

# ITS Task 2

Julian Bertol

October 24, 2024

## 1 Mit dem Server verbinden

- 1.1 Verbinden Sie sich mit Ihrem Smartphone oder eigenem PC mit dem WLAN
  - Smartphone mit freien Wlan verbunden
- 1.2 Starten Sie die VoIP-Software (App). Als Benutzernamen können Sie die Zahlen 01-30 benutzen (stets zweistellig!). Das Passwort lautet 123. Sprechen Sie sich ab, wer welchen Benutzernamen bekommt.
  - Benutzername: 12
- 1.3 Testen Sie die Verbindung, indem Sie die Nummer 1234 wählen. Was hören Sie?
  - Hello World
- 1.4 Wählen Sie die Nummer 999. Was hören Sie jetzt?
  - mich selber

## 2 Das WLAN abhören (Schritt 1)

2.1 Versetzen Sie Ihre Netzwerkkarte in den Monitor-Modus. Nutzen Sie airmon-ng. Geben Sie sich die manpages und die Hilfeseite von airmon-ng aus, um die Bedienung in Erfahrung zu bringen:

- "airmon-ng start [Wlan-Interface]"

2.2 Nutzen Sie den Befehl ip a s oder ifconfig -a, um sich die Namen Ihrer Netzwerkkarten anzeigen zu lassen. Wie lautet der Name Ihrer WLAN-Karte? Wie haben Sie dies herausgefunden?

- wlx18d6c717f736

```
root@ubuntu2204:/home/student
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
root@ubuntu2204:/home/student# airmon-ng start wlx18d6c717f736
Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      505 avahi-daemon
      509 NetworkManager
      525 wpa_supplicant
      538 avahi-daemon

      PHY     Interface      Driver      Chipset
      phy0    wlx18d6c717f736 8188eu        TP-Link TL-WN722N v2/v3 [Realtek RTL8188
EUS]
                           (monitor mode enabled)

root@ubuntu2204:/home/student# ifconfig -a
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

2.3 Starten Sie airmon-ng mit der korrekten Netzwerkkarte, um den Monitor-Modus zu aktivieren. Zeigen Sie die Ausgabe. Dokumentieren Sie: Was führten Sie aus? Welche Parameter benutzten Sie? Mussten Sie vorher etwas machen? Wenn ja: Was?

- airmon-ng check kill
- airmon-ng start wlx18d6c717f736
- man muss zuerst störende Prozesse beenden.

2.4 Es ist nicht möglich mit einer WLAN-Karte alle Kanäle gleichzeitig aufzuzeichnen. Benutzen Sie airodump, um herauszufinden, auf welchem Kanal das Netzwerk ausgestrahlt wird. Auf welchem Kanal ist das WLAN? Was können Sie aus der Ausgabe von airodump sonst noch herausfinden? Beenden Sie airodump mit q oder STRG+C.

- "airodump-ng [interface]"
- Channel = 12
- Weitere Infos:
  - bssid
  - Sicherheit
  - Beacons

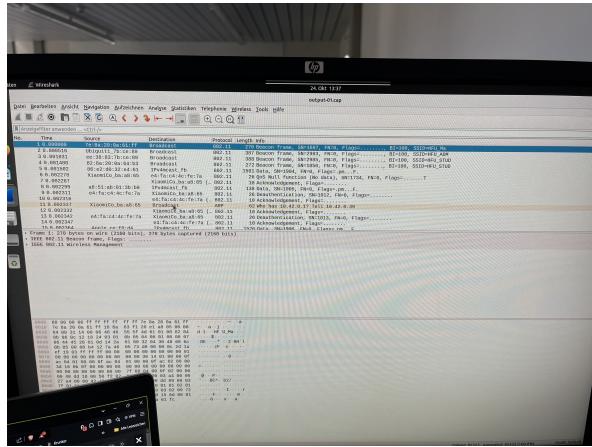
### 3 Das WLAN abhören (Schritt 2)

- 3.1 Nun muss die WLAN-Karte auf den richtigen Kanal eingestellt werden. Je nach WLAN-Karte kann es notwendig sein, den Monitor-Mode zu beenden und mit der Kanalnummer erneut zu starten. Versuchen Sie zuerst direkt mit b) weiterzumachen. a. Benutzen Sie airmon-ng stop [WLAN-Adaptername], um den Monitormode zu beenden. b. Starten Sie den Monitormode mit dem richtigen Kanal erneut.
  - Ich musste den Monitor-Mode zuerst beenden dann nochmal mit dem channel 12 starten
    - airmon-ng stop [interface]
    - airmon-ng start [interface] [channel]
- 3.2 Nun starten Sie wieder airodump-ng. Diesmal müssen Sie aber den Parameter –write und –channel benutzen, um den Kanal einzustellen und alle empfangenen Pakete in eine Datei zu schreiben. Nutzen Sie die Hilfeseite und die man-pages.
  - airodump-ng –channel [channel] –write [dateiname] [interface]

#### 4 Den Anruf aus den aufgezeichneten Daten extrahieren.

4.1 Zeigen Sie ein Screenshot von Wireshark. Was zeigt Ihnen Wireshark an?

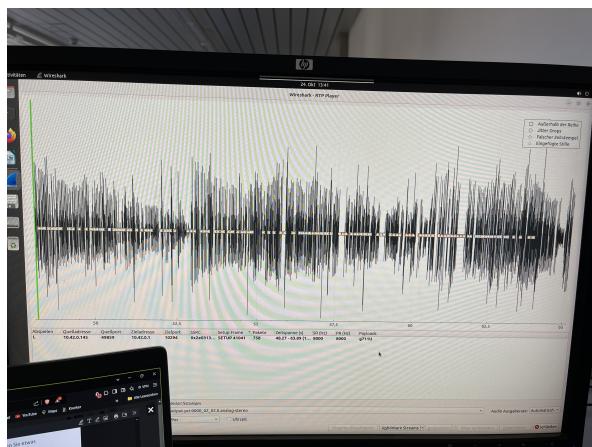
- Wireshark zeigt den traffic des Wlans an



4.2 Suchen Sie eine Funktion, um Telefonate anzuzeigen und abzuspielen. Sehen Sie vielleicht mehr als Ihren eigenen Anruf? Weswegen?

- unter Telefonie, RTP, RTP Streams sieht man alles anrufe

#### 4.3 Zeigen Sie ein Screenshot der Wellenform des Anrufs.



## **5 Wie könnten Sie sich schützen?**

### **5.1 Welches Schutzziel wurde verletzt und welche Bedrohung ist geschehen?**

- Das Schutzziel der Vertraulichkeit wurde verletzt. Der Traffic wurde über ein ungesichertes Wlan abgehört.

### **5.2 Was könnte man machen, um sich vor einem solchen Angriff zu schützen? Gibt es mehr als eine Möglichkeit?**

- Wlan Sicherheit erhöhen (WPA2)
- Telefonate verschlüsseln