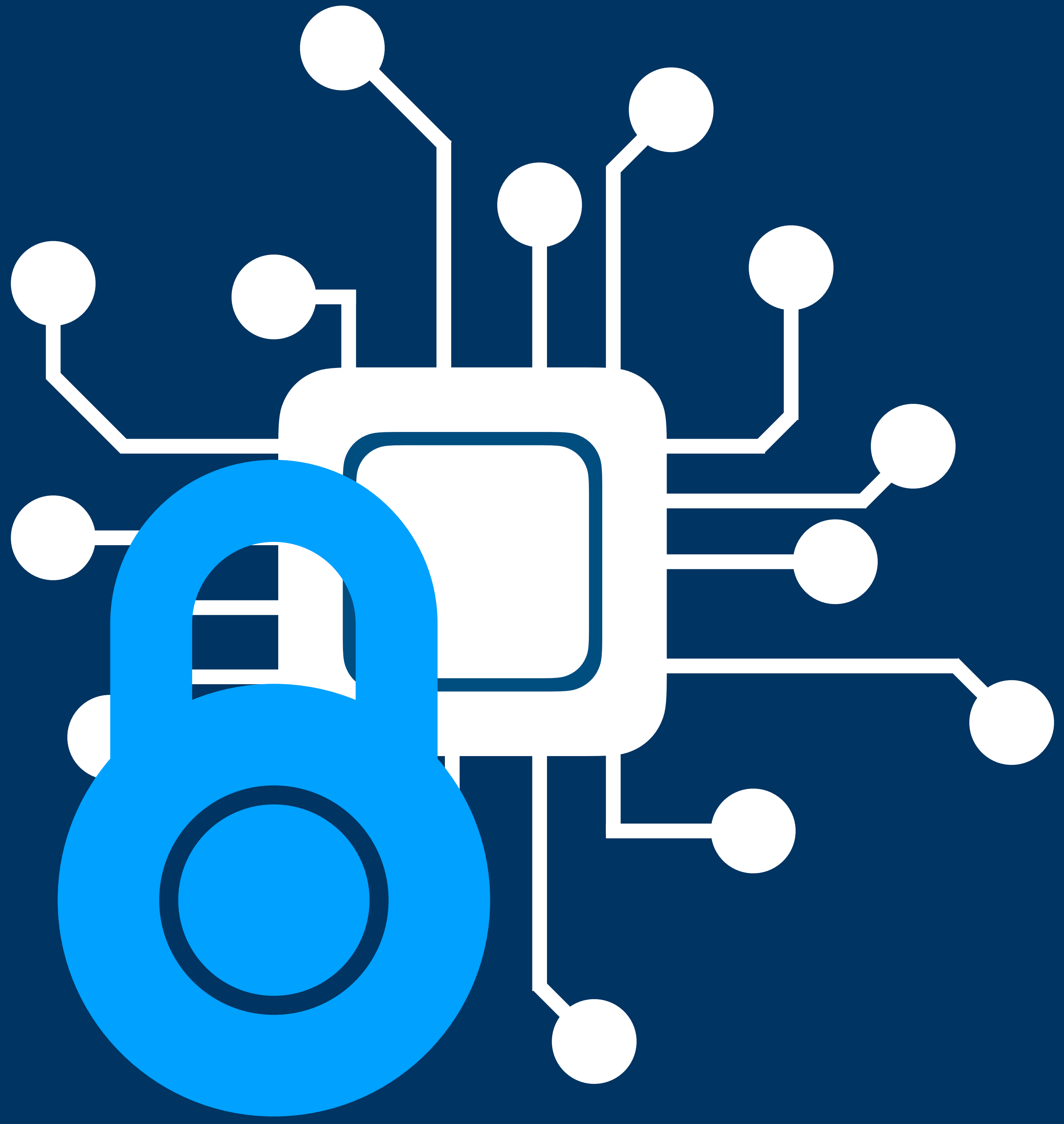
IoT Security

A Basic IoT Hardware Security Framework



The Seventh International Conference on Advances in Computation, Communications and Services (ACCSE 2022) IARIA

