"Analysis of Insecure Wireless Authentication Practices in Rwandan Enterprises & Institutions"

Prepared by: Jean René MUNYESHYAKA, Software Engineer, System Administrator and Cybersecurity Enthusiast

Our mission is not to provide a step-by-step guide on securing your network, but rather to expose the vulnerabilities within your system. These weaknesses span human factors (like social engineering, phishing, and spoofing awareness), technical flaws (such as misconfigured networks or weak Authentication, Authorization, and Accounting controls), and the absence of automated access monitoring. By highlighting these gaps, we empower you whether as an individual, business, or institution to assess whether you're ahead of the curve or falling behind in cybersecurity readiness.

1. Wireless security types

NONE: No Security Key is installed, highly risky 24/7 days

WEP: WEP (Wired Equivalent Protocol) was defined in 1997 in the original IEEE 802.11 specification. The first exploits were identified a few years later, around 2001. The exploits were so severe that many organizations stopped deploying WiFi networks. To address WEP's weaknesses, RSN (Robust Security Network) was added to the 802.11 specification.

WPA: WiFi Protected Access (WPA) specification was published by the WiFi Alliance in 2003, which supported the deployment of Temporal Key Integrity Protocol (TKIP).

WPA2: WiFi Protected Access Version 2 (WPA2) was published a year later and could support the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). TKIP has some known weaknesses and is not as secure as CCMP. It is an encryption protocol based on the U.S. federal government's Advanced Encryption Standard (AES) algorithm.

WPA3: WPA version 3, is the latest WiFi Alliance specification and encourages deploying these newer security features. Since WPA2 was defined 20 years ago, several security-related enhancements have been added to the 802.11 specification.

2. Main technical differences between WEP, WPA, WPA2 and WPA3

The technical differences between WEP, WPA, WPA2, and WPA3, relate to three fundamental security mechanisms:

- ✓ Encryption, which protects the confidentiality of messages transmitted over the WiFi network.
- ✓ Message integrity, which ensures that messages sent over-the-air have not been tampered with.
- ✓ Authentication, which determines if the user has permission to access the WiFi network.

3. Important Things to remember

Whatever the security key you chose (WEP, WPA, WPA2, and WPA3), you define the encryption method to be used (RSA, AES-CTR, or AES-GCM), encryption key size/bits (128, 192) , data integrity (Michel, AES-CBC-MAC, AES-GMAC), the mode (Enterprise/Personal), authentication (802.1x, Pre-Shared Key (PSK) or server-side rendering (SSR) and you also define the Protection Management Frame (not required/required). And by doing so, you increase or reduce your protection strength.

WiFi Alliance Certification Program	WPA		WPA2		WPA3	
Initialization vector (bits)	48					
Encryption Cipher	RSA		AES-CTR		AES-GCM	
					Personal	Enterprise
Encryption key size (bits)	128				128	128 or 192
Data integrity	Michael		AES-CBC-MAC		AES-GMAC	
Mode	Enterprise	Personal	Enterprise	Personal	Enterprise	Personal
Authentication	802.1X	PSK	802.1X	PSK	802.1x	SSR
Protect Management Frames					Required	

Figure1: Comparing WiFi features in WPA releases

4. Demonstration with a python script:

There are several information needed to hack a network device anonymously without being traced. We can even make more difficult to be traced and possible impossible:

- ✓ Network IP
- ✓ Default Gateway
- ✓ Mac Address
- ✓ WiFi Name
- ✓ Security Keys (WiFi Password)
- ✓ Etc

5. Possible Risks (since then, additional scripts can be performed):

Exposing your MAC address and IP address can create risks, primarily on local networks and for online privacy. A hacker could use your MAC address to impersonate your device and potentially gain access to your network, while knowing your IP address could make you vulnerable to various attacks like phishing and DDoS

If all these information are obtained (mac address, computer name, and IP), you can start spoofing a particular user and perform specific attacks if that user in disconnected. You must be sure that the device in off. You can use ping hostname/ip -t to test if the device is still connect or not.

