tfz Medical
Cluster Insights

«„Security by Design“ - sicher vernetzte Medizinprodukte entlang des gesamten Product-Lifecycle»

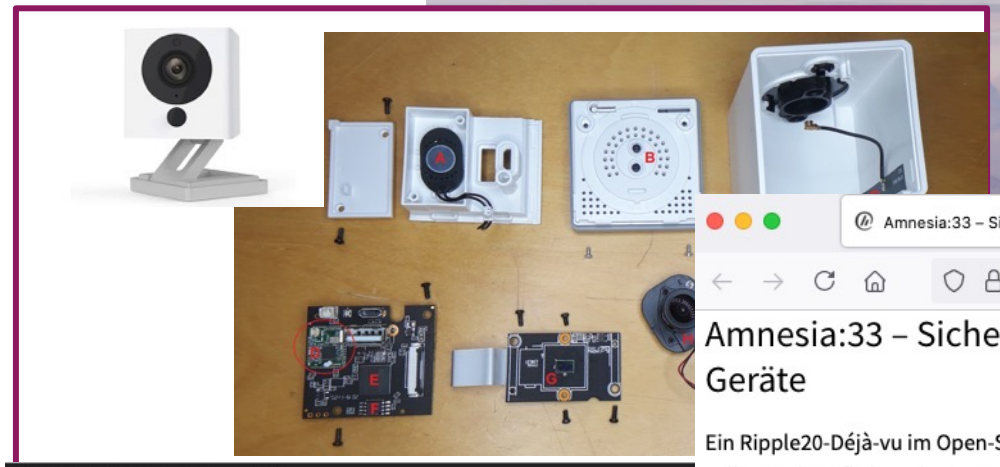
Referenten:
Prof. Dr. Nathalie Weiler, OST
Daniel Speck, Roche Diagnostics Int.

Teaser

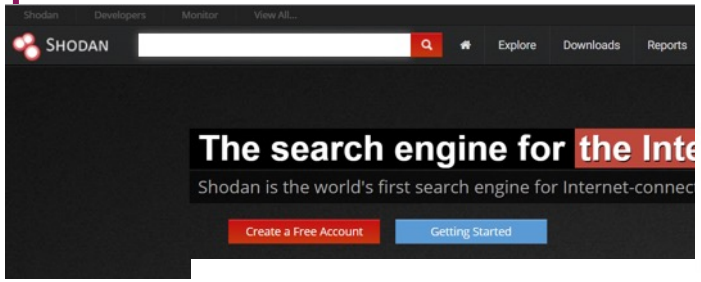
Wie auch in anderen Branchen gibt es auch in der Medizintechnikbranche eine starke Zunahme der Vernetzung von Geräten.

Den vielen Chancen dieser Vernetzung stehen die ständigen Cyber-Gefahren gegenüber. Bei Kontrolle von Herzschrittmachern per App beispielsweise, kann eine Sicherheitslücke sehr schnell Lebensbedrohung für den Patienten- und grossen Reputationsschaden inkl. wirtschaftlichen Konsequenzen für den Hersteller bedeuten.

Wie wird eine nachhaltige Security über den gesamten Product-Lifecycle sichergestellt? Muss über die regulatorischen Anforderungen von MDR oder FDA hinaus Security-Aufwand betrieben werden? Wie kann mit der hohen Komplexität der Daten, die verschiedensten Anspruchsgruppen gehören, zielgerichtet im Bereich Security umgegangen werden.



