Advanced WiFi Attacks Using Commodity Hardware

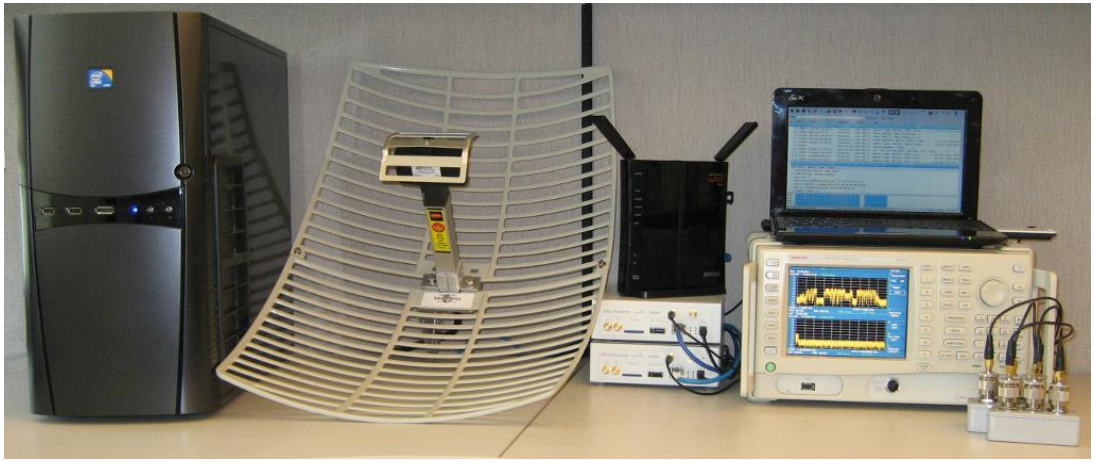
Mathy Vanhoef (@vanhoefm), KU Leuven

BruCON 2015

DistriNet
iMinds KU LEUVEN

Background

- WiFi assumes each station acts fairly



- With special hardware this isn't the case
  - Continuous jamming (channel unusable)
  - Selective jamming (block specific packets)

Background

- WiFi assumes each station acts fairly

- With special hardware this isn't the case
  - Continuous jamming (channel unusable)
  - **Selective jamming** (block specific packets)

Also with cheap hardware!

Small 15$ USB sufficient to:

- Testing selfish behavior in practice
- Continuous & selective jamming
- Reliable manipulation of encrypted traffic

Also with cheap hardware!

Attacks are cheaper than expected

- Should be able to **detect** them.

Selfish Behavior

Selfish behavior in practice?

Implement & Test!

Selfish Behavior

Steps taken to transmit a frame:

1. SIFS: let hardware process the frame
2. AIFSN: depends on priority of frame
3. Random backoff: avoid collisions
4. Send the packet

Selfish Behavior

Steps taken to transmit a frame:

Manipulate by modifying Atheros firmware:

- Disable backoff
- Reducing AIFSN
- Reducing SIFS

Selfish Behavior

Steps taken to transmit a frame:

Manipulate by modifying Atheros firmware:

- **Disable backoff**
- **Reducing AIFSN**

} **Optimal strategy:**

From 14 to 37 Mbps

- Reducing SIFS ⟶ Reduces throughput

DistriNet
iMinds KU LEUVEN

Selfish Behavior

Steps taken to transmit a frame:

Manipulate by modifying Atheros firmware:

- **Disable backoff**
- **Reducing AIFSN**

} **Optimal strategy:**

Upload!

From 1 to 37 Mbps

- Reducing SIFS ⟶ Reduces throughput

DistriNet
iMinds KU LEUVEN

How to control radio chip?

Using memory mapped registers

- Disable backoff:

```
int *GBL_IFS_MISC = (int*)0x10F0;
*GBL_IFS_MISC |= IGNORE_BACKOFF;
```

