Group Names & Photos

Team Name: Wi we cannot Fi
Number of Team Members: 2

Name: Chen Xi, Diong
Student ID: 32722656

Name: Hong Bo, Kang
Student ID: 32684673

Introduction

Cryptography is a fundamental security tool used to protect sensitive data from unauthorized access, modification and disclosure. There are various security applications of cryptography, each with its specific goals and requirements. One such application is in wireless network security, which has become increasingly important as more devices and services rely on wireless communication. As of January 2023, a total of 5.16 billion people around the world use the internet, (DataReportal 2023) therefore it is obvious that network security is one of the major concerns due to the sheer number of people's data at risk of being hacked or exploited.

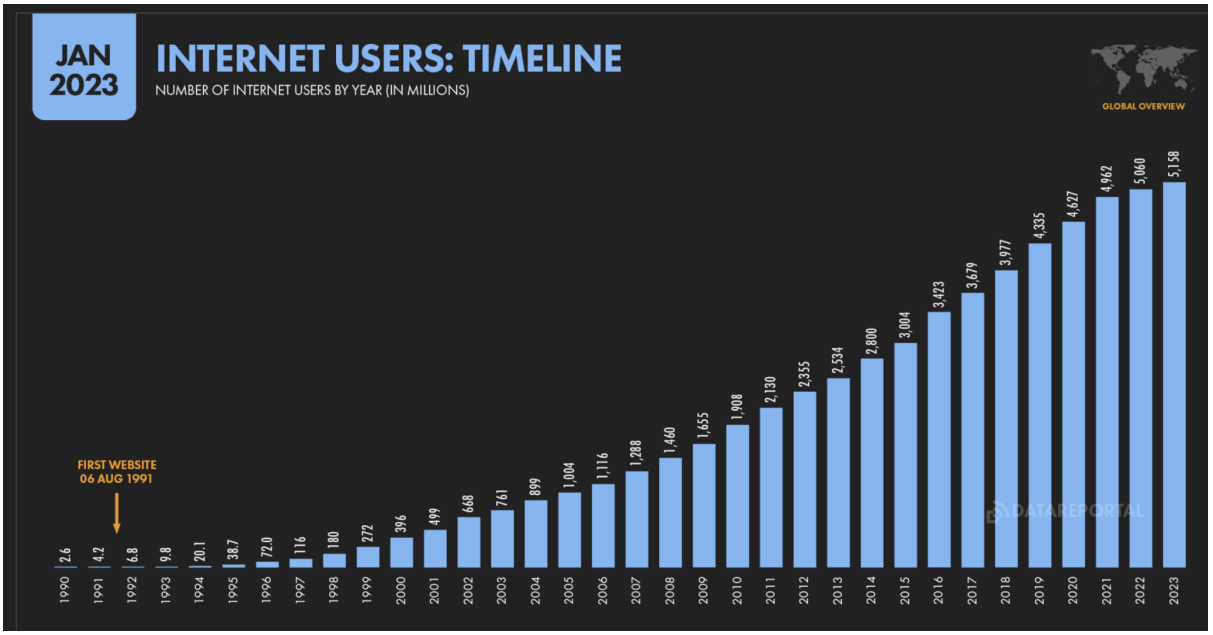

Figure 1: Number of internet users over the years (DataReportal 2023)

Safe communication across the network is achieved through various encryption techniques, with cryptography being one of them. Cryptography means "secret writing" which is the science and art of transforming messages to make them secure and immune to attacks by an unauthorized party, whereas encryption is a process to transform plain text into cipher text and decryption is the reverse process to transform cipher text back into plain text. (Vanitha, Anitha, Zubair Rahaman & Mohamed Musthafa 2018) These methods help to secure message transmission through an insecure channel, i.e. the Wi-Fi network in the context of this report.

