SBA Security Meetup

Let‘s Inspect

PD Dr. rer. nat. habil. Corinna Schmitt

FI CODE, Universität der Bundeswehr München

Conclusions

Be active

STRIDE Framework

Basic (Security-) Challenges

Is our system really secure?
- Threat Modelling -

1. Internet of Things (IoT)
Basics & (Security-) Challenges

Early Vision

„When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole.

We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do his will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.“

(Nikola Tesla 1926)

First Official ”IoT Definition”

„ If we had computers that knew everything there was to know - using data they collected without our help - we could record and count everything, significantly reducing waste, losses and costs. We would know when things need to be replaced, repaired or recalled and whether or not they have been updated.“

(Kevin Ashton, 2009)

http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Status-Quo IoT (1)

IETF [LPKC10]: "*The basic idea is that IoT will connect objects around us (electronic, electrical, non electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and co-operate each other to make the service better and accessible anytime, from anywhere.*"

ITU Y.4000 [ITU19]: "*Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*"

Status-Quo IoT (2)

EU-Parliament Briefing [Dav19]: "*The Internet of Things (IoT) has been defined in a number of different ways. Generally speaking, it refers to a global, distributed network (or networks) of physical objects that are capable of sensing or acting on their environment, and able to communicate with each other, other machines or computers. Such 'smart' objects come in a wide range of sizes and capacities, including simple objects with embedded sensors, household appliances, industrial robots, cars, trains, and wearable objects such as watches, bracelets or shirts. Their value lies in the vast quantities of data they can capture and their capacity for communication, supporting real - time control or data analysis that reveals new insights and prompts new actions. As in the case of many emerging technologies, different experts may use different terms to refer to similar or overlapping concepts. Machine to machine (M2M) processing emphasizes the sharing of data and processing that takes place between these devices. On the other hand, the Internet of Everything explicitly includes people as participants in this global network. Ubiquitous computing emphasizes the fact that network and computing resources are available almost everywhere, whereas pervasive computing highlights the fact that processors are embedded in everyday objects all around us.*"

Status-Quo IoT (3)

Cisco IBSG [Eva11]: "*IoT is simply the point in time when more "things or objects" were connected to the Internet than people. In 2003, there were approximately 6.3 billion people living on the planet and 500 million devices connected to the Internet. By dividing the number of connected devices by the world population, we find that there was less than one (0.08) device for every person. Based on Cisco IBSG's definition, IoT didn't yet exist in 2003 because the number of connected things was relatively small given that ubiquitous devices such as smartphones were just being introduced. [...] Refining these numbers further, Cisco IBSG estimates IoT was "born" sometime between 2008 and 2009.*"

SAP [HKC08]: "*A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these "smart objects" over the Internet, query their state and any information associated with them, taking into account security and privacy issues.*"

Technology Strategy Board: "*The Internet of Things (IoT) describes the revolution already under way that is seeing a growing number of Internet enabled devices that can network and communicate with each other and with other web-enabled gadgets. IoT refers to a state where Things (e.g. objects, environments, vehicles and clothing) will have more and more information associated with them and may have the ability to sense, communicate, network and produce new information, becoming an integral part of the Internet.*"

Summary: IoT Definition

IoT refers to physical devices
that are powered and can transmit data over networks,
but usually do not require interaction between humans & computers.

What is involved?

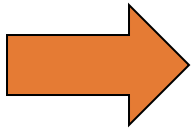
3. Classes of Constrained Devices

Despite the overwhelming variety of Internet-connected devices that can be envisioned, it may be worthwhile to have some succinct terminology for different classes of constrained devices. In this document, the class designations in Table 1 may be used as rough indications of device capabilities:

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

As of the writing of this document, these characteristics correspond to distinguishable clusters of commercially available chips and design cores for constrained devices. While it is expected that the

