
# POWER CYCLES

Chaos Communication Congress

Hamburg, 27-30 grudnia 2025

2026-01-29

39C3

# Czym jest 39C3?

## Chaos Communication Congress (39C3)

- Coroczna konferencja „hakerska” w Hamburgu

## Chaos Communication Congress (39C3)

- Coroczna konferencja „hakerska” w Hamburgu
  - „hakerska” bo choć większość dotyczy bezpieczeństwa, tak naprawdę tematykę lepiej można określić kulturą hakerską

## Chaos Communication Congress (39C3)

- Coroczna konferencja „hakerska” w Hamburgu
  - „hakerska” bo choć większość dotyczy bezpieczeństwa, tak naprawdę tematykę lepiej można określić kulturą hakerską
- 27-30 grudnia 2025

## Chaos Communication Congress (39C3)

- Coroczna konferencja „hakerska” w Hamburgu
  - „hakerska” bo choć większość dotyczy bezpieczeństwa, tak naprawdę tematykę lepiej można określić kulturą hakerską
- 27-30 grudnia 2025
- ~16 000 uczestników w 2025

## Chaos Communication Congress (39C3)

- Coroczna konferencja „hakerska” w Hamburgu
  - „hakerska” bo choć większość dotyczy bezpieczeństwa, tak naprawdę tematykę lepiej można określić kulturą hakerską
- 27-30 grudnia 2025
- ~16 000 uczestników w 2025
- Organizowana przez Chaos Computer Club (CCC)

39C3

# Zwiedzanie miejsca

# Congress Center Hamburg (CCH)

## Congress Center Hamburg (CCH)

### Główne elementy:

- Kilka sal wykładowych na prelekcje
- Dodatkowe sale dla wydarzeń społecznościowych
- Strefy Assembly - przestrzenie społeczności
- Bary, strefy relaksu, itp.

