

# SICHERHEIT IN MICROSERVICE-UMGEBUNGEN

TOBIAS TEFKE UND RALF C. STAUEMEYER

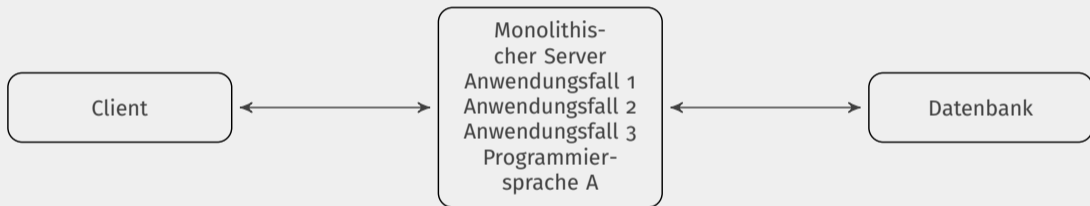
HOCHSCHULE SCHMALKALDEN

30. DFN-KONFERENZ "SICHERHEIT IN VERNETZTEN SYSTEMEN"

8.-10. FEBRUAR 2023

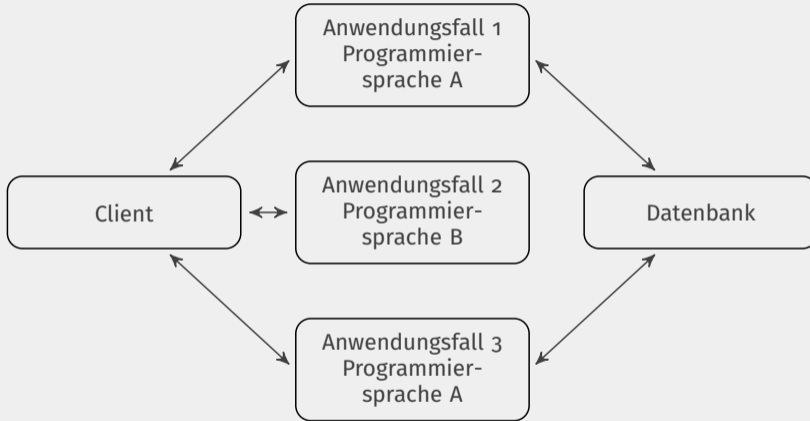
- 1 Microservices
- 2 Sicherheit in Bezug auf Microservices
- 3 Microservices am Beispiel einer Lehrumgebung
- 4 Sicherheitsanalyse der Lehrumgebung

# MICROSERVICES



Schematische Darstellung einer monolithischen Softwarearchitektur

- Begrenzter Kontext
- Geringer Codeumfang (Größe)
- Unabhängigkeit



Schematische Darstellung einer Microservice-Softwarearchitektur

- Intern vs. extern
- Synchron vs. asynchron

Oft Containerization, da

- Automatisierung
- Unabhängigkeit
- Portabilität
- Leichtgewichtigkeit
- Isolation (Sicherheit)



- Zugriffsschutz
- Abhängigkeiten zwischen Microservices
- Ausfallkaskaden → Circuit Breaker

# **SICHERHEIT IN BEZUG AUF MICROSERVICES**

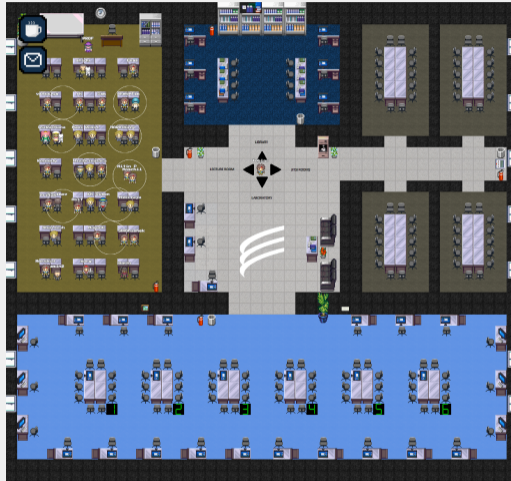
- Durch HTTP ermöglichte Verfahren (z.B. Basic, Bearer)
- JSON Web Token (JWT)
- Sidecars → zentrale Implementierung

- Vom Host und untereinander
- Nutzung von Namespaces
- AppArmor und SELinux
- Netzwerkisolation