Christoph Haar (haar-christoph@gmx.de), Erik Buchmann (buchmann@uni-leipzig.de)

Christoph Haar

- 2010-2015 Business Informatics (Bachelor) Martin-Luther-University Halle/Wittenberg, Germany
- 2015-2017 Business Informatics (Master) Martin-Luther-University Halle/Wittenberg, Germany
- 2018-2022 Scientific Assistant Hochschule für Telekommunikation Leipzig, Chair for Data Privacy and Security in Information Systems

Agenda

1. Introduction
2. IoT Security Standards
3. Risk Identification
4. The Basic IoT Hardware Security Framework
5. Discussion
6. Conclusion

Motivation and Problem

- Due to the rapidly growing number of IoT devices, official security authorities have already integrated IoT security into their standards. ✓

- These standards focus on planning and usage of IoT devices, as well as software security and how to protect the data. ✓

- Most of them also consider hardware threats and security practices for IoT devices but there is no uniform process for IoT hardware security. ✗

Method and Goal

- The aim of our work is to develop a basic IoT hardware security framework that can be used to protect any IoT device on a basic level.
- We analyze three official IoT security standards to identify important hardware threats.
- The result of this comparison serves as a basis for a risk identification for four commonly used IoT devices.
- Based on the results, we derive a basic IoT hardware security framework that includes the identified risks.