The main purpose of this report is to explore the security goals of cryptography in wireless network security, with focus on the WPA2 (Wi-Fi Protected Access II) protocol. The report will be divided into four sections:

First we will provide an overview of the cryptographic techniques used in WPA2, including CCMP-AES (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol and Advanced Encryption Standard), CBC-MAC (Cipher Block Chaining and Message Authentication Code), and PSK authentication (Pre-Shared Key authentication) drawn from the paper “A comparative study of WLAN security protocols: WPA, WPA2” by Adnan et al. (2015). We will also provide an explanation of the 802.1X framework established by the WPA2 network security protocol.

Second, we will present the results of a performance study of the WPA2 protocol, drawing from a research paper titled “Effect of WPA2 Security on IEEE 802.11n Bandwidth and Round Trip Time in Peer-Peer Wireless Local Area Networks” , which was published by Kolahi, Li, Safdarim, and Argawe (2017) . The research evaluates the effectiveness of data transmission whilst WPA2 security is in effect compared to open systems. We will also go through the usability of authentication provided by WPA2 networks drawn from a paper published by Tucker (n.d.) and the compatibility of WPA2 networks drawn from a study by Sari and Karay (2015).

Third, we will look at the security vulnerabilities of WPA2, drawing from the papers "Effects of the WPA2 KRACK Attack in Real Environment" by Fehér & Sándor (2018) and “Vulnerabilities of Wireless Security Protocols (WEP and WPA2)” by Kumkar, Tiwari, Tiwari, Gupta & Shrawne (2012). The first paper reviews the attack carried out to decipher WEP, WPA, and WPA2 passwords using an attack known as KRACK, whereas the second paper demonstrates a dictionary attack on WPA2 secured networks, which provides a deeper insight into WPA2 cracking.

Fourth, we will provide an analysis of the results reported in the papers reviewed. We will give a conclusion of the report, discuss possible improvements that can be made to the WPA2 network security protocol, and break down the costs of setting up such a protocol on a wireless network.

The security goals that the protocol aims to achieve are Confidentiality, Integrity and Authentication. Some possible attacks on confidentiality are wormholes, traffic analysis, and eavesdropping; attacks on integrity are spoofing, modification, fabrication, sybil, and replay attack; whereas attacks on authentication are password attacks, man-in-the-middle attacks, social engineering attacks, etc. The application of cryptography on network security hopes to protect sensitive information from unauthorized access or disclosure (Confidentiality), as well as ensure data is not modified or tampered with by unauthorized entities or mechanisms (Integrity).

Application Protocol/System Description

According to Adnan et al. (2015), WPA2 was introduced in 2004 as an improvement over WPA, which in turn succeeds the original Wired Equivalent Privacy (WEP) algorithm. WPA2 is a security protocol used to secure wireless computer networks which are based on IEEE 802.11i standard. It provides stronger security than WPA by having CCMP-AES as a security protocol instead of TKIP.

CCMP-AES is a protocol based on Advanced Encryption Standard (AES) cipher that provides strong message authenticity and integrity checking. It is significantly stronger in protection for both privacy and integrity than the RC4-based TKIP that is used in WPA. WPA2 also changed the algorithm for data integrity from the Micheal algorithm to Cipher Block Chaining Message Authentication Code (CBC-MAC). Based on Bellar, Kilian, and Rogaway (2000), CBC-MAC is a technique for constructing a Message Authentication Code (MAC) from a block cipher. The message is encrypted using a block cipher algorithm in Cipher Block Chaining (CBC) mode, resulting in a sequence of interconnected blocks, where each block relies on the accurate encryption of the preceding block. This interconnection guarantees that altering any part of the original message would modify the final encrypted block in a manner that is impossible to anticipate or undo without knowledge of the block cipher key. For authenticity in WPA2, enterprise networks use 802.1X/EAP frameworks for centralized mutual authentication systems.

