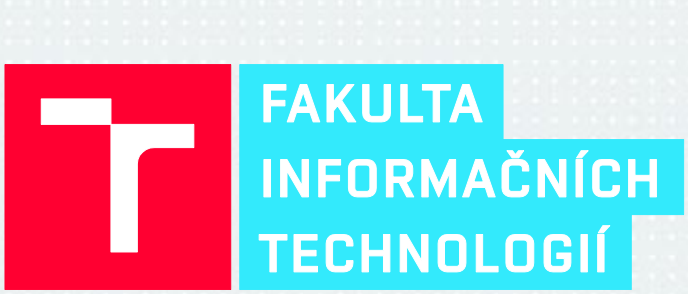
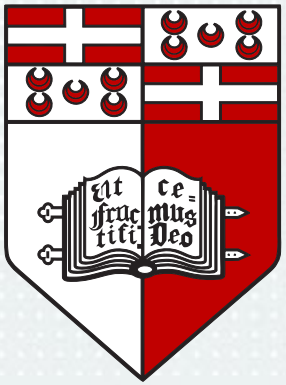




Automation of MitM Attack on WiFi Networks

Author: Martin Vondráček
Supervisor: Ing. Jan Pluskal
Foreign supervisor: Dr Johann A. Briffa

Brno University of Technology

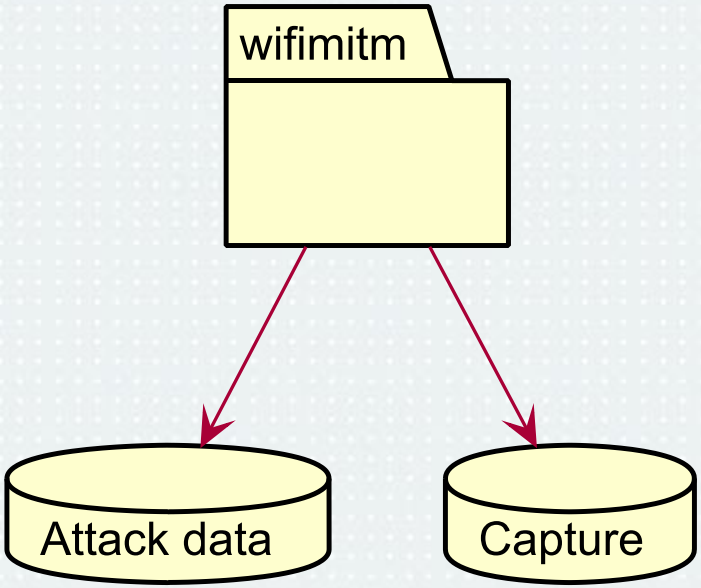
University of Malta

Available Tools for Specific Phases of the MitM Attack on Wireless Networks

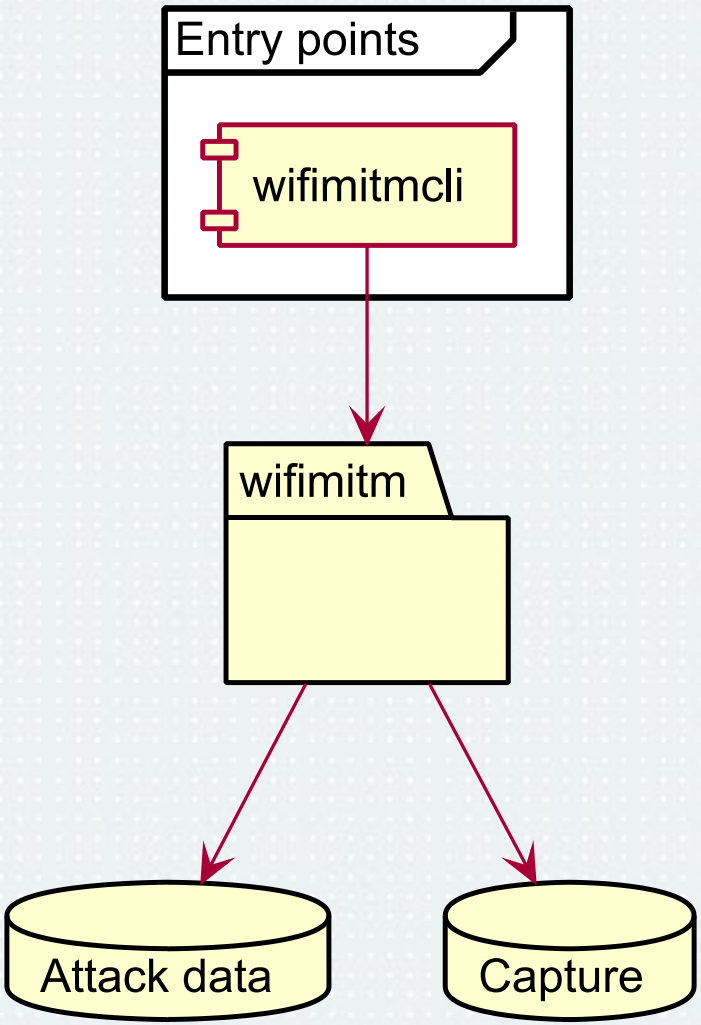
- Accessing wireless network
  - **airmon-ng**, **airodump-ng**, **aircrack-ng,** **aireplay-ng**, wifite, **upc_keys**, **wifiphisher**, Reaver Open Source, **wpaclean**, **netctl**
- Tampering network topology
  - **Framework for Man-In-The-Middle attacks**, Scapy, dsniff, arpspoof, Yersinia
- Capturing network traffic
  - **Dumpcap**

Wi-Fi Machine-in-the-Middle

- Python package `wifimitm`
- Attack data for repetitive attacks
- Captured traffic

