ZEESHAN AFZAL

Doktorand

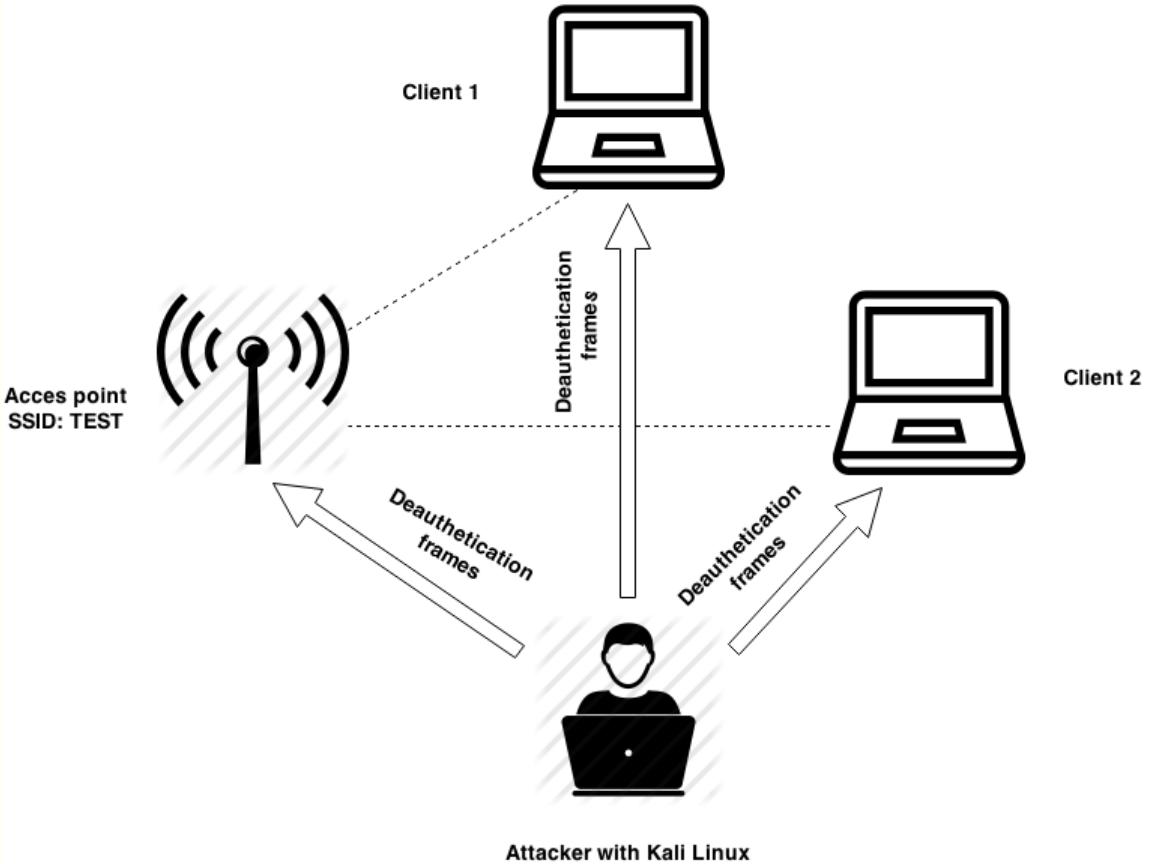
zeeshan.afzal@kau.se

Agenda

- Previous Work
  - Development & evaluation of a Wireless IDS
- Future Research Plan
  - Trade-offs between performance & security

DEVELOPMENT & EVALUATION OF A WIRELESS IDS

MASTER THESIS



CHALMERS

ABB

Outline

- Motivation
- Background
- Attacks
- Proposed Wireless IDS
- Evaluation Results
- Conclusions

Motivation

- Wireless offers convenience but concerns over security are growing
- Wireless networks are different than wired networks
- Updated standards and protocols are vulnerable
- Security mechanisms operate at OSI Layer 3 and higher