Prepared content:
Good examples of application of IoT security principles in medical field



"Cheat Sheets"

OWASP IoT Top 10

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

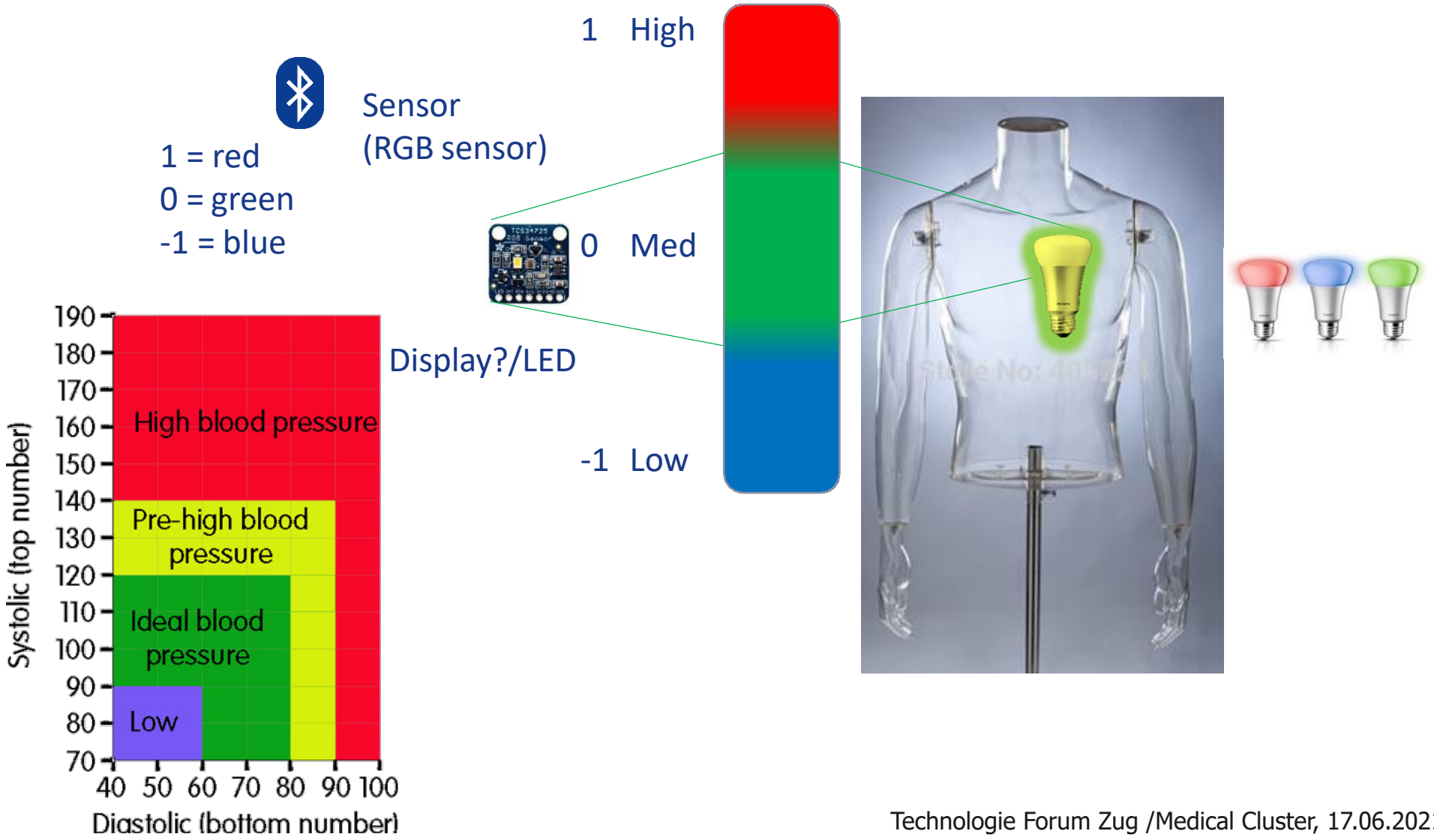
(Bild: NicoElNino/Shutterstock.com)