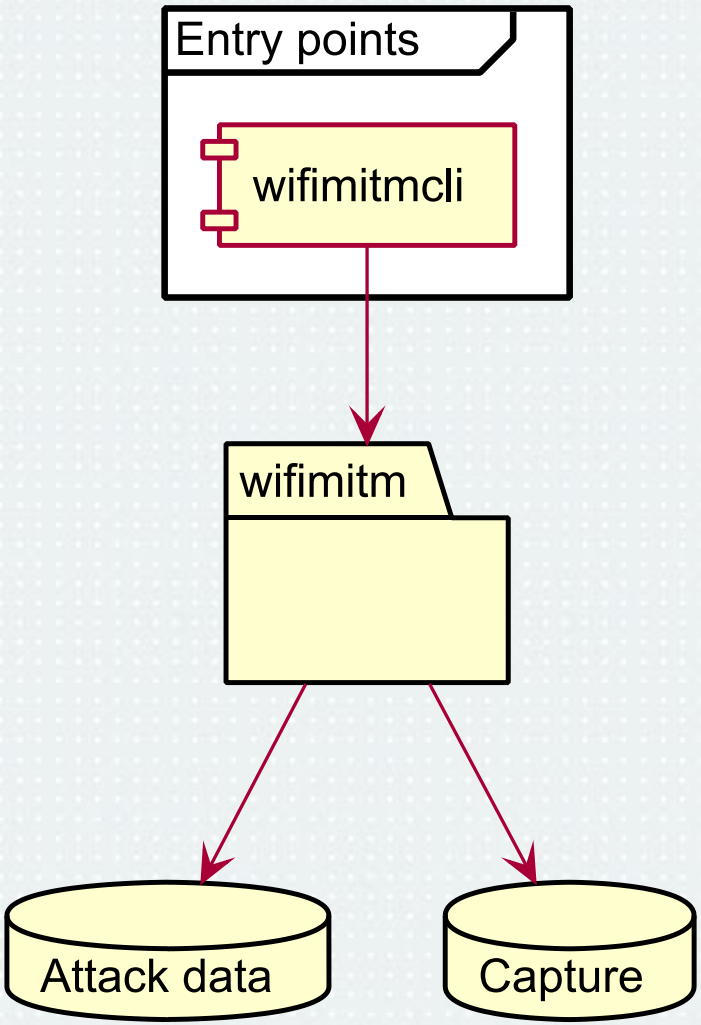


Wi-Fi Machine-in-the-Middle



- Python package `wifimitm`
- Attack data for repetitive attacks
- Captured traffic
- CLI tool `wifimitmcli`

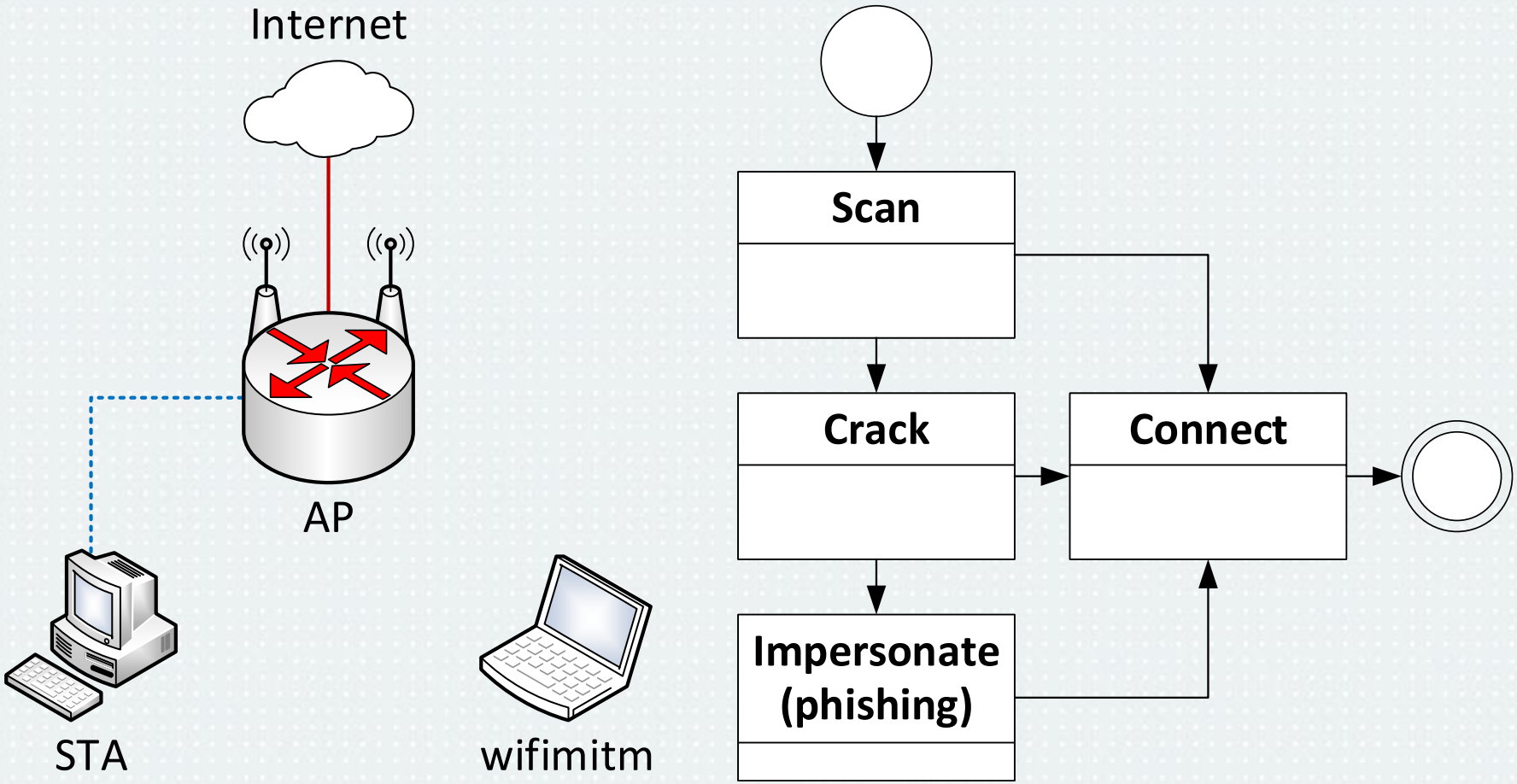
Wi-Fi Machine-in-the-Middle



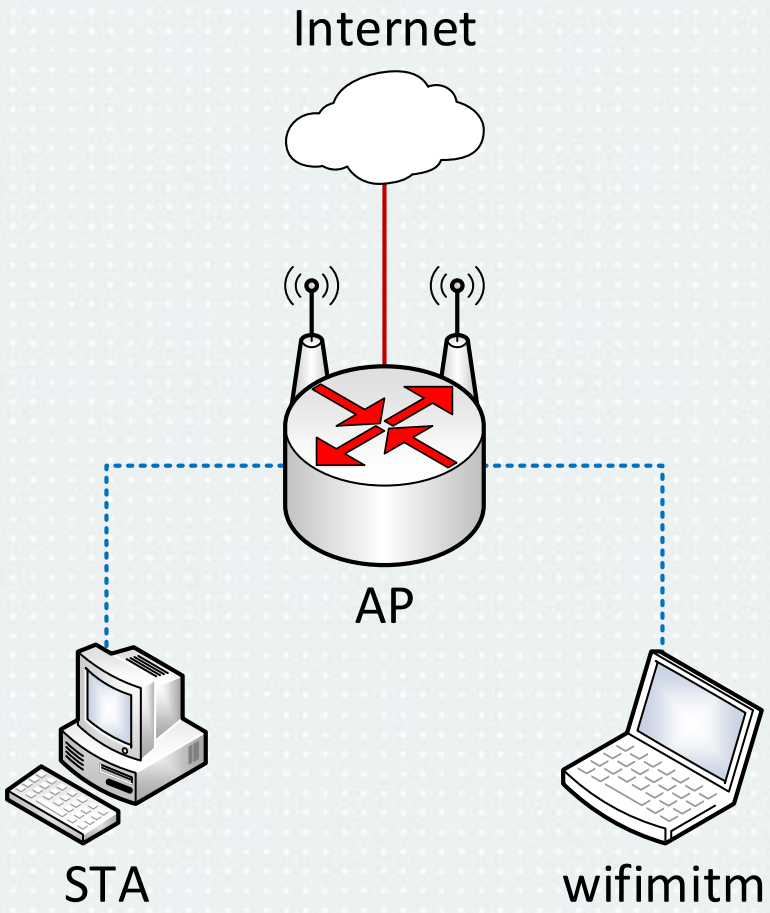
- Python package `wifimitm`
- Attack data for repetitive attacks
- Captured traffic
- CLI tool `wifimitmcli`

