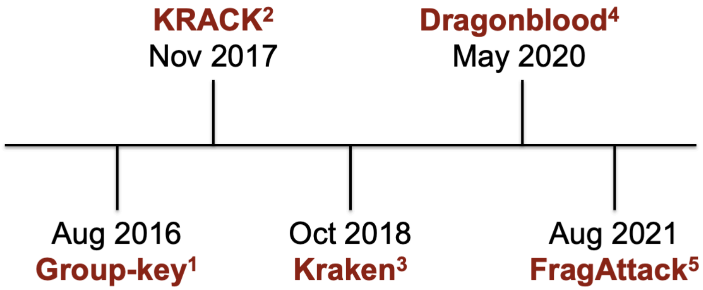
Systematically Analyzing Vulnerabilities in the Connection Establishment Phase of Wi-Fi Systems

Naureen Hoque, Hanif Rahbari, and Cullen Rezendes
Golisano College of Computing and Information Sciences
Rochester Institute of Technology (RIT), NY

IEEE Conference on Communications and Network Security (CNS)
3–5 October 2022

Connection Establishment Phase

- ❑ Currently not protected
    - ❑ Pre-authentication phase → infeasible to protect by WPA2/3
    - ❑ Exploited by several compound attacks
        - ❑ *Multi-channel man-in-the-middle (MitM)*



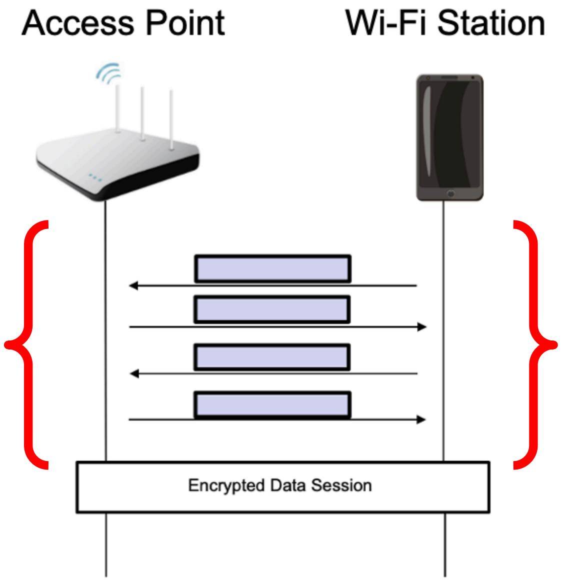
KRACK[2]
Nov 2017

Dragonblood[4]
May 2020

Aug 2016
Group-key[1]

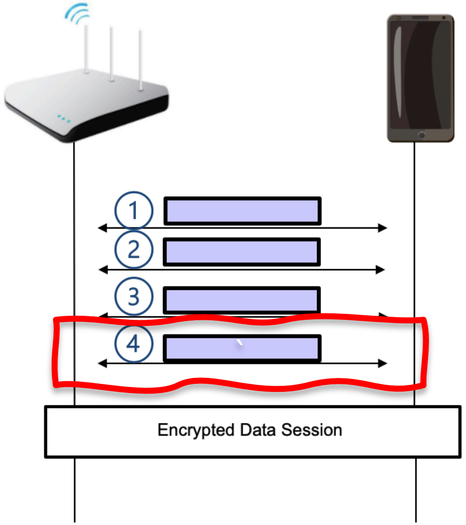
Oct 2018
Kraken[3]

Aug 2021
FragAttack[5]

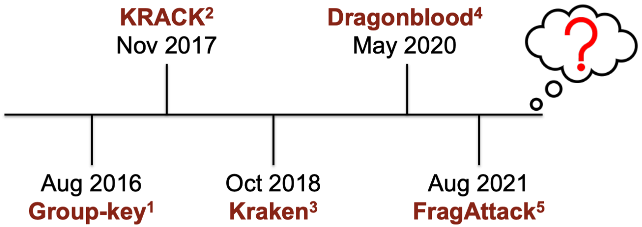


Possibility of More Attacks?

- □ Connection establishment (CE) phase
  - □ Formal analysis by Cremers *et al.*[6]
    - □ 4-way handshake and session key
    - □ Concluded no vulnerability beyond KRACK
    - □ Could not capture Multi-channel MitM
- □ Our contribution: Formal analysis of CE



① Network discovery
② Authentication & association
③ (EAP authentication)
④ 4-way handshake



KRACK[2]
Nov 2017

Dragonblood[4]
May 2020

Aug 2016
Group-key[1]

