political or social agenda
- DoS, fraud, and identity theft
- Primarily aim to promote and publicize their cause
- Skill-level: Apprentice
COMPETITORS AND ORGANIZED CRIME

✓ Commercial competitors that compete for revenues or resources, and private criminal organizations

✓ Botnets, ransomware, and inside information

✓ Competitive advantage, CI, and monetization

✓ Skill-level: Journeyman
TERRORISTS

✓ Individuals that rely on violence or fear-related behavior to support personal socio-political agenda

✓ Damage/loss, outages, and physical attacks

✓ Terrorism

✓ Skill-level: Master
NATION STATES

- Highly sophisticated individuals that are funded by governments and associated with a military unit
- Customized malware, spear phishing attacks, and zero-day attacks
- Cyber warfare, (counter-)intelligence
- Skill-level: Master
<table>
<thead>
<tr>
<th>Threat Agent Skills</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Skills</td>
<td>Minimal technical skills</td>
<td>Sufficient technical skills</td>
<td>High-level technical skills</td>
</tr>
<tr>
<td></td>
<td>Largest number of attackers</td>
<td>Locate new vulnerabilities</td>
<td>Write new powerful attack toolkits</td>
</tr>
<tr>
<td></td>
<td>Easiest to defend against</td>
<td>Threat agents with such skills are likely found in all classes</td>
<td>Hardest to defend against</td>
</tr>
</tbody>
</table>
Countermeasures
<table>
<thead>
<tr>
<th>Threat</th>
<th>Against</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Trojans</td>
<td>All</td>
</tr>
<tr>
<td>Side-channel attacks</td>
<td>C,AU,NR,P</td>
</tr>
<tr>
<td>DoS</td>
<td>A,AC,AU,NR,P</td>
</tr>
<tr>
<td>Physical attacks</td>
<td>All</td>
</tr>
<tr>
<td>Node replication attacks</td>
<td>All</td>
</tr>
<tr>
<td>Camouflage</td>
<td>All</td>
</tr>
<tr>
<td>Corrupted node</td>
<td>All</td>
</tr>
<tr>
<td>Tracking</td>
<td>P, NR</td>
</tr>
<tr>
<td>Inventorying</td>
<td>P, NR</td>
</tr>
<tr>
<td>Tag cloning</td>
<td>All</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td>All</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>C,NR,P</td>
</tr>
<tr>
<td>Injecting fraudulent packets</td>
<td>P,I,AU,TW,NR</td>
</tr>
<tr>
<td>Routing attacks</td>
<td>C,I,AC,NR,P</td>
</tr>
<tr>
<td>Unauthorized conversation</td>
<td>All</td>
</tr>
<tr>
<td>Malicious injection</td>
<td>All</td>
</tr>
<tr>
<td>Integrity attacks against learning</td>
<td>C,I</td>
</tr>
<tr>
<td>Non-standard frameworks and inadequate testing</td>
<td>All</td>
</tr>
<tr>
<td>Insufficient/Inessential logging</td>
<td>C,AC,NR,P</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Countermeasures</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Side-channel signal analysis</td>
<td></td>
</tr>
<tr>
<td>Trojan activation methods</td>
<td></td>
</tr>
<tr>
<td>IDSs</td>
<td></td>
</tr>
<tr>
<td>Securing firmware update</td>
<td></td>
</tr>
<tr>
<td>Circuit/design modification</td>
<td></td>
</tr>
<tr>
<td>Kill/sleep command</td>
<td></td>
</tr>
<tr>
<td>Isolation</td>
<td></td>
</tr>
<tr>
<td>Blocking</td>
<td></td>
</tr>
<tr>
<td>Anonymous tag</td>
<td></td>
</tr>
<tr>
<td>Distance estimation</td>
<td></td>
</tr>
<tr>
<td>Personal firewall</td>
<td></td>
</tr>
<tr>
<td>Cryptographic schemes</td>
<td></td>
</tr>
<tr>
<td>Reliable routing</td>
<td></td>
</tr>
<tr>
<td>De-patterning and Decentralization</td>
<td></td>
</tr>
<tr>
<td>Role-based authorization</td>
<td></td>
</tr>
<tr>
<td>Information Flooding</td>
<td></td>
</tr>
<tr>
<td>Pre-testing</td>
<td></td>
</tr>
<tr>
<td>Outlier detection</td>
<td></td>
</tr>
</tbody>
</table>

**Summary of IoT Security Threats and Countermeasures**

Joseph Bugeja

IoT Security
IDSs provide a reliable approach to defend against battery-draining and sleep deprivation attacks by detecting unusual requests to the node.

Certain IDSs are designed to meet the requirements of IPv6 connected nodes of IoT, making it possible to detect various routing attacks.

IDSs can also detect the existence of a malicious node that tries to inject invalid information, including code injection attacks, into the system or violate a policy.
Secure routing is vital to the acceptance and use of sensor networks for many applications.

Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against the majority of outsider attacks.

Careful protocol design is needed for different threats, e.g., to prevent against insiders and ‘laptop-class’ adversaries.
Pre-testing attempts to identify the set of possible attack scenarios and simulate these scenarios to see how the system responds.

It also specifies what information should be logged and what information is too sensitive to be stored.

In addition, the input files should be closely examined to prevent the danger of malicious injection. For example, the attacker should not be able to execute any command by injecting it into the input files.
<table>
<thead>
<tr>
<th><strong>IoT Devices</strong></th>
<th><strong>IoT Network</strong></th>
<th><strong>IoT Services</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• H/W enc, fail-secure design, and device authZ</td>
<td>• VPNs, firewalls, IDS, and IPS</td>
<td>• Security testing, secure design, and data masking</td>
</tr>
<tr>
<td>• Enhanced algorithms, e.g. DTLS and ECSDA</td>
<td>• TOR-based systems</td>
<td>• Cryptographic schemes</td>
</tr>
<tr>
<td>• Platforms such as RERUM</td>
<td>• Devices such as Cujo, Dojo, and Keezel</td>
<td>• OWASP, Builditsecure.ly, I Am the Cavalry</td>
</tr>
<tr>
<td>• CC and EMVCo IC SE</td>
<td>• ENISA, CSA, etc.</td>
<td>• Sites such as BugCrowd</td>
</tr>
</tbody>
</table>
Final Remarks

✓ IoT influences many application areas of our society

✓ Despite its benefits, several security concerns exist at different layers in an IoT system

✓ We explored different IoT security attacks, countermeasures, and threat agents

✓ Nonetheless, several open issues need to be addressed by industrial/academic research communities as well as manufacturers
THANK YOU FOR YOUR ATTENTION!

bugejajoseph.com