By research from Lashkari, Danesh, and Samadi (2010), the 802.1X wireless setup consists of three main components: client, access point, and authentication server. The client connects to the access point and having this connection the client can then gain further network access. The client and access point will first negotiate capabilities. These consist of three items: The pairwise cipher suite, used to encrypt unicast traffic, The group cipher suite, used to encrypt multicast and broadcast traffic, and the use of either a pre-shared key (PSK) or 802.1x authentication.

	WEP	802.11i Methods	
		WPA	WPA2
Security Protocols	RC4	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Length	40 or 104 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24 bit IV	48 bit IV	
Key Generation	Concatenation	Two phase mixing function	Not needed
Data Integrity	CRC-32	Michael	CBC-MAC
Header Integrity	None	Michael	CBC-MAC
Replay Protection	None	Packet Number	
Key Management	None	EAS-based	
Authentication	Open or Shared key	802.11x or Pre-Shared Key (PSK)	

Figure 2: Summary of 802.11 security methods.(Adnan et al. (2015))

WPA2 assumes that there are three parties involved in the communication: the wireless access point (AP), the wireless client, and the attacker. The AP and client share a secret key that is used to encrypt and decrypt data transmitted over the wireless network. The attacker is an external party that attempts to gain unauthorized access to the network by intercepting or modifying the data transmitted between the AP and the client. WPA2 uses several cryptographic mechanisms to provide security, including encryption and authentication. For encryption, WPA2 uses the Advanced Encryption Standard (AES) to encrypt wireless traffic between the access point and the client devices as stated above. WPA2 uses the 802.1X authentication protocol, which is an authentication framework used in wired and wireless networks. It requires users to provide a username and password or digital certificate to access the network. So, the main threats that WPA2 is designed to protect against are various types of attacks such as Brute-force attacks, Dictionary attacks, and Replay attacks.

WPA2 uses a strong encryption algorithm (AES) and a long key length to prevent attackers from guessing the wireless key through brute-force attacks. For dictionary attacks, WPA2 uses a key derivation function (KDF) for the passphrase. From a book written by Camenisch, Fischer-Hübner, and Rannenberg (2011), KDF is an algorithm that derives a secret key from a secret value and this algorithm makes it difficult for attackers to guess the wireless key. WPA2 uses a nonce (a random number that is used only once) in the 4-way handshake to prevent attackers from replaying captured packets to gain access to the network. This is done by having each side of the connection generate a nonce. The nonce is then used to encrypt the key exchange. By using a nonce, an attacker cannot replay a previously captured packet because the nonce will have changed the next time a handshake is initiated.

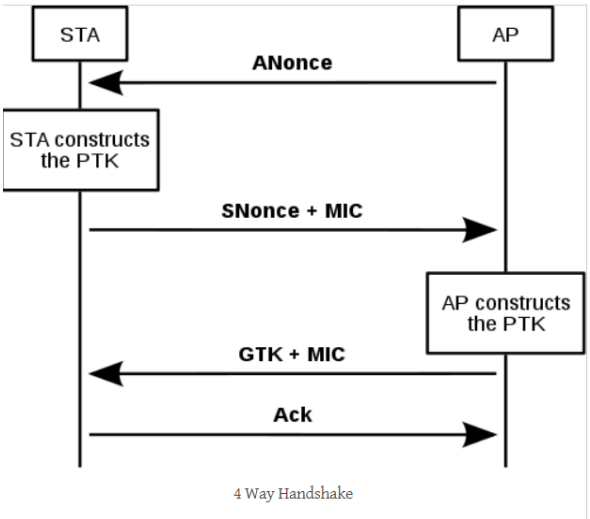

Figure 3. 4-way handshake used in WPA (mtroi (2014))

Application Protocol/System Performance & Usability Results

According to research from Kolahi et al. (2017), the implementation of WPA2 has quite an impact on the performance of wireless networks. They have conducted research to investigate the effect of WPA2 on TCP throughput and delay for both IPv4 and IPv6 in two different operating systems, Windows 7 and Fedora 12. The study found that enabling WPA2 resulted in a decrease in TCP (Transmission Control Protocol) throughput and an increase in TCP RTT (Round Trip Time) or delay compared to an open system. In Windows 7, the difference was approximately 2.8 Mbps less throughput and 0.18 ms more delay for both IPv4 and IPv6. Similarly, in Fedora 12, enabling WPA2 caused 3 Mbps less TCP throughput and 0.20 ms more delay for both IPv4 and IPv6. For a wireless network with lesser throughput and greater delay, it means that it can transmit data at a slower rate. These results highlight the importance of carefully considering the design and implementation of wireless networks to ensure optimal performance and security.