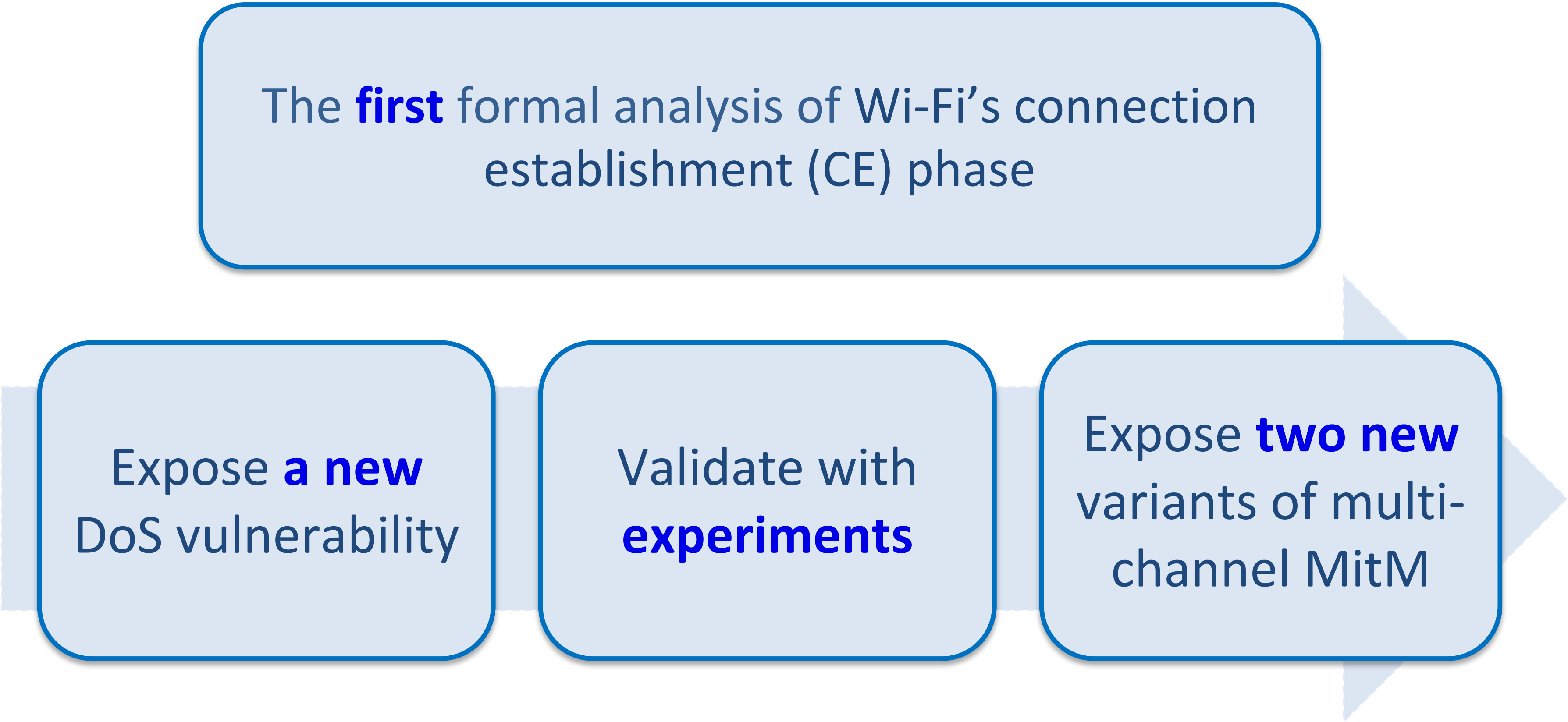
Oct 2018
Kraken[3]

Aug 2021
FragAttack[5]

?

[6] C. Cremers *et al*. A formal analysis of IEEE 802.11's WPA2: Countering the kracks caused by cracking the counters. USENIX Security Symposium, 2020.