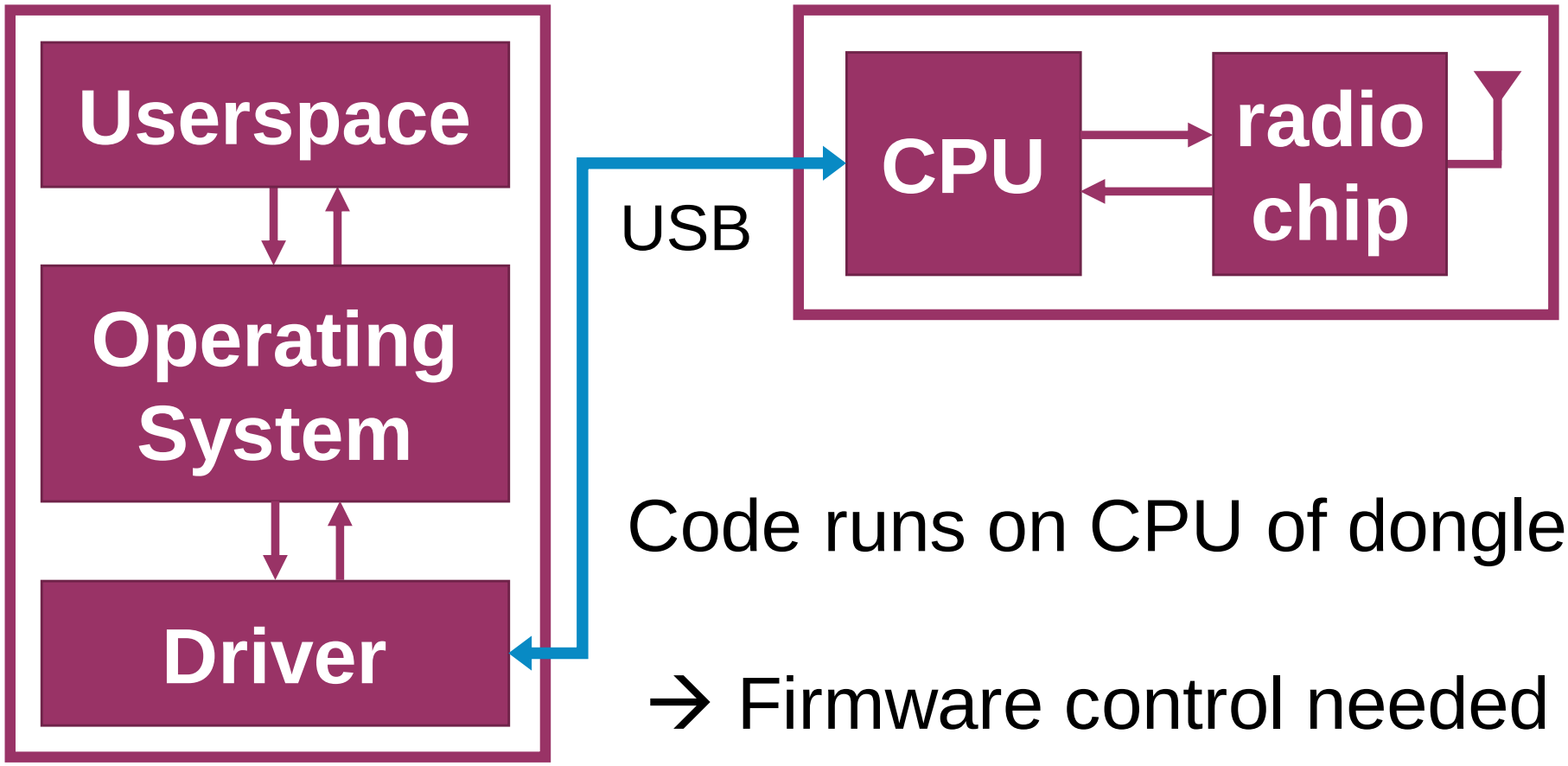
- Reset AIFSN and SIFS:

```
int *AR_DLCL_IFS = (int*)0x1040;
*AR_DLCL_IFS = 0;
```

Location of this code?

Main machine

WiFi Dongle



Code runs on CPU of dongle

→ Firmware control needed

Countermeasures

DOMINO defense system reliably detects selfish behavior [1].

More on this later!

Selfish Behavior

What if there are multiple selfish stations?

- ~~In a collision, both frames are lost.~~
- Capture effect: in a collision, frame with the best signal and lowest bitrate is decoded.

Similar to FM radio

Demo: The Queen station generally "wins" the collision with others.

FM Radio Demo

DistriNet
iMinds
KU LEUVEN

Selfish Behavior

Attacker can abuse capture effect

- Selfish clients will **lower** their bitrate to beat other selfish stations!
- Until this gives no more advantage.

To **increase** throughput, bitrate is **lowered**!

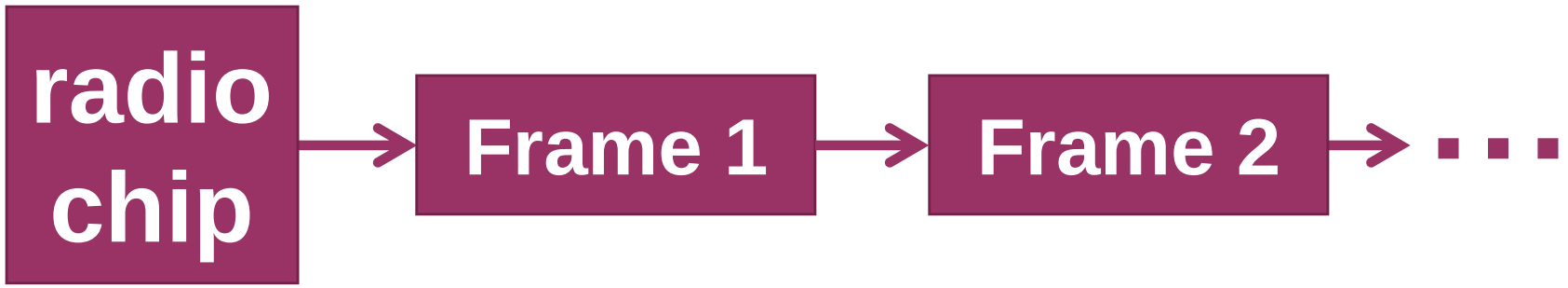
→ Other station = background noise

Continuous Jammer

Want to build a continuous jammer

1. Instant transmit: disable carrier sense
2. No interruptions: queue infinite #packets

Frames to be transmitted are in a linked list:

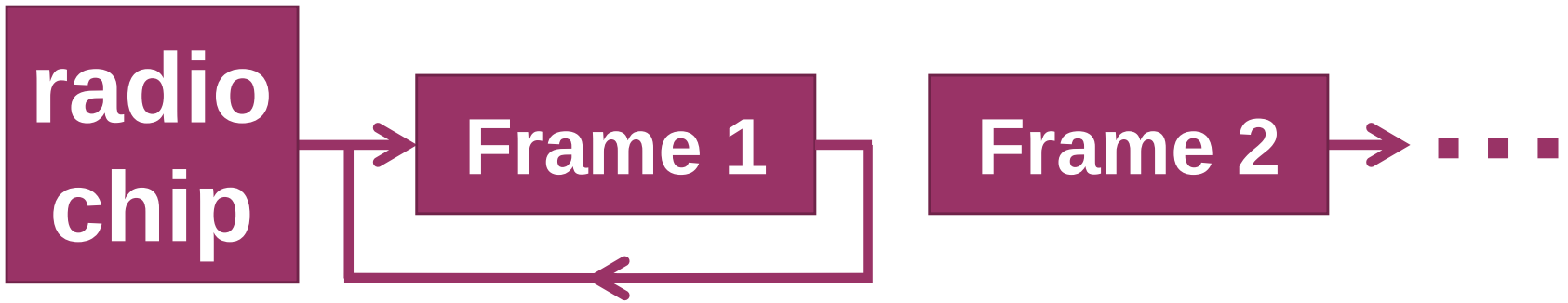


Continuous Jammer

Want to build a continuous jammer

1. Instant transmit: disable carrier sense
2. No interruptions: queue infinite #packets

Frames to be transmitted are in a linked list:



Infinite list!