- Externe Schnittstellen: TLS
- Interne Schnittstellen: MTLS

# **MICROSERVICES AM BEISPIEL EINER LEHRUMGE- BUNG**

# BEWEGEN VON CHARAKTEREN ÜBER EINE KARTE



Karte unseres virtuellen Internet-der-Dinge-Labors

# GRUPPENKOMMUNIKATION



Gruppenkommunikation in WorkAdventure





Aktionen werden nach Bestätigung durch den Nutzer ausgeführt

# AKTIONEN (FORTS.)



Aktionen sind erweiterbar

# INTEGRATION VON BIGBLUEBUTTON FÜR ONLINE-VORLESUNGEN

Public Chat

Welcome to lecture!

For help on using BigBlueButton see these (short) [tutorial](#) [videos](#).

To join the audio bridge click the phone button. Use a headset to avoid causing background noise for others.

This server is running BigBlueButton.

Thomas 12:00 PM  
Hallo

Luca 12:04 PM  
Why shouldn't we use ECB?

Tobias 12:55 PM  
Because each byte is encrypted using the same function?

Simon 1:02 PM  
Does the counter mode operate in parallel?

Franz 1:03 PM  
Kerckhoffs principle is fundamental for modern cryptosystems?

**block cyphers**  
modes of operation – CTR

(5) Counter mode (recommended)

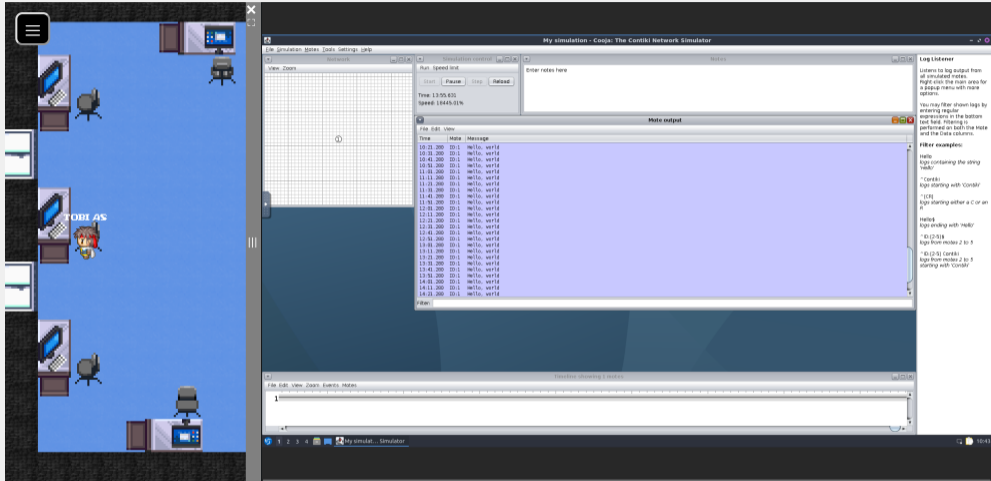
- initialisation of counter  $R$  with random number
- series of counter values  $R(i) = R(i-1) + 1$  with  $1 \leq i \leq m$
- counter values must not repeat

principle:  $C_i = M_i \oplus E(R(i), K)$  (decryption:  $M_i = C_i \oplus E^{-1}(R(i), K)$ )

$$\begin{array}{cccc} R & R+1 & R+2 & R+m-1 \\ \downarrow n & \downarrow n & \downarrow n & \downarrow n \\ K \xrightarrow{k} \boxed{E} & K \xrightarrow{k} \boxed{E} & K \xrightarrow{k} \boxed{E} & \dots & K \xrightarrow{k} \boxed{E} \\ \uparrow n & \uparrow n & \uparrow n & & \uparrow n \\ M_1 & M_2 & M_3 & & M_m \\ \oplus & \oplus & \oplus & & \oplus \\ \downarrow n & \downarrow n & \downarrow n & & \downarrow n \\ C_1 & C_2 & C_3 & & C_m \end{array}$$

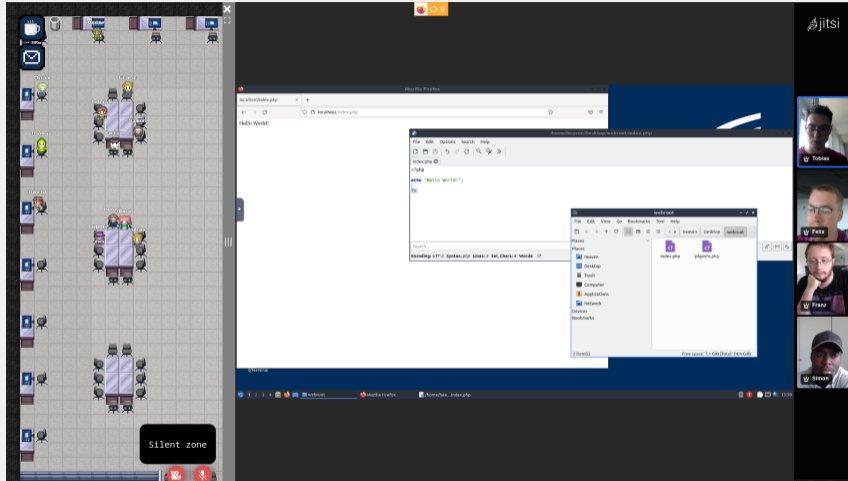
Studierende können während der Vorlesung miteinander kommunizieren

# ARBEITEN AN VIRTUELLEN RECHNERN



Ausführung eines Programms auf einem virtuellen Rechner

# PC-POOL



Gemeinsames Arbeiten im PC-Pool

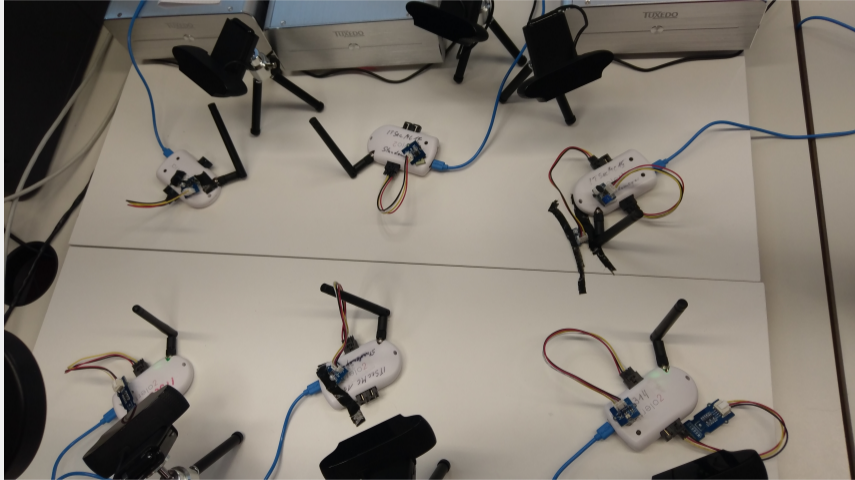
# DEZENTRALES ARBEITEN AN PHYSISCHEN GERÄTEN

The screenshot displays a Jitsi video conference interface. On the left, there is a virtual lab environment with various equipment and a 'Silent zone' button. The main area shows a terminal window with the following code:

```
CC ..../core/net/mc-debug.c
CC ..../core/net/link-status.c
CC ..../core/net/mac/nullnac.c
CC ..../core/net/mac/nullrdc-noframer.c
CC ..../core/net/mac/nordc.c
CC ..../core/net/mac/framer82154-ie.c
CC ..../core/net/mac/nac-sequence.c
CC ..../core/net/mac/framer-nullnac.c
CC ..../core/net/mac/framer82154.c
CC ..../core/net/mac/nac.c
CC ..../core/net/mac/framer-802154.c
CC ..../core/net/mac/cna.c
CC ..../core/net/mac/phase.c
CC ..../core/net/mac/nullrdc.c
CC ..../core/net/mac/contikinac/contikinac.c
CC ..../core/net/mac/contikinac/contikinac-framer.c
CC ..../core/net/l1sec/nullsec.c
CC ..../core/net/l1sec/antl-replay.c
CC ..../core/net/l1sec/can-star-packetbuf.c
CC ..../core/net/l1sec/nmacrespc/nmacrespc.c
CC ..../dev/cc1200/cc1200-800-fsk-1-3kpps.c
CC ..../dev/cc1200/cc1200.c
CC ..../dev/cc1200/cc1200-802154g-863-870-fsk-50kpps.c
CC ..../cpu/cc2538/cc2538.ld
CC ..../cpu/cc2538/_startup-gcc.c
CC ..../hello-world.c
LD ..../hello-world.elf
arm-none-eabi-obcopy -O text ..../hello-world.elf ..../hello-world.hex
arm-none-eabi-obcopy -O binary -gap-fill 0xff ..../hello-world.elf ..../hello-world.bin
cp ..../hello-world.elf ..../hello-world.zoul
rm ..../hello-world.co obj_zoul/startup-gcc.o
make -C ..../lab -C ..../contiki-examples/zolertia/tutorial/01-basics make ..../hello-world.upload
using saved target 'zoul'
CC ..../cpu/cc2538/_fleece-addr.c
```

On the right, a vertical stack of video thumbnails shows participants: Tobias, Felix, Franz, and Simon. The top right corner features the Jitsi logo.

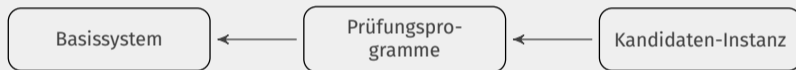
Gemeinsames dezentrales Arbeiten an Laborhardware



RE-Motes im Labor, auf welche online zugegriffen werden kann

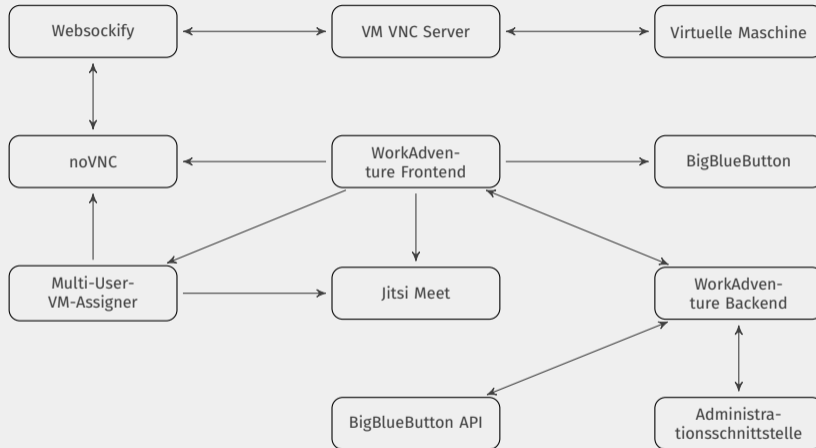
- Jeder Kandidat erhält einen Rechner, um Lösungen zu erarbeiten
- Benötigte Entwicklungsumgebung ist vorinstalliert
- Nach Ablauf der Zeit werden die Lösungen auf einen Server hochgeladen
- Dort können diese vom Korrektor eingesehen werden





Struktur eines virtuellen Rechners im Prüfungsmodus

# STRUKTURELLER AUFBAU DER LEHRUMGEBUNG



Schematische Darstellung der Labor Basisarchitektur

# **SICHERHEITSANALYSE DER LEHRUMGEBUNG**

- Spezielle HTTP-Anfragen, die an Microservices geschickt werden
- Mittels HTTP-Client (curl) gefunden
- Standard-Administrationstoken in der Community-Version

Mehrere Lücken, z.B.:

- Überlastungsmeldung zeigen
- Zugang zu Debug-Informationen
- DoS durch inkorrekte Fehlerbehandlung

## BEISPIEL: ABRUFEN VON DEBUG-INFORMATIONEN

Request:

```
curl -i -k -X GET -H "Content-Type: application/json"  
https://your.instance/pusher/dump?token=123
```

Response:

```
HTTP/2 200  
content-type: application/json  
uwebsockets: 18  
content-length: 16327  
date: Fri, 22 Jul 2022 21:46:36 GMT  
  
// Debug-Informationen
```




# BEISPIEL: ÜBERLASTUNGSMELDUNG ZEIGEN



Überlastungsmeldung in fast leerem Raum

- Offene Standard- und Debugzugänge deaktivieren
- Authentifizierung von Nutzern immer erzwingen
- Sicherstellen, dass keine privaten Schnittstellen öffentlich angeboten werden
- Alle Eingaben prüfen



-  SUASecLab
-  t.tefke@stud.fh-sm.de
-  r.staudemeyer@hs-sm.de