Operating Channel Validation

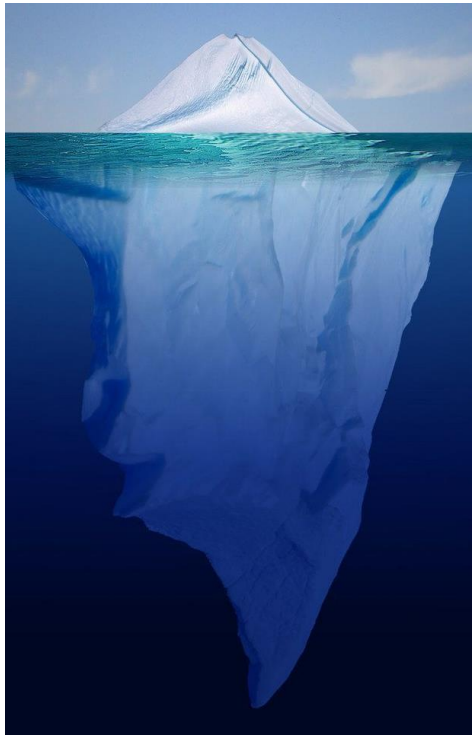
M. Vanhoef[1], N. Bhandaru[2], T. Derham[2], I. Ouzieli[3], F. Piessens[1]

[1] KU Leuven – [2] Broadcom – [3] Intel

WiSec, Stockholm (Sweden), 18 June 2018

KU LEUVEN DistriNet

Contributions

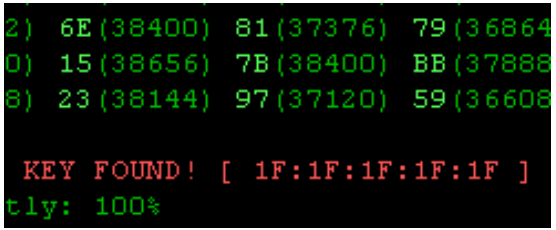


Paper: attacks & high-level defense

Specification: text for inclusion in 802.11

Implementation: modified hostap

Old attacks don’t need Man-in-the-Middle (MitM)



Breaking WEP

Dictionary attacks

Breaking WPS

Rogue APs

New attacks do require MitM

Traffic Analysis

- **Capture all** encrypted frames
- **Block** certain encrypted frames

Attacking broadcast TKIP

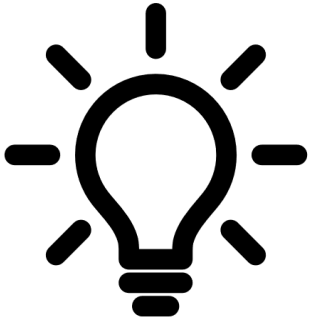
- **Block** MIC failures
- **Modify** encrypted frames

ChopChop

New attacks do require MitM

Exploit implementation bugs

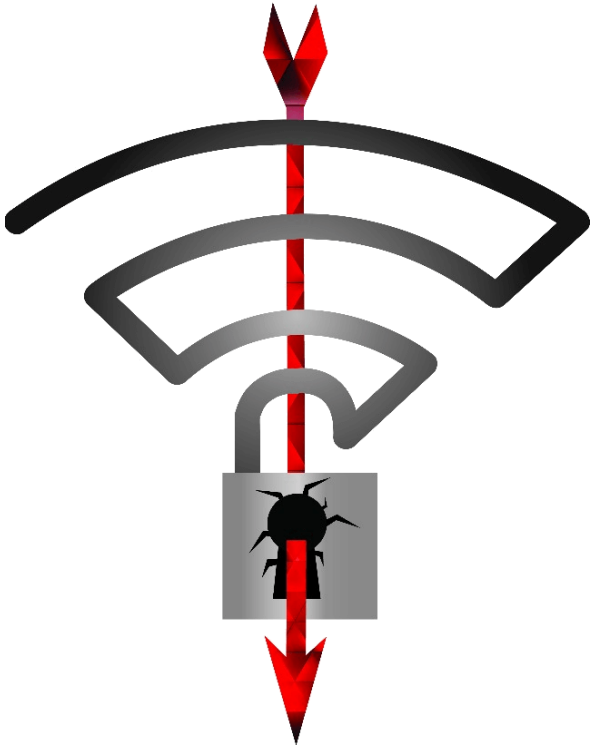
- **Block** certain handshake messages
- E.g. bugs in 4-way handshake



New attack scenarios

- See paper for details
- E.g. **modify** advertised capabilities

The elephant in the room



Key Reinstallation Attacks (KRACKs)

- **Block & delay** handshake frames
- E.g. 4-way & group handshake

Not all KRACKs require MitM

- E.g. FT handshake (802.11r)

Obtaining multi-channel MitM

Clone AP on **different channel!**

Handshake succeeds &
can reliably manipulate frames!