Background: 802.11 Operating mode

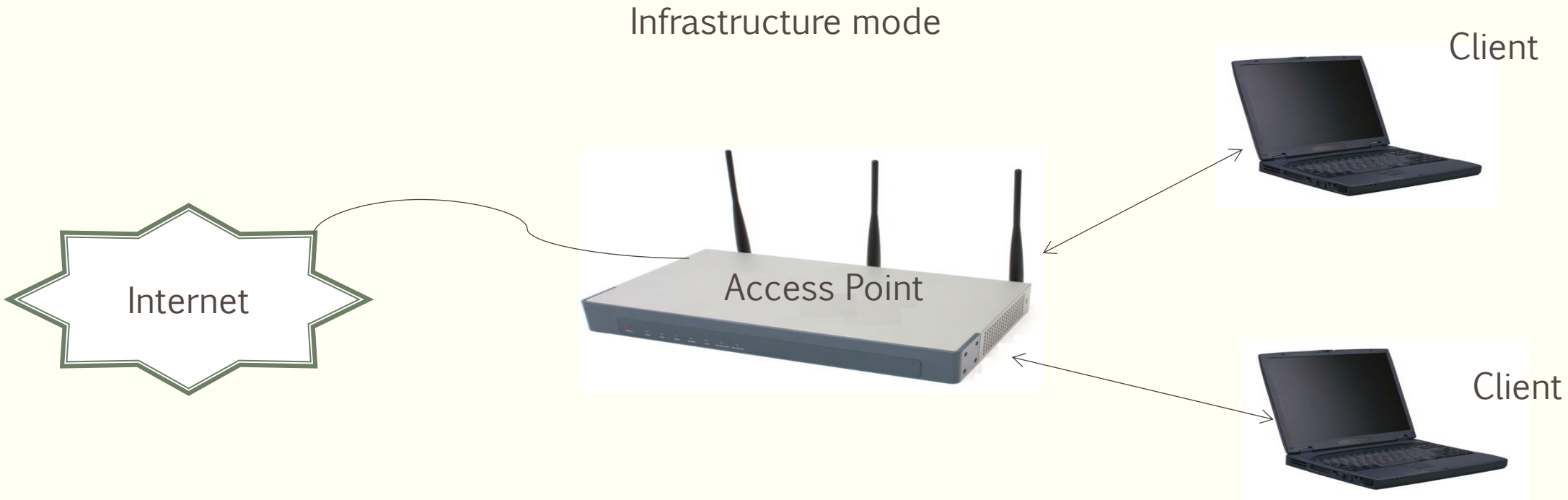


Figure 1: 802.11 Operating Mode

Background: 802.11 Frames

- Data frames
- Management frames
- Control frames

Background: Vulnerability in standard

Identity Spoofing or Impersonation

- Nodes at MAC layer can only by identified with MAC address
- Easy to spoof
- 802.11 standard has no mechanism to verify the self reported identity

Result

- Nodes have to blindly trust the source
- Management & control frames vulnerable

De-authentication Frame

- A subtype of Management frames
- Used by a station to terminate an existing authentication
- Not a request but a notification (can not be refused)

1. De-authentication Attack (DoS)

- Attacker sends spoofed de-authentication frames
- Can target one station or all using BC MAC
- Victim/s will get disconnected from the network