Continuous Jammer

Experiments

- Only first packet visible in monitor mode!
- Other devices are **silenced**.

Default antenna gives range of ~80 meters.

Amplifier gives range of ~120 meters

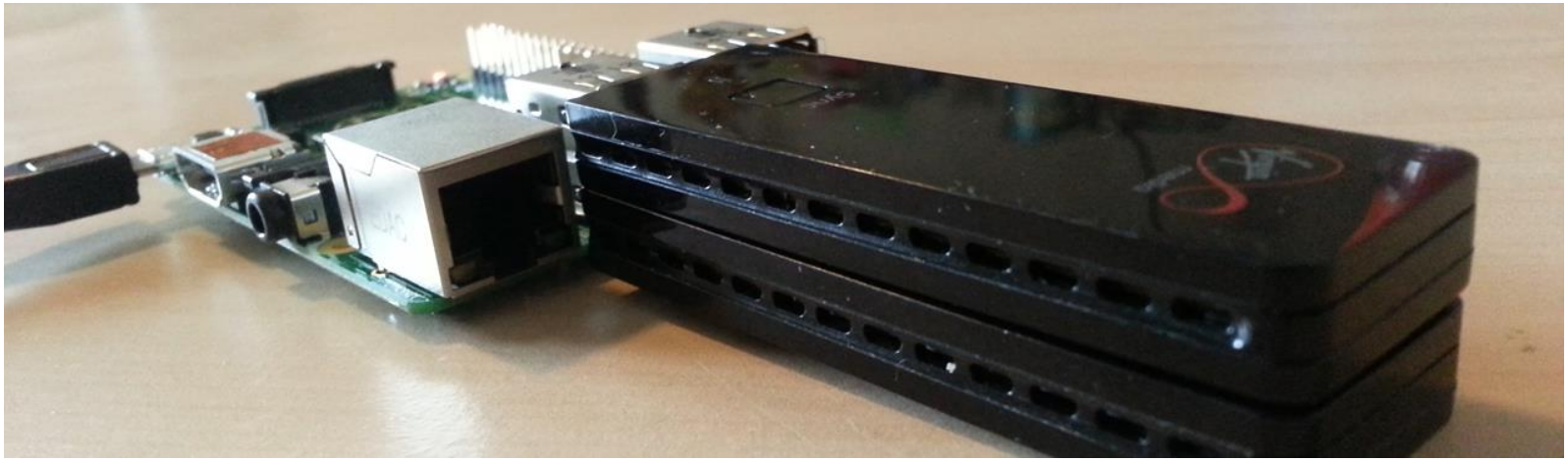
Demo: Continuous Jammer

Ideally done in a shielded room …

… but we can try it here as well ☺

To prevent harm, only active for a few seconds.

Raspberry Pi Supported!



Practical Implications

Devices in 2.4 and 5 GHz bands?

- Home automation
- Industrial control
- Internet of Things
- …

Can easily be jammed!

Practical Implications

Devices in 2.4 and 5 GHz bands?

Practical Implications

Devices in 2.4 and 5 GHz bands?

Not just wild speculation …

… jammers are already used by thieves!

$45 Chinese jammer to prevent cars from being locked [6]

GPS jammer to disable anti-theft tracking devices in stolen cars [7]

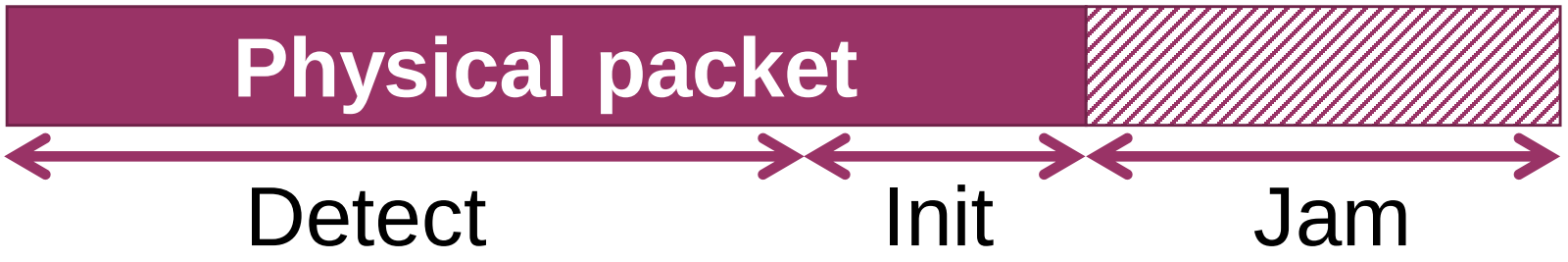
Disable mobile phone service after cutting phone and alarm cables [8]

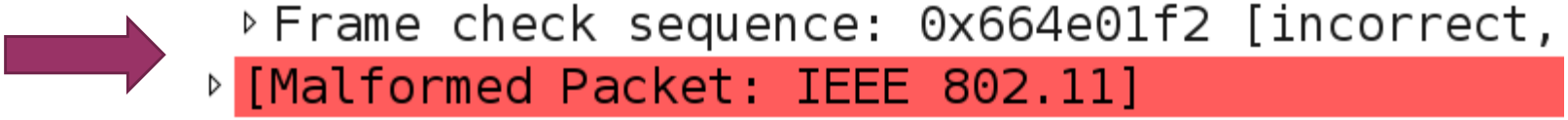
Selective Jammer

Decides, based on the header, whether to jam the frame.