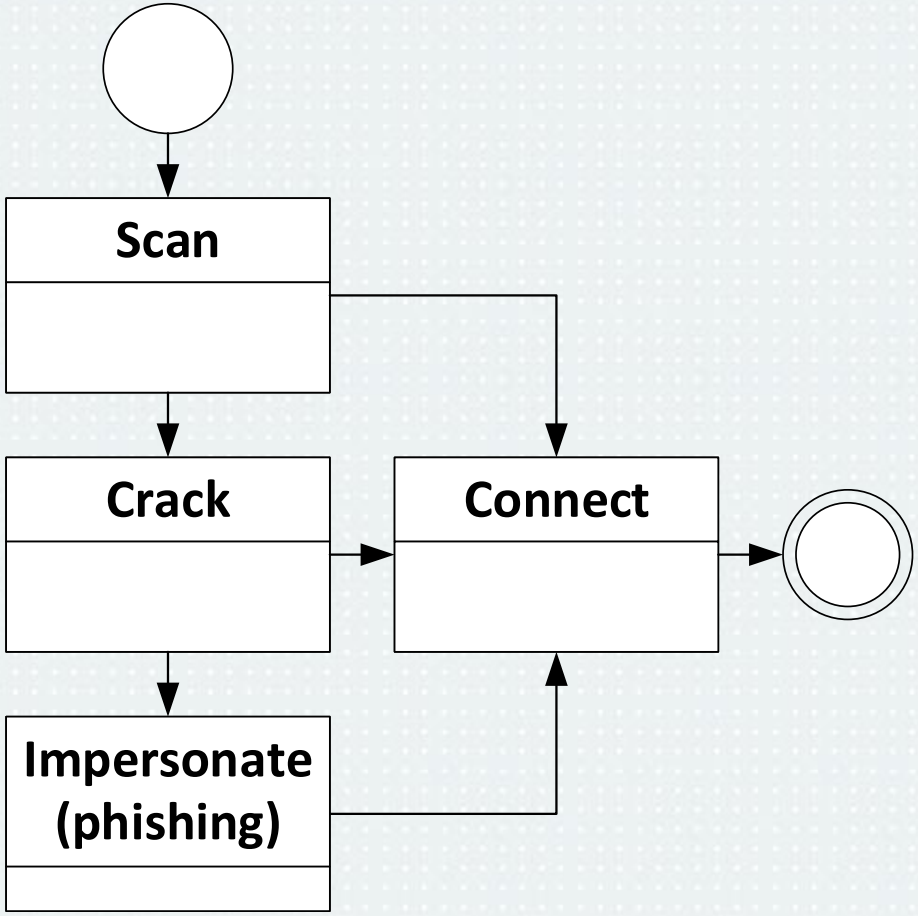
- Installation scripts
- Requirements check
- Python package setup
- Documentation, man page

Accessing wireless network

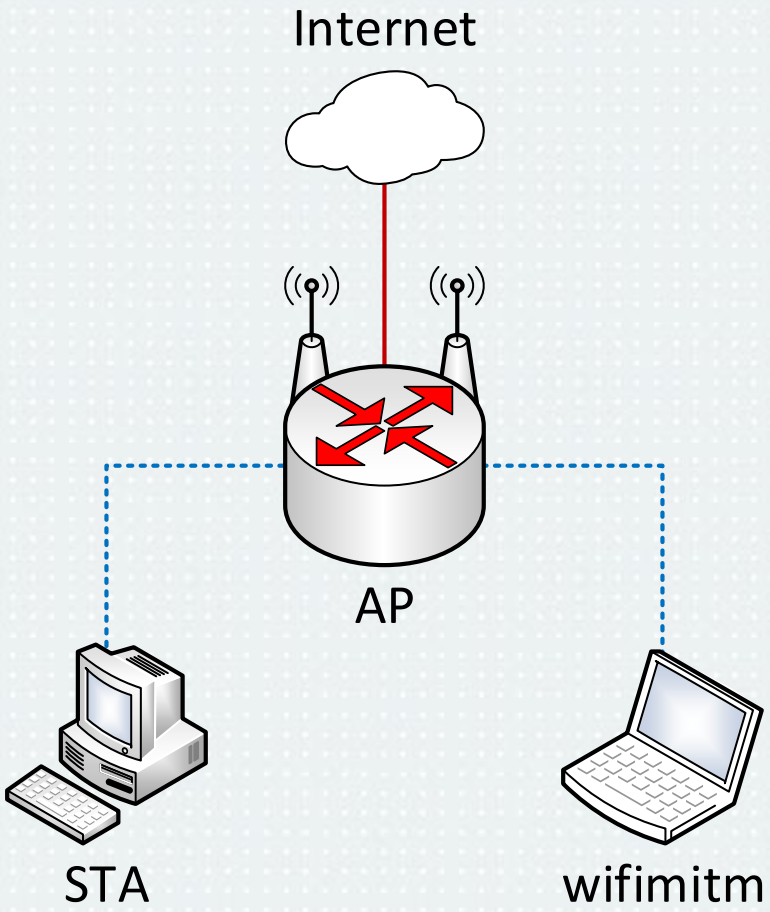


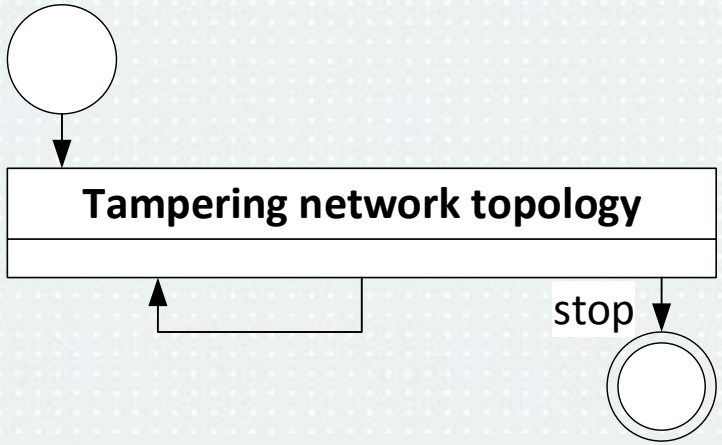
Accessing wireless network



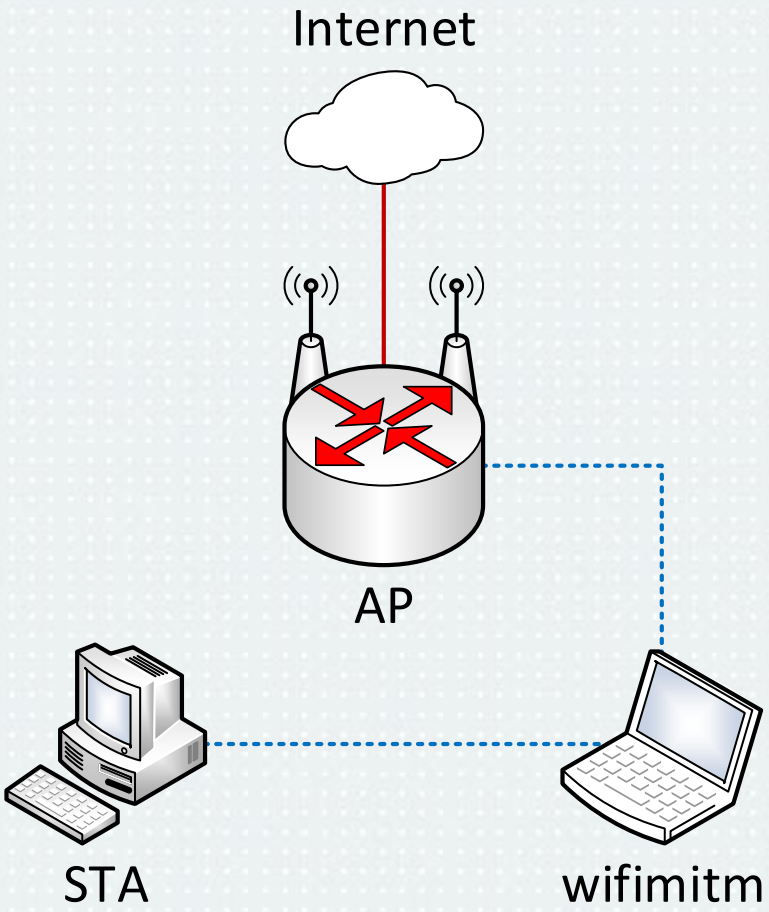


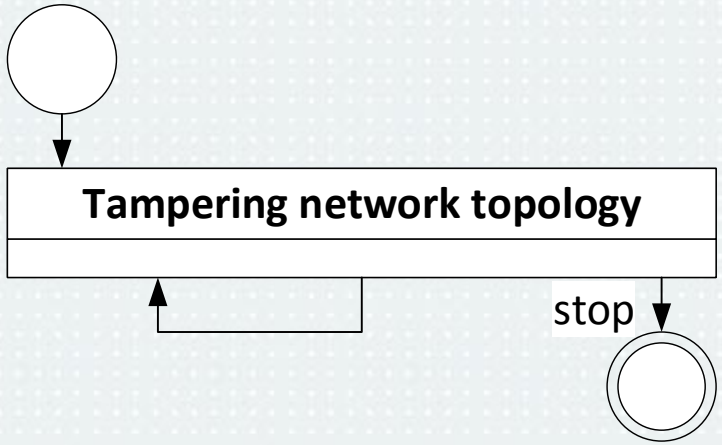
Tampering network topology



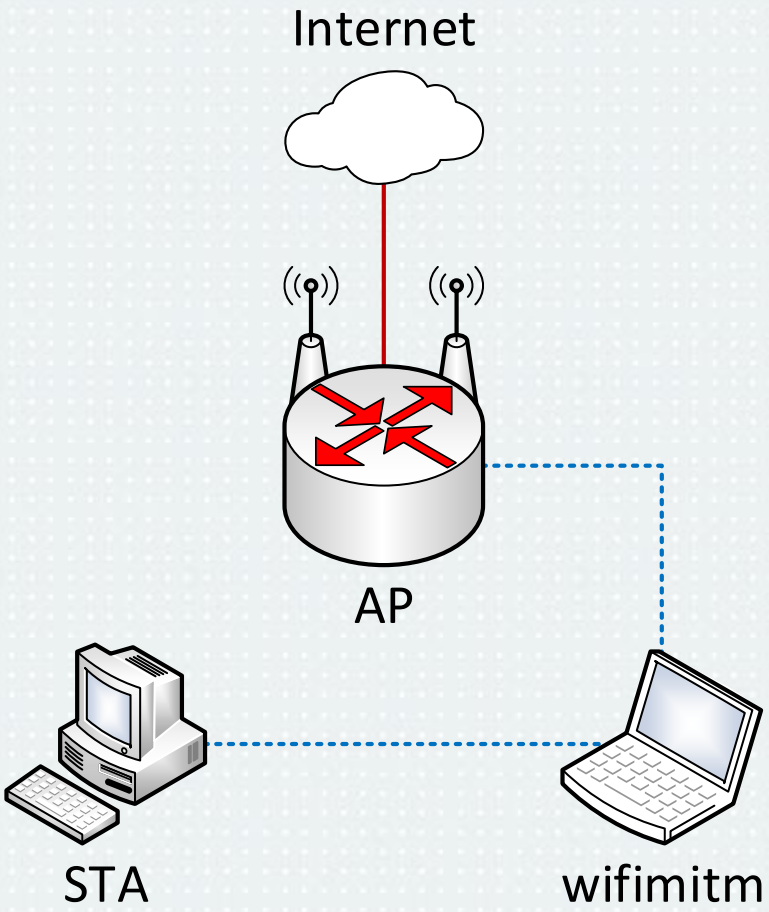