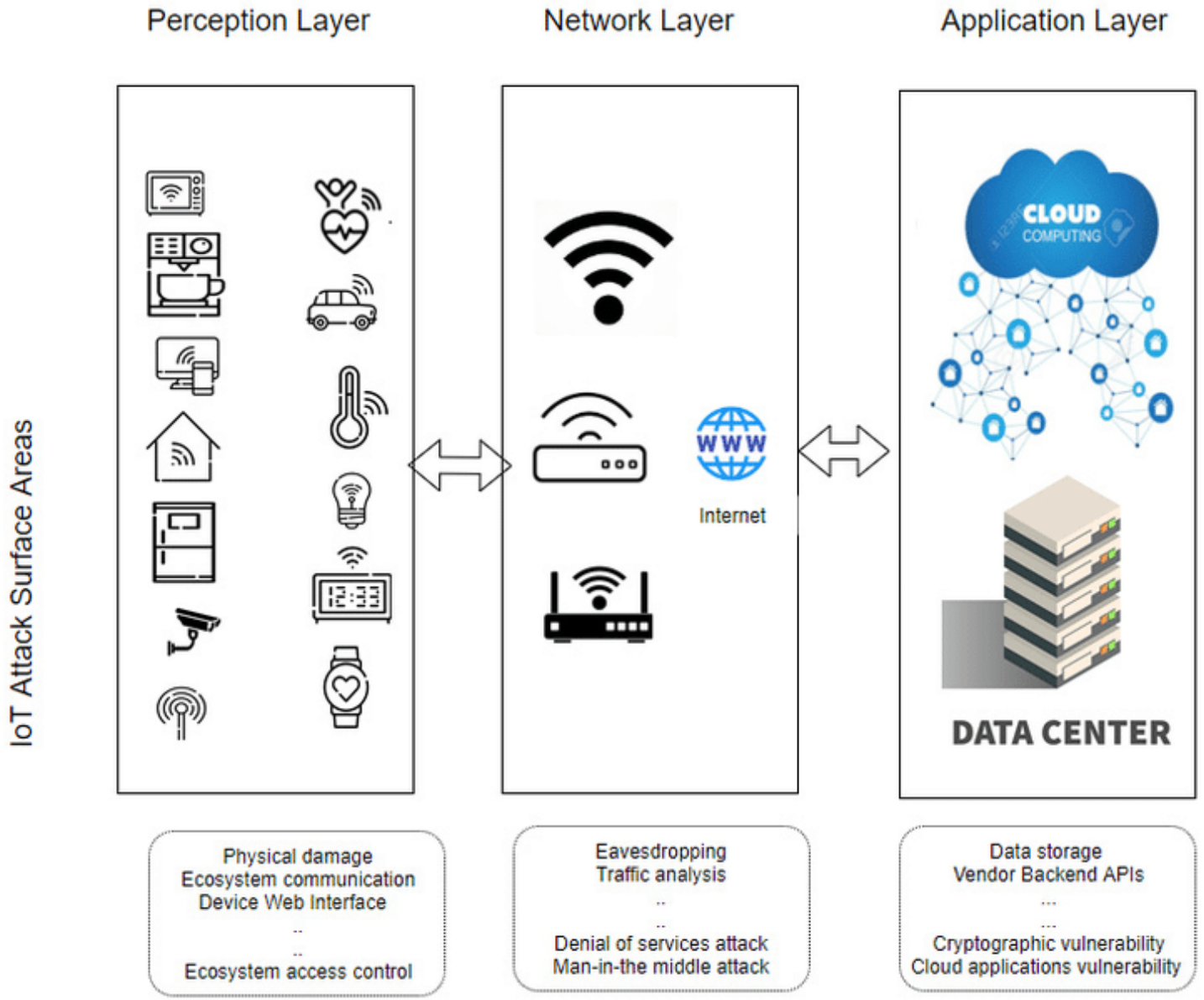


Group	Name	data size (e.g., RAM)	code size (e.g., Flash)	Examples
M	Class 0, C0	<< 10 KiB	<< 100 KiB	ATtiny
M	Class 1, C1	~ 10 KiB	~ 100 KiB	STM32F103CB
M	Class 2, C2	~ 50 KiB	~ 250 KiB	STM32F103RC
M	Class 3, C3	~ 100 KiB	~ 500..1000 KiB	STM32F103RG
M	Class 4, C4	~ 300..1000 KiB	~ 1000..2000 KiB	"Luxury"
J	Class 10, C10	(16..)32..64..128 MiB	4..8..16 MiB	OpenWRT routers
J	Class 15, C15	0.5..1 GiB	(lots)	Raspberry PI
J	Class 16, C16	1..4 GiB	(lots)	Smartphones
J	Class 17, C17	4..32 GiB	(lots)	Laptops
J	Class 19, C19	(lots)	(lots)	Servers

Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

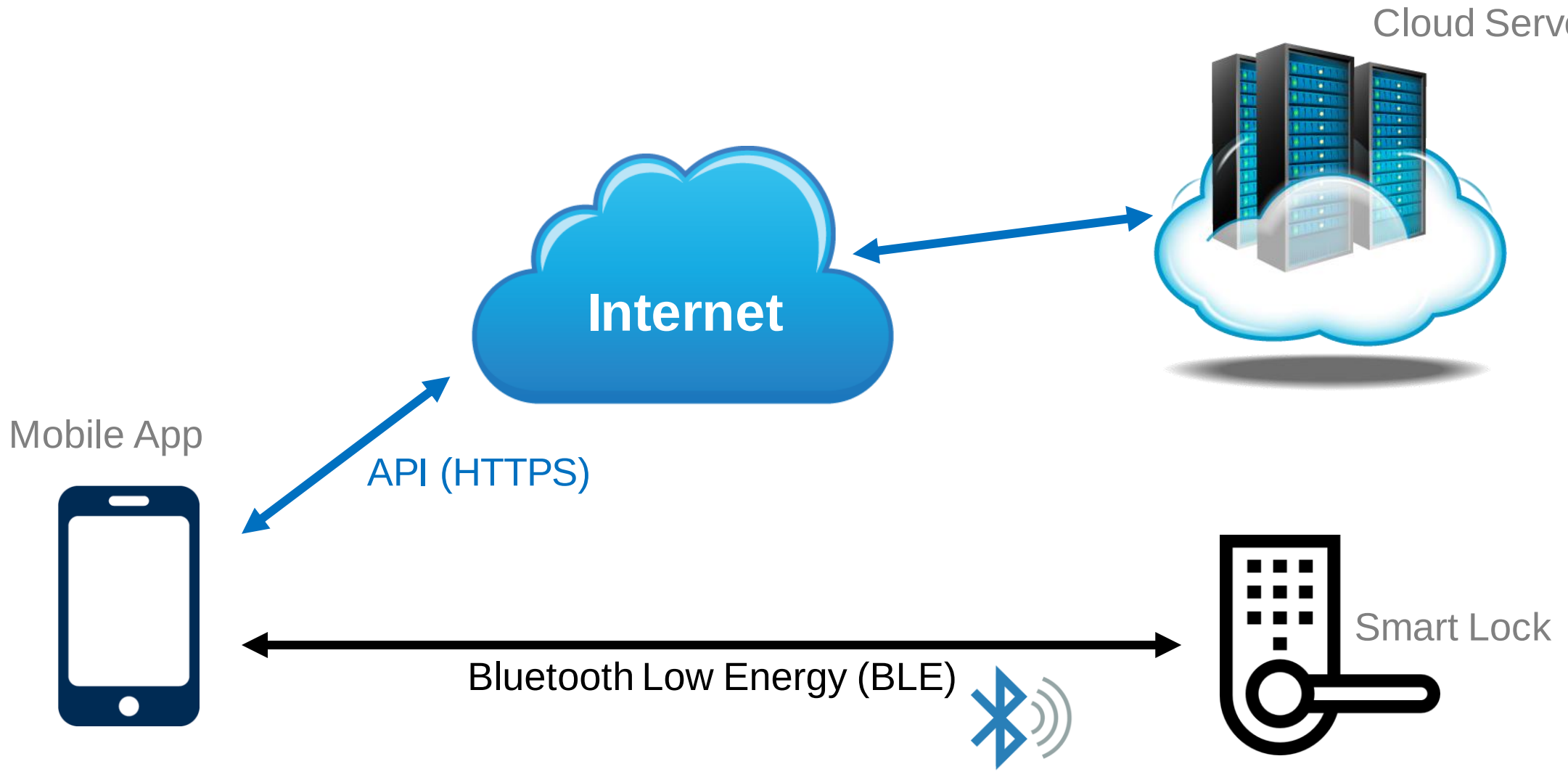
https://www.ietf.org/archive/id/draft-ietf-lwig-7228bis-00.txt

IoT Architectur & Layer Attacks



Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J.; Alazab, A. A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. Electronics 2019, 8, 1210. https://doi.org/10.3390/electronics8111210

Example: Intelligent Locking System



Problem

- A simple attack to bypass a lockout is an example of the types of vulnerabilities you will encounter when hacking IoT systems.

- Use of small, low-power and low-cost embedded devices

→ System insecurity

- Securing the communication channels
  - Instead of resource-intensive public key cryptography (PKI)
  - mostly symmetric keys used
    - Very often not unique
    - Hard-coded in the firmware or hardware

    → Attacker can extract them and then reuse them in other devices

Frameworks, Standards, and Recommendations

- Solution: Implementation of standards

  → Addressing various aspects of the security and trust problem in the IoT system

- Goal: Consolidation of accepted "best practice" approaches
- But
  - Many standards exist in parallel → Fragmented landscape
  - Disagreement

  → No consensus on the best way to secure IoT devices

2. Is our system really secure?
- Threat Modelling -

MEDTECH

3 in 4 infusion pumps vulnerable to cyberattacks: study

By **Conor Hale** • Mar 4, 2022 09:10am

28.04.2017·Fachbeitrag ·Medizinprodukte

Vorsicht vor «Medjacking»

| Hacker konnten bereits Insulinpumpen, Defibrillatoren und Infusionspumpen umprogrammieren. Die FDA fordert von einem Medizinprodukte-Hersteller nun rasch Massnahmen. |