Our Contributions



The **first** formal analysis of Wi-Fi’s connection establishment (CE) phase

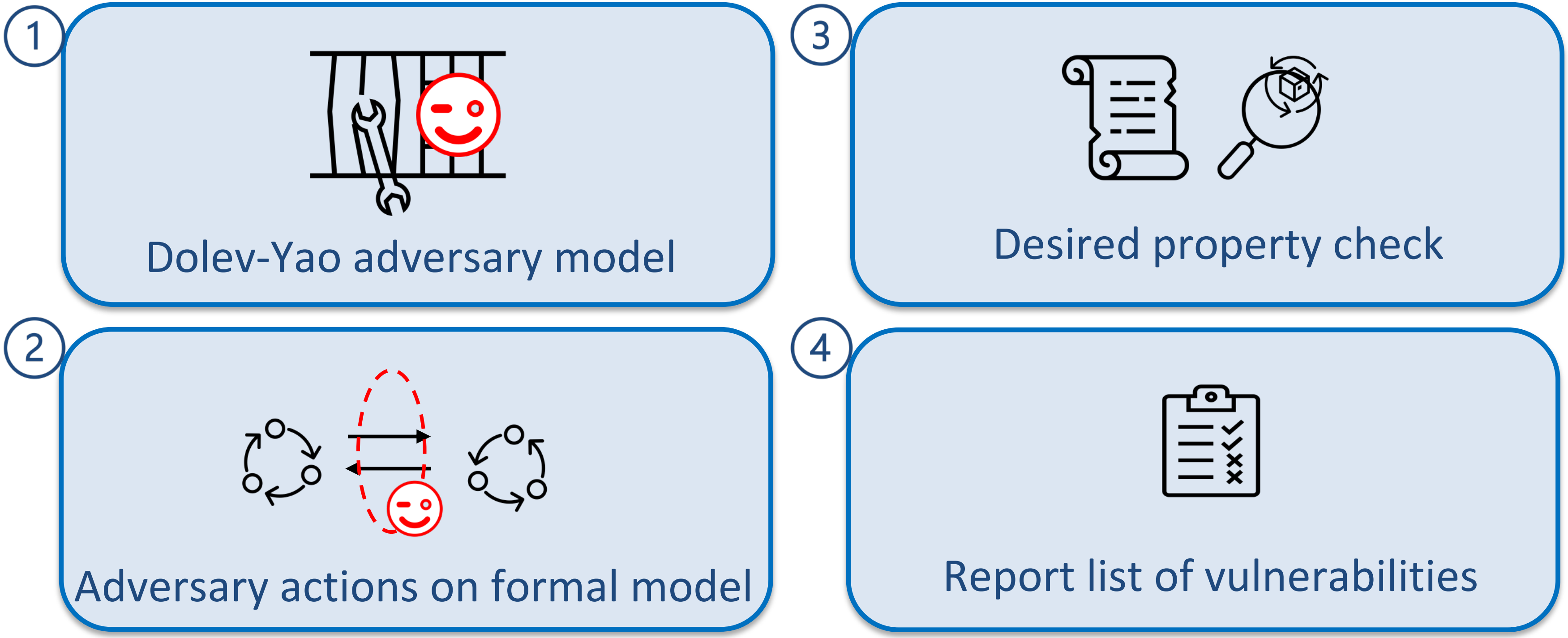
Expose **a new** DoS vulnerability

Validate with **experiments**

Expose **two new** variants of multi-channel MitM

Formal Analysis of CE

- ❑ Based on IEEE 802.11-2020 rollup
  - ❑ IEEE 802.11ax (2021) does not amend the CE components



1 Dolev-Yao adversary model

2 Adversary actions on formal model

3 Desired property check

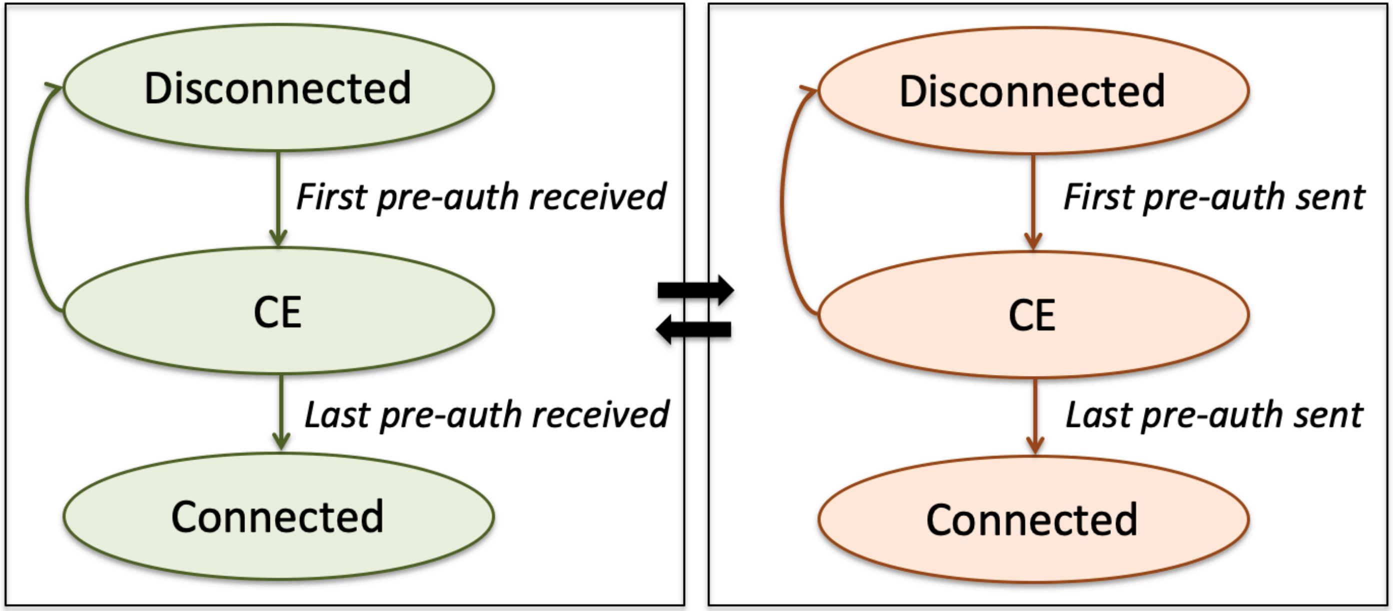
4 Report list of vulnerabilities

Threat Model

- *Dolev-Yao* adversary model
  - Can eavesdrop, drop, inject, and modify
  - Cannot encrypt/decrypt
- System model
  - Personal, enterprise, and public Wi-Fi systems
  - Assume latest security protocol
    - WPA3 or WPA2+802.11w
    - 802.11w: Management frame protection, mandatory in WPA3
  - Model the optional mechanisms in IEEE 802.11-2020 rollup separately