# Mapka

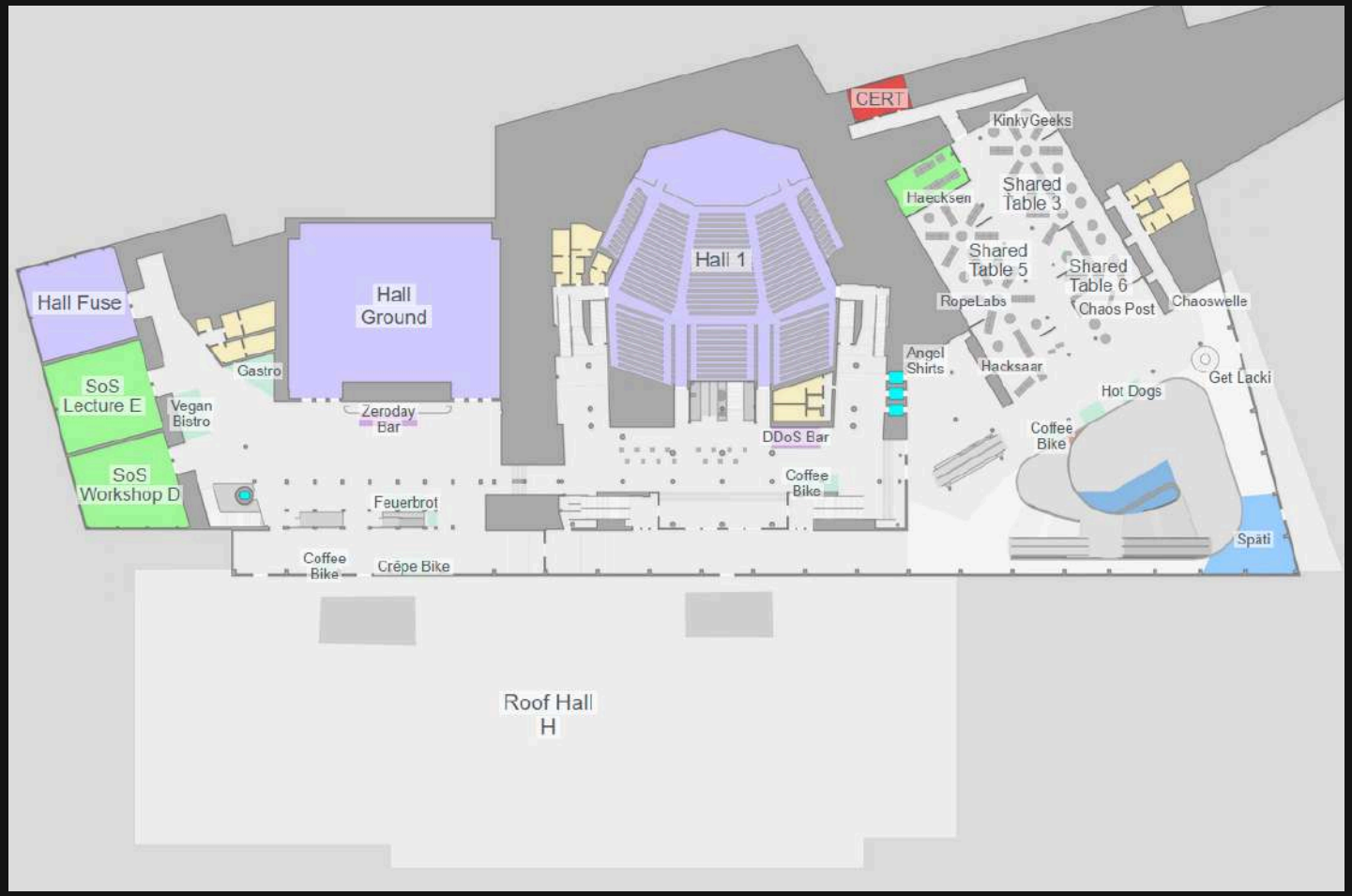



Gate A
Gate B
Gate C
Gate D
Gate F
Gate H2
(W)ICMP, Bits'n'Bugs & ZAM
K4CG
Chaos Mauldasch Workshop
Cloakroom / Lost & Found
Special Purpose Welcome Desk
KalkSpace
Chaos-West
Shared Table 7
Segmentation Vault
WupLUG Linux User Group Wuppertal
CTF
Shared Table 9
C3MA and friends
CyberPetrol
Chaos Furs
Shared Table 12
Gastro
Shared Table 2
mhackeroni
Moormaker
SFT
Shared Table 13
Cashdesk / Registration
Bits&Bäume Living Room
ChaosZone
WüSpace
xil
CDC Triangle
iroh
Shared Table 22
Cebula Cluster
Bits&Bäume Hackcenter
OpenStreetMap
CDC Circle
work in progress
Art & Play: Bus Stage
SoS Stage H
c-base
milliways
Shared Table 18
Faxgeräteclub