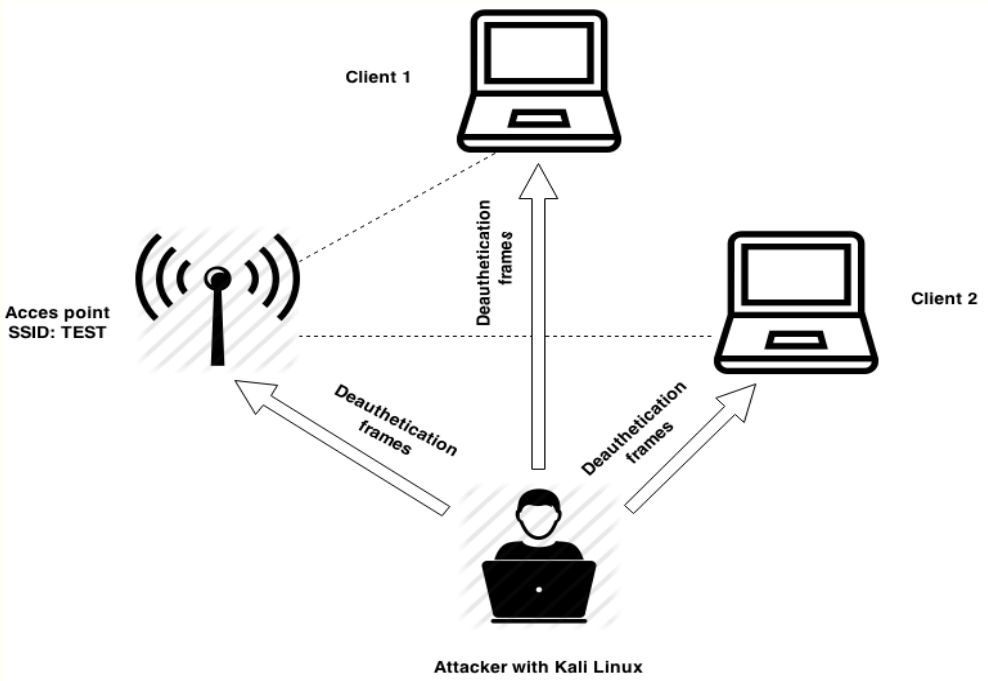
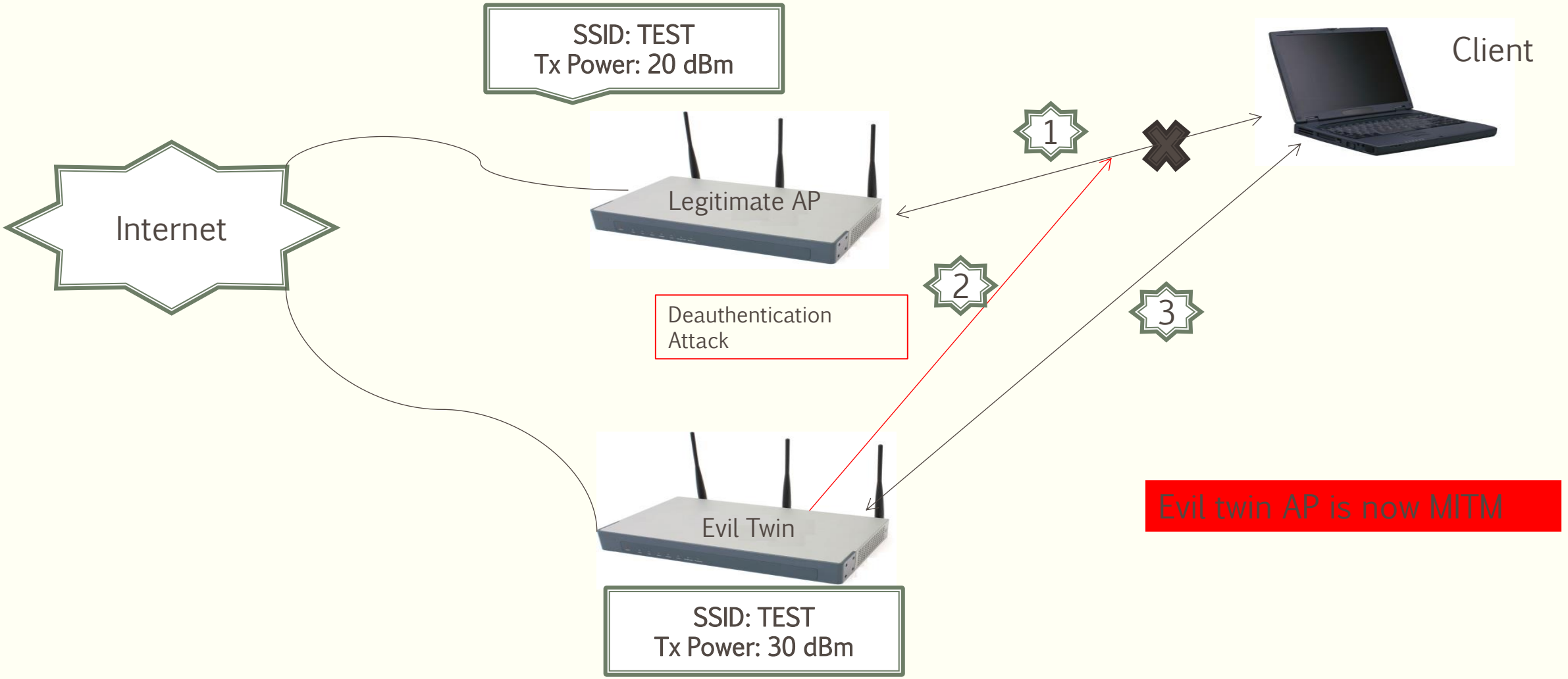