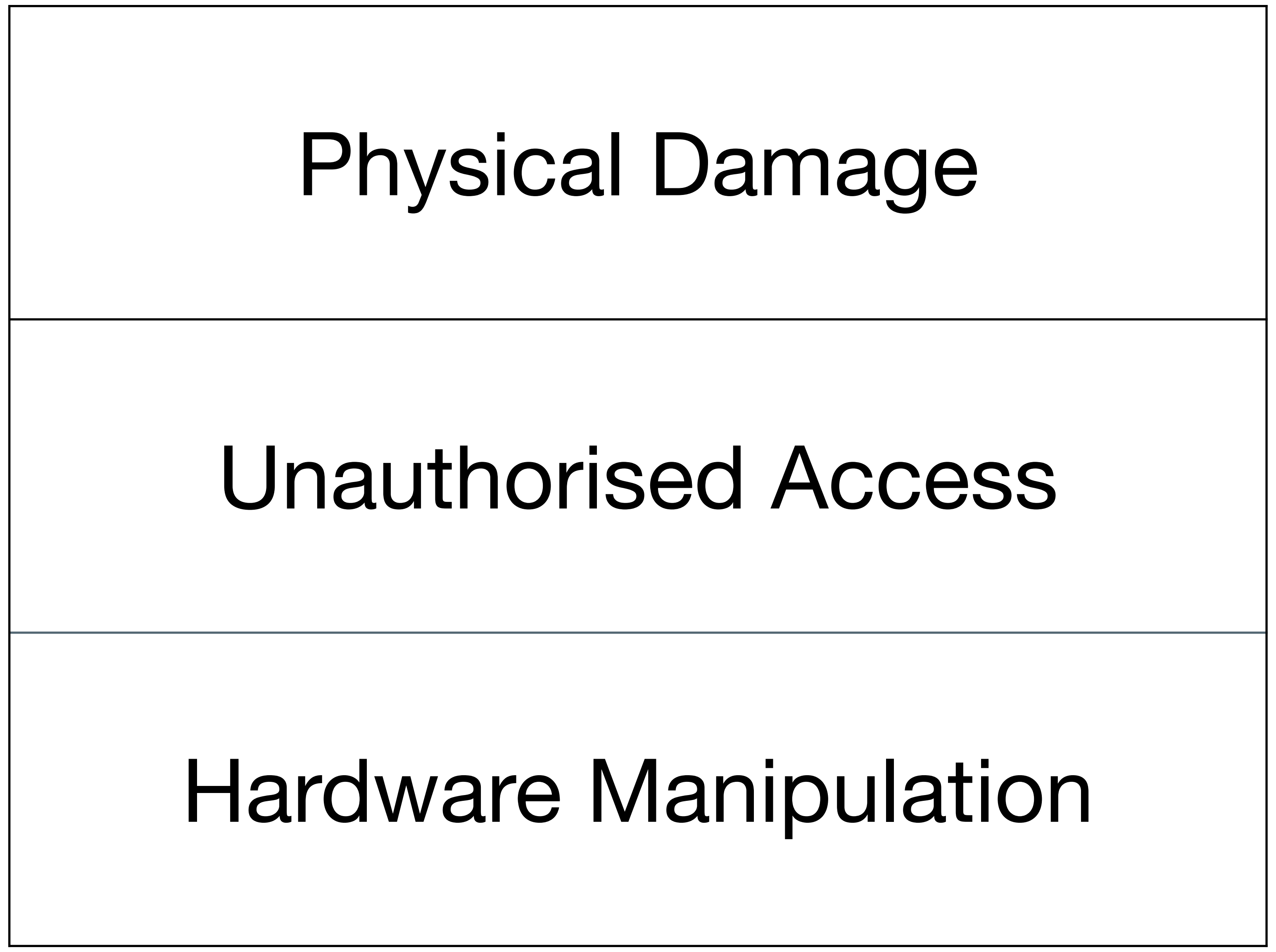
BSI Elementary Threats for IoT Devices

- The BSI describes 47 elementary threats for IoT devices in the BSI standard 200-3.
- 20 of them occur for IoT devices in the IT Grundschutz Compendium Module „SYS.4.4 General IoT Devices“.

G 0.2 Bad Environmental Conditions
G 0.4 Pollution, Dust, Corrosion
G 0.8 Disruption of Power Supply
G 0.9 Failure or Disruption of Communication…
G 0.14 Interception of Information / Espionage
G 0.16 Theft of Devices, Storage and Media…
G 0.18 Poor Planning or Lack of Adaption
G 0.19 Disclosure of Sensitive Information
G 0.20 Information or Products from a…
G 0.21 Manipulation with Hardware
G 0.23 Access to IT Systems
G 0.24 Destruction of Devices or Storage Media
G 0.25 Failure of Device or System
G 0.26 Malfuncrion of Device or Systems
G 0.28 Software Vulnerabilities or Errors
G 0.29 Violation of Laws or Regulations
G 0.30 Unauthorized Use or Administration of…
G 0.38 Misuse of Personal Information
G 0.39 Malware
G 0.40 Denial of Service

NIST Hardware Threats for IoT Devices

- The NIST published several drafts for IoT security.
- These drafts consider:
    - acquisition and implementation of IoT devices in companies
    - Important steps when planning to use IoT devices
    - how the data flow can be protected
- They also consider different threats.



Physical Damage

Unauthorised Access

Hardware Manipulation

ENISA Hardware Threats for IoT Devices

- The ENISA published the Baseline Security Recommendations for IoT.
- It contains a Hardware Security Section that addresses:
  - IoT Security Challenges
  - General Security Recommendations
  - Hardware Threats

Elemental Threats
Environmental Threats
Physical Damage
Hardware Manipulation
Power Loss
Data Interception

Selection of IoT Devices for the Risk Identification

- For our Investigation, we select 4 different IoT devices and list all their hardware components.
- The application scenarios are as different as possible.
- In this way, we are able to determine if the mentioned threats really apply to a wide range of different application scenarios.