Immer mehr Medizinprodukte sind mit dem Internet, Smartphones oder mit Netzwerken verbunden. Im Januar hatte die US-Arzneimittelbehörde FDA vor möglichem Hacking implantierter Defibrillatoren der Firma St. Jude Medical gewarnt. Dabei ging es um das «Merlin@home» System, das über einen Transmitter in der Nähe des Patienten sowohl Daten übermittelt, als auch Uploads empfängt. Nun moniert die FDA, dass die Software, die das Problem beheben sollte, ungenügend getestet worden sei. Sie gibt dem Hersteller 15 Werktage Zeit für Gegenmassnahmen. Dass «Medjacking» prinzipiell möglich ist, haben Hacker bereits gezeigt, allerdings mit teils erheblichen Aufwand. Sicherheitsexperten raten, Implantate - falls möglich - so einzustellen, dass kein automatischer Datentransfer via WLAN stattfindet und etwaige Vernetzungen nur zu aktivieren,

PIPETTE – SWISS LABORATORY MEDICINE | WWW.SULM.CH | NR. 4 | AUGUST 2018 | NEWS

Nicolas Krämer[1]

Angriff aus der Dunkelheit

Cyberangriff auf ein Krankenhaus: IT-Systeme werden heruntergefahren, Erpressung durch kriminelle Hacker. Intensivpatienten sterben durch ferngesteuerte Medikamentenpumpen und Beatmungsgeräte. Das FBI ermittelt. Wenn das in der US-Serie «CSI:CYBER» auf RTL läuft, können wir uns bequem im Sessel zurücklehnen …

DIVE BRIEF

75% of infusion pumps have cyber flaws, putting them at risk from hackers: study

Published March 3, 2022

March 25, 2019, 6:21 AM CET

By Alex Johnson

The world's largest medical device company has acknowledged that many of its implanted cardiac defibrillators use an unencrypted wireless protocol that could allow an attacker to change the settings of the lifesaving devices.

The vulnerability affects more than 20 defibrillator models, monitors and programmer units made by Medtronic Inc. of Fridley, Minnesota. The devices include implantable cardioverter defibrillators, or ICDs, which can correct dangerously fast or irregular heartbeat, and cardiac resynchronization therapy defibrillators, or CRT-Ds, which essentially are pacemakers that deliver small electrical charges to help keep the heart's ventricles pumping in sync.

CYBERSECURITY NEWS

Infusion Pump Vulnerabilities Point to Gaps in Medical Device Security

McAfee researchers discovered significant gaps in medical device security that may allow hackers to administer deadly doses of medications through an infusion pump.

Definition

- The threat modeling process
  - systematically identifies possible attacks on a device and
  - then prioritizes specific problems based on their severity.

- Threat modeling can be time-consuming → is sometimes overlooked.
- But it is essential!
  - You need to understand the threats, their impact and the corresponding mitigation measures,
  - To be able to take them and
  - To eliminate them.

Different Methods With Different Goals (1)

Method	
STRIDE	• Helps to identify relevant risk mitigation techniques • Is the most mature • Is easy to use but time consuming
P.A.S.T.A.	• Helps to identify relevant risk mitigation techniques • Contributes directly to risk management • Promotes collaboration between stakeholders • Contains built-in prioritization of risk mitigation • Takes a lot of time, but has extensive documentation
Trike	• Helps to identify relevant risk mitigation techniques • Contributes directly to risk management • Includes integrated prioritization of threat mitigation • Promotes collaboration between stakeholders • Has automated components • Has vague, inadequate documentation

Different Methods With Different Goals (2)

Method	
OCTAVE	• Helps to identify relevant risk mitigation techniques • Contributes directly to risk management • Includes integrated prioritization of threat mitigation • Promotes collaboration between stakeholders • Delivers consistent results when repeated • Has automated components • Is explicitly designed for scalability • Has little publicly available documentation
Attack trees	• Helps to identify relevant risk mitigation techniques • Provides consistent results when repeated • Is easy to use if you already know the system well

3. Let‘s Inspects - STRIDE

STRIDE Framework (1)

- Threat classification model
  - Goal: Identification of vulnerabilities in the technology
  - But does not focus on vulnerable points/things or potential attackers


Spoofing: When an actor pretends to play the role of a system component


Tampering (Manipulation): If an actor violates the integrity of data or a system

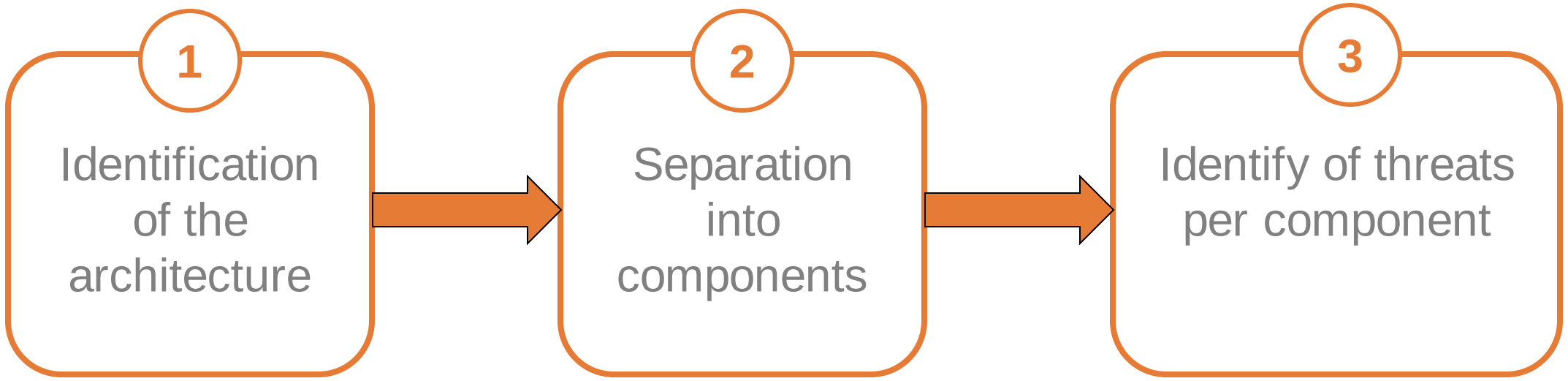

Repudiation: If users can deny that they have performed certain actions on the system


Information Disclosure: If an actor violates the confidentiality of the system's data.


Denial of Service (DoS): If an actor disrupts the availability of a system component or the system as a whole


Elevation of Privilege: If users or system components can elevate themselves to an authorization level to which they should not have access.