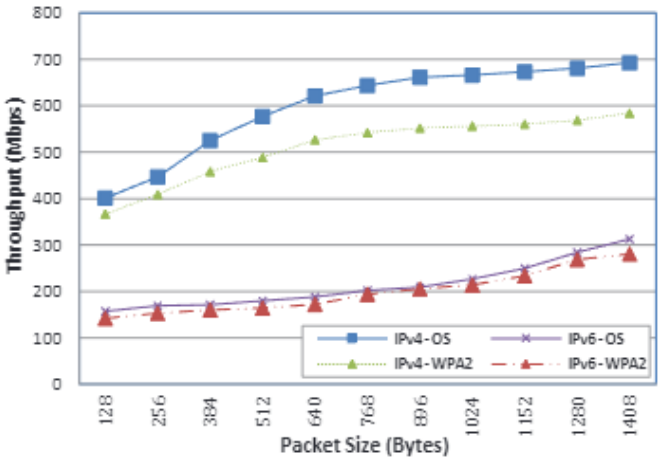

Figure 4: TCP Throughput Comparison for IPv4 and IPv6 in 802.11ac WLAN, Open System vs. WPA2 security Kolahi et al. (2017)

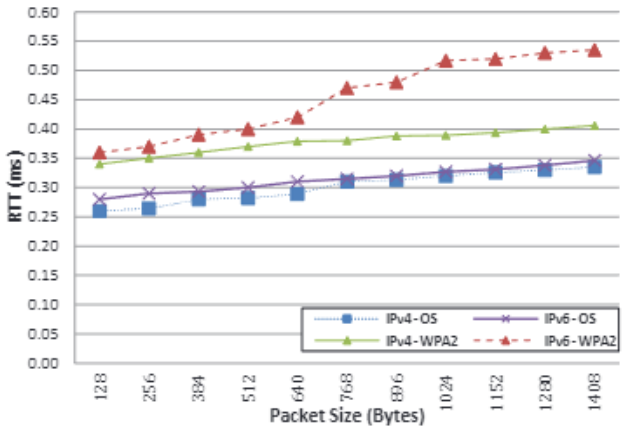

Figure 5: TCP RTT Comparison for IPv4 and IPv6 on 802.11acWLAN, Open System vs. WPA2 security Kolahi et al. (2017)

WPA2 uses the 802.1x authentication protocol which we have discussed above. It is a framework and this protocol has different types of authentication. Based on Tucker (n.d.), there are three types of authentication: PEAP-MSCHAPv2, EAP-TTLS/PAP, and EAP-TLS. The researchers have judged the effectiveness of each of these authentication types and concluded in the table shown below.

WPA2 & WPA3 Enterprise Common Protocols	Level of Encryption	Authentication Speed	Directory Support	Credentials
EAP-TLS	Public-Private Key Cryptography	Fast - 12 Steps	Universal	Passwordless
PEAP-MSCHAPv2	Bad Encryption (MD4, Compromised since 1995)	Slow - 22 Steps	Active Directory	Passwords
EAP-TTLS/PAP	No Credential Encryption	Slowest - 25 Steps	Non-AD LDAP Servers	Passwords

Figure 6: Comparison of the WPA2 Enterprise protocols on Encryption, Speed, Support, and User Experience. Tucker (n.d.)