Security Camera	**Smoke Detector**
Cables, Camera, Case, Infrared LED’s, Micro SD Socket, Microphone, Motherboard, Processor, Sensors	Battery, Case, LED, Motherboard, Processor, Reset Button, Sensors, Speakers

Soil Temp. Sensor	**Power Outlet**
Antenna, Battery, Case, Motherboard, Processor, Sensors	Case, Motherboard, Processor, Sensors, Socket Connector

Potential IoT Hardware Threats

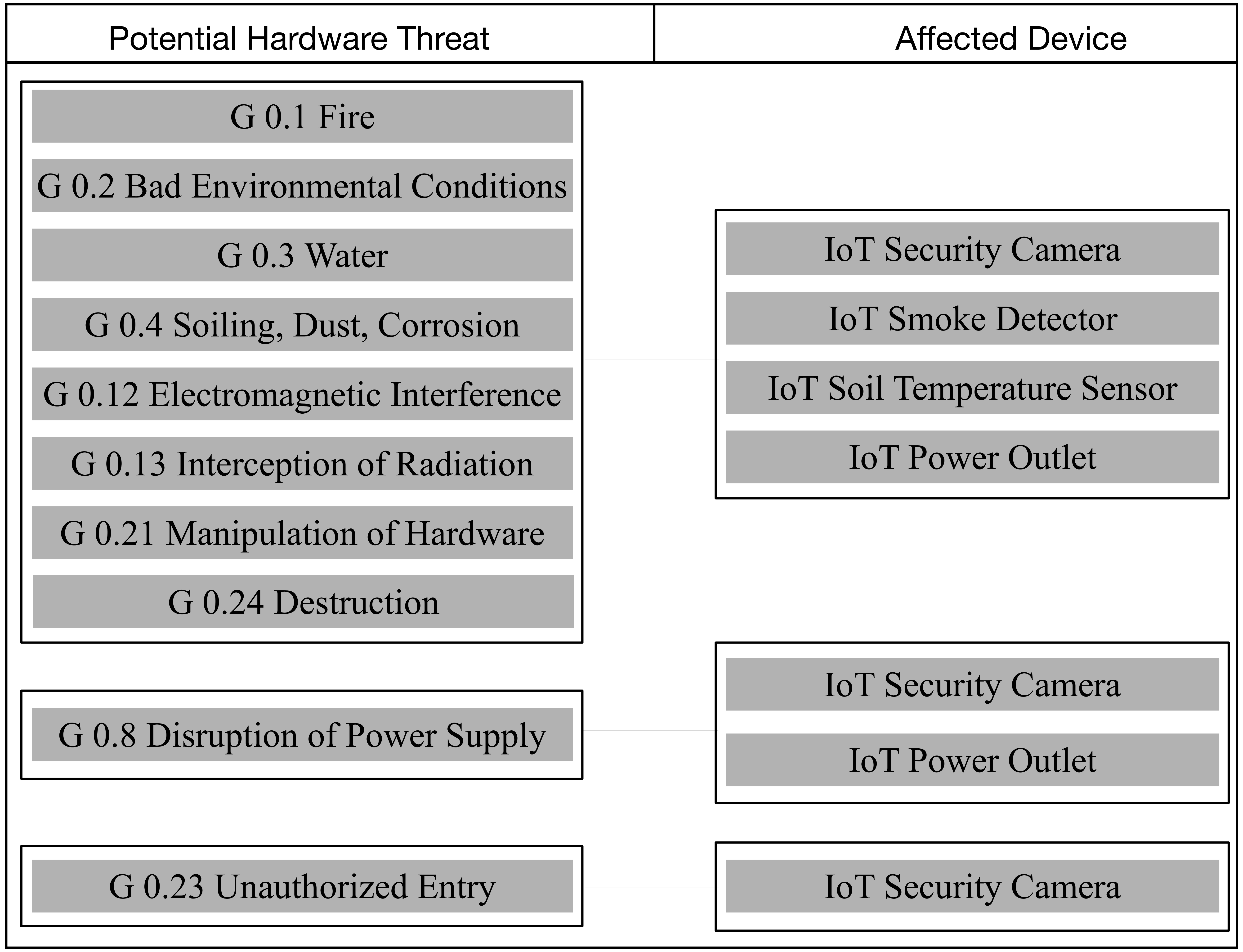
Potential IoT Hardware Threats

- The elementary threats from the BSI cover a wide range of threats for an entire company.
- They are not limited to the hardware.
- Because we focus on hardware security, we select those elementary threats addressing the hardware of IoT devices.