Simplified CE Model

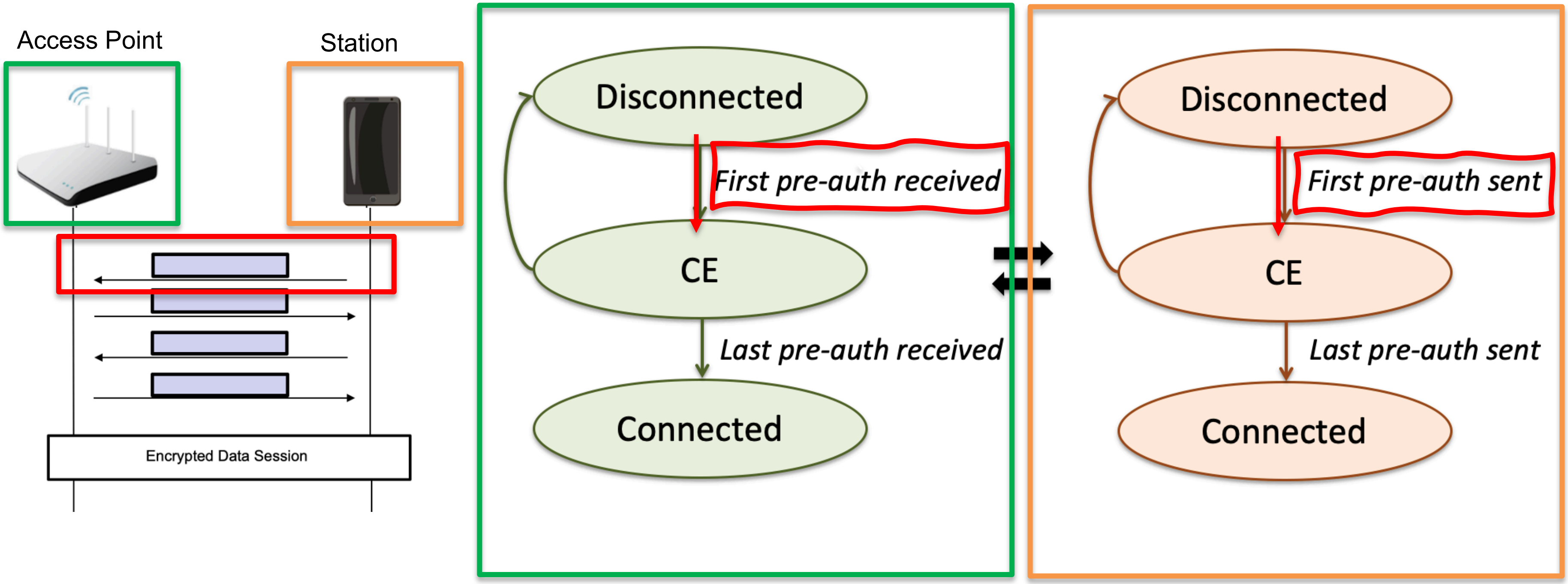
- ❑ Implemented in *NuSMV* model checker



AP’s FSM Station’s FSM

Our more detailed model can be found in the paper.

Interaction between FSMs



Property to Check

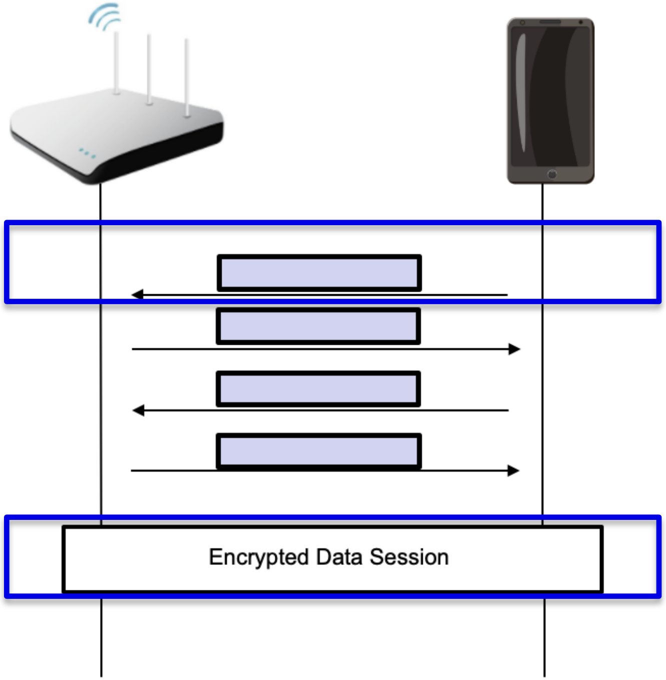
(1) It is always the case that a station and an AP will eventually move to the connected state *(checks for DoS vulnerability),*

and

(2) There does not exist a case when they connect to each other over two different channels *(checks for multi-channel MitM)*