Figure 2: De-authentication Attack

2. Evil Twin Attack



Proposed WIDS

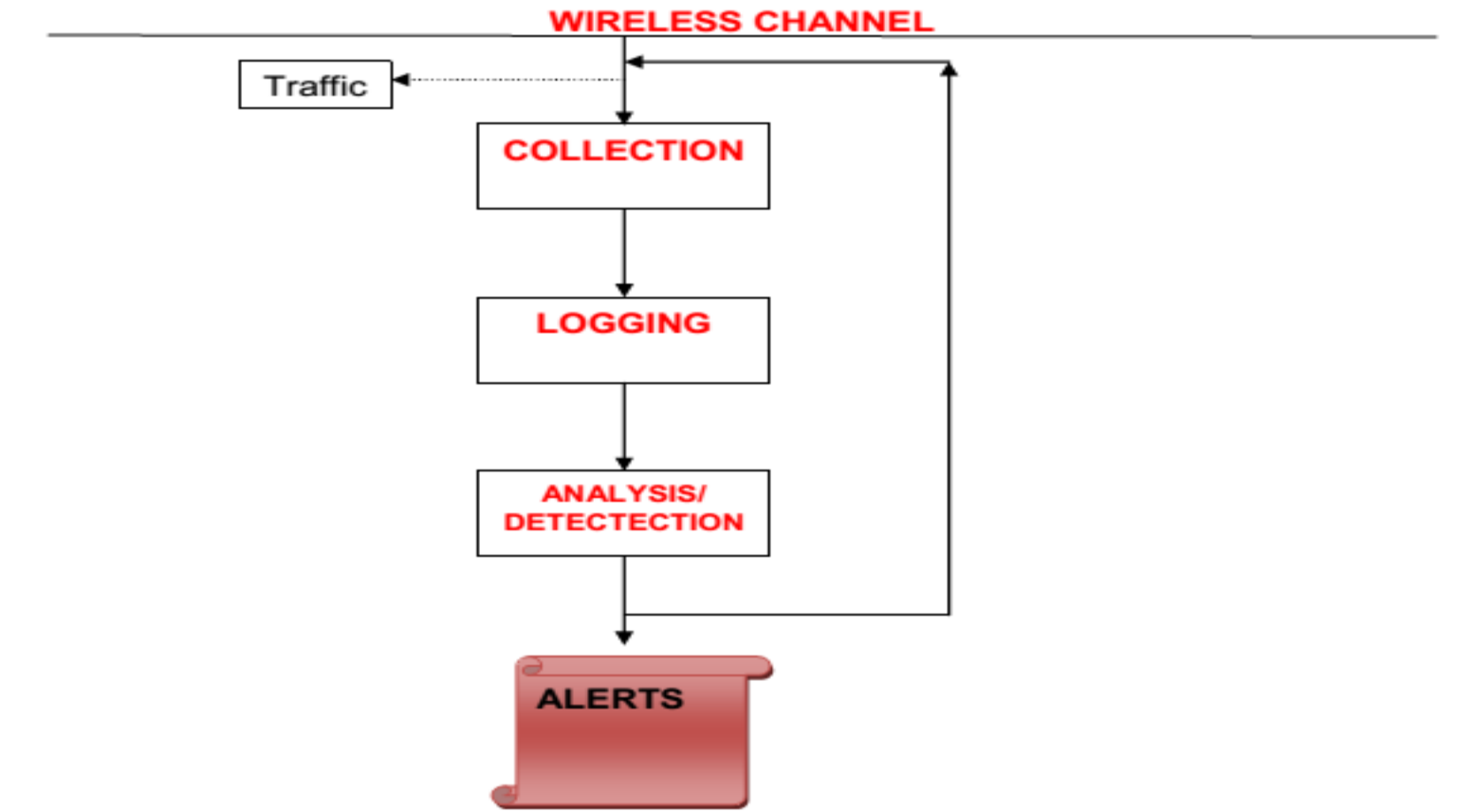


Figure 3: WIDS components

De-authentication Attack Indicators

- Frame type/subtype
- Number of frames in one snapshot (threshold)
- Number of duplicates (same source MAC -> destination MAC)
- Reason for deauthentication
- Data frames after deauthentication

```
De-Auth from SA:20:30:5a:34:07:11 Vendor:Cisco to DA:01:24:32:4b:c1:cc Vendor:Murata Manufacturing Co., Ltd. DeAuthentication: Disassociated due to inactivity
De-Auth from SA:20:30:5a:34:07:11 Vendor:Cisco to DA:01:24:32:4b:c1:cc Vendor:Murata Manufacturing Co., Ltd. DeAuthentication: Disassociated due to inactivity
De-Auth from SA:20:30:5a:34:07:11 Vendor:Cisco to DA:01:24:32:4b:c1:cc Vendor:Murata Manufacturing Co., Ltd. DeAuthentication: Disassociated due to inactivity
De-Auth from SA:20:30:5a:34:07:11 Vendor:Cisco to DA:01:24:32:4b:c1:cc Vendor:Murata Manufacturing Co., Ltd. DeAuthentication: Disassociated due to inactivity
```