G 0.1 Fire
G 0.2 Bad Environmental Conditions
G 0.3 Water
G 0.4 Soiling, Dust, Corrosion
G 0.8 Disruption of Power Supply
G 0.12 Electromagnetic Interference
G 0.13 Interception of Radiation
G 0.21 Manipulation of Hardware
G 0.23 Unauthorized Entry
G 0.24 Destruction

Affected IoT Devices

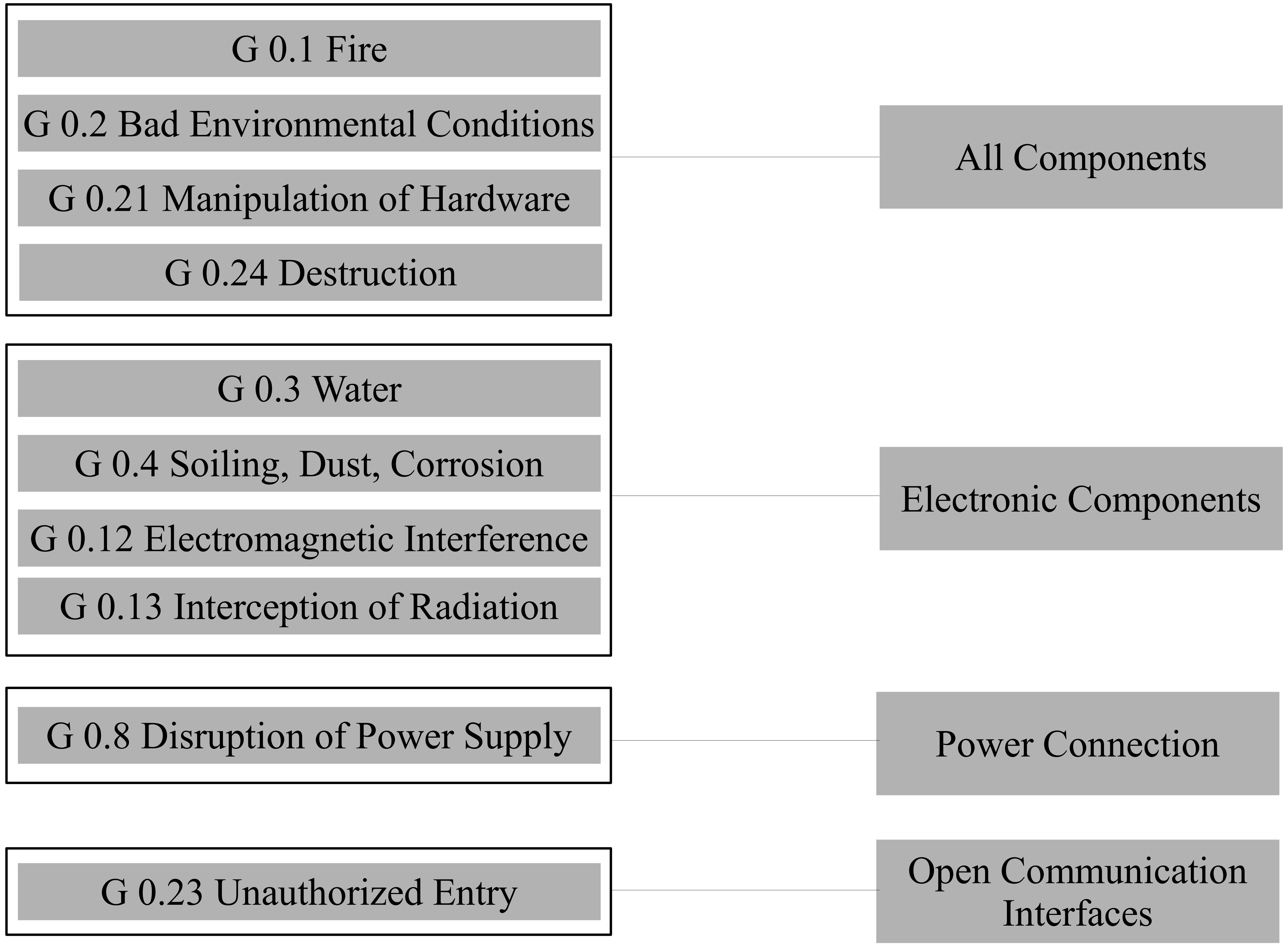
- In the next step, we implemented the risk identification.
- We checked if each device have the hardware component that a certain threat is addressing.
- If the device has the addressed hardware component, it is affected by the threat.