We can observe that EAP-TLS is the most effective type of authentication compared to other authentication in the 802.1x protocol. EAP-TLS authentication is a certificate-based authentication system, users' identities are authenticated by digital certificates instead of credentials. The identity of users can be stored in Active Directory or any LDAP (Lightweight Directory Access Protocol) or SAML (Security Assertion Markup Language) based directory. We can see that by using the EAP-TLS authentication, WPA2 has a higher level of encryption, has faster authentication speed, uses a universal directory and it is passwordless.

Compatibility of network security is also an essential factor that will affect the user base. In a study by Sari and Karay (2015), they tabulated a comparison of the three network security protocols WEP, WPA, and WPA2. It is stated that WPA2 is compatible with devices nowadays since it supports network interface cards which were produced from 2006 onwards. This ensures that WiFi network users can have much stronger network security with the implementation of WPA2.

Application Protocol/System Security Vulnerabilities or Security Analysis Results

Despite being widely used for security, WPA2 is still vulnerable to attacks such as KRACK, dictionary and brute force attacks. We will introduce the said attacks and their impacts on WPA2, as well as some countermeasures proposed against the vulnerabilities. We will also investigate the implementation flaws of WPA2 and its encryption weaknesses.

According to Fehér & Sándor (2018), the KRACK (Key Reinstallation Attack) vulnerability is a serious flaw in WPA2 that was discovered in October 2017. It has a profound impact on most WPA2 devices with the WPA-TKIP, AES-CCMP and GCMP cipher, regardless of whether it is a personal or enterprise network. As of 2020, 63.7% of access points in Malaysia use WPA2 as its network security protocol. This implies that without the appropriate patches, almost two-thirds of the access points can be easily compromised using the KRACK. KRACK is done by exploiting the vulnerability of the 4-way handshake. By manipulating and replaying cryptographic handshake messages, the attacker fools the victim into reinstalling an already used or already-in-use key. With knowledge of the key currently in-use, the attacker is able to intercept and decrypt the communication of messages between the client and the access point. The attacker can also inject malware or other malicious code into the network, thus compromising the security of the access point. In the report, Fehér & Sándor proposed several solutions to mitigate the risk of such vulnerability. They suggested patching the firmware of the affected devices, enforcing HTTPS (Hypertext Transfer Protocol Secure) for communication in every website, and using VPNs (Virtual Private Networks) to send data and information in an encrypted form over a shared network infrastructure. It is also emphasized that user knowledge and user awareness are the most critical essential elements to prevent such an exploitation.

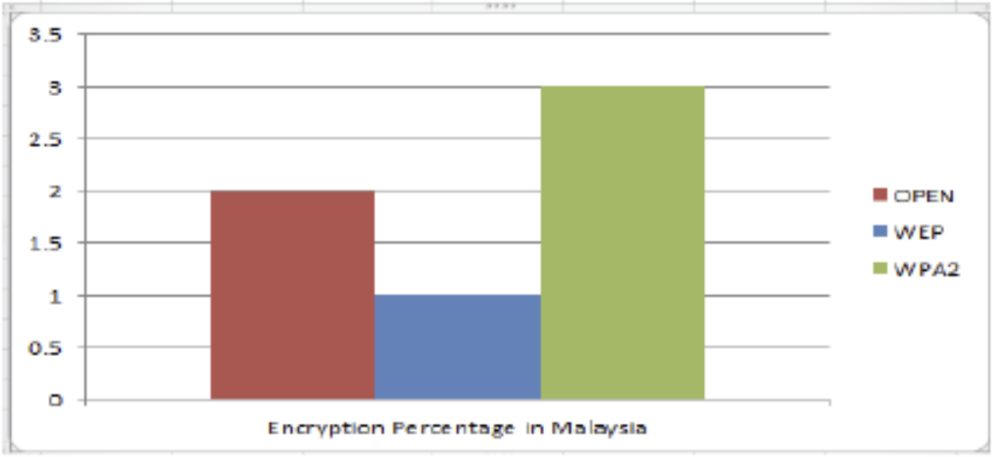

Figure 8: Encryption types of access points in Malaysia (Noman, Noman, Al-Maatouk 2020)