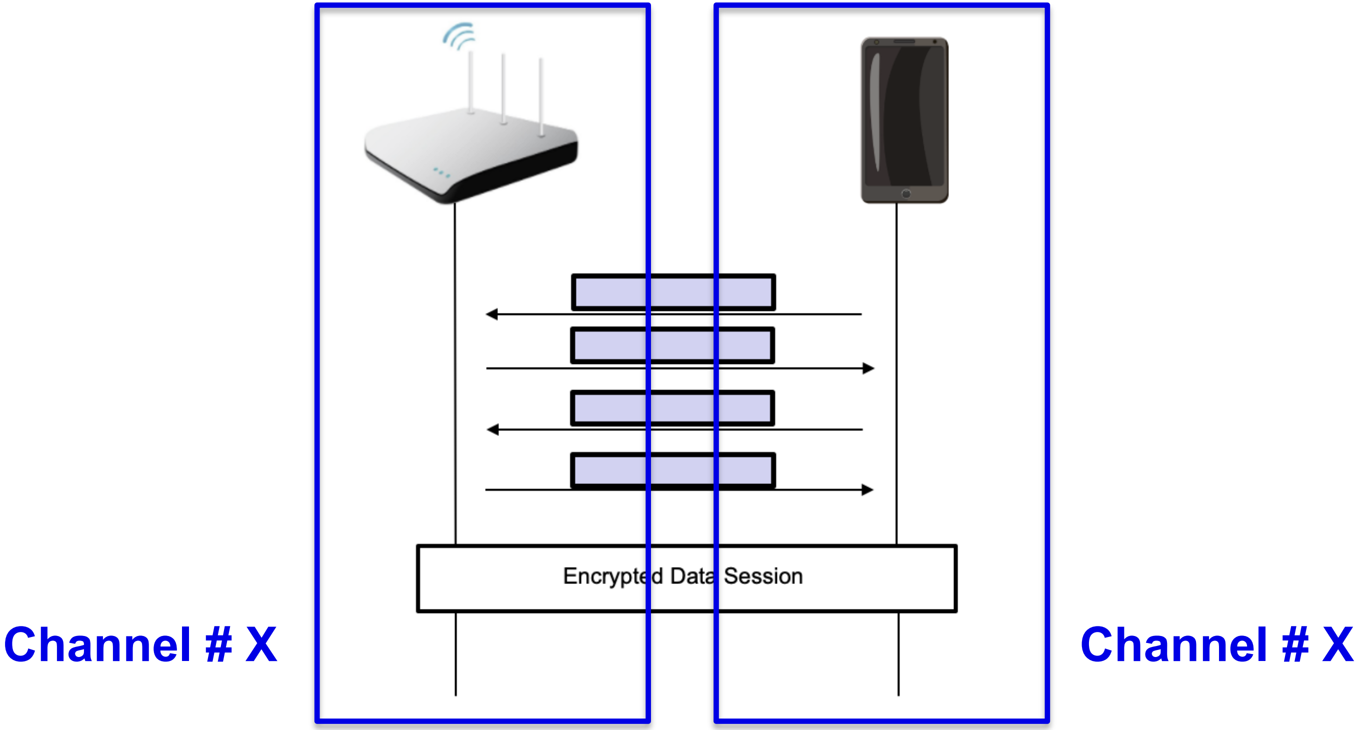
Property to Check

(1) It is always the case that a station and an AP will eventually move to the connected state



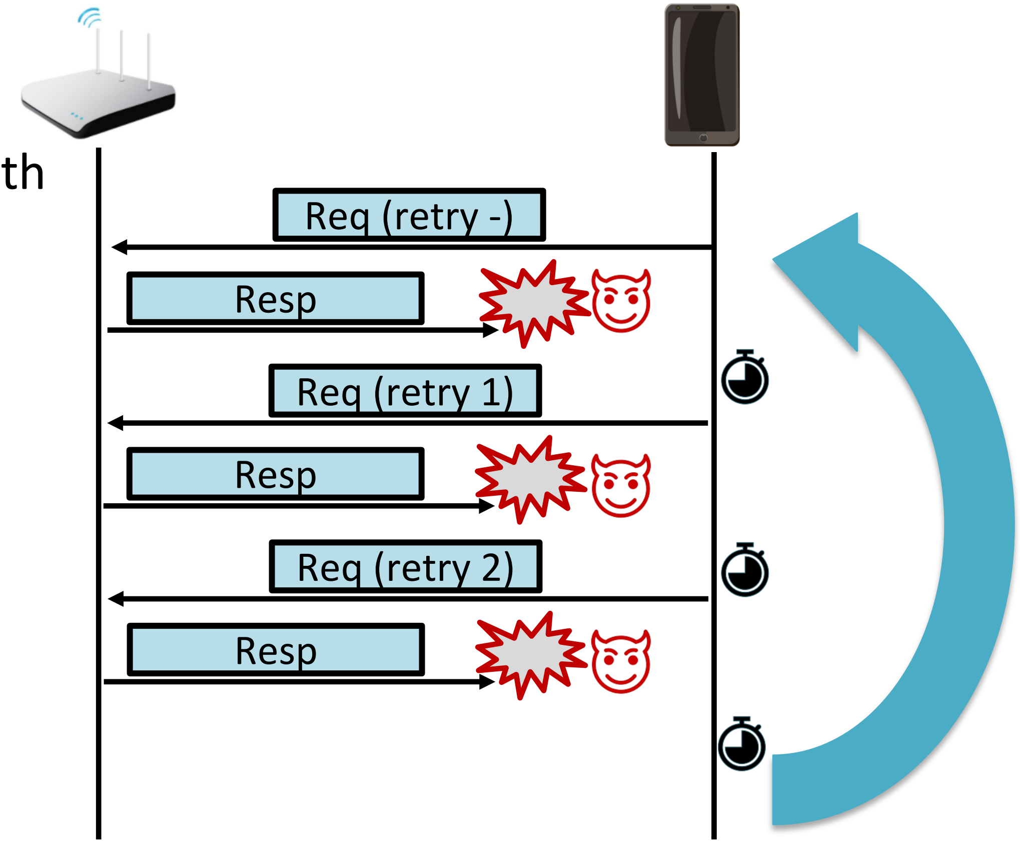
Property to Check

(2) There does not exist a case when they connect to each other over two different channels



Formal Analysis – New DoS Finding

- ❑ Continuous resetting
    - ❑ Exhaust retransmissions
    - ❑ Same AP, same signal strength
- ❑ Potential consequences
    - ❑ Denial-of-service
    - ❑ Battery depletion
    - ❑ User frustration
        - ❑ Can end up connecting with a rogue AP

