Advanced WiFi Attacks Using Commodity Hardware

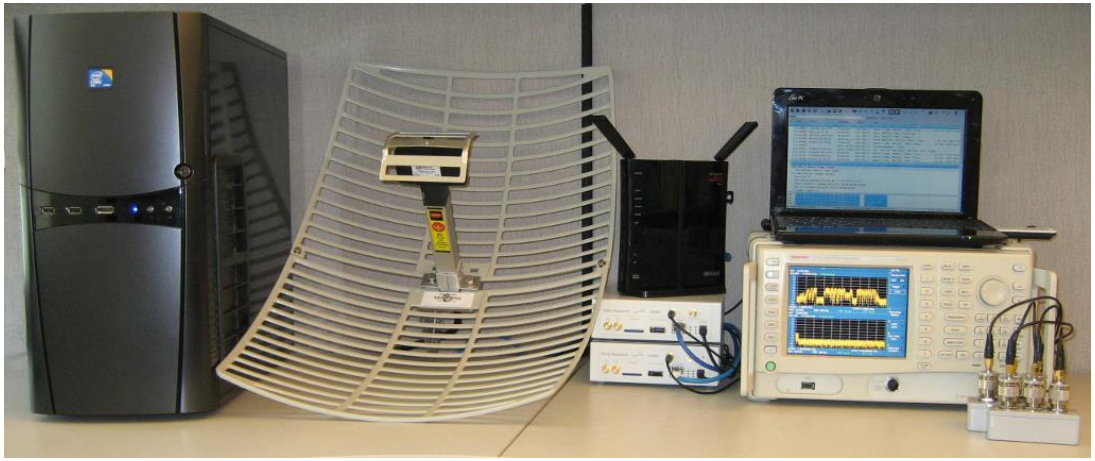
Mathy Vanhoef and Frank Piessens (KU Leuven)

ACSAC 2014

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)

Our Contributions

A small 15$ USB allows:

- Study of selfish behavior
- Continuous & selective jamming
- Reliable manipulation of encrypted traffic

Selfish Behavior

Implement & study selfish behavior

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

Countermeasure

DOMINO defense system [MobiSys ‘04] detects this selfish behavior.

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.

Result:

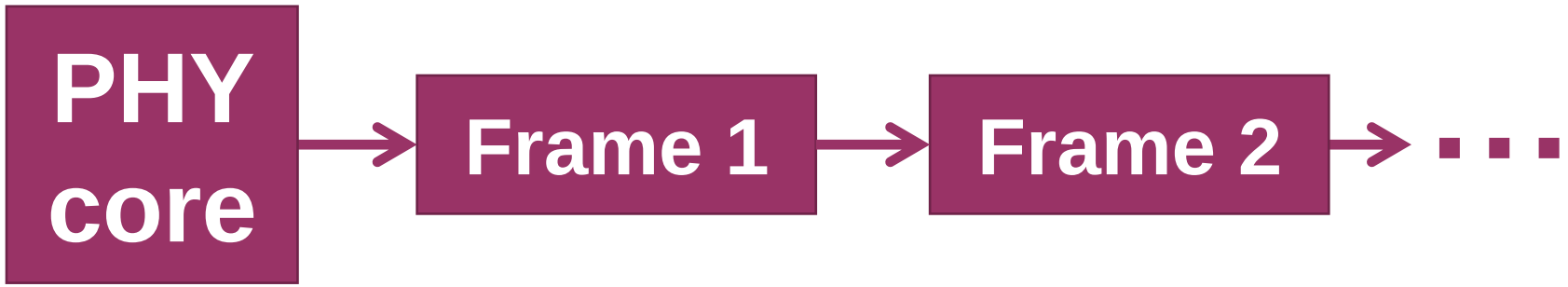
- Selfish clients will **lower** their bitrate to beat other selfish stations!
- Until this gives no more gain.

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:

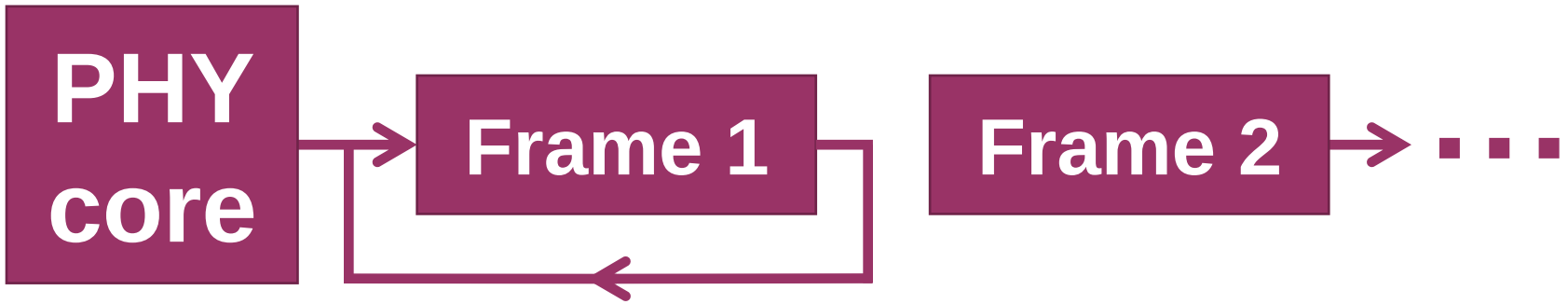


Continuous Jammer

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

- No packets visible in monitor mode!
- Other devices are **silenced**.

Default antenna gives range of ~80 meters.

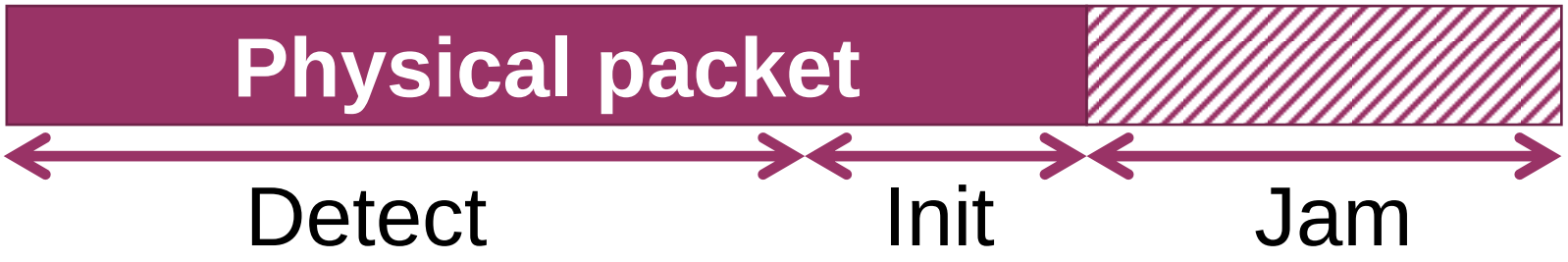
Amplifier gives range of ~120 meters

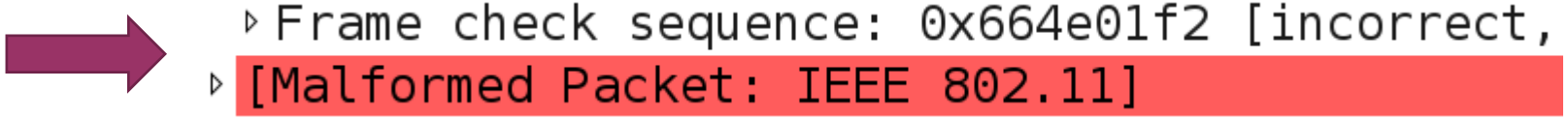
Selective Jammer

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

How does it work?

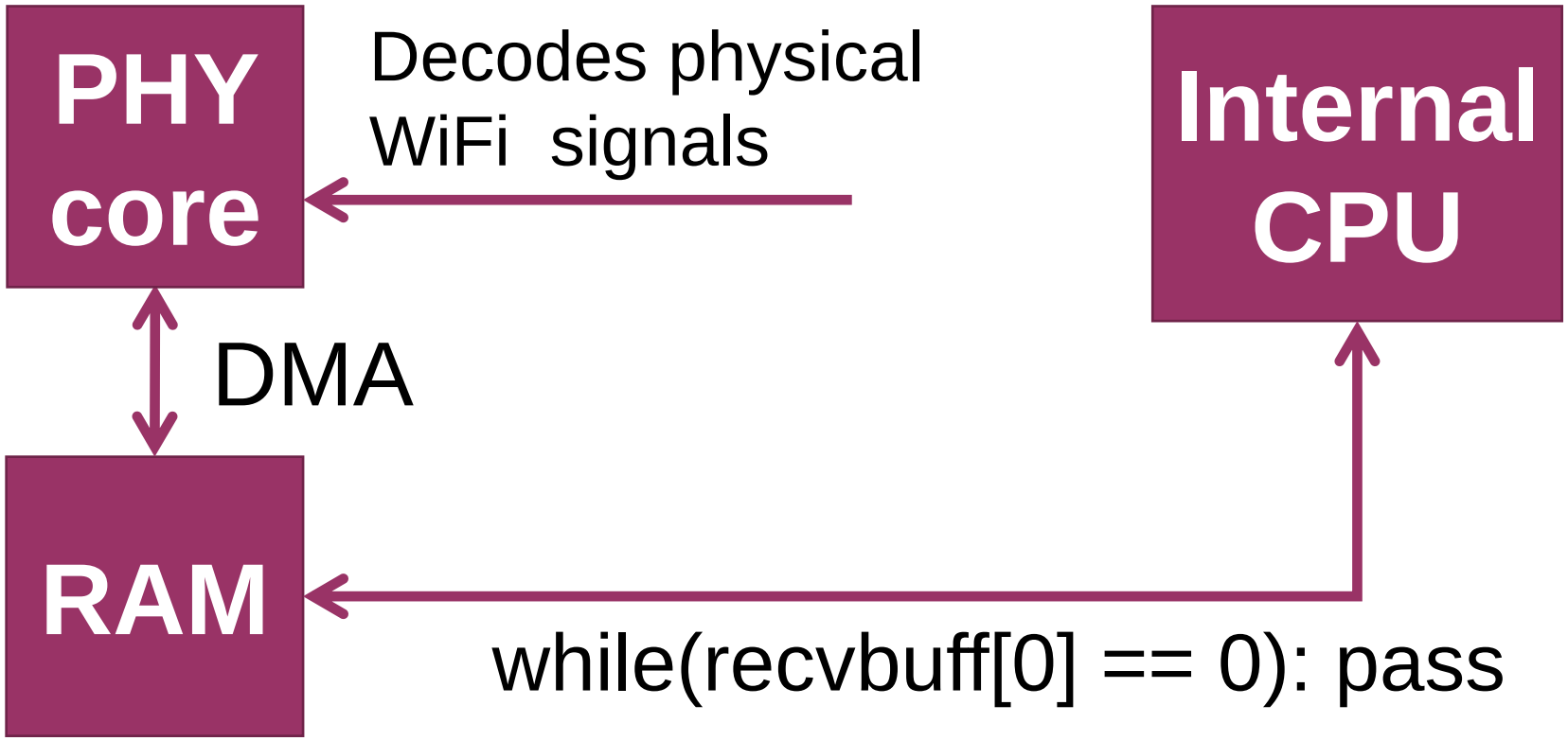
1. **Detect and decode header** } **Hard**
2. Abort receiving current frame } Easy
3. Inject dummy packet





DistriNet
iMinds KU LEUVEN

Detecting frame headers?



→ Can read header of frames still in the air.

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!

Countermeasures

DOMINO defense system [MobiSys '04]:

- 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.

Impact on higher-layers

What about higher-layer protocols?

Impact on higher-layers

What if we could reliably manipulate encrypted traffic?

Impact on higher-layers

What if we could reliably manipulate encrypted traffic?

not decrypt!

We could attack TKIP!

Reliably Intercepting Traffic!

Channel-based MiTM attack

- Works against encrypted networks
- Can **reliably** manipulate encrypted traffic.

Reliably Intercepting Traffic?

Create rogue AP with MAC address …

- ≠ AP → handshake fails
- = AP → devices communicate directly

Same MAC address but **different channel**

- We forward frames between channels
- Handshake OK, all traffic via rogue AP
- Jammers will force clients to our rogue AP

Example: attacking TKIP

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

Example: 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 TKIP.

TKIP Usage (2014)

Found ~6000 networks

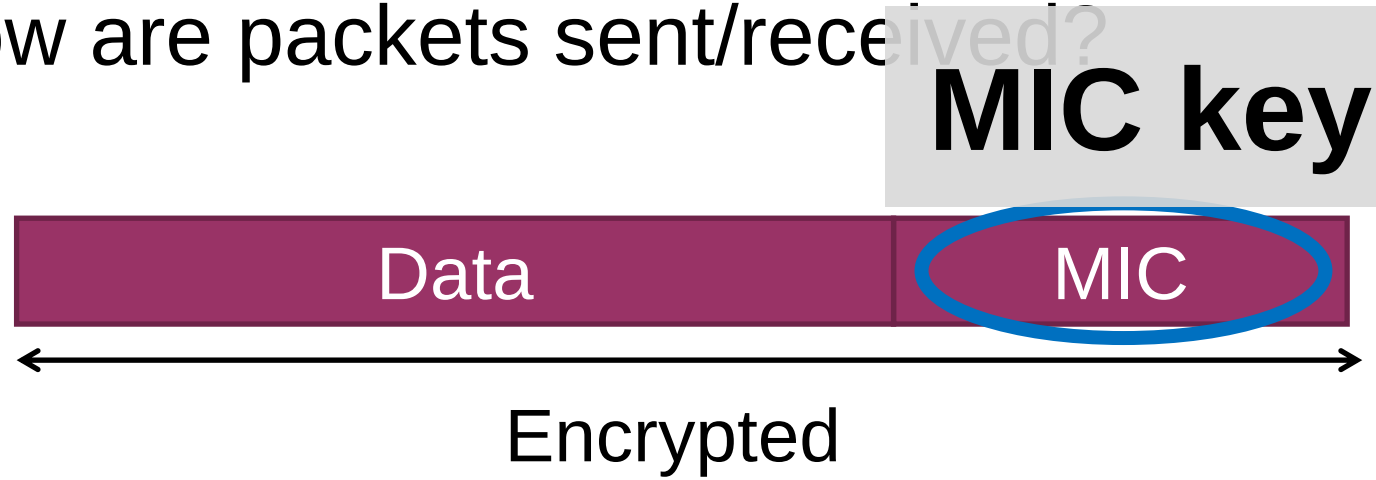
7% support *only* TKIP

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

MIC Countermeasures

If decrypted, reveals MIC key.

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

Oracle to decrypt last byte [WiSec '09]

TKIP Group Cipher

For broadcast, all clients send a MIC failure.

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

Results

- Can obtain MIC key within 7 minutes.
- Inject/decrypt some packets [AsiaCCS ‘13]
- **Use *only* AES-CCMP!**

Questions?