How does it work?

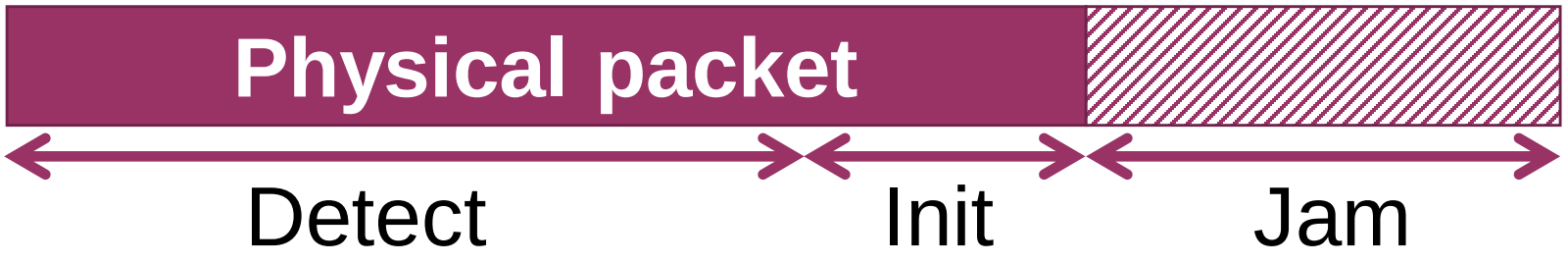
1. Detect and decode header
2. Abort receiving current frame
3. Inject dummy packet

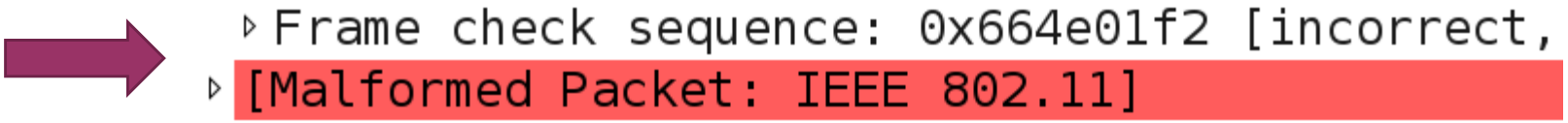




How does it work?

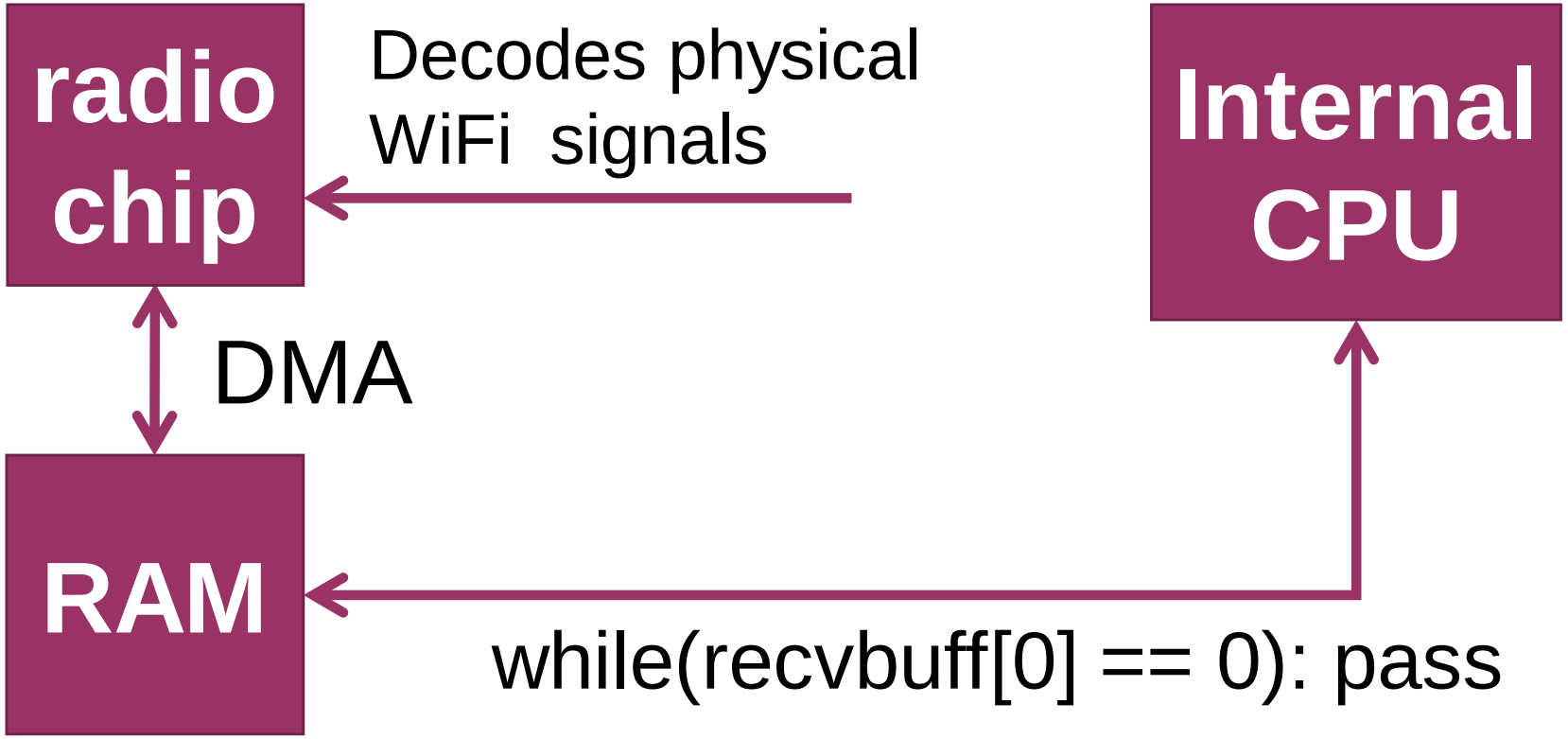
1. **Detect and decode header** } **Hard**
2. Abort receiving current frame } Easy
3. Inject dummy packet