# Mapka

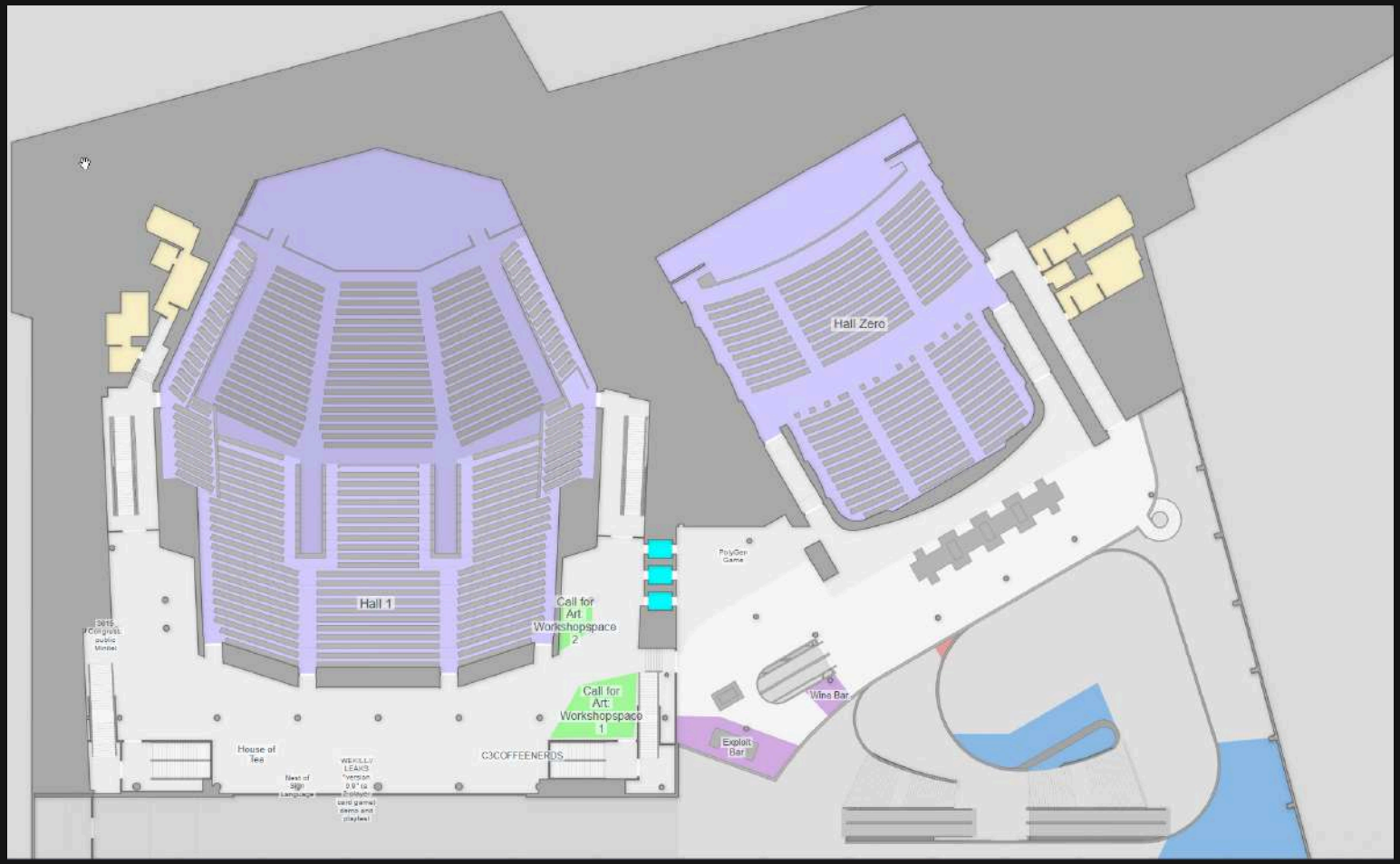

Sendezentrum
Stage (Hall X 07)
Heaven Quiet Room
Heaven
Port39 // CCC Stralsund
Digitalcourage
Sendezentrum
Komonin
Jugend hackt
4lthangrund
Wohnzimmerbühne
The Spectrum
PoC
Lockpicking Area
Kidspace C
Kidspace
Kidspace B
Fashion Operation Center / March
Internetmanufaktur
chaos.jetzt
xHain
Infodesk
Hall 8
Speakers' Desk
SoS Hall 6
Free Knowledge Habitat

# Mapka


CERT
KinkyGeeks
Haecksen
Shared Table 3
Shared Table 5
Shared Table 6
Hall 1
Hall Fuse
Hall Ground
RopeLabs
Chaos Post
Chaoswelle
Angel Shirts
Hacksaar
Get Lacki
Hot Dogs
Coffee Bike
Gastro
SoS Lecture E
Vegan Bistro
Zeroday Bar
DDoS Bar
Coffee Bike
SoS Workshop D
Feuerbrot
Coffee Bike
Crêpe Bike
Späti
Roof Hall H

# Mapka



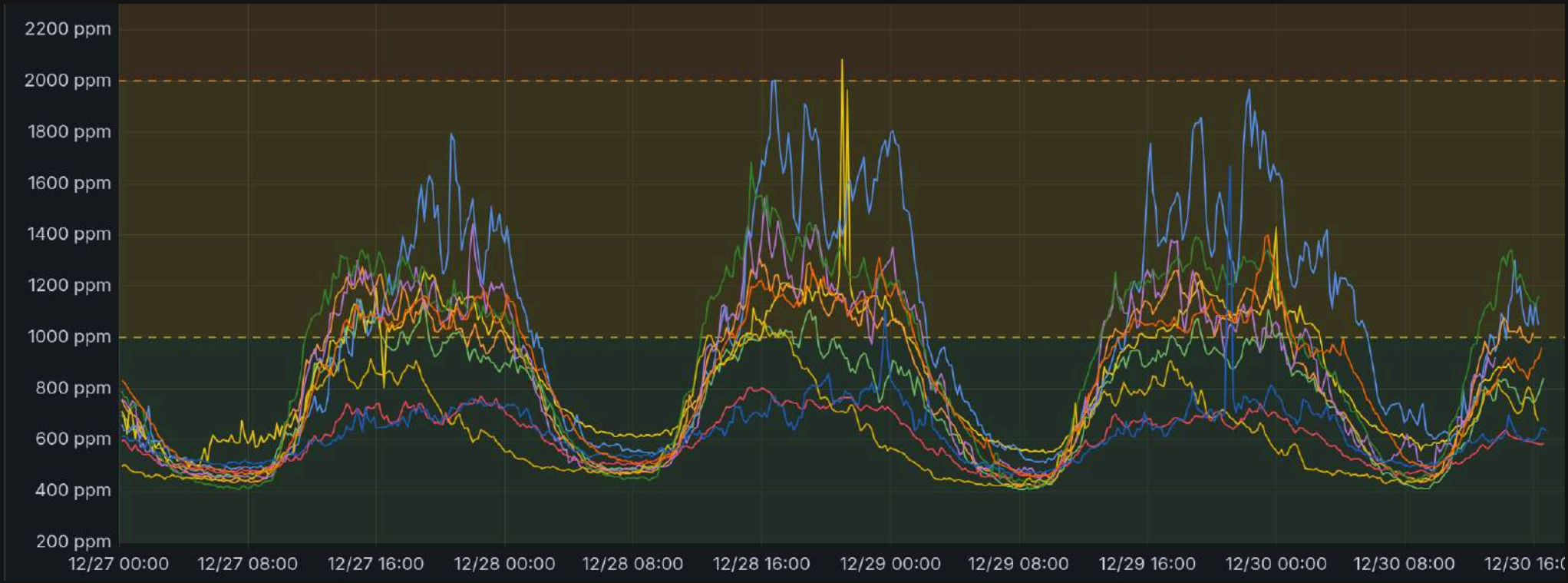

Hall Zero
Hall 1
Call for Art Workshopspace 2
Call for Art Workshopspace 1
Wine Bar
Exploit Bar
House of Tea
C3COFFEENEROS

# O infrastrukturze



- własne sieci GSM, LTE (słabo działało...) i DECT
- dobrze działające WiFi dające dostęp do kilku dodatkowych rzeczy
  - audio.c3lingo.org - audio z prelekcji i tłumaczenia na żywo
  - low latency stream
  - szybszy dostęp do media.ccc.de
  - kilka społecznościowych projektów gate'owało dostęp byciem w sieci C3
  - C3Nav - lokalizacja po beaconach WiFi (nie wymagała połączenia się z siecią)

- Dane środowiskowe z czujników rozsianych po całym CCH, np. CO2:



- a co się stało 2 dnia ok. 21-22? (hint: żółty to Food Hacking Base)

## eCO2 = H2 + etanol

20:30
-
22:30
Day 2

# Whiskey Tasting

Food Hacking Base  English

ASSEMBLY-EVENT  TASTING  WHISKEY

We provide a number of interesting whiskeys to show you the wide range of things the world calls whiskey, and give you some insight in what makes it get its characteristic tastes. You are invited to bring your own bottle to this event to make it even more insane. If you let us know in advance, we'll add them to this list.

- Wolontariusze utrzymujący sporą część kongresu
- Różne role: od rejestracji, przez pomoc techniczną, po pracę w barach :)
- W zamian za wyrobienie określonej liczby godzin dostaje się:
  - dostęp do Heaven
  - jedzenie i picie w trakcie kongresu
  - specjalną koszulkę
  - voucher na wcześniejszą turę biletów na kolejny kongres

39C3

# Moje doświadczenia z Assembly

## Czym są Assembly?

## Czym są Assembly?

- Przestrzenie organizowane przez społeczność
- Miejsca spotkań z ludźmi o podobnych zainteresowaniach
- Pokazy i projekty „hands-on”
- Centra społecznościowe podczas wydarzenia