STRIDE Framework (2)



3.1. Our example: Infusion pump in a hospital

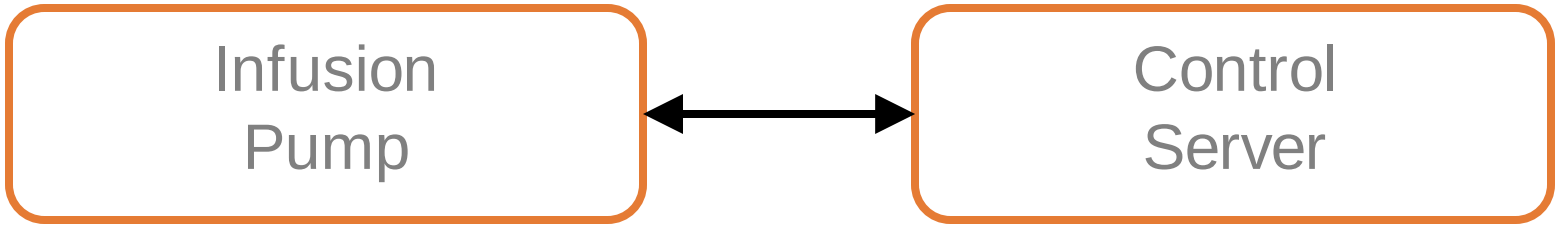
Our example: Infusion ump in a hospital

- Assumptions:
  - The pump is connected to a control server in the hospital via WiFi.
  - The network is insecure and has no segmentation

→ Visitors to the hospital could connect to the WiFi and passively monitor the pump's data traffic.

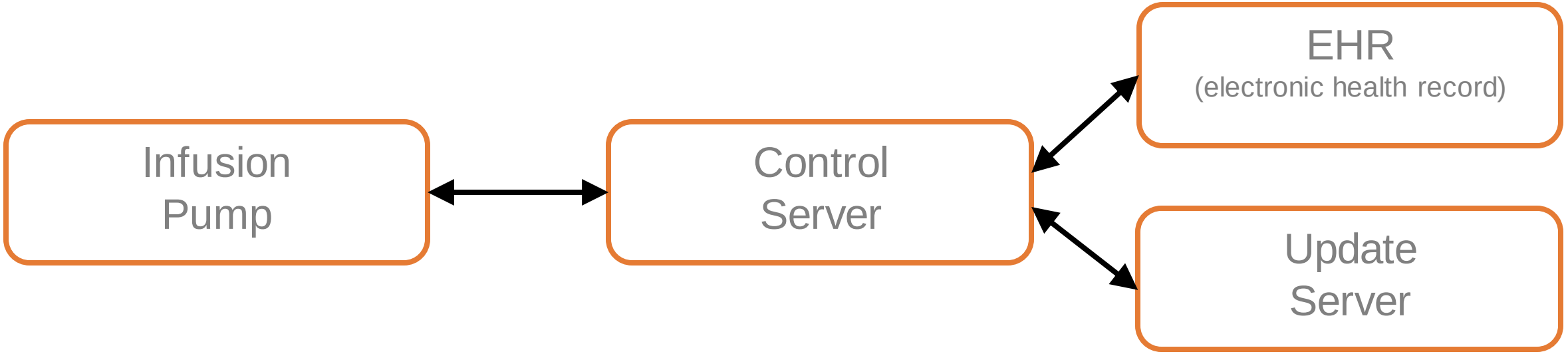
STRIDE – Step 1
Identification ot the architecture

What do we have …



- Server is operated by nursing staff
- In some cases, authorized IT administrators can also access it

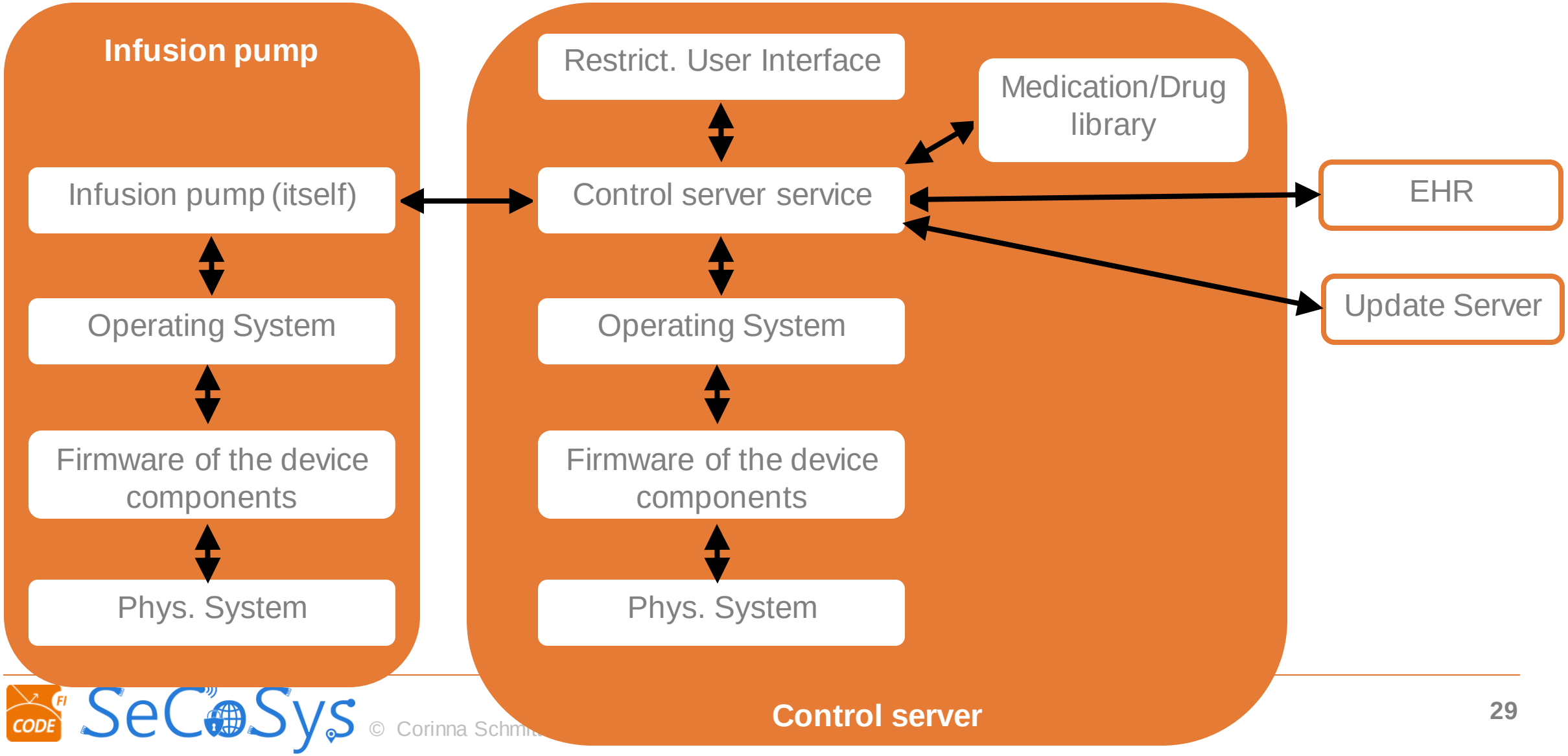
… in total?