UPDATE 08.12.2020 08:02 Uhr | Security

von Westernhagen

Ripple20

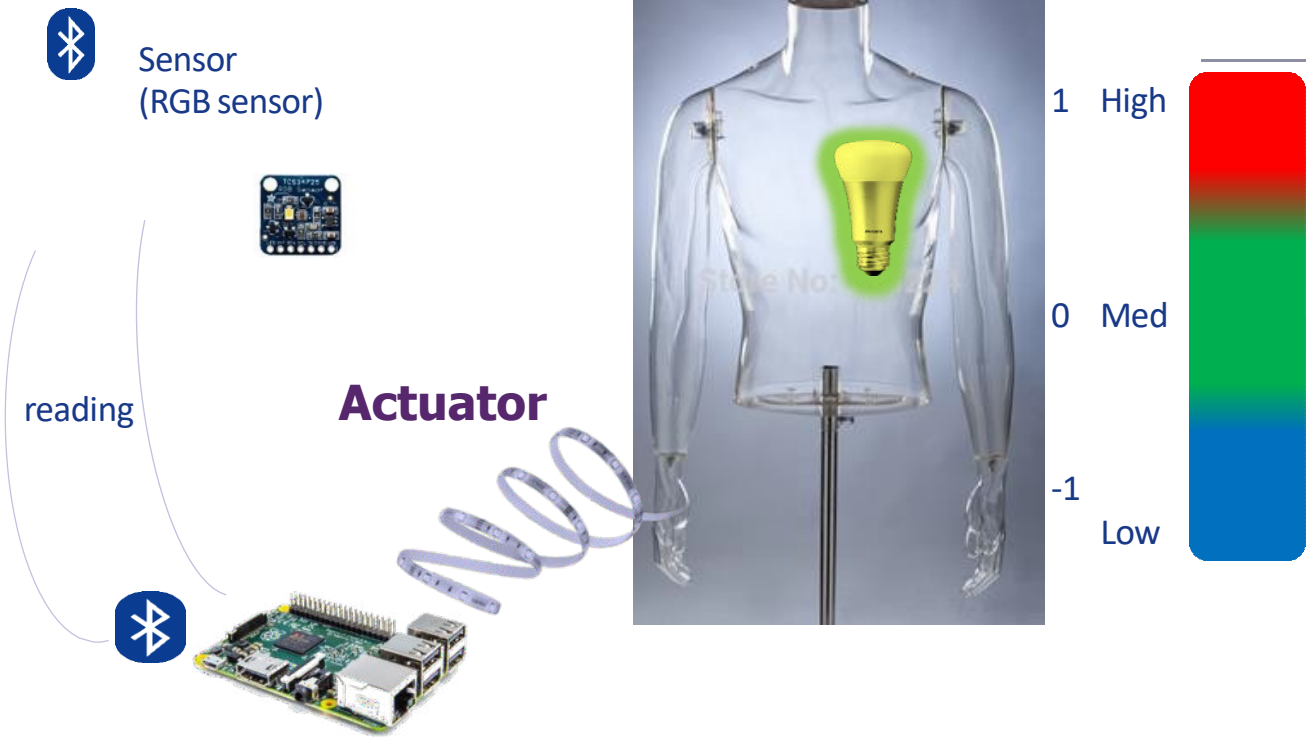
Let's look at an example



OST

Interconnectivity & Decision Making

1 = red
0 = green
-1 = blue