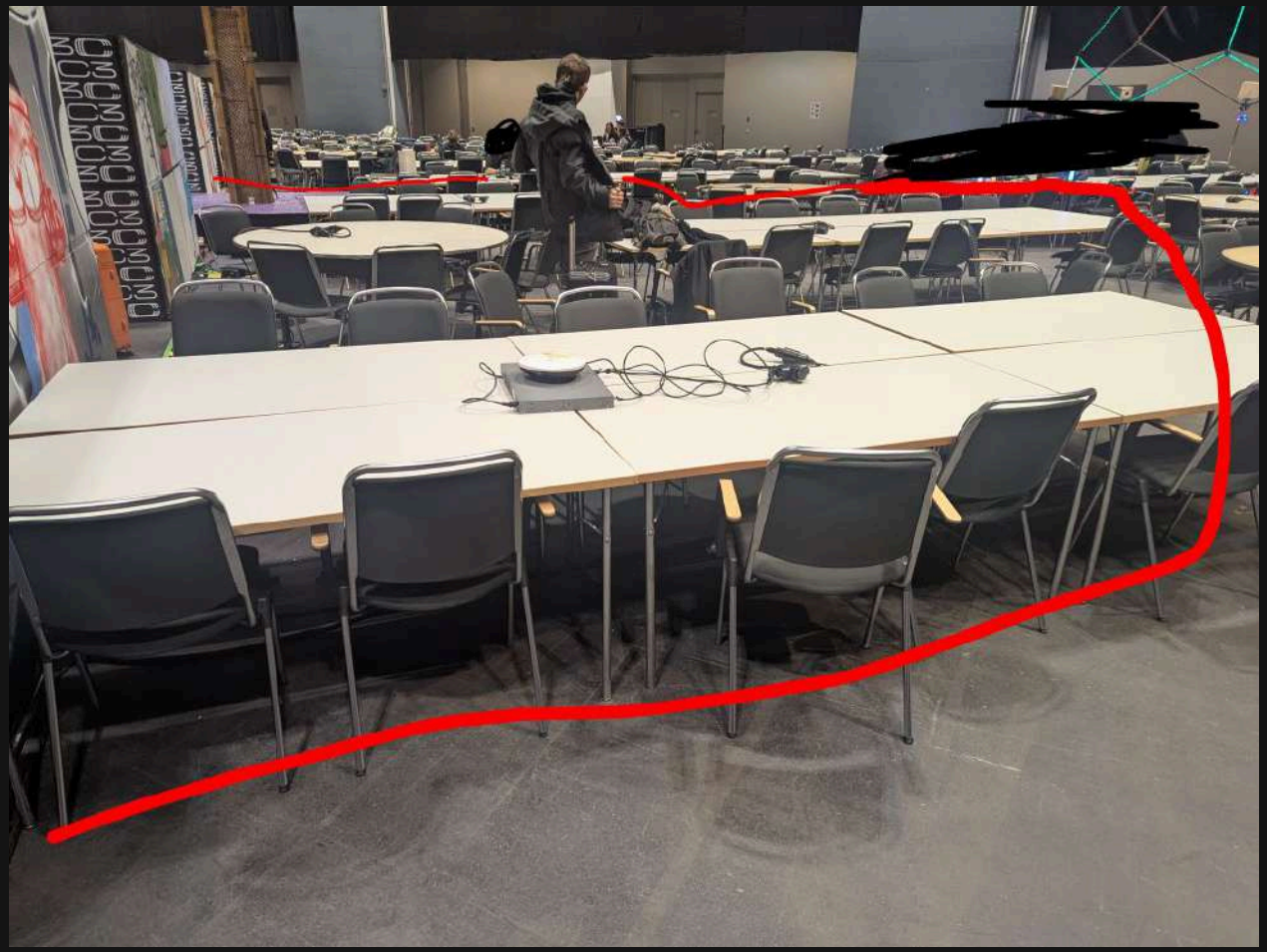
# Cebula Cluster



- Polskie Hackerspace'y

# Cebula Cluster





# Cebula Cluster

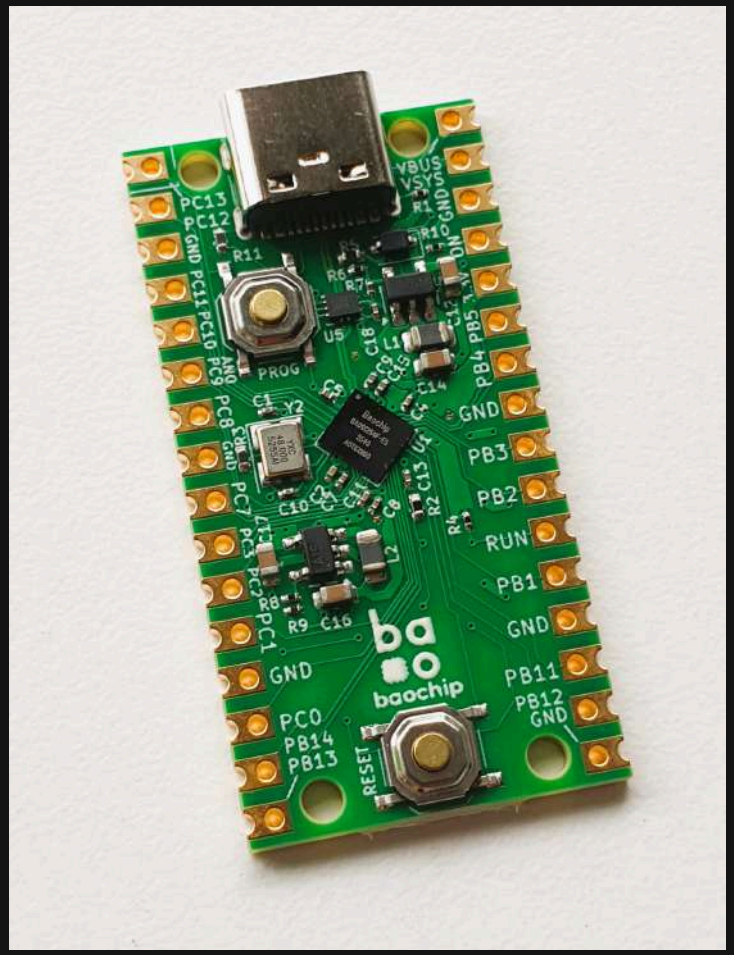


# Critical Decentralization Cluster

- Głównie krypto, w obu znaczeniach :)
- W tym trochę hardware'u
- Badge!

- Głównie krypto, w obu znaczeniach :)
- W tym trochę hardware'u
- Badge!

- Trochę prelegentów od HW i kryptografii
- Rzecz której najbardziej żałuję: nie udało się dostać devboardu Baochip zanim się skończyły :(



39C3

# Kilka Prelekcji

# Demistyfikacja fuzzerów



- trochę o tym jak ogólnie fuzzery działają, jakie są ich ograniczenia, itp.
- bardziej filozoficzno-teoretyczna
- polecam obejrzeć jak ktoś się interesuje fuzzowaniem :)

https://media.ccc.de/v/39c3-demystifying-fuzzer-behaviour

## Atak na TEE: niestety tylko Beanpod

- Beanpod po prostu ma znaczące problemy z bezpieczeństwem
- Nawet Xiaomi od niego odchodzi

## Atak na TEE: niestety tylko Beanpod

- Beanpod po prostu ma znaczące problemy z bezpieczeństwem
- Nawet Xiaomi od niego odchodzi

## Ogólne:

- W środowiskach mikrojądra szukaj wysoko uprzywilejowanych procesów użytkownika
- Wysokie uprawnienia w procesie TEE = potencjał na poważne ataki mimo mikrojądra

## Atak na TEE: niestety tylko Beanpod

- Beanpod po prostu ma znaczące problemy z bezpieczeństwem
- Nawet Xiaomi od niego odchodzi

## Ogólne:

- W środowiskach mikrojądra szukaj wysoko uprzywilejowanych procesów użytkownika
- Wysokie uprawnienia w procesie TEE = potencjał na poważne ataki mimo mikrojądra

## TEEGris:

- Znacznie lepsze mechanizmy mitygacji ataków
- Podobne ataki byłyby trudniejsze

https://media.ccc.de/v/39c3-not-to-be-trusted-a-fiasco-in--android-tees

## Podatności formatów obrazów:

- Formaty z kodami operacji (filtry, funkcje) często mają błędy
- DNG (Digital Negative) posiada sekcję opcodes

## Podatności formatów obrazów:

- Formaty z kodami operacji (filtry, funkcje) często mają błędy
- DNG (Digital Negative) posiada sekcję opcodes

## Podatności iOS:

- Przepełnienie przy mnożeniu szerokość × wysokość
- CVE: szerokość × liczba komponentów nie była sprawdzana, tylko sama szerokość

**Podatności formatów obrazów:**

- Formaty z kodami operacji (filtry, funkcje) często mają błędy
- DNG (Digital Negative) posiada sekcję opcodes

**Podatności iOS:**

- Przepełnienie przy mnożeniu szerokość × wysokość
- CVE: szerokość × liczba komponentów nie była sprawdzana, tylko sama szerokość

**Wektor ataku WhatsApp:**

- Poprzez generowanie podglądu URL
- Powinien być generowany u nadawcy, ale API klienta webowego pozwalało na wyzwalanie go na innych urządzeniach

- błędy w userspace, w szczególności w bibliotekach do przetwarzania obrazów
  - np. **libimagecodec.quram.so** w Samsungu
  - szczególnie formaty z jakimś embedowanym programowaniem (np. do filtrów)
- niestety to była tylko analiza patchy i szukanie błędów w diffach + eksperymentowanie
  - więc błędy znane i metodologia mało dla nas użyteczna

https://media.ccc.de/v/39c3-dngerouslink-a-deep-dive-into-whatsapp-0-click-exploits-on-ios-and-samsung-devices

# Build a Fake Phone, Find Real Bugs



- w końcu Qualcomm zajmuje się emulacją swoich urządzeń :)
  - na razie: GPU do Cuttlefisha

# Build a Fake Phone, Find Real Bugs



- w końcu Qualcomm zajmuje się emulacją swoich urządzeń :)
  - na razie: GPU do Cuttlefisha
- Ogólnie status pracy:
  - Dodanie wsparcia GPU do Cuttlefish
  - Ulepszenia współpracy libAFL z QEMU
  - Kompatybilność KCOV z libAFL
  - wizualizacja dt: https://github.com/rmalmain/fdtviz

- w końcu Qualcomm zajmuje się emulacją swoich urządzeń :)
  - na razie: GPU do Cuttlefisha
- Ogólnie status pracy:
  - Dodanie wsparcia GPU do Cuttlefish
  - Ulepszenia współpracy libAFL z QEMU
  - Kompatybilność KCOV z libAFL
  - wizualizacja dt: https://github.com/rmalmain/fdtviz
- kontakt do autora na https://github.com/rmalmain

https://media.ccc.de/v/39c3-build-a-fake-phone-find-real-bugs-qualcomm-gpu-emulation-and-fuzzing-with-libafl-qemu

**talk o atakach na PSP od AMD. Ciekawe dla nas:**

- fault injection przez przejęcie kontroli nad regulatorem napięcia
  - Protokół SVI - rozszerzone I2C
  - Odniesienie: „One Glitch to Rule Them All”

**talk o atakach na PSP od AMD. Ciekawe dla nas:**

- fault injection przez przejęcie kontroli nad regulatorem napięcia
  - Protokół SVI - rozszerzone I2C
  - Odniesienie: „One Glitch to Rule Them All”
- błędy w bootloaderach potrafią być ciekawe
  - np. tutaj niektóre etapy bootloadera mogą pisać do slotów do których nie powinny mieć dostępu

## talk o atakach na PSP od AMD. Ciekawe dla nas:

- fault injection przez przejęcie kontroli nad regulatorem napięcia
  - Protokół SVI - rozszerzone I2C
  - Odniesienie: „One Glitch to Rule Them All"
- błędy w bootloaderach potrafią być ciekawe
  - np. tutaj niektóre etapy bootloadera mogą pisać do slotów do których nie powinny mieć dostępu
- współczesne mcu robią za dobre modchipy

## talk o atakach na PSP od AMD. Ciekawe dla nas:

- fault injection przez przejęcie kontroli nad regulatorem napi
  - Protokół SVI - rozszerzone I2C
  - Odniesienie: „One Glitch to Rule Them All”
- błędy w bootloaderach potrafią być ciekawe
  - np. tutaj niektóre etapy bootloadera mogą pisać do slotów do których nie powinny mieć dostępu
- współczesne mcu robią za dobre modchipy

https://media.ccc.de/v/39c3-opening-pamdora-s-box-and-
-unleashing-a-thousand-paths-on-the-journey-to-play-beatsaber-
-custom-songs