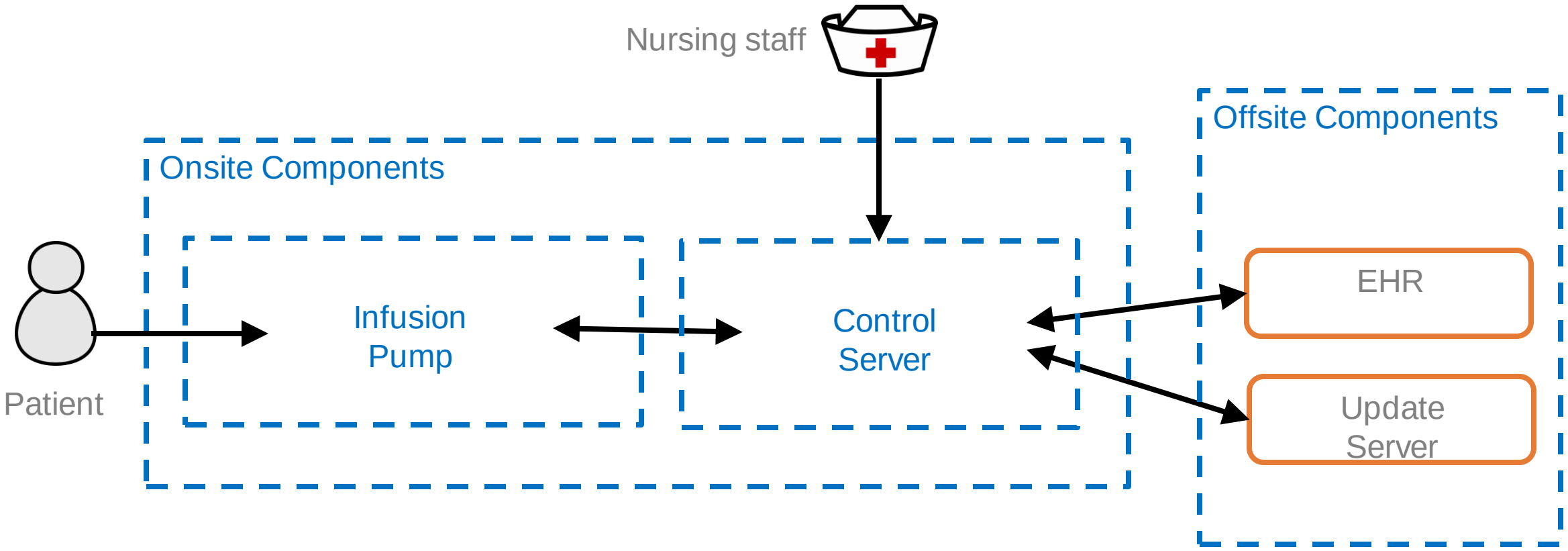
- Updates necessary
  - Software
  - Medication/Drug library
  - Patent file (EHR)

STRIDE – Step 2
Separation into components

Zoom-In

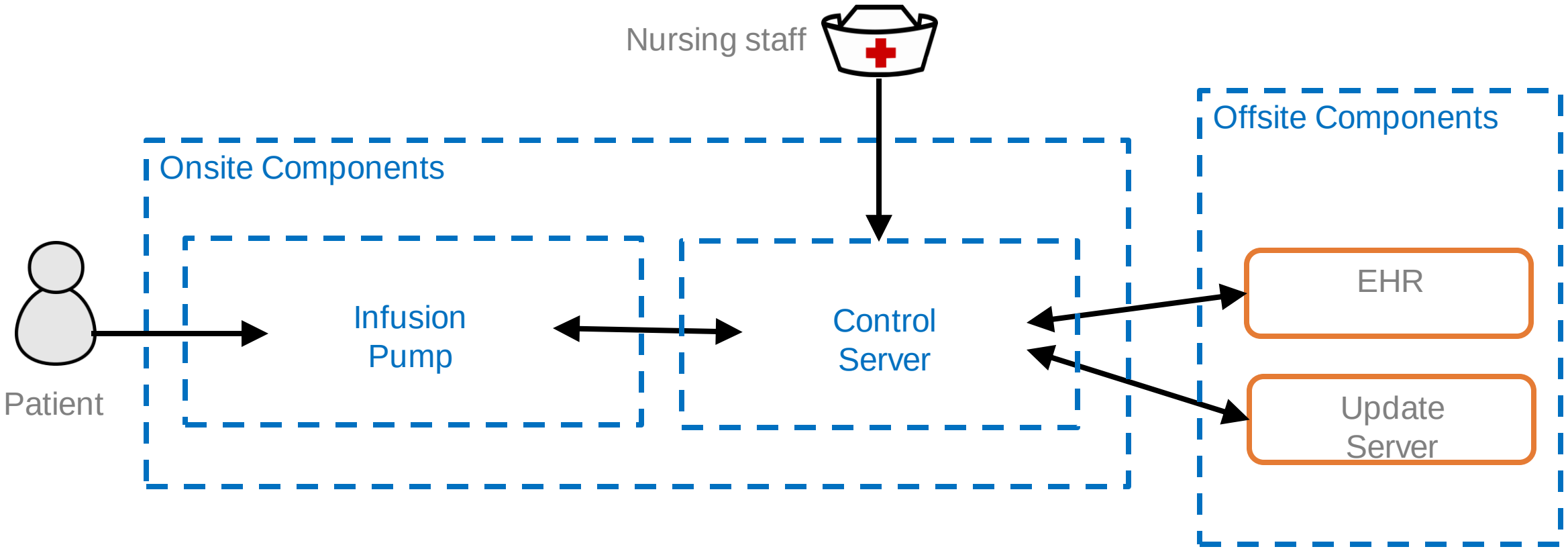

Infusion pump
Infusion pump (itself)
Operating System
Firmware of the device components
Phys. System
Restrict. User Interface
Control server service
Operating System
Firmware of the device components
Phys. System
Medication/Drug library
EHR
Update Server
Control server

Confidence limits (1)