Force client on rogue channel?

Jam channel of real AP

- Victim will connect on rogue AP
- Stop jamming when client connects

We found an easier way while making the defense!

- **Abuse channel switch announcements**

Channel Switch Announcements (CSAs)

Background:

- AP may dynamically switch channels
- E.g. when radar pulses are detected
- Sends CSAs to connected clients
- **Clients switch to new channel in CSA**

Adversary can forge CSAs

- **Abuse to switch victim to rogue channel!**

Can we prevent MitMs?

Threat model

- Focus on verifying channel and bandwidth
- We exclude low-layer attacks such as beamforming

Goal is to make attacks harder, not impossible!

Similar to the idea of stack canaries.

Proposed Defense

Verify operating channel when connecting to a network

- E.g. in the 4-way and FT handshake

Also verify channel in

- WNM-Sleep exit frames: avoid tricky edge cases
- Group key handshake: defense in depth

Encoding the current channel

Operating Channel Information **(OCI) element:**

Operating class	Channel number	Segment index 1

1. Operating class: defines the bandwidth
2. Channel number: defines primary channel
   - Together this also defines the central frequency
3. Seg idx 1: for 80+80 MHz channels

Problem: Channel Switch Announcements (CSAs)

Unauthenticated CSAs

› Need to verify securely

Authenticated CSAs

› May not arrive → need to verify reception!

Solution: authenticate CSA using SA query

Limitations

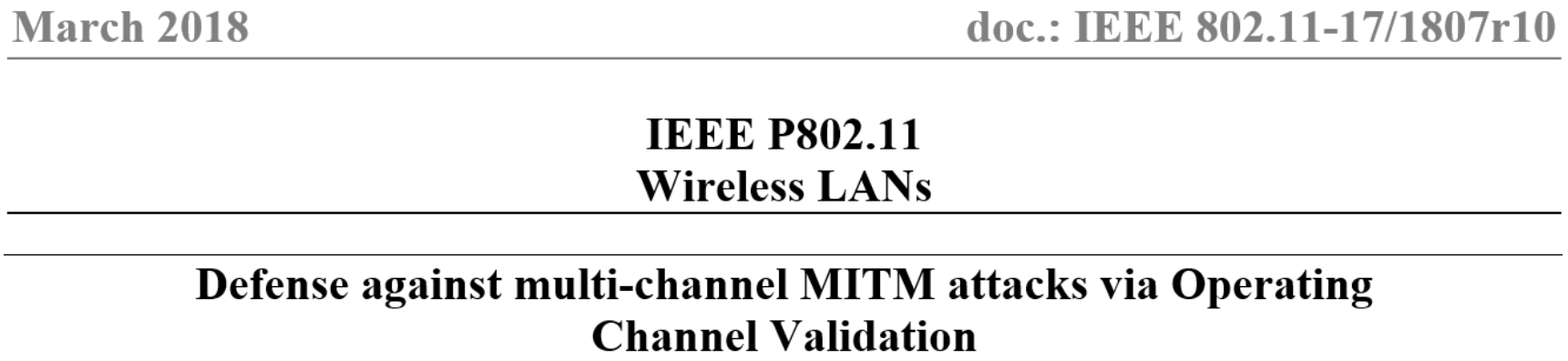
Other (partial) MitM attacks still possible:

- Partial MitM when client didn’t receive CSA
- Adversary can act as repeater
- Other physical-layer tricks

So why use this defense?

- **Remaining attacks are harder & not always possible**
- Straightforward to implement

Standardization efforts



March 2018 doc.: IEEE 802.11-17/1807r10

IEEE P802.11
Wireless LANs

Defense against multi-channel MITM attacks via Operating Channel Validation

- Detailed technical specification
- **Has extra discussions not present in paper!**
- Hopefully ratified soon ☺

Proof-of-concept

github.com/vanhoefm/hostap-channel-validation

- Code for 4-way handshake
- Other handshakes in progress

Some remarks:

- Has many automated tests!
- Kernel may change bandwidth

Conclusion

› Easy MitM with channel switches

› We prevent multi-channel MitM

› Other MitM still possible

› Being standardized!

Thank you!

Questions?