Figure 4: Captured De-authentication frames

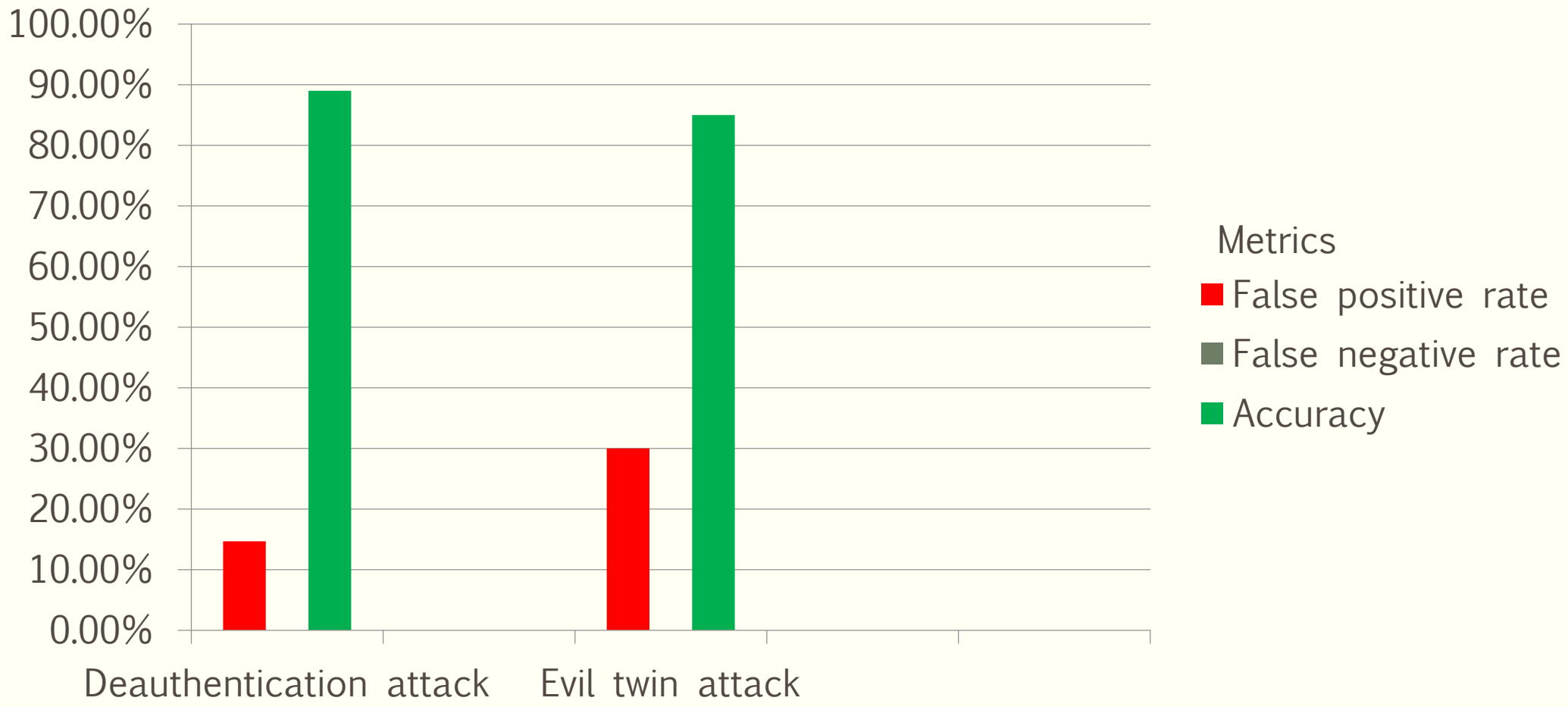
Evil Twin Attack Detection

- Detection based on transmit power difference
- Keep track of all SSIDs in range and the RSS
- A large change in RSS indicates a likely attack

```
SSID:(ABB-Guest) MAC: 1c:9d:69:c4:9d:1d RSS: -71 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:76:16 RSS: -79 CH: 1
SSID:(AddPro2) MAC: 00:45:2d:6a:dc:ca RSS: -90 CH: 1
SSID:(Gjestenett/Guest) MAC: 00:12:69:01:11:16 RSS: -89 CH: 1
SSID:(ABB-Guest) MAC: 00:62:b0:ca:1e:18 RSS: -85 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:26:32:16 RSS: -89 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:07:13 RSS: -86 CH: 1
SSID:(ABB-Guest) MAC: c0:9d:69:c4:d9:1d RSS: -68 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:76:16 RSS: -79 CH: 1
SSID:(Gjestenett/Guest) MAC: 00:32:96:20:32:81 RSS: -89 CH: 1
SSID:(ABB-Guest) MAC: 00:62:b0:ca:1e:18 RSS: -86 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:07:13 RSS: -86 CH: 1
SSID:(ABB-Guest) MAC: c0:9d:69:c4:d9:1d RSS: -71 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:76:16 RSS: -79 CH: 1
SSID:(Gjestenett/Guest) MAC: 00:32:99:20:32:81 RSS: -88 CH: 1
SSID:(ABB-Guest) MAC: 00:62:b0:ca:1e:18 RSS: -83 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:07:11 RSS: -85 CH: 1
SSID:(ABB-Guest) MAC: c0:9d:69:c4:d9:1d RSS: -68 CH: 1
SSID:(ABB-Guest) MAC: 07:01:c5:43:76:16 RSS: -80 CH: 1
SSID:(Gjestenett/Guest) MAC: 00:32:96:29:32:81 RSS: -90 CH: 1
```

Figure 5: SSID Info file

Evaluation - I



Evaluation - II

- Inspired by NSA and NIST defined benchmark requirements
- A total of 13 requirements selected
- WIDS scored **9** out of **13** possible points