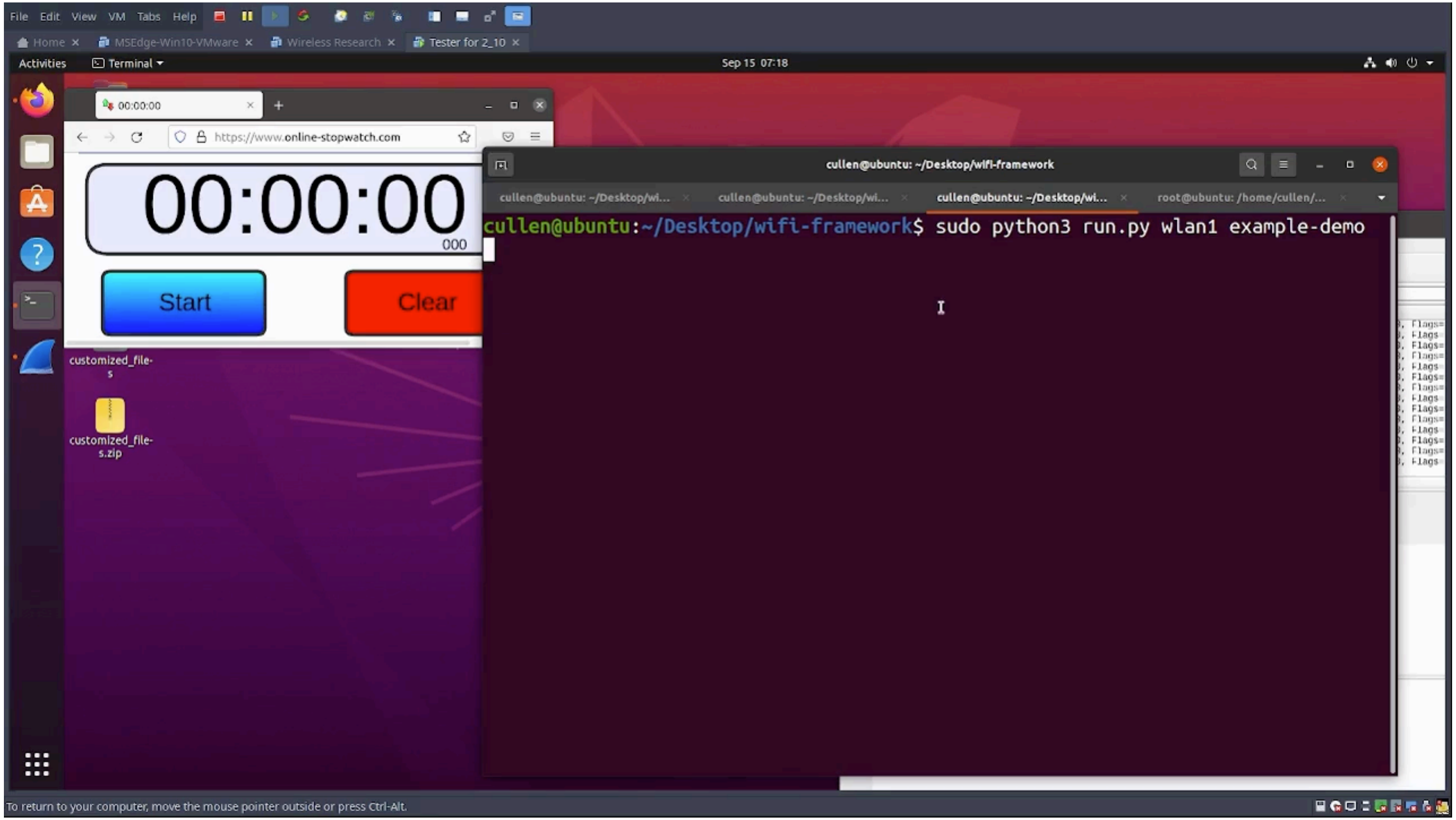


Experimental Validation

- ❑ Based on *hostapd* and *wpa_supplicant* (latest 2022 update)
  - ❑ Wi-Fi framework[7]
- ❑ WPA3-Personal
- ❑ Experimental scenario
  - ❑ Blocking pre-authentication frame sent by AP
  - ❑ Observe behavior at the station
- ❑ Responsible and timely disclosure to Wi-Fi Alliance

[7] D. Schepers *et al*. A framework to test and Fuzz Wi-Fi devices. In Proc. of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec). 2021.