Spora podatność w słuchawkach bluetooth

## Spora podatność w słuchawkach bluetooth

- TL;DR wystawiony protokół RACE
  - zależnie od wersji, odczyt/zapis pamięci flash **i nawet RAM**
  - Aktualizacje FOTA
  - konfiguracje, np. ID i klucze połączonych urządzeń
  - **Brak uwierzytelniania. Nawet parowania.**

## Spora podatność w słuchawkach bluetooth

- TL;DR wystawiony protokół RACE
  - zależnie od wersji, odczyt/zapis pamięci flash **i nawet RAM**
  - Aktualizacje FOTA
  - konfiguracje, np. ID i klucze połączonych urządzeń
  - **Brak uwierzytelniania. Nawet parowania.**

## Skutki:

- Możliwość odczytu/zapisu RAM dowolnych słuchawek w pobliżu
- Całkowite przejęcie słuchawek
- można się podszyć pod słuchawki i manipulować telefonem
  - np. używać asystenta...

- Znalezione słuchawki (część):
  - Sony (część naprawiona)
  - Bose
  - JBL
  - Marshall (naprawione)
  - Jabra (naprawione)
- narzędzie do sprawdzenia czy ma się podatne słuchawki:
  - https://github.com/auracast-research/race-toolkit

https://media.ccc.de/v/39c3-bluetooth-headphone-jacking-a--key-to-your-phone

# Łamanie chińskich aplikacji mobilnych

Problem: ponad 50% najpopularniejszych chińskich aplikacji nie używało TLS

# Łamanie chińskich aplikacji mobilnych



## Problem: ponad 50% najpopularniejszych chińskich aplikacji nie używało TLS

- Szczególnie problematyczne: chińskie aplikacje klawiatury
  - Naciśnięcia klawiszy wysyłane bez szyfrowania
  - to, że klawiatura = keylogger znormalizowane, ale to nawet nie były dobre keyloggery!

# Łamanie chińskich aplikacji mobilnych



## Problem: ponad 50% najpopularniejszych chińskich aplikacji nie używało TLS

- Szczególnie problematyczne: chińskie aplikacje klawiatury
  - Naciśnięcia klawiszy wysyłane bez szyfrowania
  - to, że klawiatura = keylogger znormalizowane, ale to nawet nie były dobre keyloggery!
- 8/9 zbadanych własnych szyfrów udało się złamać
  - tj. odszyfrować zawartość
  - jedyny który przeżył to MMTLS od WeChat
  - większość zgłoszeń zakończyła się naprawą!

# Inne ciekawe prelekcje

## How to render cloud FPGAs useless

- celowe starzenie czyiś FPGA i odrobinę o tym jak działają VPSy F1 w AWS

# Inne ciekawe prelekcje



## How to render cloud FPGAs useless

- celowe starzenie czyiś FPGA i odrobinę o tym jak działają VPSy F1 w AWS

## Xous: A Pure-Rust Rethink of the Embedded Operating System

- poza samym ciekawym projektem, trochę o problemach z krzemem OSS

# Inne ciekawe prelekcje



## How to render cloud FPGAs useless

- celowe starzenie czyiś FPGA i odrobinę o tym jak działają VPSy F1 w AWS

## Xous: A Pure-Rust Rethink of the Embedded Operating System

- poza samym ciekawym projektem, trochę o problemach z krzemem OSS

## APT Down and the mystery of the burning data centers

- ciekawa sprawa z atakiem na APT i teorie spiskowe o tym pożarze w rządowej chmurze Korei :)

# Inne ciekawe prelekcje



## How to render cloud FPGAs useless

- celowe starzenie czyiś FPGA i odrobinę o tym jak działają VPSy F1 w AWS

## Xous: A Pure-Rust Rethink of the Embedded Operating System

- poza samym ciekawym projektem, trochę o problemach z krzemem OSS

## APT Down and the mystery of the burning data centers

- ciekawa sprawa z atakiem na APT i teorie spiskowe o tym pożarze w rządowej chmurze Korei :)

## The Heartbreak Machine: Nazis in the Echo Chamber

- o problemach z alt-techowym portalu randkowym tylko dla białych z demo w postaci usuwania go z internetu live :)

# Inne ciekawe prelekcje

## All my Deutschlandtickets gone: Fraud at an industrial scale

- ciekawe śledztwo w sprawie dziwnych biletów

# Inne ciekawe prelekcje



## All my Deutschlandtickets gone: Fraud at an industrial scale

- ciekawe śledztwo w sprawie dziwnych biletów

## CSS Clicker Training: Making games in a „styling" language

- o tym dlaczego CSS **jest** językiem programowania, szczególnie gdy połączy się go z HTMLem (ale osobno też :)

## Escaping Containment: A Security Analysis of FreeBSD Jails

- mocno technicznie o szukaniu i znajdowaniu podatności w jailach

# Inne ciekawe prelekcje



## All my Deutschlandtickets gone: Fraud at an industrial scale

- ciekawe śledztwo w sprawie dziwnych biletów

## CSS Clicker Training: Making games in a „styling" language

- o tym dlaczego CSS **jest** językiem programowania, szczególnie gdy połączy się go z HTMLem (ale osobno też :)

## Escaping Containment: A Security Analysis of FreeBSD Jails

- mocno technicznie o szukaniu i znajdowaniu podatności w jailach

39C3

# Główne wnioski

# Lekcje praktyczne

1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć

# Lekcje praktyczne

# Lekcje praktyczne



1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć
2. **Niemiecka prelekcja to nie bariera**
   - Tłumaczenia na żywo na angielski są okej!
   - Czasami nawet są na Polski

# Lekcje praktyczne

# Lekcje praktyczne



1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć
2. **Niemiecka prelekcja to nie bariera**
   - Tłumaczenia na żywo na angielski są okej!
   - Czasami nawet są na Polski
3. **Jakiś badge się przydaje**
   - Warto albo z czymś przyjechać albo wcześnie sobie załatwić
   - Są dostępne na różnych assembly albo do kupienia albo w formie warsztatów z lutowania :)

# Lekcje praktyczne

# Lekcje praktyczne



1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć
2. **Niemiecka prelekcja to nie bariera**
   - Tłumaczenia na żywo na angielski są okej!
   - Czasami nawet są na Polski
3. **Jakiś badge się przydaje**
   - Warto albo z czymś przyjechać albo wcześnie sobie załatwić
   - Są dostępne na różnych assembly albo do kupienia albo w formie warsztatów z lutowania :)
4. **Sporo okazji do zbierania naklejek**
   - Brać póki dają :)

# Lekcje praktyczne

# Lekcje praktyczne



1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć
2. **Niemiecka prelekcja to nie bariera**
   - Tłumaczenia na żywo na angielski są okej!
   - Czasami nawet są na Polski
3. **Jakiś badge się przydaje**
   - Warto albo z czymś przyjechać albo wcześnie sobie załatwić
   - Są dostępne na różnych assembly albo do kupienia albo w formie warsztatów z lutowania :)
4. **Sporo okazji do zbierania naklejek**
   - Brać póki dają :)

5. **Warto wkręcić się w jakąś powiązaną społeczność**
   - Dostęp do biletów wcześniej
   - Miejsce na assembly by zostawić rzeczy i gdzieś przysiąść

# Lekcje praktyczne



1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć
2. **Niemiecka prelekcja to nie bariera**
   - Tłumaczenia na żywo na angielski są okej!
   - Czasami nawet są na Polski
3. **Jakiś badge się przydaje**
   - Warto albo z czymś przyjechać albo wcześnie sobie załatwić
   - Są dostępne na różnych assembly albo do kupienia albo w formie warsztatów z lutowania :)
4. **Sporo okazji do zbierania naklejek**
   - Brać póki dają :)

5. **Warto wkręcić się w jakąś powiązaną społeczność**
   - Dostęp do biletów wcześniej
   - Miejsce na assembly by zostawić rzeczy i gdzieś przysiąść
6. **Warto brać hardware**
   - Czy to własne projekty, czy jak się ma coś potencjalnie przydatnego

# Lekcje praktyczne



1. **Większe skupienie na Assembly**
   - Najlepszy sposób na poznanie ludzi i naukę praktyczną
   - Bardziej interaktywne niż samo uczestnictwo w prelekcjach
   - Są streamy low-latency jak coś chce się obejrzeć
2. **Niemiecka prelekcja to nie bariera**
   - Tłumaczenia na żywo na angielski są okej!
   - Czasami nawet są na Polski
3. **Jakiś badge się przydaje**
   - Warto albo z czymś przyjechać albo wcześnie sobie załatwić
   - Są dostępne na różnych assembly albo do kupienia albo w formie warsztatów z lutowania :)
4. **Sporo okazji do zbierania naklejek**
   - Brać póki dają :)

5. **Warto wkręcić się w jakąś powiązaną społeczność**
   - Dostęp do biletów wcześniej
   - Miejsce na assembly by zostawić rzeczy i gdzieś przysiąść
6. **Warto brać hardware**
   - Czy to własne projekty, czy jak się ma coś potencjalnie przydatnego
7. **Najtaniej jest kupować indywidualne/krótkookresowe bilety**
   - Większość czasu spędzi się na CCH, bilet okresowy - nawet tygodniowy - wychodzi drożej niż indywidualne przejazdy/powroty gdzieś blisko
8. **Warto wziąć trochę gotówki**
   - poza jedzeniem praktycznie cała sprzedaż na terenie CCH była cash-only

39C3

# Nadchodzące wydarzenia

## 40C3

- Hamburg, Niemcy
- 27-30 grudnia 2026
- To samo miejsce (CCH)

## 40C3

- Hamburg, Niemcy
- 27-30 grudnia 2026
- To samo miejsce (CCH)

## FOSDEM

- Bruksela, Belgia
- 31 stycznia - 1 lutego 2026
- Europejskie spotkanie twórców wolnego i otwartego oprogramowania
- Sporo społeczności z okolic CCC tam się też pojawia

39C3

# Pytania?