Potential Hardware Threat	Affected Device
G 0.1 Fire G 0.2 Bad Environmental Conditions G 0.3 Water G 0.4 Soiling, Dust, Corrosion G 0.12 Electromagnetic Interference G 0.13 Interception of Radiation G 0.21 Manipulation of Hardware G 0.24 Destruction	IoT Security Camera IoT Smoke Detector IoT Soil Temperature Sensor IoT Power Outlet
G 0.8 Disruption of Power Supply	IoT Security Camera IoT Power Outlet
G 0.23 Unauthorized Entry	IoT Security Camera

Generalization of the Results

- Hardware threats only arise for devices with addressed component.
- G 0.1, G 0.2, G 0.21 and G 0.24 are affecting all components.
- G 0.3, G 0.4, G 0.12 and G 0.13 are affecting all electronic components.
- G 0.8 is affecting devices with a power supply.
- G 0.23 is affecting devices with open communication interfaces.



G 0.1 Fire
G 0.2 Bad Environmental Conditions
G 0.21 Manipulation of Hardware
G 0.24 Destruction
All Components

G 0.3 Water
G 0.4 Soiling, Dust, Corrosion
G 0.12 Electromagnetic Interference
G 0.13 Interception of Radiation
Electronic Components

G 0.8 Disruption of Power Supply
Power Connection

G 0.23 Unauthorized Entry
Open Communication Interfaces

Definition of the Framework Basis

- Our risk identification confirms that the hardware threats mentioned in the three IoT security standards really apply to different IoT devices.
- These threats must be considered for all IoT devices or at least for a large number of different applications scenarios.
- For these threats, we define our basic IoT hardware security framework.

Definition of the Framework

- X is representing a certain IoT device which goes through the framework.
- SECURE indicates a function.
- If SECURE is ON, the hardware threat is affecting the device and a security practice has to be considered.
- Otherwise, the hardware threat is not affecting the device and no security practices has to be implemented.

```
For EACH IoT-Device x do
SECURE G 0.1, G 0.2, G 0.3, G 0.4, G 0.12,
G 0.13, G 0.21, G 0.24 ON x

    If x has power connection then
    SECURE G 0.8 ON x
    end if

    If x has open communication interface then
    SECURE G 0.23 ON x
    end if

end for
```

Discussion

- Our framework serves as a basic hardware protection for IoT devices but further security measures are necessary according to the security requirements and application scenarios of the devices.
- Our framework can be integrated into existing security concepts.
- Our framework does not consider appropriate security measures because the implemented threats are based on known threats that are described in the BSI.

Conclusion

- In this work, we developed a basic IoT hardware security framework that can be implemented into existing security concepts.
- We analyzed 3 official security standards and compared the mentioned threats.
- By performing a risk identification for 4 different IoT devices, we were able to confirm the importance of the mentioned threats.
- We used the results of the risk identification to develop our basic IoT hardware security framework that consists of 10 different hardware threats.

Thank You For Your Attention