Demonstration

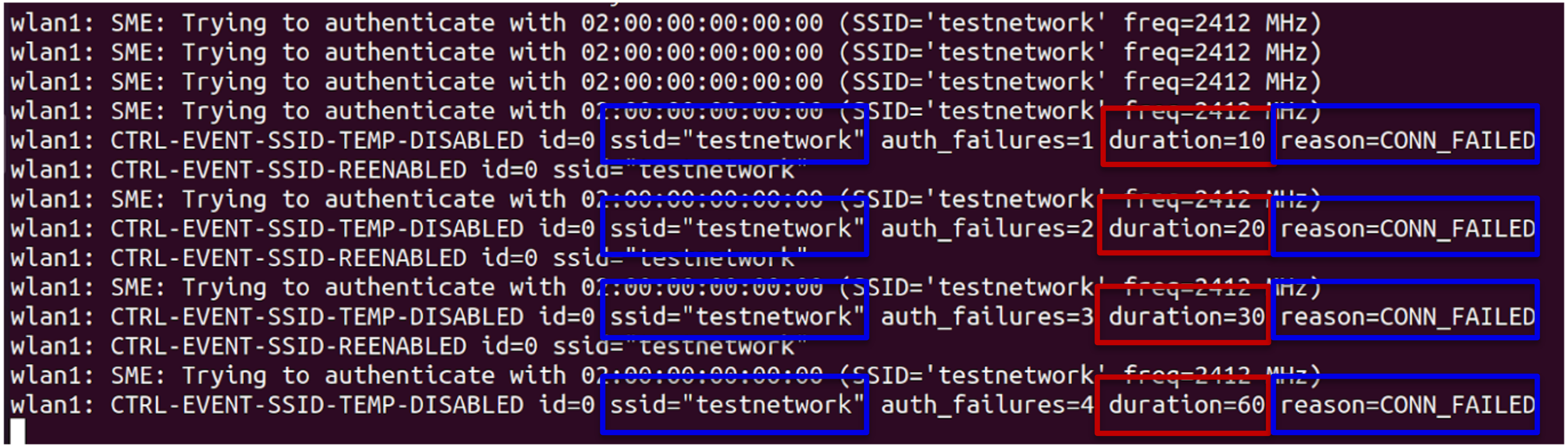

File Edit View VM Tabs Help
Home
MSEdge-Win10-VMware
Wireless Research
Tester for 2_10
Activities
Terminal
Sep 15 07:18
00:00:00
https://www.online-stopwatch.com
00:00:00
000
Start
Clear
customized_files
customized_files.zip
cullen@ubuntu: ~/Desktop/wifi-framework
cullen@ubuntu: ~/Desktop/wi...
cullen@ubuntu: ~/Desktop/wi...
cullen@ubuntu: ~/Desktop/wi...
root@ubuntu: /home/cullen/...

```
cullen@ubuntu:~/Desktop/wifi-framework$ sudo python3 run.py wlan1 example-demo
```

To return to your computer, move the mouse pointer outside or press Ctrl-Alt.

Experimental Result

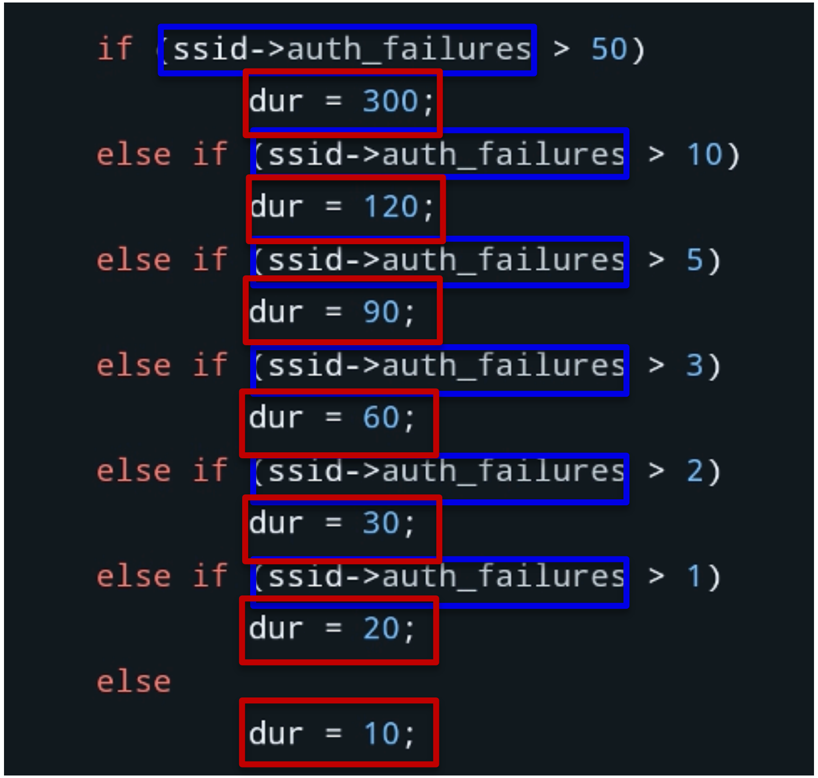
- ❑ DoS vulnerability validated
  - ❑ Continuous resetting with the same AP
- ❑ Duration (?)



```
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: CTRL-EVENT-SSID-TEMP-DISABLED id=0 ssid="testnetwork" auth_failures=1 duration=10 reason=CONN_FAILED
wlan1: CTRL-EVENT-SSID-REENABLED id=0 ssid="testnetwork"
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: CTRL-EVENT-SSID-TEMP-DISABLED id=0 ssid="testnetwork" auth_failures=2 duration=20 reason=CONN_FAILED
wlan1: CTRL-EVENT-SSID-REENABLED id=0 ssid="testnetwork"
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: CTRL-EVENT-SSID-TEMP-DISABLED id=0 ssid="testnetwork" auth_failures=3 duration=30 reason=CONN_FAILED
wlan1: CTRL-EVENT-SSID-REENABLED id=0 ssid="testnetwork"
wlan1: SME: Trying to authenticate with 02:00:00:00:00:00 (SSID='testnetwork' freq=2412 MHz)
wlan1: CTRL-EVENT-SSID-TEMP-DISABLED id=0 ssid="testnetwork" auth_failures=4 duration=60 reason=CONN_FAILED
```

Code Snippet - *wpa_supplicant*

- ❑ *wpa_supplicant*
  - ❑ Retransmission limit exhaust
    - ❑ One failure
  - ❑ Defines a delay between resets
  - ❑ Documentation – unexplained
  - ❑ Conjecture – waiting time for better channel condition, etc.
  - ❑ Problem? – known and accumulated delay



```
if (ssid->auth_failures > 50)
        dur = 300;
else if (ssid->auth_failures > 10)
        dur = 120;
else if (ssid->auth_failures > 5)
        dur = 90;
else if (ssid->auth_failures > 3)
        dur = 60;
else if (ssid->auth_failures > 2)
        dur = 30;
else if (ssid->auth_failures > 1)
        dur = 20;
else
        dur = 10;
```