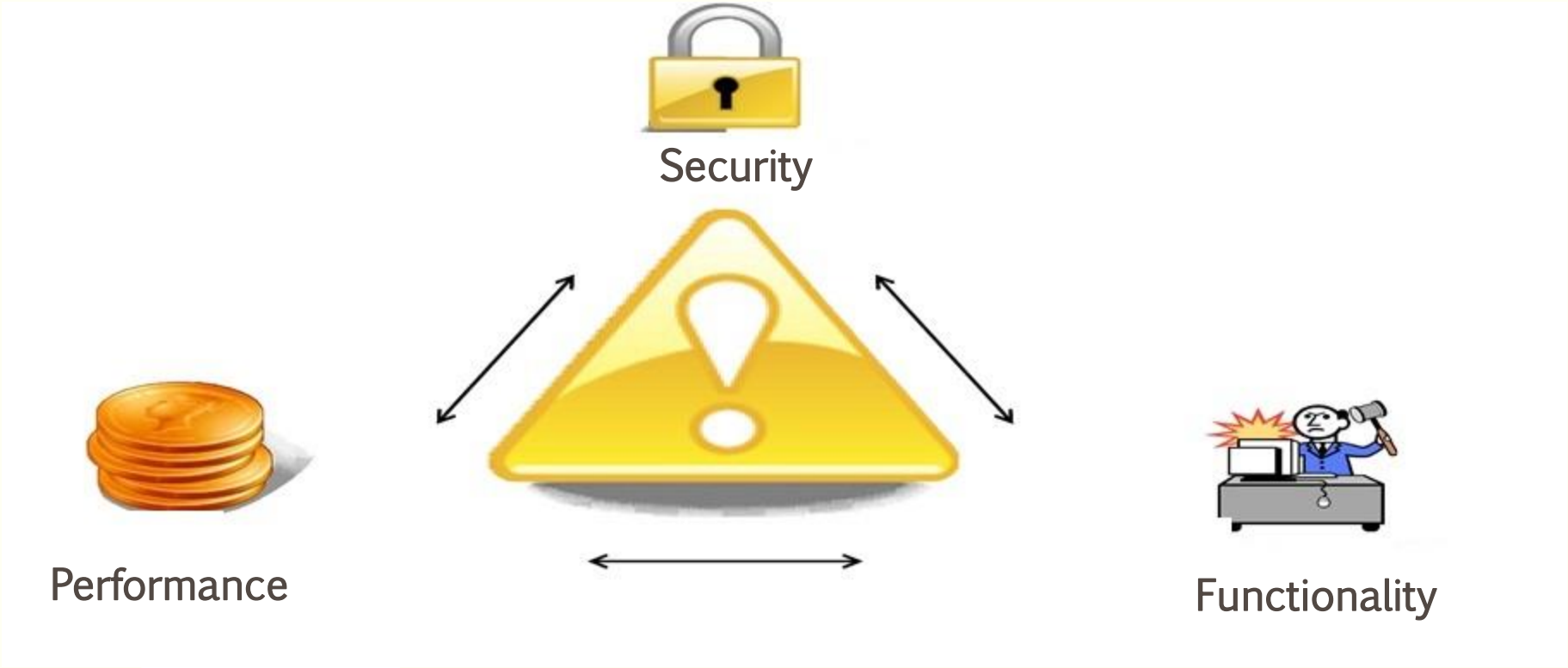
Conclusions

- Attacks exploit vulnerabilities in the standards
- Wireless IDS is able to detect but can not do much to prevent
- Need to find a good balance between security & performance

FUTURE RESEARCH PLAN

Trade-offs between performance & security

Trade-offs



Example

- Password length ⬆ = Security ⬆ = Performance ⬇
- Longer password length generally increases security
- But beyond a particular length, security level may remain same
- Goal: Find the optimal password length which gives the best security & performance

Research Questions

- Performance can be measured or quantified
- Cost of performance can be quantified
- Can we measure security?
- Can we trade one against the other?

THANK YOU

QUESTIONS/DISCUSSION