Photo by Towfiqu barbhuiya: https://pexels.com/photo/close-up-of-a-smart-phone-with-a-lock-11391947/

Assignment 2: WiFi DoS Attacks and Scapy

Security and Privacy in Mobile Systems

Echo Meißner

Summer Term ’24

Interactive Discussion

- Your private WiFi at home
- Eduroam
- Public WiFi in the city

Frame Types

Data

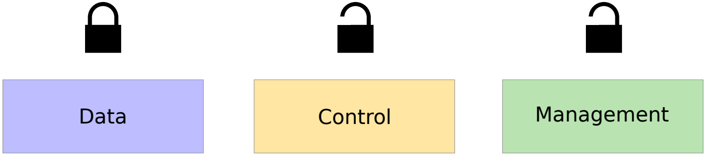
Control

Management

Reliability

Compensate openness (e.g. Association, Authentication)

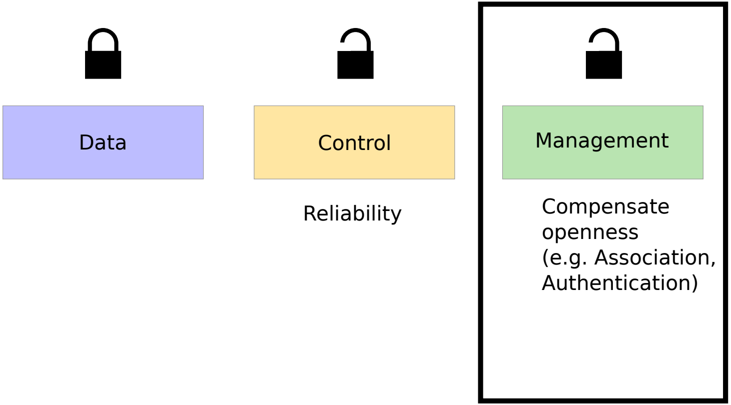
Frame Types



Reliability

Compensate
openness
(e.g. Association,
Authentication)

Frame Types



Data

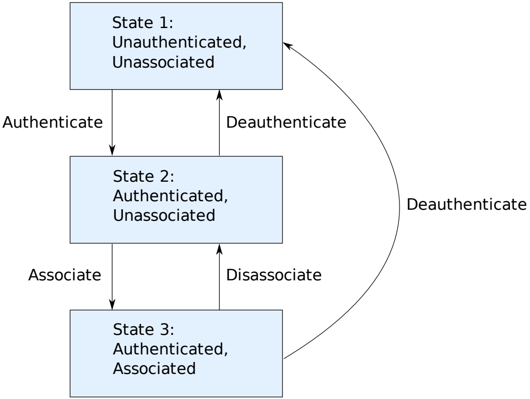
Control

Reliability

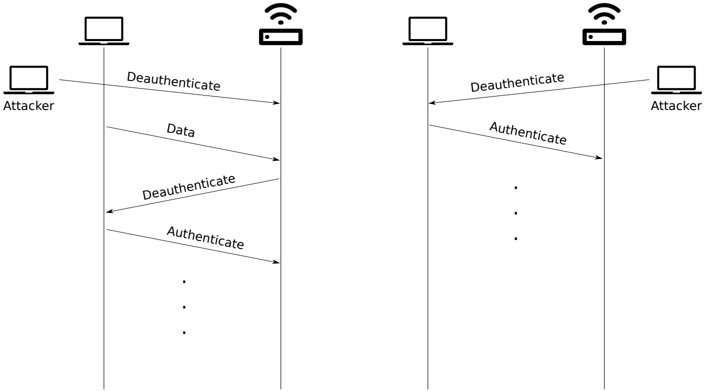
Management

Compensate openness (e.g. Association, Authentication)

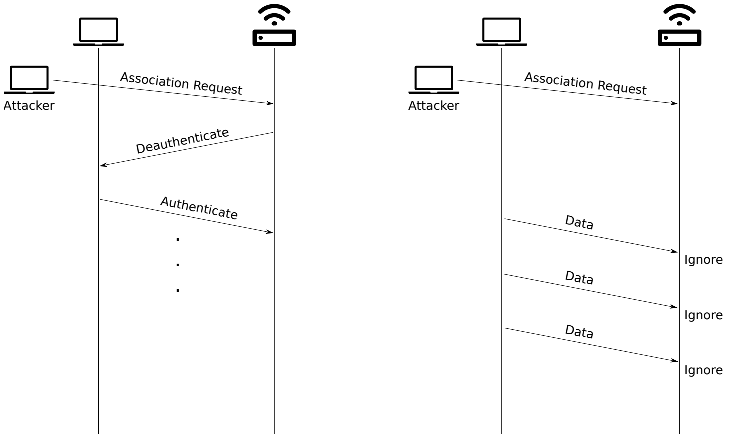
Authentication and Association State machine



Deauthentication attack



Association Request attack



Channel Switch Attack

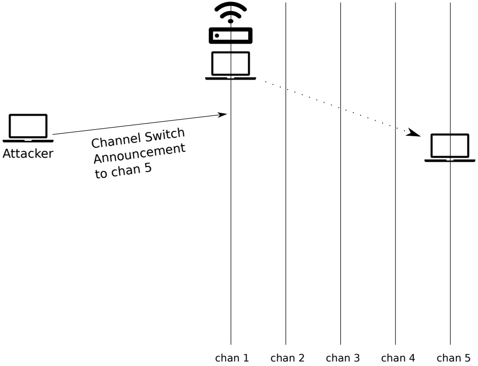
Dynamic Frequency Selection
DFS

Measurement of channels and approriate reactions (e.g. Measurement, Channel Switch)

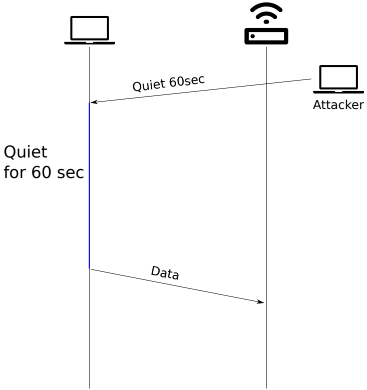
Transmit Power Control
TPC

Regulation of transmit power (e.g. Constraints, Capabilties)

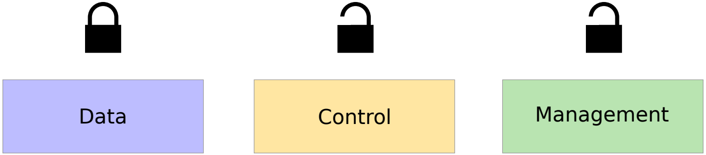
Channel Switch Attack



Quiet Attack



Frame Types



🔒 Data

🔓 Control

Reliability

🔓 Management

Compensate openness
(e.g. Association, Authentication)

Short introduction to scapy

- `https://scapy.net/`
- Interactive packet manipulation tool written in python.
- Many built-in ready to use layers.
- Able to send packets on layer 2 and 3.

Short introduction to scapy

- Start monitor mode:
  # airmon-ng start iface [channel]
- Import scapy functionality into python code:
  from scapy.all import *

Short introduction to scapy

- Show all protocols:
  >>> **ls()**
- Show all commands:
  >>> **lsc()**
- Show python help page, e. g. for the IP() packet class:
  >>> **help(IP())**

Short introduction to scapy

- Show fields of a protocol layer, e.g.:
  ```
  >>> IP().show()
  ```
- Create IP packet with destination ”uni-ulm.de”:
  ```
  >>> p = IP(dst=”uni-ulm.de”)
  ```
- Create packets with several layers, e.g.:
  ```
  >>> p = IP(dst=”uni-ulm.de”) / ICMP() / ”XXXXXX”
  ```
- Print packet fields and content:
  ```
  >>> p
  >>> p.show()
  ```

Short introduction to scapy

- Check if packet contains a specific layer, e.g.:
  ```
  >>> p.haslayer(IP)
  ```
- Get a specific layer, e.g.:
  ```
  >>> tcp = p[TCP]
  ```
- Get the payload, i.e. the next higher layer:
  ```
  >>> p.payload
  ```
- Get the next surrounding layer, i.e. the next lower layer:
  ```
  >>> p.underlayer
  ```

Short introduction to scapy

- Send a packet on layer 3:
  ```
  >>> send(p, iface=”iface”)
  ```
- Send a packet on layer 2:
  ```
  >>> sendp(p, iface=”iface”, count=100)
  ```
- Send a packet and wait for an answer:
  ```
  >>> sr1(p, iface=”iface”)
  >>> srp1(p, iface=”iface”)
  ```
- Start a sniffer with a callback method:
  ```
  >>> sniff(iface=”iface”, prn=callback)
  ```

(CC BY) The Noun Project

(CC BY) The Noun Project

(CC BY) Joe Harrison, from The Noun Project