Failures and Accumulated Delay

Number of failures (num_f)	Delay between retries (t_d)	Accumulated delay (sec)
1	10	10
2	20	30
3	30	60
$4\ or\ 5$	60	$120\ (num_f = 4)$
$5 < num_f \leq 10$	90	$270\ (num_f = 6)$
$10 < num_f \leq 50$	120	$750\ (num_f = 11)$
$num_f > 51$	300	$\boxed{5370}\ (num_f = 51)$

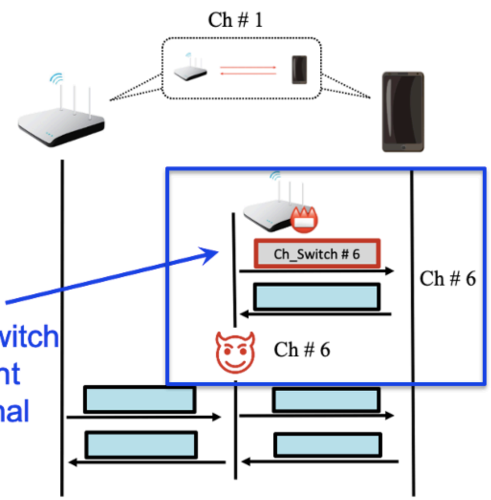
~ 90 minutes!!

Possible Mitigation Technique

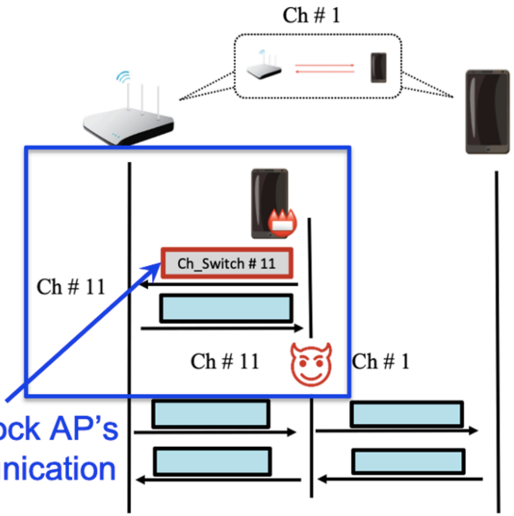
- ❑ The problem: Fixed delay values
  - ❑ Long (and fixed) waiting time between retries
  - ❑ Predictable to an adversary
  - ❑ Allows selectively and stealthily activate DoS
- ❑ Mitigation: Random delay values
  - ❑ Between 5 and 60 seconds
  - ❑ Reduces the accumulated delay
  - ❑ Forces costly (consistent) jamming

Formal Analysis – MitM Finding

- ❑ Multi-channel MitM
  - ❑ Three variants (two new)
    - ❑ (1) Target: station, (2) Target: AP, and (3) Target: both



1. Channel switch announcement
2. Higher signal strength

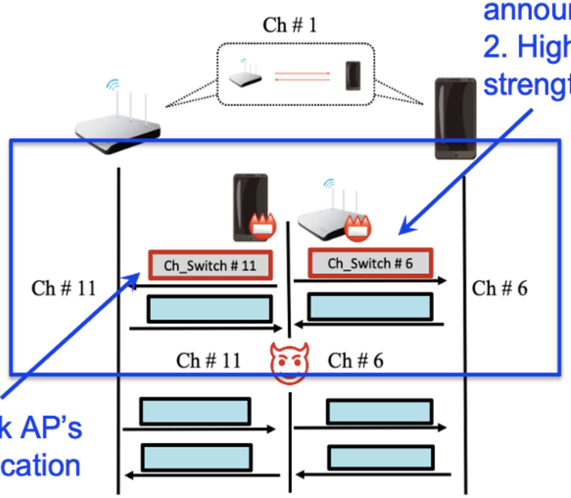


Jam/block AP's communication

New variant # 1

Formal Analysis – MitM Finding

- ❑ Multi-channel MitM
  - ❑ Three variants (two new)
    - ❑ (1) Target: station, (2) Target: AP, and (3) Target: both



1. Channel switch announcement
2. Higher signal strength

Jam/block AP's communication

New variant # 2

Conclusion & Future Work

- ❑ Existing formal analysis efforts
  - ❑ 4-way handshake
  - ❑ But not CE/pre-authentication phase
- ❑ Findings
  - ❑ One new DOS vulnerability
    - ❑ 90-minutes with additional 5-minute
  - ❑ Two new variants of multi-channel MitM
- ❑ Future work

References

[1] M. Vanhoef and F. Piessens, “Predicting, decrypting, and abusing WPA2/802.11 group keys”. in USENIX Security Symposium, 2016.

[2] M. Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proc. of the ACM Conference on Computer and Communications Security (CCS), 2017.

[3] M. Vanhoef and F. Piessens. Release the Kraken: New KRACKs in the 802.11 Standard. In Proc. of the ACM Conference on Computer and Communication Security (CCS), 2018.

[4] M. Vanhoef and Eyal Ronen. Dragonblood: analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In Proc. of the IEEE Symposium on Security & Privacy (S&P), 2020.

[5] M. Vanhoef. Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. In USENIX Security Symposium, 2021.

[6] C. Cremers. A formal analysis of IEEE 802.11’s WPA2: Countering the kracks caused by cracking the counters. In USENIX Security Symposium, 2020.

[7] D. Schepers, M. Vanhoef, and A. Ranganathan, “A framework to test and Fuzz Wi-Fi devices,” In Proc. of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec). 2021.

Questions..?

https://www.rit.edu/wisplab/

GitHub Link: