



## Hacking into AURACAST

- Auracast: Neuer Bluetooth Standard für Sound-Broadcast, z.B. direktes streamen auf Hörgeräte (Bahnhof, Stadion, etc.)
- Projekt baut auf bestehender Analyse/Angriff auf:
  - Fehlende Keyderivation (KDF) und zu kurze Schlüssel:
    - CCC-Vortrag: <https://media.ccc.de/v/38c3-auracast-breaking-broadcast-le-audio-before-it-hits-the-shelves>
    - Github Projekt mit bestehenden Angriffstools: <https://github.com/auracast-research>



## Projekthalte

*- Abhängig von Teamgröße und Vorwissen -*

- Angriffsverifizierung: Nachbauen des Setups
- Analyse: Weitere Angriffe möglich ? (Standard und auf konkreten Geräten)
  - Praktisches Testen auf Geräten
- Portierung des Angriffes auf Flipper Zero
- Praktisches Übernehmen von Streams
  - Mittels starkem Sender (USRP / HackRF...)