Based on reading, we want to increase or decrease value to get optimal state

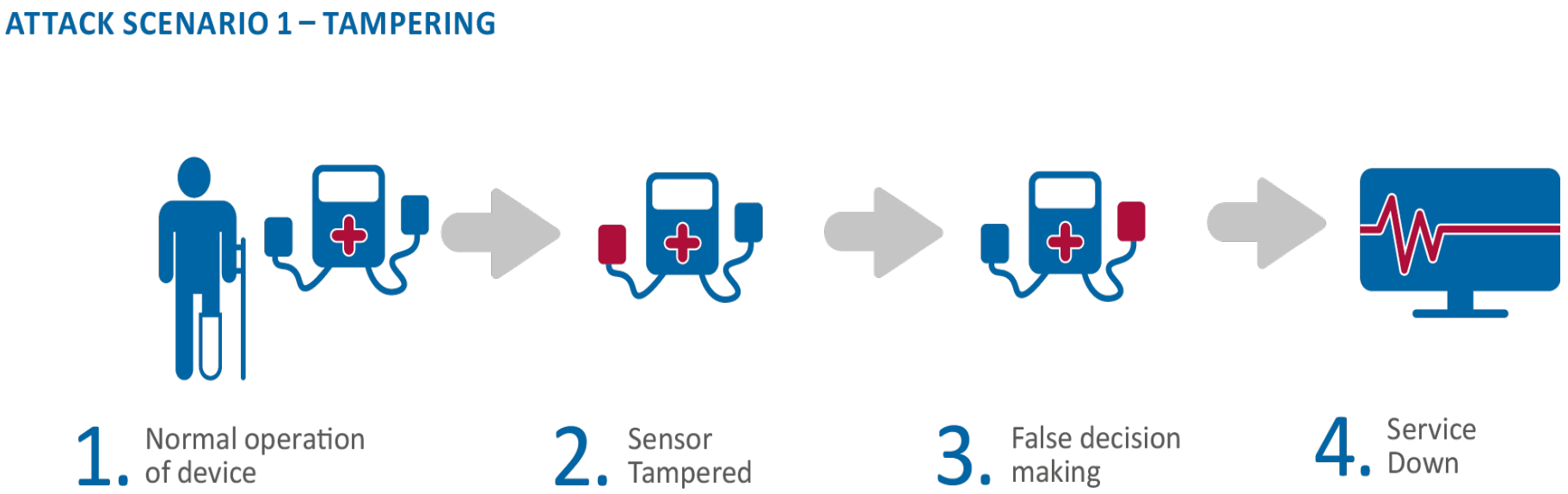
If(red)
add blue

If(green)
do nothing

If(blue)
add red

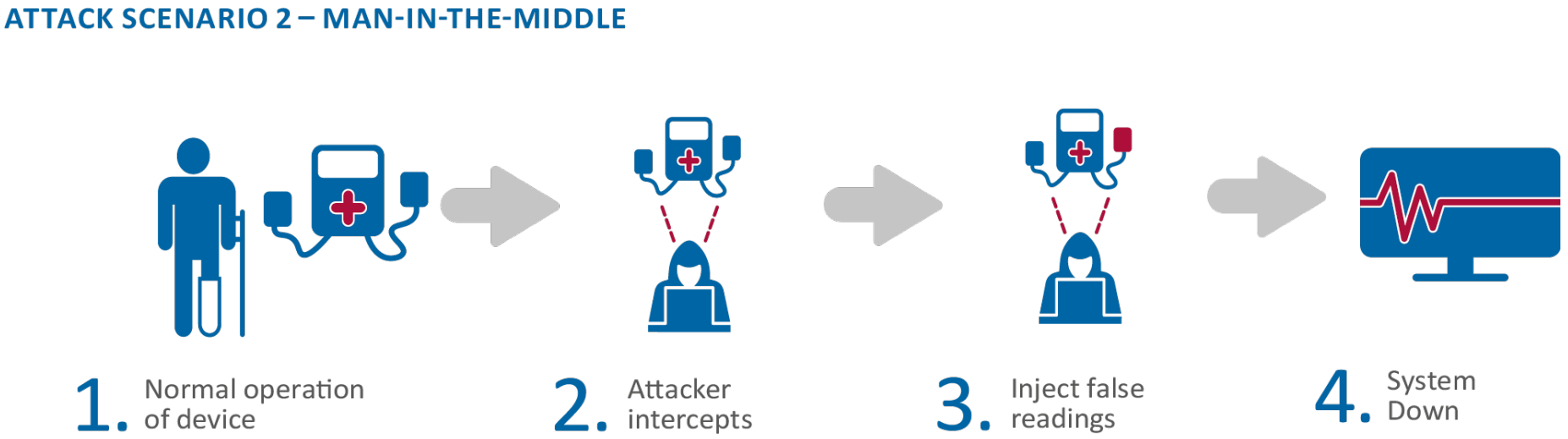
Scenario 1: Sensor Tampering (Blood Pressure Measurement)