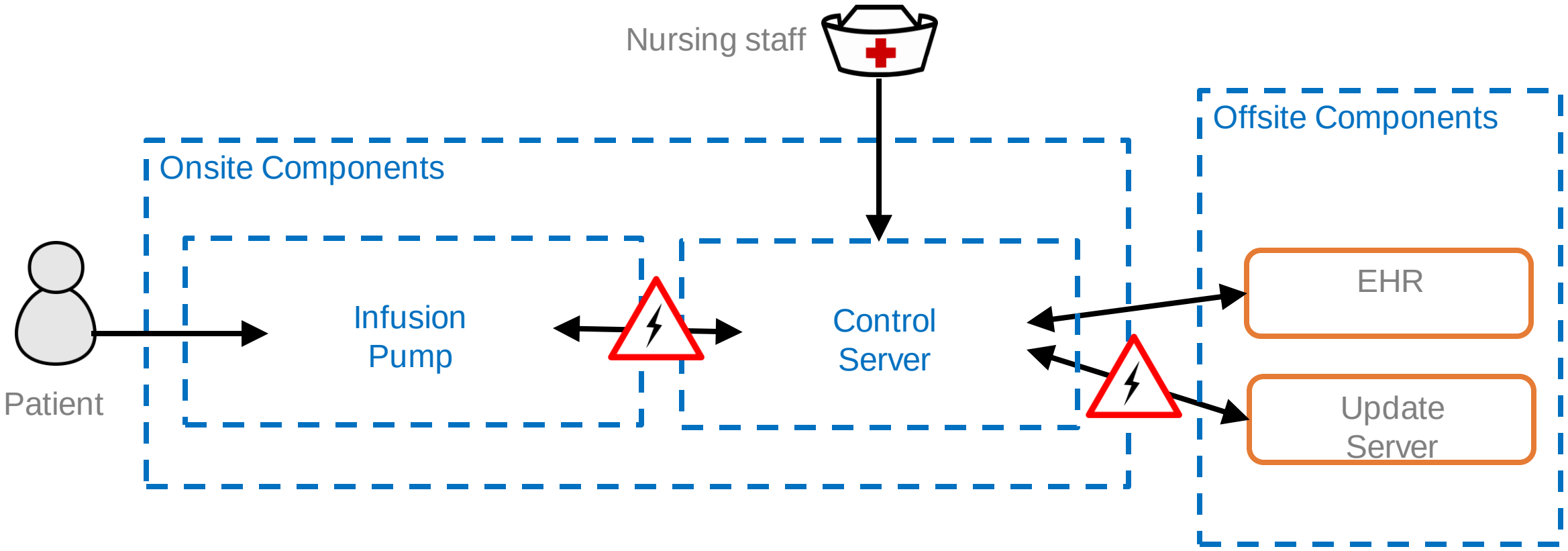
- Confidence limits (- - -) surround groups with the same security attributes
  → Indicate data flow entry points that may be suspicious for threats

Confidence limits (2)



Where can we already recognize the first threat?

Confidence limits (3)



- Patient data from the pump can reach the third-party update server via the control server.

STRIDE – Step 3

Identify of threats per component

What is the plan?

- Apply the STRIDE framework to the components 
  → Comprehensive list of threats

- Examine the general safety requirements of the product
  – Specific requirement of the manufacturer
  – Device documentation

- Example of medication infusion pumps
  – As medical devices, must guarantee patient safety and data protection
  – Certifications should be available → "Conformité Européenne" (CE) test mark

Restrictive User Interface (1)

- Restrictive user interface (RUI) is the "kiosk app"
  - Interacts with control server service
  - Severely restricts the actions a user can perform.
    - It's like an ATM app; you can interact with the software, but only in a handful of ways.

- RUI also has its own specific limitations
  - User should not be able to exit the app.
  - User must authenticate with valid credentials to access it.

Restrictive User Interface (2)

- Spoofing
  - RUI authenticates users with a weak (e.g. 4-digit) PIN
  - Easily predictable by attacker → Access to authorized accounts possible
  - →  Attacker could send commands to the infusion pump

- Tampering
  - RUI can receive other than the limited set of allowed inputs
  - Even if most keyboard keys have been disabled, the system can still allow key combinations
  - e.g. shortcuts, hotkey, accessibility functions - ALT+F4 → Closes window)
  - →  Users can bypass RUI and exit the application

Restrictive User Interface (3)

Repudiation

– RUI only supports a single user account for medical staff

→ Log files useless as it is not possible to determine who exactly used the device.

→ Any team member can access the control server & operate the infusion pump

Information Disclosure

– User displayed debugging messages/errors can reveal patient information or system internals

→ Attackers can decrypt message

→ System technology information collection

→ Vulnerability exploitation

Restrictives User Interface (4)

Denial of Service

– RUI is vulnerable to this because it has a brute force protection mechanism

- N consecutive incorrect login attempts → Locked out of the system

→ Lockout may lead to breach of patient safety requirement

→ Protection against threats vs. causing threats

Elevation of Privilege

– Medical systems usually have remote support solutions → Immediate access for technicians

→ Services vulnerable to hacking and possible misuse by attackers

→ Remote administrative access to the RUI or control server service.

→ Authentication required, but login information may be publicly accessible & the same for all products

1. Split up into the groups according to the number you have!

2. Apply STRIDE for the assigned component!
   - You receive a brief description.
   - You have to make perhaps further assumptions.

3. Present the inspection result to the audience!

What are your results

Group 1 – Control server services

- Application for operating the control server
- Responsible for communication with
  - RUI,
  - Medication library,
  - infusion pump
  - EHR (to receive information about the patients) and ← HTTPS
  - Update server (to receive software and medication library updates) ← TCP

- Additional safety requirements
  - Identification and verification of the infusion pump → Avoidance of skimming attacks
  - Data should be protected during transmission → Prevention of eavesdropping and replay attacks
  - Prevention of compromising the security controls of the hosting platform

Workshop Results Group 1 *(no pic available)*

- Spoofing
  - – Possible because the control server does not have a solid method of identifying the infusion pump
  - →  Analysis of the communication protocol enables imitation of the pump and communication with the control server → Threat
- Tampering
  - – Possible because control server does not have a solid method for data integrity verification
  - →  Man-in-the-middle (MITM) attacks possible → Changes to transmitted data/measured values
  - →  Direct impact on patient health and safety
- Repudiation
  - – Control server uses globally writable logs to monitor its actions
  - →  Overwriting of system users possible → Manipulation possible

Workshop Results Group 1 *(no pic available)*

Information Disclosure

– Unnecessarily sending sensitive patient information to update server or infusion pump