DistriNet
iMinds KU LEUVEN

Detecting frame headers?

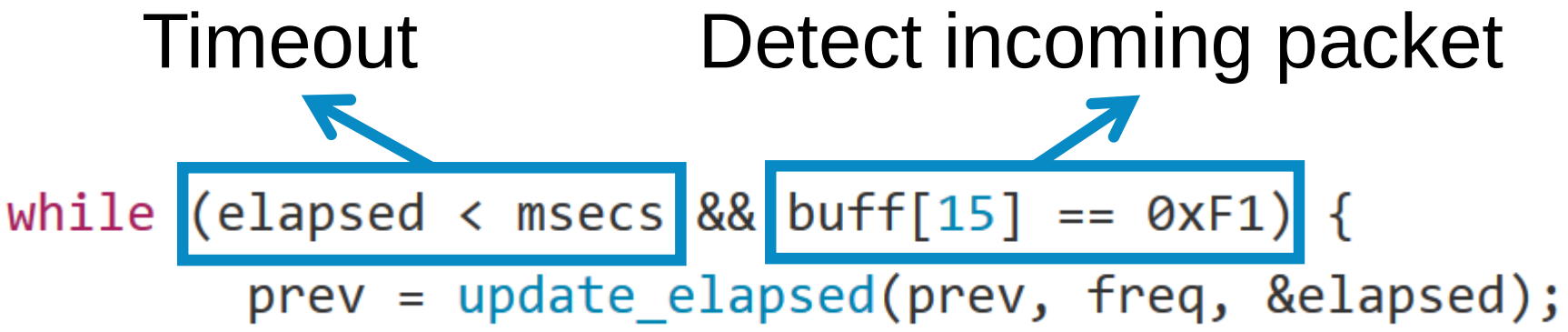


→ Can read header of frames still in the air.

In practice

1. **Detect and decode header**
2. Abort receiving current frame
3. Inject dummy packet

Poll memory until data is being written:



In practice

1. **Detect and decode header**
2. Abort receiving current frame
3. Inject dummy packet

Probe request or beacon?

```
if ( (buff[0] == 0x80 || buff[0] == 0x50)
     && ((source[0] & 1) || A_MEMCMP(source, buff + 10, 6) == 0) )
{
```

`buff + 10`: sender of packet

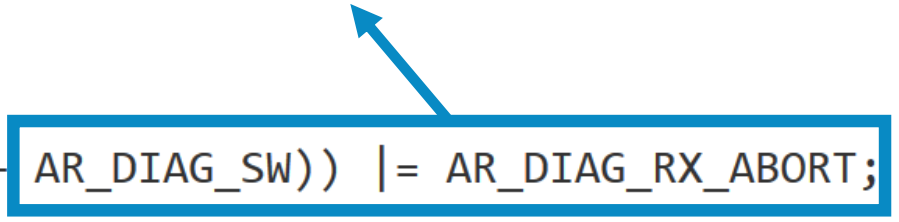
`source` : target MAC address

In practice

1. Detect and decode header
2. **Abort receiving current frame**
3. Inject dummy packet

Set specific bit in register

```
// Abort Rx
*((a_uint32_t *)(WLAN_BASE_ADDRESS + AR_DIAG_SW)) |= AR_DIAG_RX_ABORT;
```



In practice

1. Detect and decode header
2. Abort receiving current frame
3. **Inject dummy packet**

Pointer to dummy packet

```
// Jam the packet
*((a_uint32_t *)(WLAN_BASE_ADDRESS + AR_QTXDP(TXQUEUE))) = (a_uint32_t)txads;
*((a_uint32_t *)(WLAN_BASE_ADDRESS + AR_Q_TXE)) = 1 << TXQUEUE;
```

TXE: Transmit (TX) enable (E)

DistriNet iMinds KU LEUVEN

Selective Jammer: Reliability

Jammed beacons with many devices/positions

How fast can it react?

- Position of first mangled byte?
- 1 Mpbs beacon in 2.4 GHz: position 52
- 6 Mpbs beacon in 5 GHz: position 88

Context:

- MAC header is 34 bytes

Selective Jammer: Reliability

Jammed beacons with many devices/positions

Conclusion

- 100% reliable selective jammer not possible
- Medium to large packets can be jammed
- Surprising this is possible with a limited API!

DOMINO defense system

Also capable of detecting selective jammers

- Assumes MAC header is still valid.
- Attacker has low #(corrupted frames)
- Thrown of the network

Unfortunately it's flawed

- Jammed (corrupted) frames are not authenticated, we can forge them.
- Pretend that a client is jamming others.