We modify the values read by sensors or their threshold values and settings



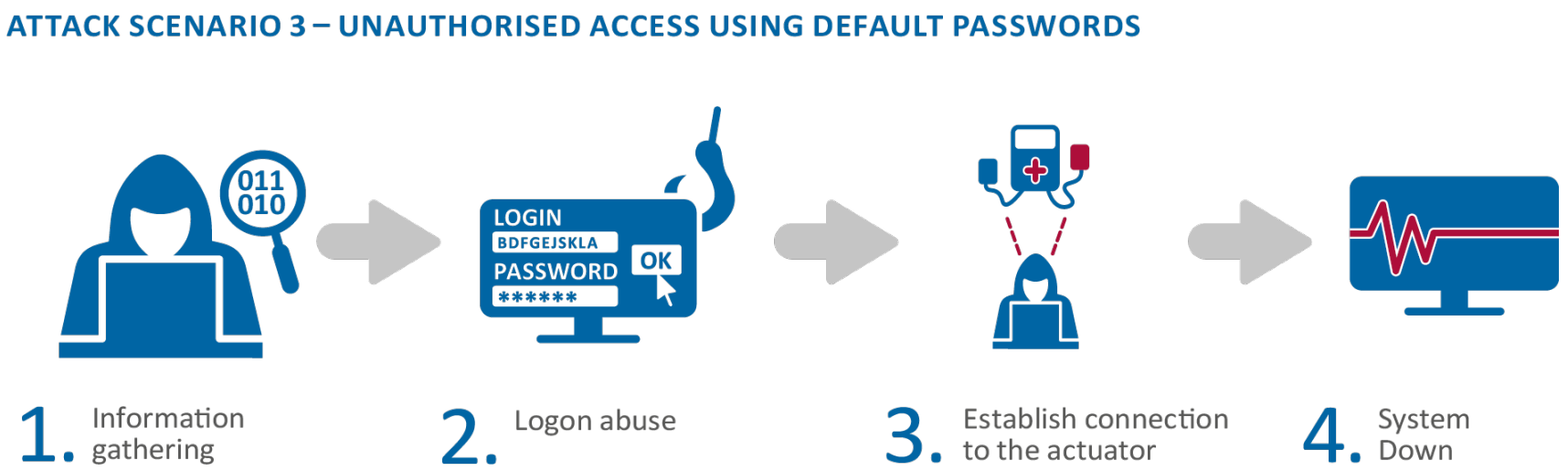
Scenario 2: Man-in-the-Middle

We modify the values intercepted from the man in the middle



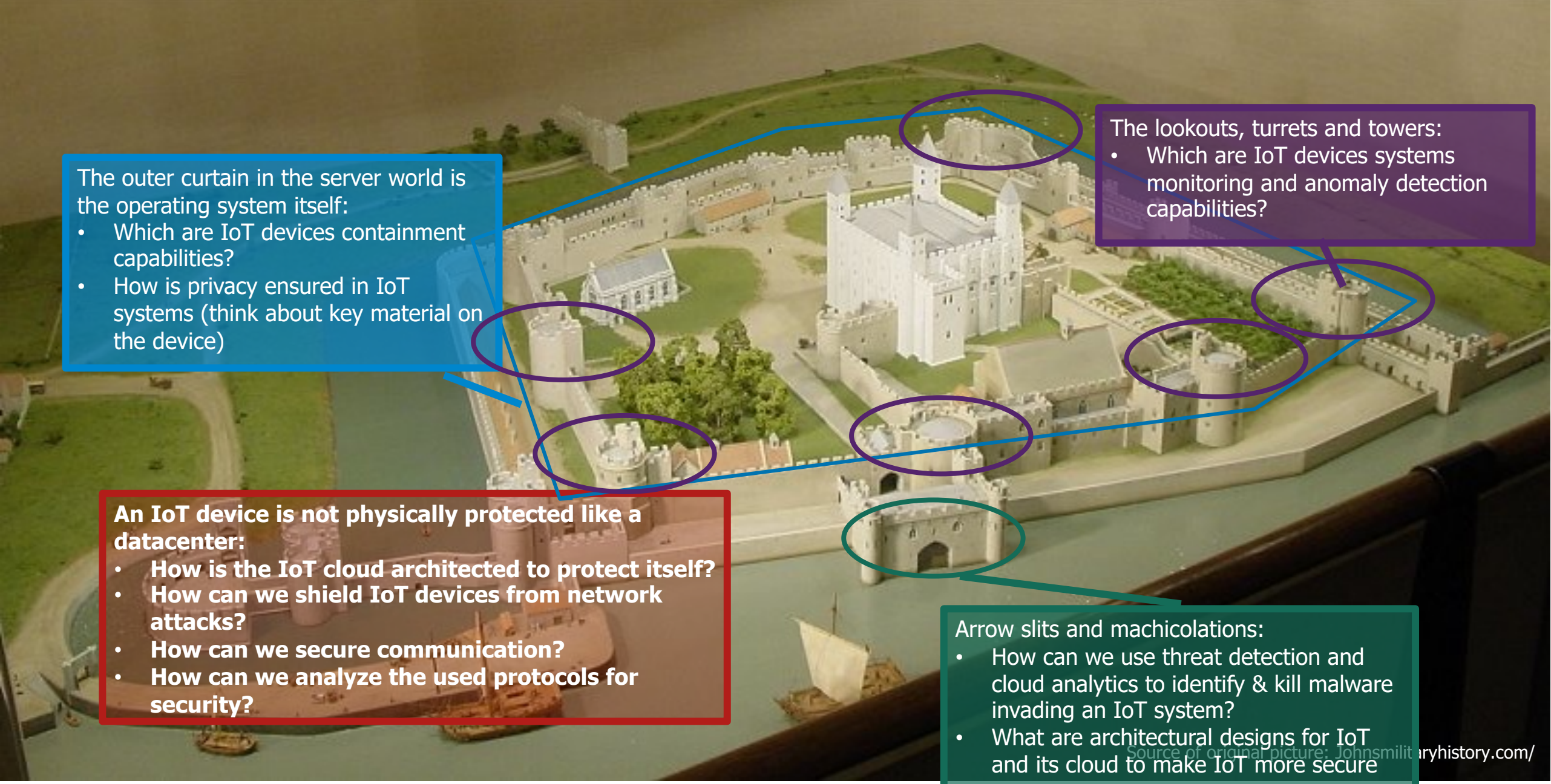
Scenario 3: Unauthorised access (device not disclosed)

We modify normal settings of the device



OWASP IoT Top 10 (2018) Revisited

1. **Weak, guessable, or hardcoded passwords**
2. **Insecure network services**
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. **Use of insecure or outdated components**
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. **Insecure default settings**
10. Lack of physical hardening


The outer curtain in the server world is the operating system itself:
• Which are IoT devices containment capabilities?
• How is privacy ensured in IoT systems (think about key material on the device)
The lookouts, turrets and towers:
• Which are IoT devices systems monitoring and anomaly detection capabilities?
An IoT device is not physically protected like a datacenter:
• How is the IoT cloud architected to protect itself?
• How can we shield IoT devices from network attacks?
• How can we secure communication?
• How can we analyze the used protocols for security?
Arrow slits and machicolations:
• How can we use threat detection and cloud analytics to identify & kill malware invading an IoT system?
• What are architectural designs for IoT and its cloud to make IoT more secure
Source of original picture: Johnsmilitaryhistory.com/