→ Misuse of data

Denial of Service

– Attackers in the vicinity can interfere with the signal

→ Deactivation of communication with the infusion pump → System unusable

Elevation of Privilege

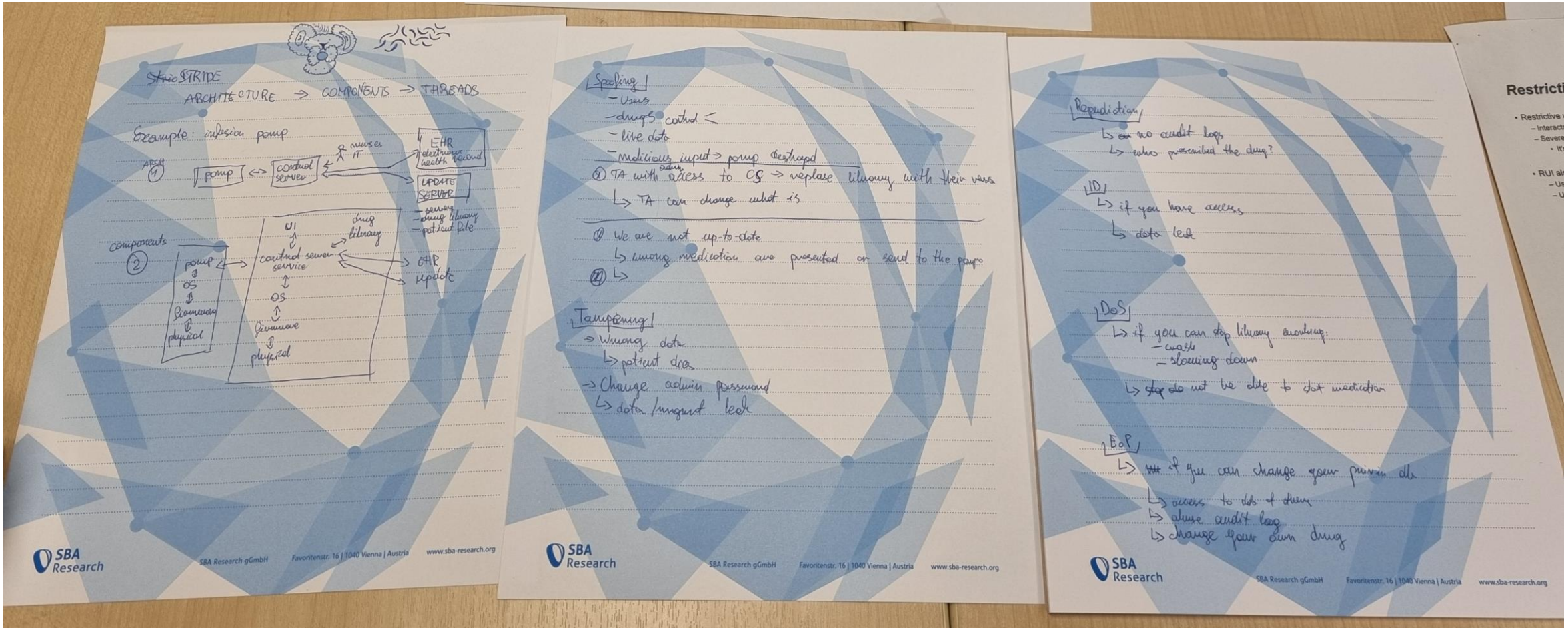
– Disclosure of API services

→ Unauthenticated attackers could perform "top-secret" functions (e.g. dosage changes)

Group 2 - Medication/Drug library

- Main database of the system
- Contains all information about the medication
- Can also control the user management system

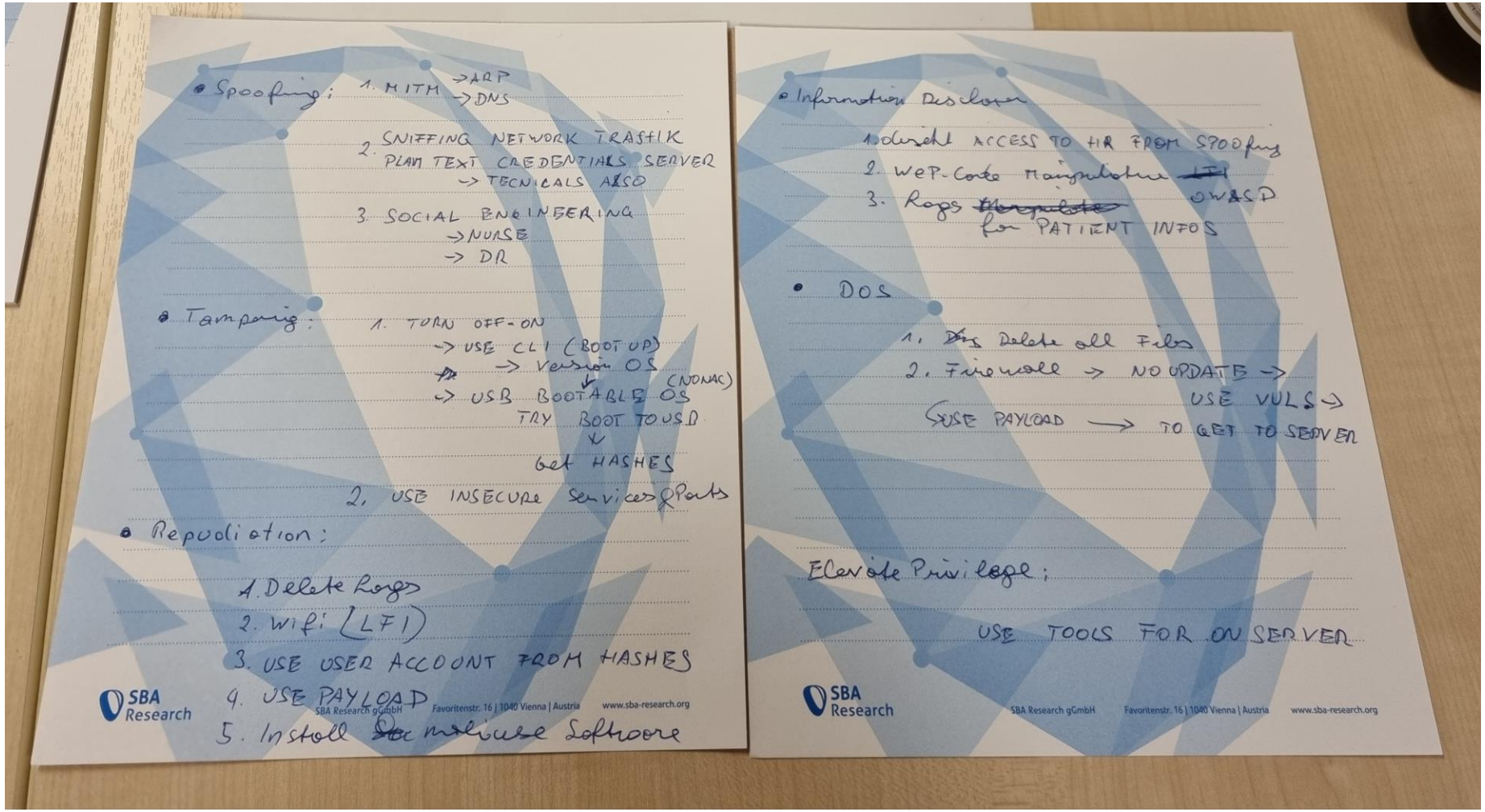
Workshop Results Group 2



Group 3 – Operating System

- Receives input from the control server service
- Integrity check mechanisms and basic configurations should exist
  - Enable update procedures, enable network firewalls and detect malicious code

Workshop Results Group 3



Group 4 - Firmware of the device components

- Provides certain low-level operations
- Stored in non-volatile memory or loaded into the component by drivers during initialization
- Signing of the firmware by the manufacturer desirable
- Device should verify signature

- Examples: CD/DVD drive, controller, display, keyboard, mouse, motherboard, network card, sound card, video card

Workshop Results Group 4 (no pic available)

- Spoofing
  - Logical errors in firmware
  - →  Attacker can downgrade firmware to older versions with known vulnerabilities
  - →  Installation of custom firmware possible

- Tampering
  - – Installation of manipulated firmware (malware)
  - →  Advanced Persistent (APT) attacks possible
  - →  Trojan horse
  - →  Manipulation of configuration variables

IoT devices often do not check the integrity of the digital signature and firmware!

Workshop Results Group 4 (no pic available)

Information Disclosure

- Communication channel with the server of a third-party provider (analysis purposes, update status)

→ Disclosure of patient data

→ Disclosure of unnecessary security-relevant API functions

Denial of Service

– Over-the-air updates (OTA) for the distribution of firmware

→ Attacker can block update → insecure/unstable state

→ Direct interaction with communication interface possible

Elevation of Privilege

– Drivers may have known vulnerabilities

– Delivery with embedded default passwords

→ Abuse of undocumented, exposed management interfaces

Group 5 – Phys. Equipment (System)

- This also includes the housing, which contains the control server processor and the RUI screen

- Further security requirements
  - Control server in separate room
  - Access only for authorized employees
  - Components should support hardware attestation & have secure boot process
  - Device should have active memory protection
  - Ability to perform secure, hardware-assisted key management, storage and generation as well as secure cryptographic operations
  - Critical components should be sealed with e.g. epoxy resin → Circuit analysis difficult

If attackers have physical access, they usually also have administrative access!

Workshop Results Group 5 (1)

- Assumptions:
  - 1 device, including pc, screen, and keyboard
  - Room is locked with key lock

- Spoofing:
  - If room keycard protected: Clone Keycard
  - Social engineer way to key from reception desk
  - Copy key?
  - Tallgate into room
  - Spoof Remote Access (IT Admin)
  - Malicious Keyboard/KeyLogger/Remote Keyboard
  - Spoof control server, pump, external dependencies (EHR, Update server)
  - Replay attacks

- Tampering:
  - Physical damage to server (magnet over drive)
  - Replace drivers/lock
  - Fill up drive with logs
  - Cut power (curcuit breakers)
  - Epox can be bypassed using documentation
  - Bad USB

- Repudiation
  - Single key to room

Workshop Results Group 5 (2)

- Information Disclosure:
  - Camera in room
  - Keylogger
  - Steal drive
  - Screen mirror cast device
  - Bad USB

- Denial of Service:
  - Cut power (curcuit breakers)
  - Glue lock closed
  - Steal only key
  - Disable router
  - WiFi Jamming/Disconnect attack

- Elevation of Privileges:
  - Alt+F4
  - Get console access
  - MITM/Compromise Remote Access for IT Admin
  - Bad USB

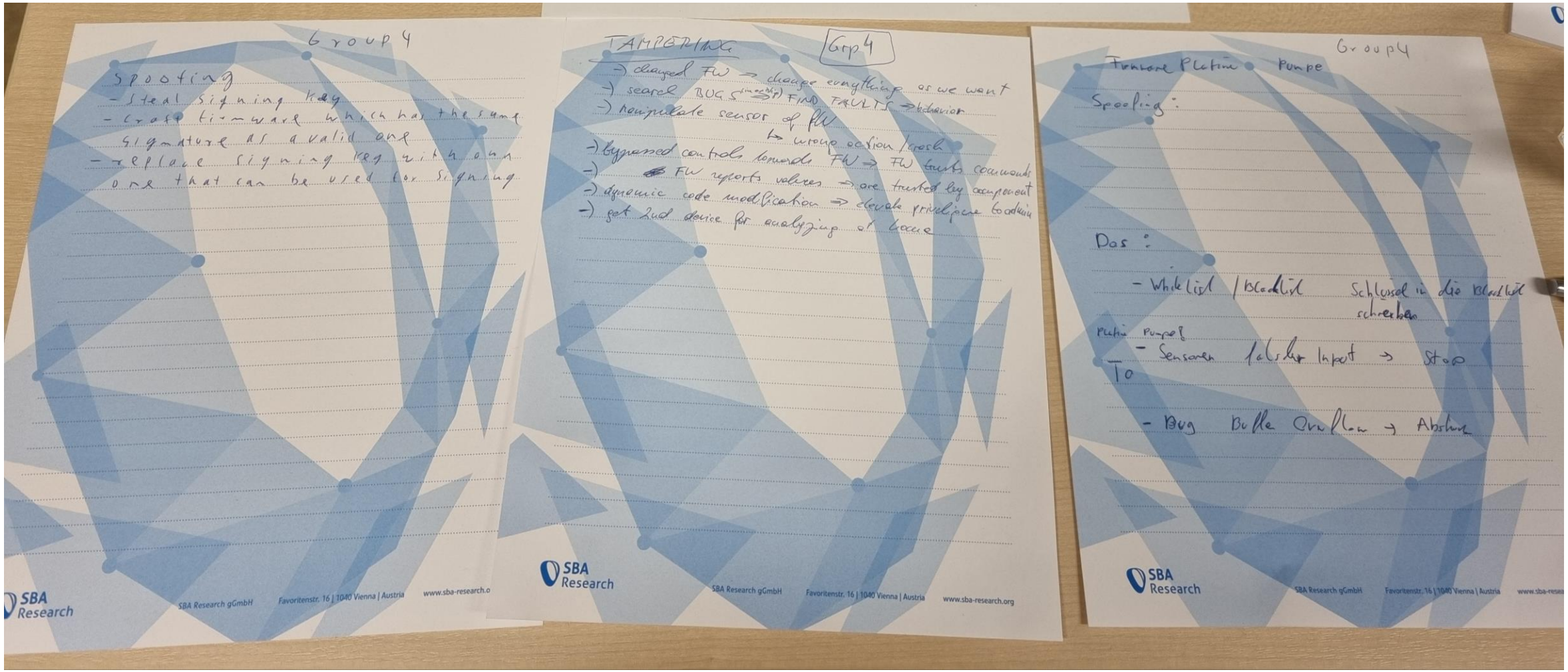
Group 6 – Infusion pump resp. its service

- Nothing other than software that operates physical units

- Components:
  - Communication protocol
  - Microcontroller

- Additional security requirements
  - Detecting the integrity of the control server service
  - Checking the integrity of the control server service
  - Communication protocol should be secure → Prevention of replay attacks

Workshop Results Group 6



What do you think about STRIDE

Conclusions

- STRIDE
  - Is helpful for the overview
  - Should be carried out with different "glasses on the nose"
  - E.g. technician, business economist, sales
  - Can also be used for the organization to me
  - Should be applied several times over time
  - If necessary, break down the globally viewed component even further → "Zoom-In"

- STRIDE can also be combined with other thread models
  - Changing perspectives and
  - Prioritization!

Universität der Bundeswehr München

PD Dr. rer. nat. habil. Corinna Schmitt

Head of Secure Communication Systems

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT
DEUTSCHLAND

CODE RI

Research Institute CODE
Werner-Heisenberg-Weg 39
85577 Neubiberg • Germany

Phone: +49 (0)89 6004-7314
Email: corinna.schmitt@unibw.de

https://www.unibw.de/code https://www.corinna-schmitt.de