6. Attack preparation steps:

- ✓ Socialize with a victim, make her/him believe your her/his fan/friend, be sure she/he not in from the school of ICT. Let him/her believe, you need a help, you just want to use her/his laptop to send a email or modify an urgently need file to be submitted.
- ✓ Access the laptop with administrator privileges to install VS code if not installed
- ✓ Run the two previous scripts for gathering information (don't run the attack file)
- ✓ Go back and prepare a computer for this particular purpose (spoofing attack)
- ✓ Spoof one of the existing computer: The hacking computer must advertise the spoofed IP, computer name, and mac address one of authorized users
- ✓ Chose a target or more targets

And since you have the default gateway, it is possible to scan all device Ips on the same network and then their mac address. We can also make a more complicated attack to be duplicated to any other device on the network creating meshing and bring down any device trying to access this network.

- ✓ Initiate the attack (3rd script) if and only if all steps are correct

7. Conclusion:

For window users the scripts will run only under the following command: `python script_name.py`

For Linux users the scripts will run only under the following command: `sudo python3 script_name.py`

Then we run `ls` in terminal (like Visual Studio Code) to list newly created report in the same fold as our scripts. You will notice that all available WiFi were listed in "wifi_passwords_20250428_114744.txt" file. And all shared keys for WiFi you have connected to in the passed days, are also listed in the same file. Only Enterprise WiFi are listed without their security keys!

In "extractor_report.txt" file, information related to Default Gateway, Host Name and IP are stored.

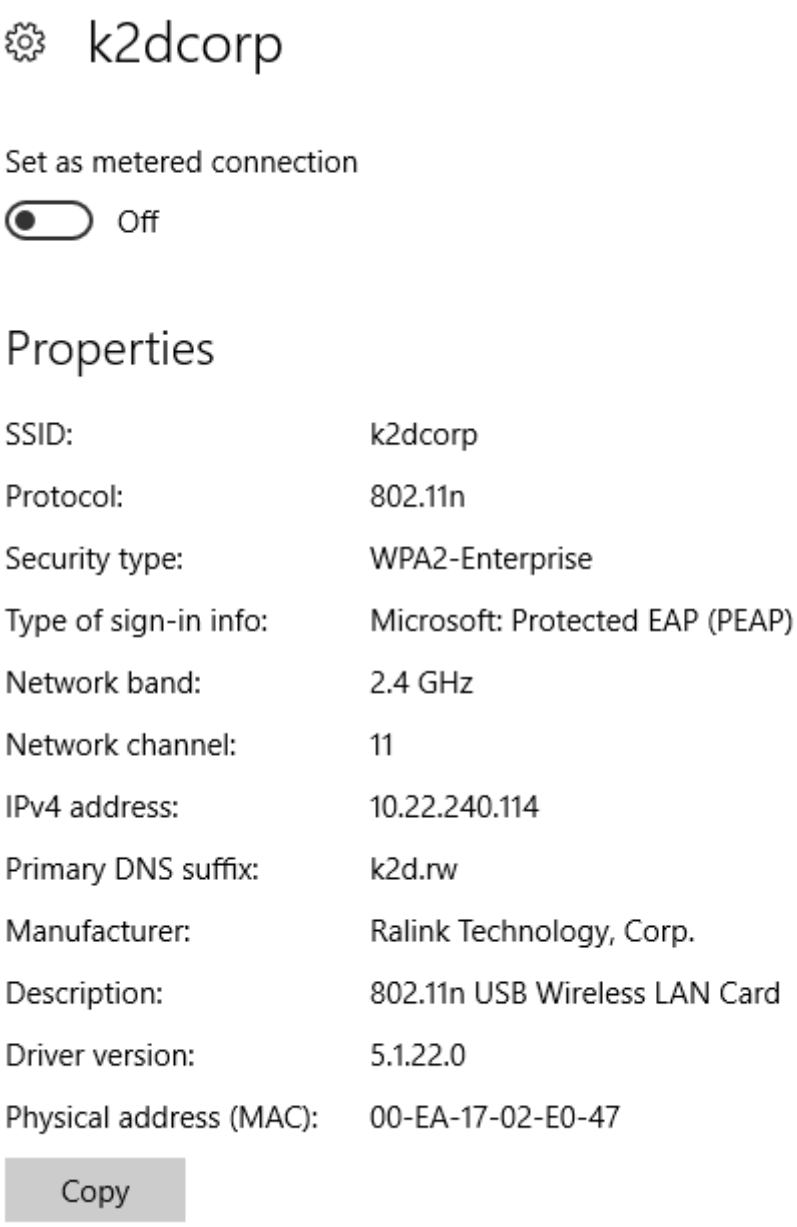
All shared keys are high risky. The ideal solution is to consider changing your network configurations. For WiFi Certificate (WPA, WPA2 or WPAs), remember that the personal Mode and PSK authentication will lead to a shared key whereas Enterprise mode and 802.1x Authentication enable

you to comply with Authentication, Authorization, and Accounting (AAA) the security management framework for network access control. All devices have different security keys and every key is bounded to its mac address. Breaking this security is not easy, and even if you do, affecting other network devices is not straight forward as for personal mode and PSK authentication. Device are in different range of IP and different VLN mostly closed to outside communication.

Most AP such as Ubiquiti AP provide a mean of authentication via WPA2 an WPA3 Enterprise, Mac address registration and Radius Server for a proper Authentication, authorization, and accounting (AAA) mechanisms to controls access to computer resources, enforces policies, and audits usage.

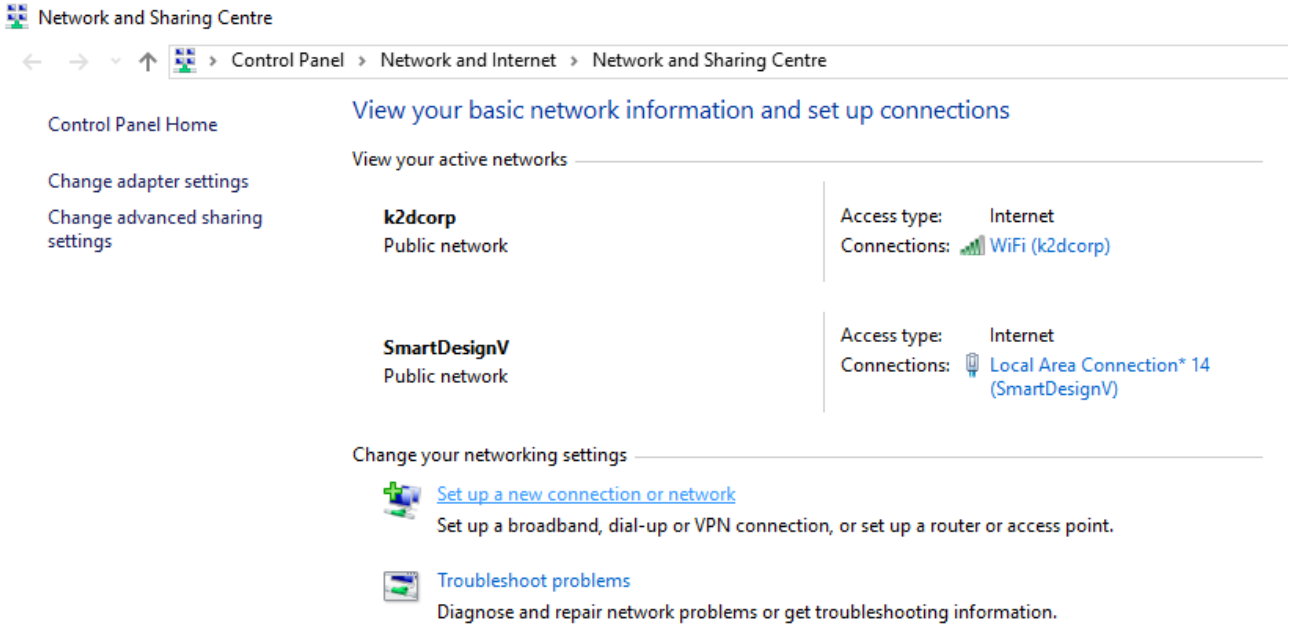
Appendices

WPA2 Enterprise

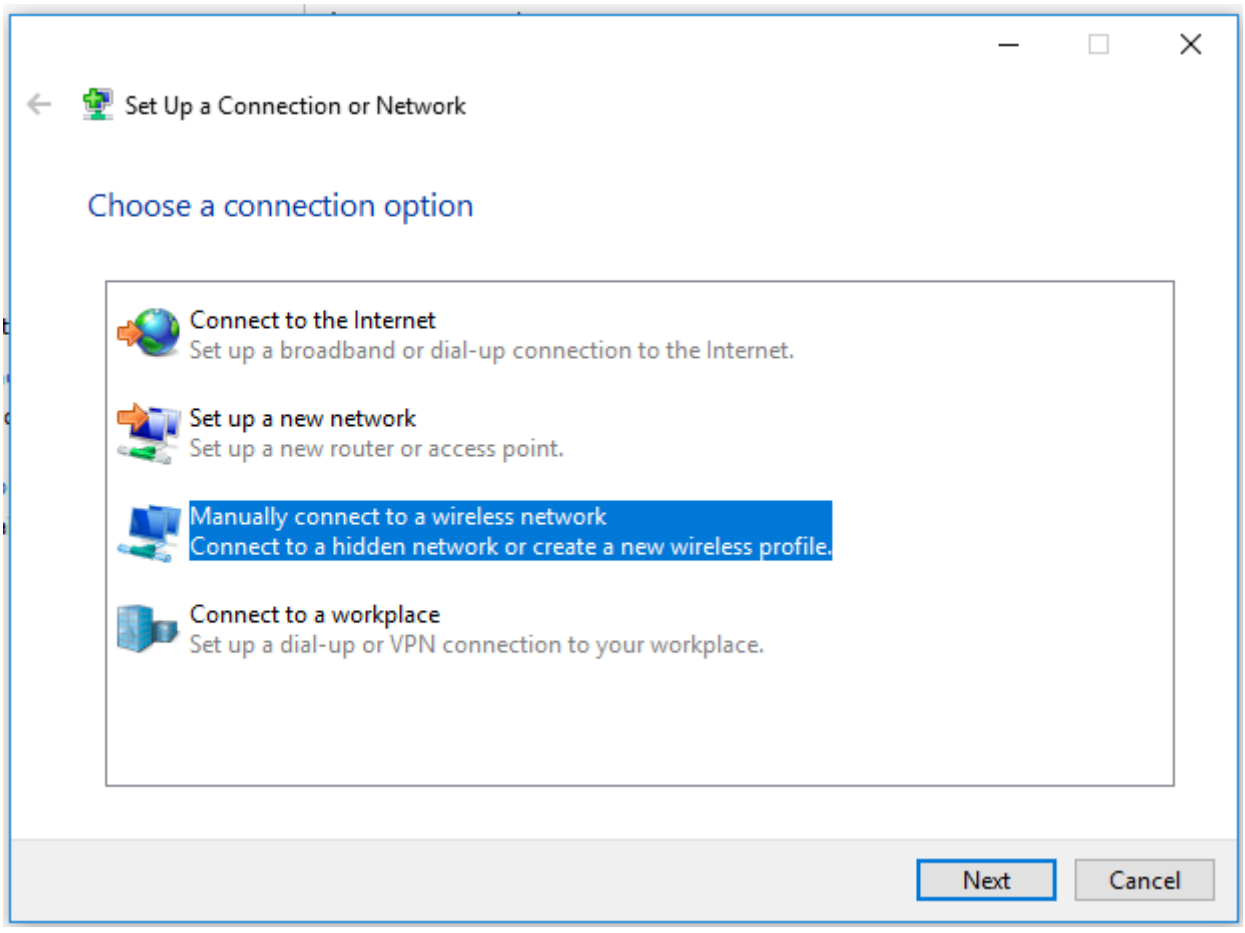


Creation of WPA Enterprise WiFi on Windows

1

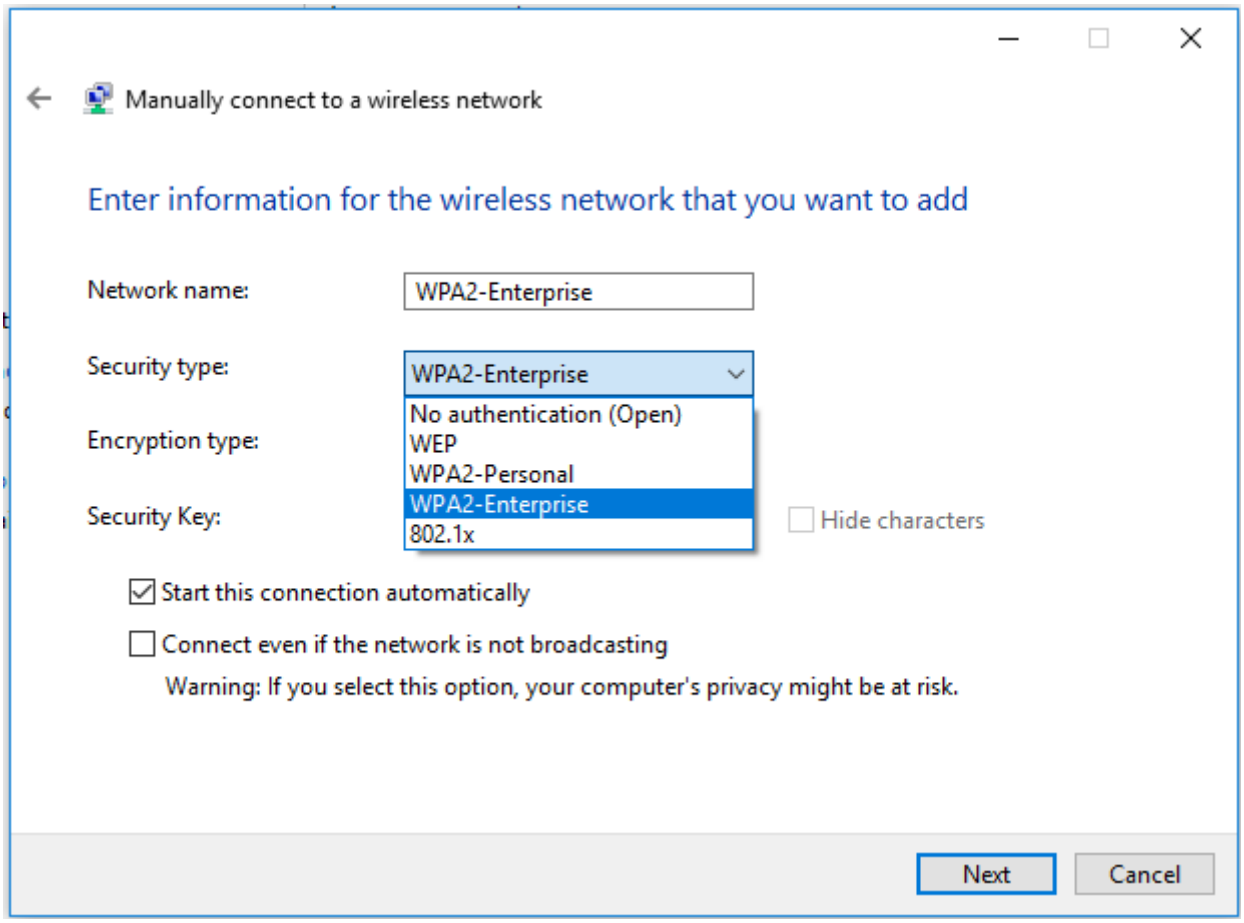


2



6th / 7th

3.


Manually connect to a wireless network
Enter information for the wireless network that you want to add
Network name:
WPA2-Enterprise
Security type:
WPA2-Enterprise
Encryption type:
Security Key:
No authentication (Open)
WEP
WPA2-Personal
WPA2-Enterprise
802.1x
Hide characters
Start this connection automatically
Connect even if the network is not broadcasting
Warning: If you select this option, your computer's privacy might be at risk.
Next
Cancel