Demo: Selective Jammer

Avoiding harmful interference:

- Target is in (unused?) 5 GHz channel
- Will only run for a few seconds

If you do more extensive tests …

Code is online!

modwifi.bitbucket.org

(github.com/vanhoefm/modwifi)

Scenarios where (selective) jammers are useful?

1. Attack WiFi geolocation

Location determined by nearby SSIDs.

Geolocation attack [9]

- Inject SSIDs present at other location
- Can only spoof location having more APs
- Solution: selectively jam nearby APs

→ Never blindly trust WiFi geolocation!

2. As defense system

Turn the tables around:

Use jamming to protect a network

- Selectively jam rouge APs
- Wearable shield to protect medical implants that constantly sends jamming signal. [10]
- …. (active research topic)

2. As defense system

May not be legal?

Blocking personal hotspots:

- Done by Marriott and Smart City Holdings
- Complaint was filled to the FCC
- Settled for fine of $600,000 and $750,000

Is blocking malicious or rogue hotspots legal?

Impact on higher-layers

What about higher-layer protocols?

Impact on higher-layers

What if we could reliably manipulate encrypted traffic?

not decrypt!

We could attack WPA-TKIP!

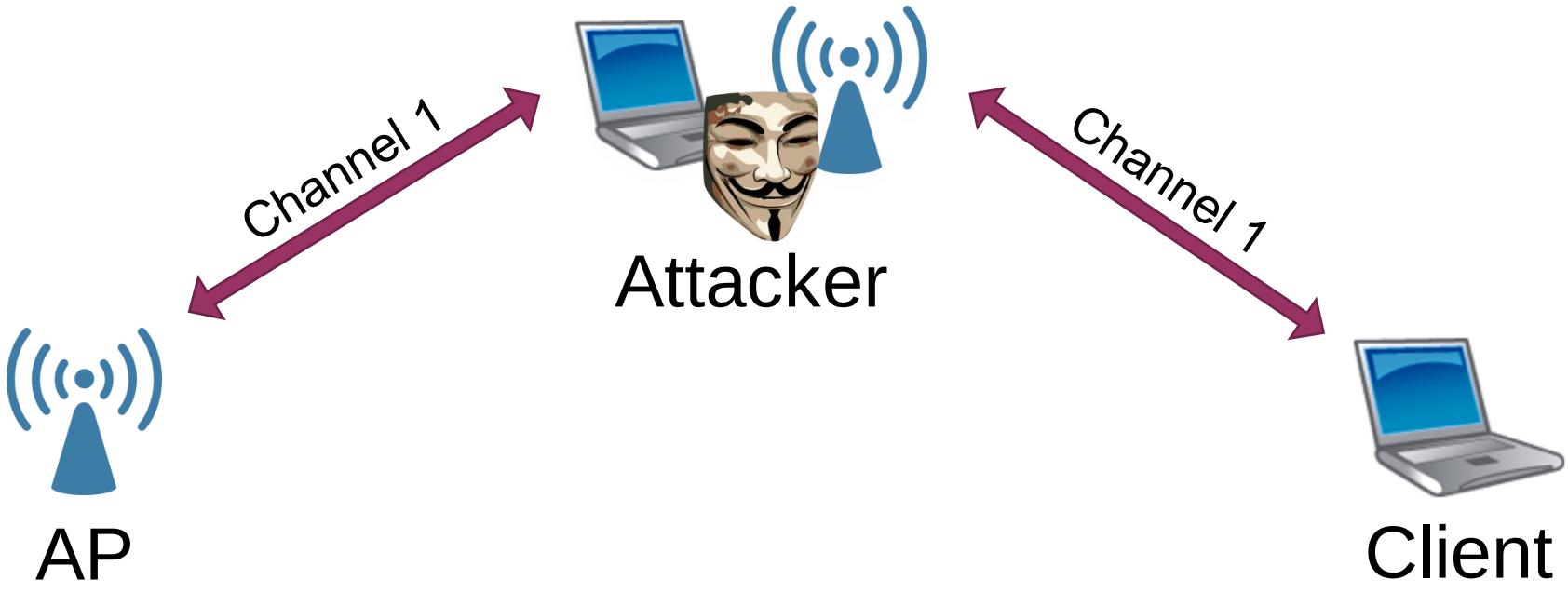
Reliably Intercepting Traffic!

Channel-based MiTM attack

- Works against any encrypted network
- Can **reliably** manipulate encrypted traffic.

Strawman: different MAC

Cloned MAC addresses different from target?



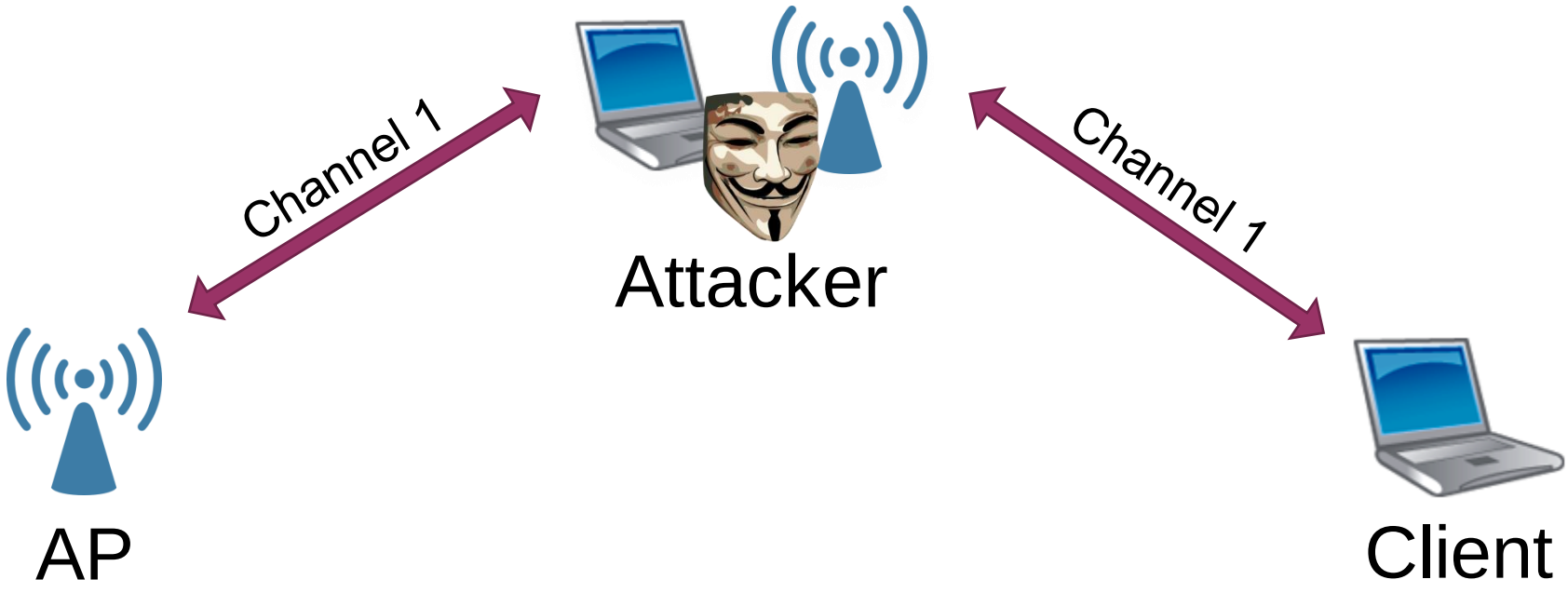
Strawman: different MAC

Cloned MAC addresses different from target?

Handshake verifies MAC addresses and fails.

Strawman: different MAC

Same MAC addresses (as AP and client)?



Strawman: different MAC

Same MAC addresses (as AP and client)?

AP and client directly communicate.

Solution: channel-based

Same addresses, rouge AP on different channel

Handshake will succeed

→ Intercept traffic!

Example 1: attacking TKIP

- It would allow us to attack TKIP.
- But why research TKIP? Isn't it dead?

Example 1: attacking TKIP

- It would allow us to attack TKIP.
- But why research TKIP? Isn't it dead?

Example 1: attacking TKIP

- It would allow us to attack TKIP.
- But why research TKIP? Isn't it dead?

WEP	TKIP	AES-CCMP
Not used	~~Not used?~~	Mainly used
	Used!!	

Why research TKIP?

Network can allow both TKIP and CCMP:

- New devices uses CCMP
- Old devices uses TKIP

} **Unicast** traffic

Broadcast traffic:

- Old devices must be able to decrypt it …

Why research TKIP?

If a network supports TKIP, all broadcast traffic is encrypted using it.

TKIP Usage (2014)

Found ~6000 networks

7% support *only* TKIP

67% support TKIP

TKIP is still widely used!

Quick Background

How are packets sent/received?

1. Add Message Integrity Check (**MIC**)
2. Encrypt using RC4

Bad! See rc4nomore.com

MIC Countermeasures

If decrypted, reveals MIC key.

If (two MIC failures within a minute)
AP halts all traffic for 1 minute

Client sends MIC failure report to AP

MIC Countermeasures

If decrypted, reveals MIC key.

If (two MIC failures within a minute)
AP halts all traffic for 1 minute

Client sends MIC failure report to AP

Abuse to decrypt last byte(s) [3]

TKIP Group Cipher

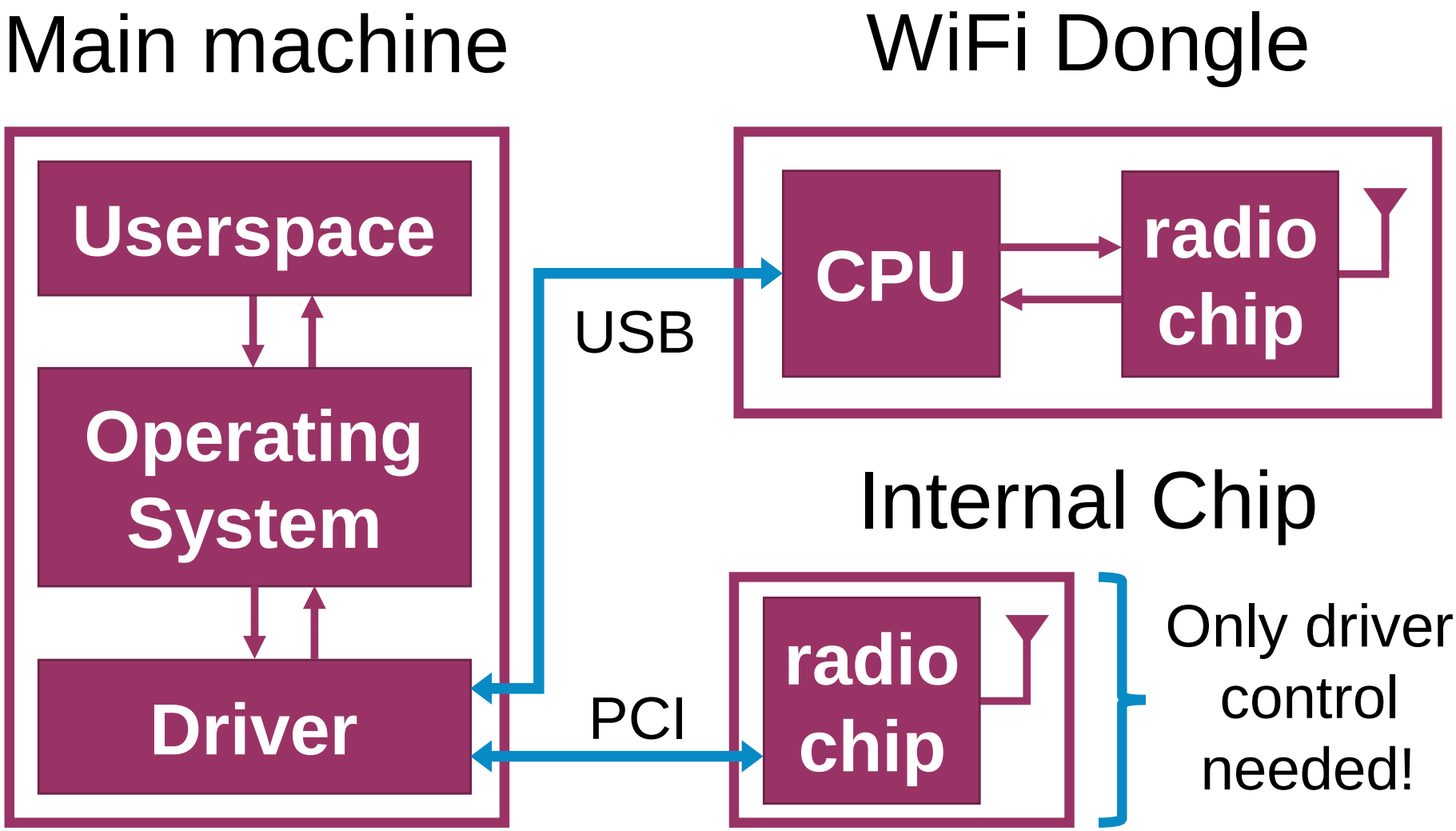
For broadcast, all clients send a MIC failure.

- Use channel-based MiTM and drop them
- Avoids MIC countermeasures

Resulting attack

- Can obtain MIC key within 7 minutes.
- Inject & decrypt some packets [3,4]
- ***Only* allow AES-CCMP!**

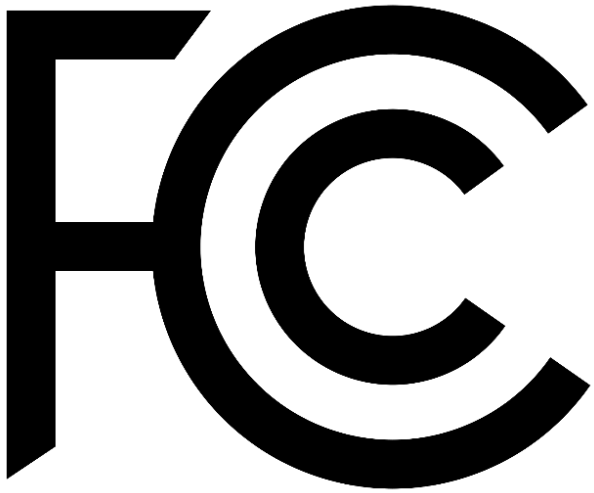
Firmware vs. driver



FCC Security Proposal

How to mitigate low-layer attacks?

- Secure either hardware or software



Relevant FCC proposal:
"only software that has been approved with a particular radio can be loaded into that radio"

→ Device will only run signed software

Goal: prevent interference

Weather radar example:

- Operate in 5 GHz band
- WiFi can interfere with them
- FCC had to deal with several cases of intentional interference

Software control of frequency, transmit power,…

- Prevent operation outside allowed ranges

Reason for concern

The proposed rule is too strict

- Requires signed software, no alternatives
- No definition of “radio” or “device” is given!

Better proposal:

- “implement security features so the device **never operates outside radio parameters for which the device was certified**”

→ Unclear how to best prevent our attacks …

… cheap triangulators??

Reason for concern

The proposed rule is too strict

- Requires signed software, no alternatives
- No definition of “radio” or “device” is given!

See “A case for open radio firmware”

Better proposal:

- “implement security features so the device **never operates outside radio parameters for which the device was certified**”

→ Unclear how to best prevent our attacks …

… cheap triangulators??

@vanhoefm

modwifi.bitbucket.com

Questions?

DistriNet
iMinds
KU LEUVEN

References

1. M. Raya, J.-P. Hubaux, and I. Aad. DOMINO: a system to detect greedy behavior in EEE 802.11 hotspots. In MobiSys, 2004.
2. A. Cassola, W. Robertson, E. Kirda, and G. Noubir. A practical, targeted, and stealthy attack against wpa enterprise authentication. In NDSS, Apr. 2013.
3. M. Vanhoef and F. Piessens. Practical verification of wpa-tkip vulnerabilities. In ASIACCS, 2013.
4. M. Vanhoef and F. Piessens. Advanced Wi-Fi attacks using commodity hardware. In ACSAC, 2014.
5. J. Robertson and M. Riley. Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar. In Bloomberg, 2014.
6. C. Cox. Hi-tech car thieves hit the streets with £30 jamming devices bought over the internet. In Manchester Evening News, 2014.

References

7. C. Arthur. Car thieves using GPS 'jammers'. In The Guardian, 2010.
8. J. Weiner. High-tech thieves used phone-jammer in $74k sunglass heist, cops say. In Orlando Sentinel, 2011.
9. P. Dandumont. Don’t trust geolocation! Retrieved 5 October, 2015, from journaldulapin.com/2013/08/26/dont-trust-geolocation/
10. Gollakota et al. They can hear your heartbeats: non-invasive security for implantable medical devices. In SIGCOMM, 2011.