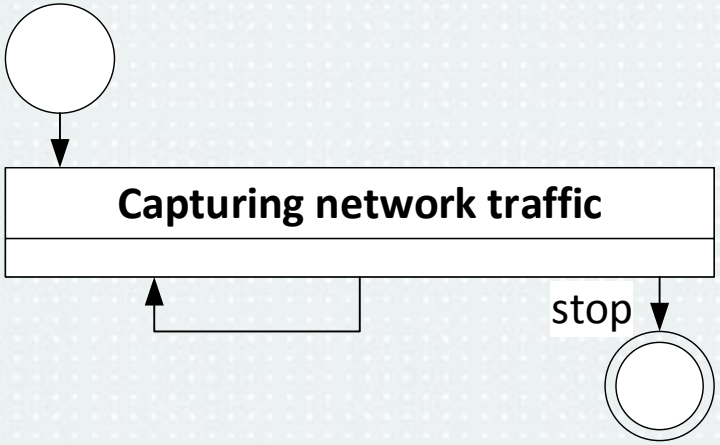
Tampering network topology



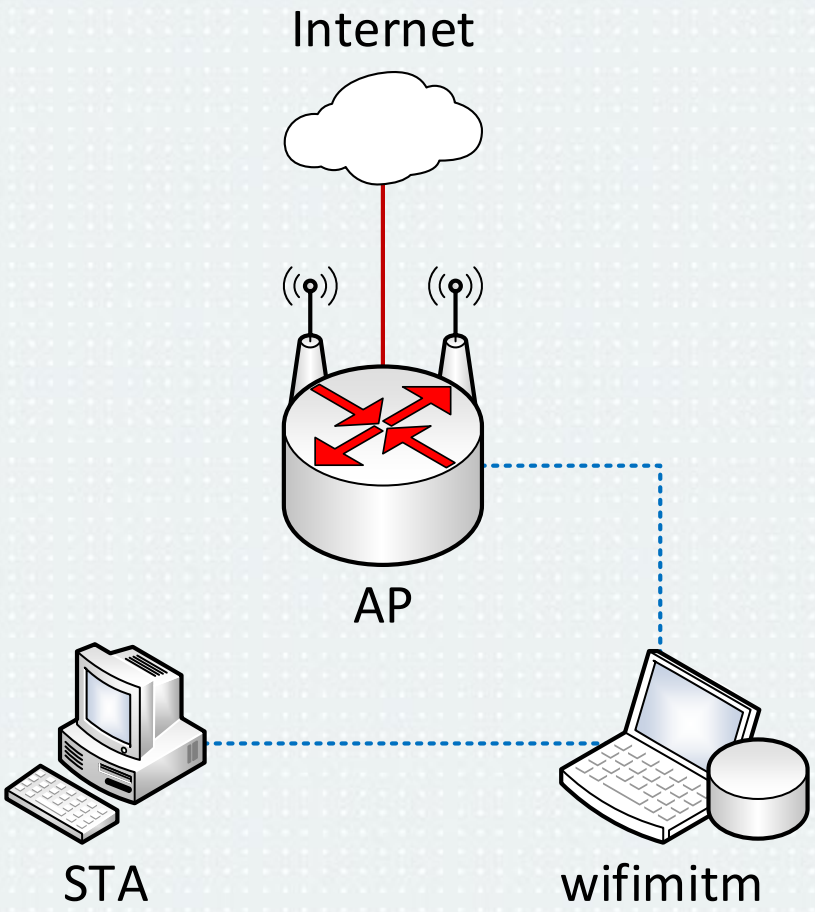


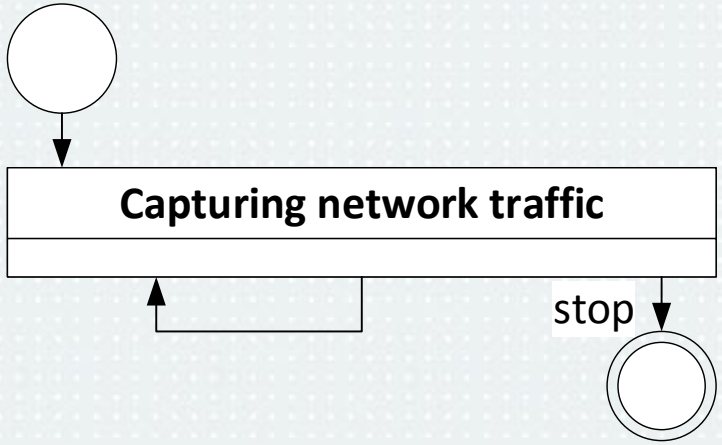
Capturing network traffic





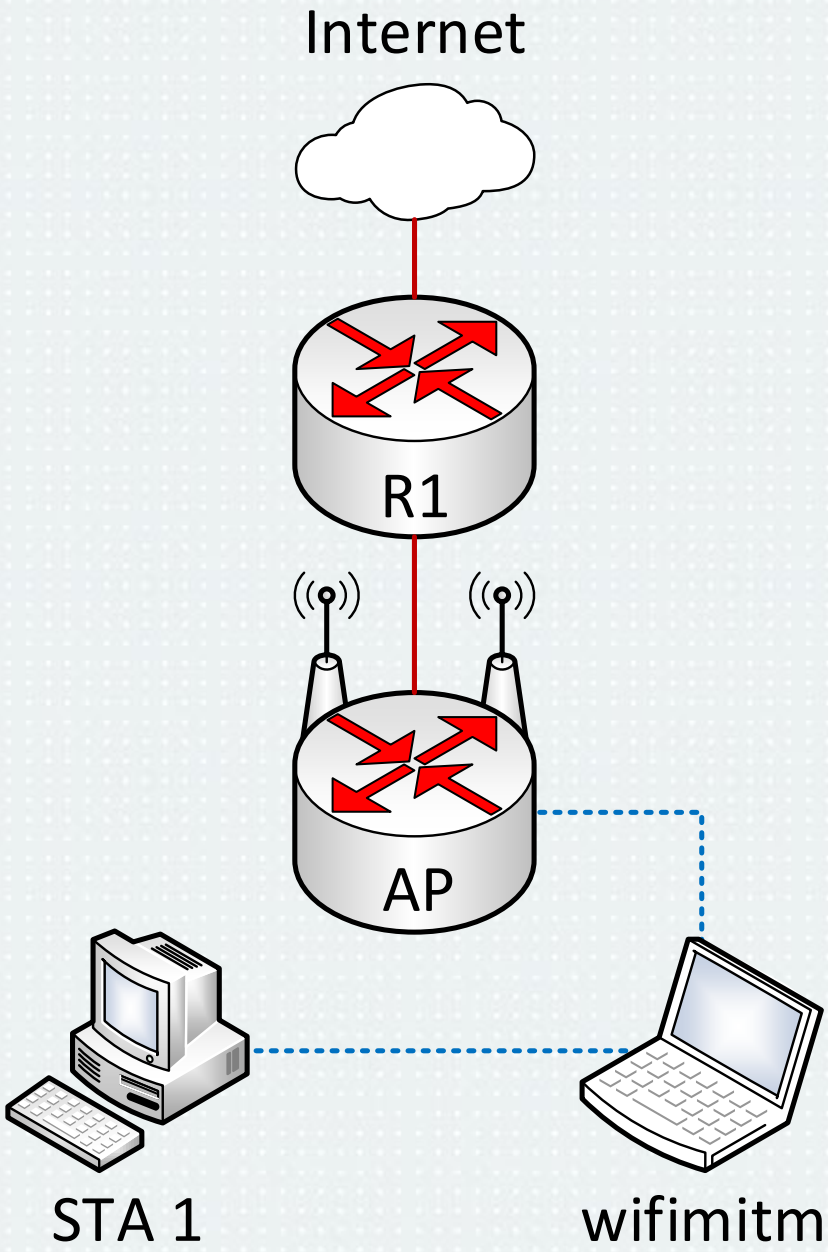
Capturing network traffic



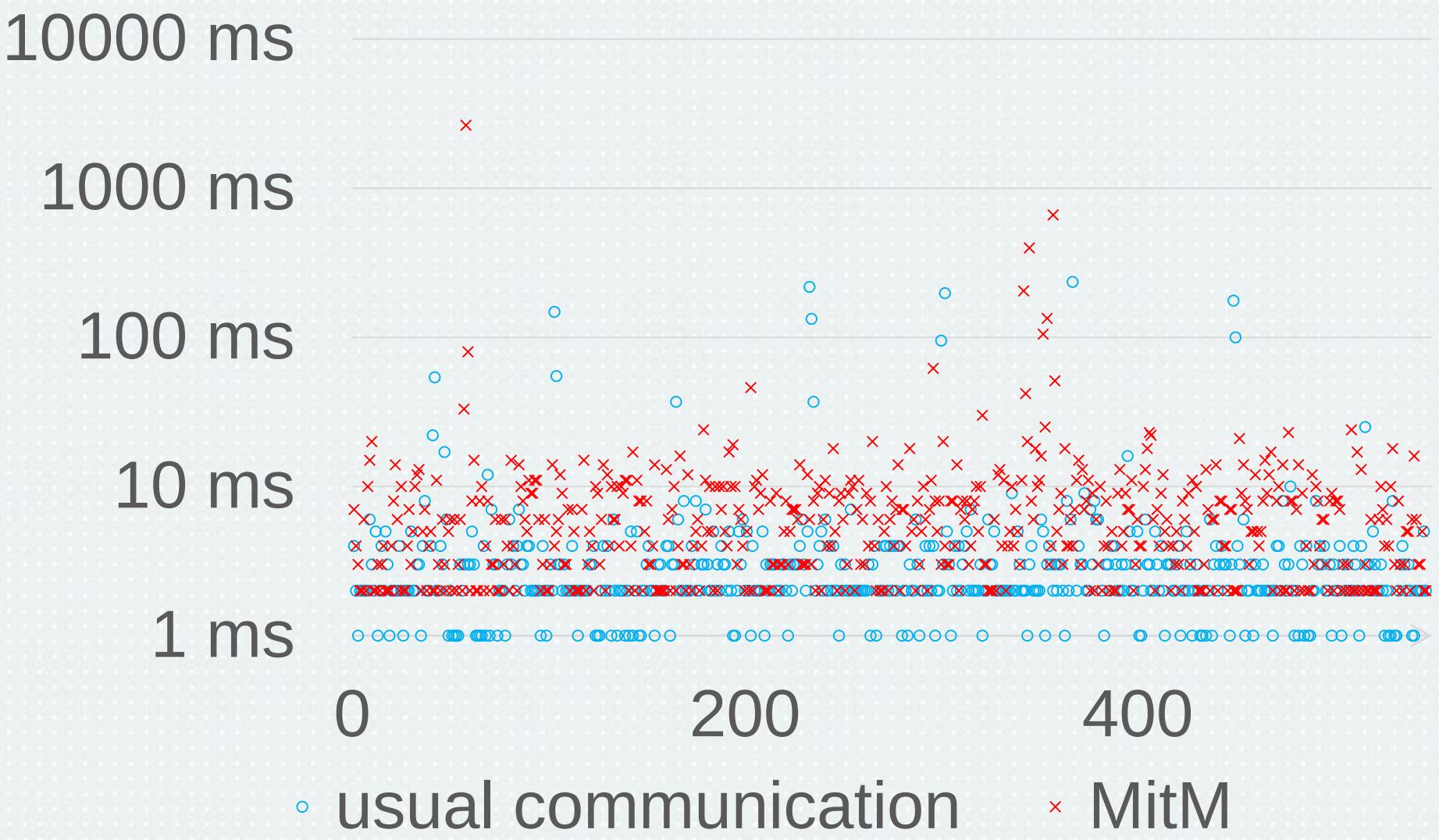


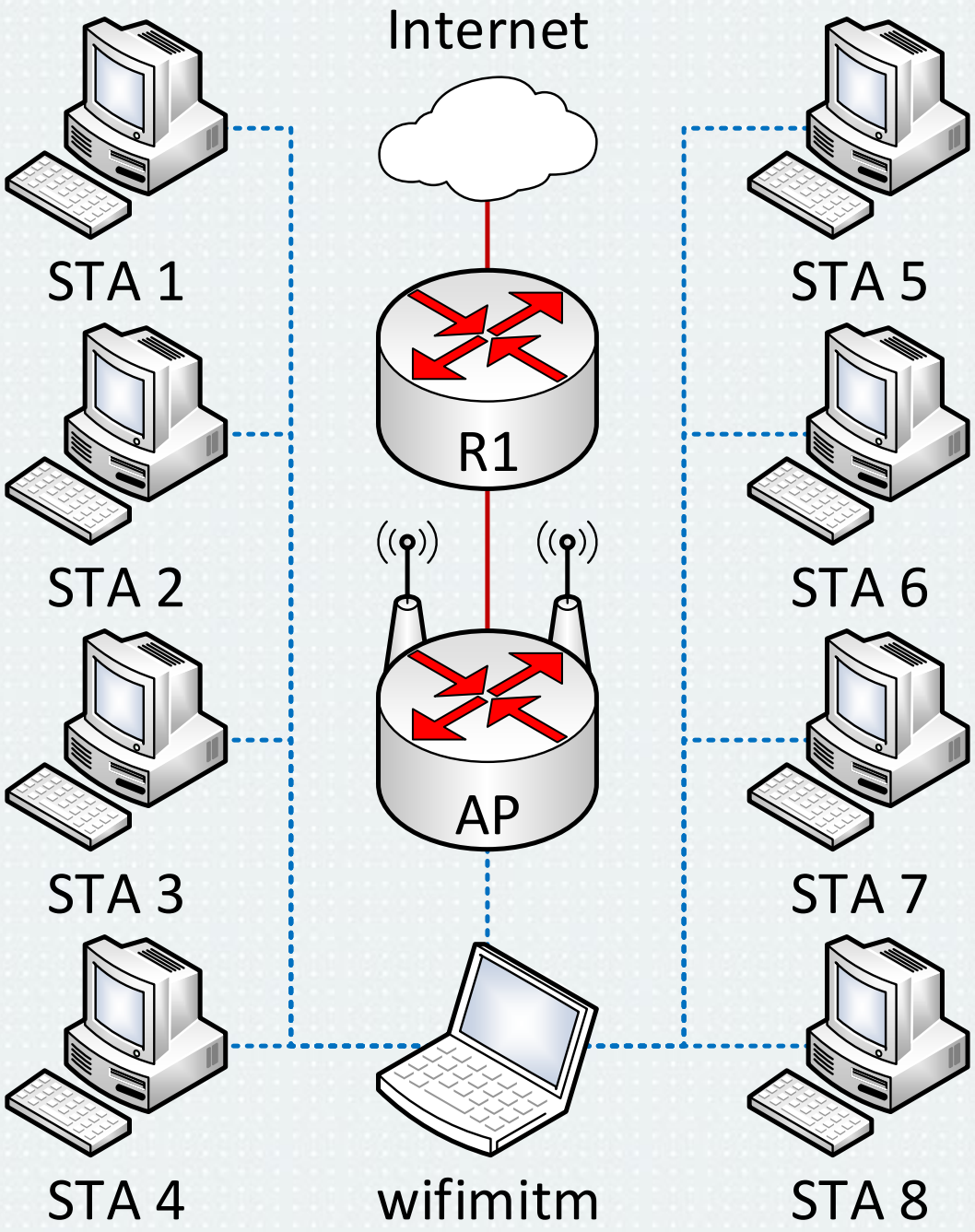
Performance testing

- 1 STA and 1 AP connected to the Internet
  - The performance impact is not critical.
  - Users of the network had no suspicion.
- 8 STAs and 1 AP connected to the Internet
  - The performance impact is more severe.
  - Despite the performance impact, users had no suspicion.

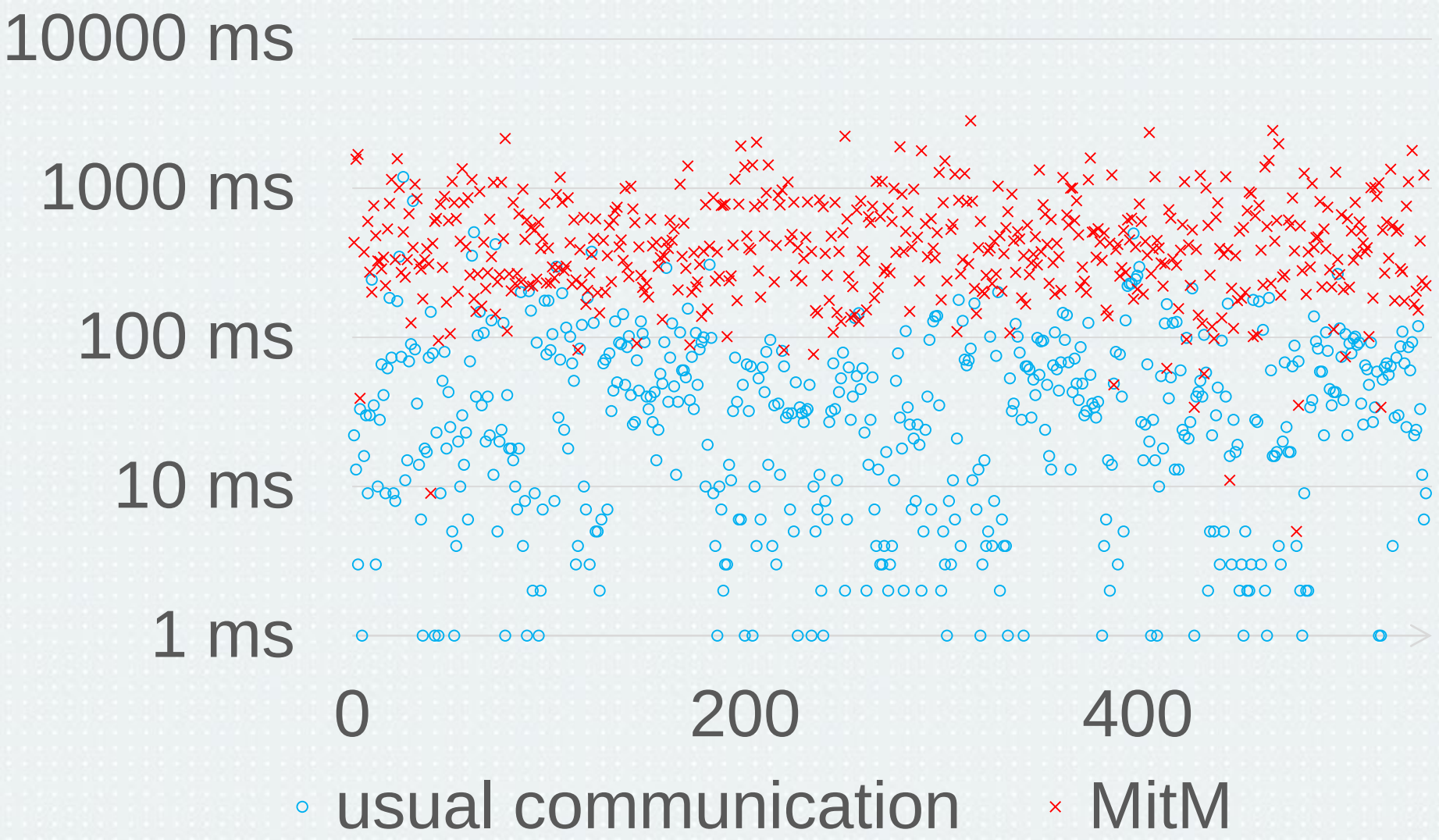

Internet
R1
AP
STA 1
wifimitm

RTT STA1–R1

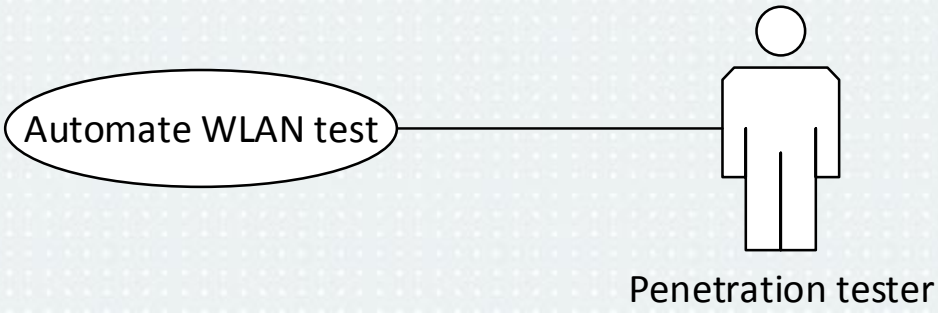

10000 ms
1000 ms
100 ms
10 ms
1 ms
0
200
400
usual communication
MitM


Internet
STA 1
STA 2
STA 3
STA 4
R1
AP
wifimitm
STA 5
STA 6
STA 7
STA 8

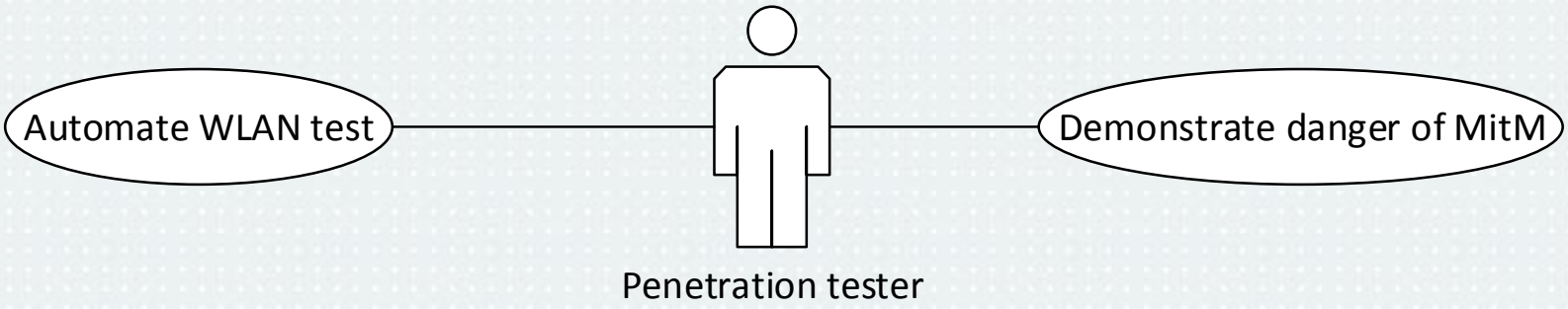
RTT STA1–R1


10000 ms
1000 ms
100 ms
10 ms
1 ms
0
200
400
usual communication
MitM

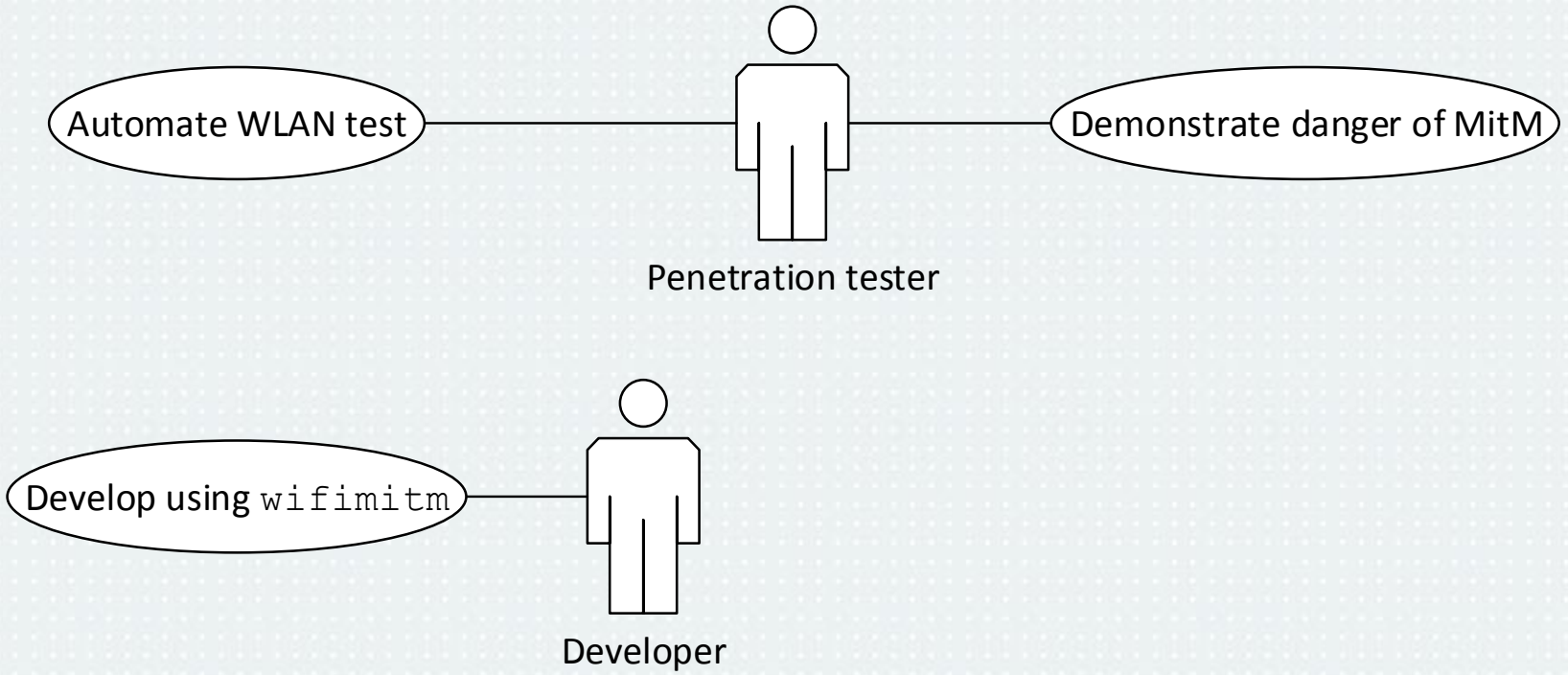
Utilization



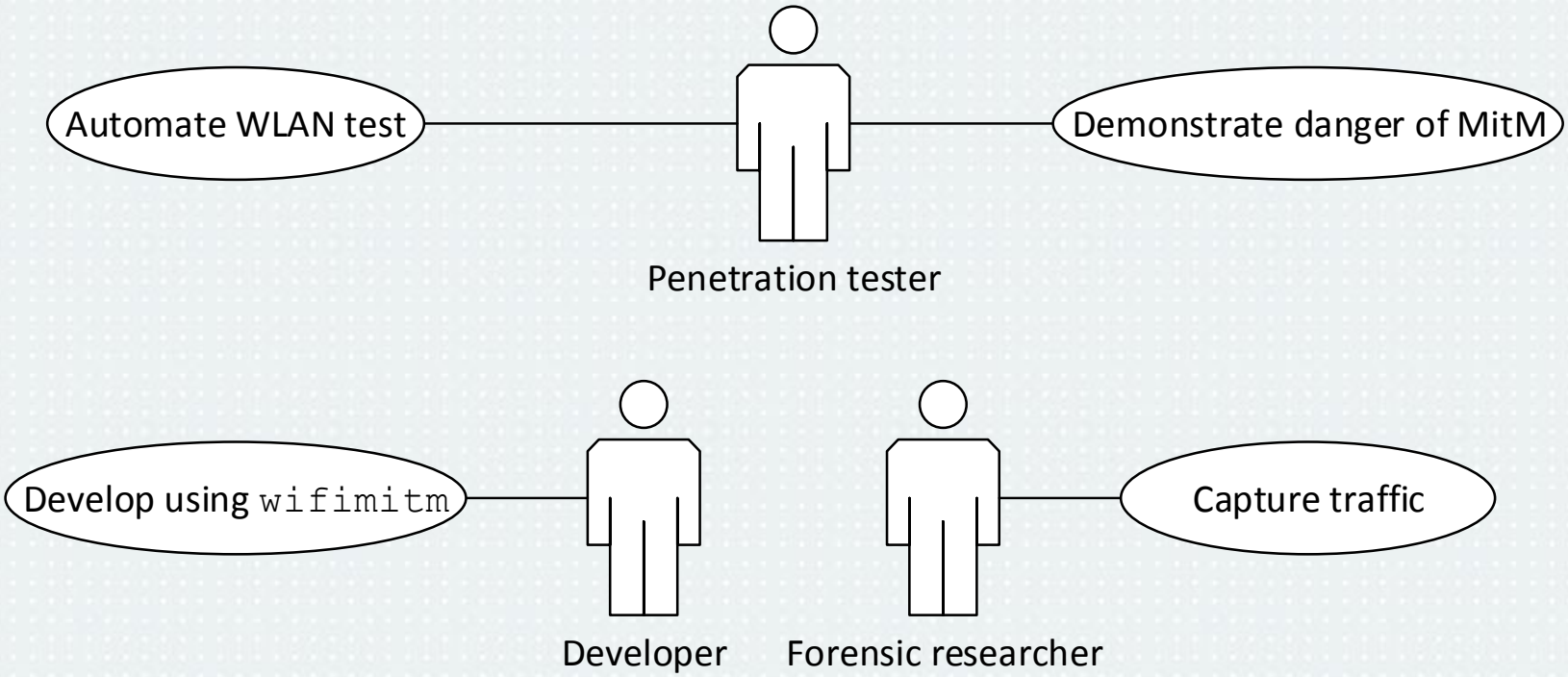
Utilization



Utilization



Utilization



Conclusion

- Research published as bachelor's thesis and software product in *NES@FIT* research group in May 2016.
- Author received dean's award and rector's award in 2016.
- Wi-Fi Machine-in-the-Middle (open-source)
- Penetration testing, forensic investigation

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