In a study conducted by Kumkar et al. (2012), it is stated that despite using strong encryption via dynamic keys, WPA2 can still be vulnerable to dictionary attacks. It is demonstrated that by exploiting the 4-Way Handshake between the client and the access point, the attacker can obtain information to start the attack, such as the SSID of the network, the MAC addresses of the access point and the client, and the PMK (Pairwise Master Key). The weakness of the system lies in the fact that the PMK is derived from the concatenation of the passphrase, SSID, length of the SSID and a number or bit string used only once (nonce). With a pre-computed passphrase dictionary, the attacker can launch a dictionary attack by computing different PMKs and comparing them with the extracted PMK of the handshake. If the attacker is successful in guessing the password, they can use it to connect to the network and potentially access sensitive data. The PMK can be used further to derive the so-called Pairwise Transient Key (PSK) used to decrypt the data transmitted between the client and the access point. In a snapshot of their attack, it can be observed that they have successfully found a passphrase with a format that is quite commonly used by people nowadays, and the time required to crack the passphrase is only 10 minutes. Some ways to counter dictionary attacks are slowing down repeated logins (i.e. penalize failed attempts) or locking accounts after a threshold, using two-factor authentication (2FA), and using OTPs (One-Time Passwords).

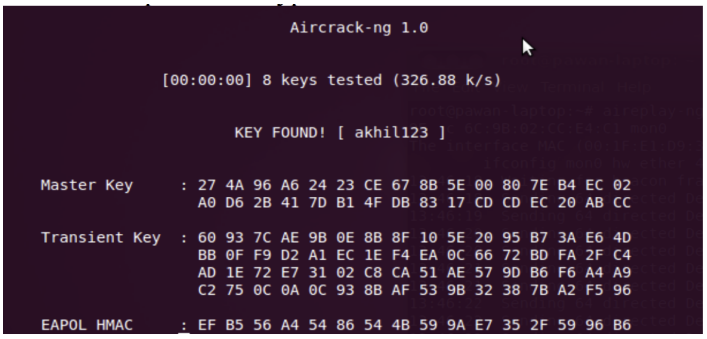

Fig 9. Snapshot output aircrack-ng. i.e applying dictionary attack.

Test Results:

Security Mechanism: WPA2

Mode: Infrastructure

Time Required: 10 min

Attack Type: Dictionary.

Result: Successful.

Figure 3: Snapshot of passphrase found and time required (Kumkar et al. 2012)

Critical Analysis of Results

It is an undeniable fact that WPA2 has certainly provided stronger protection against network attacks compared to its predecessors WPA and WPA2. It has stronger security with the use of the Advanced Encryption Standard (AES) as its encryption algorithm for data transmission through an insecure wireless network. The encryption keys used by WPA2 are also longer and more complex, thus making it harder for attackers to crack the encryption.

Additionally, WPA2 has an improved authentication protocol called 802.1x which provides faster, universal and passwordless authentication. This protocol allows users to authenticate with a central server before accessing the network, ensuring that only authorized users can connect. This authentication protocol is faster than previous authentication methods and is considered to be more secure since passwords are not stored on the device, thus reducing the risk of password-based attacks.

However, as a trade off for stronger security, networks secured by WPA2 have a slight detriment to their usability. Due to the time for computation needed to ensure the confidentiality and integrity of the data sent over the network, there is observed delay in data transmission. This delay is usually minimal, but it can become more noticeable in larger networks with many users. The network capacity may also be reduced due to the additional processing required to encrypt and decrypt data. This can result in increased latency and poor signal quality, which in turn negatively affects user experience.

From our WPA2 vulnerability analysis, we noted that WPA2 is susceptible to KRACK attacks and dictionary attacks. This is due to the exploitation of the 4-way handshake to obtain the encryption key. Some improvements can be made to prevent these attacks such as using a much stronger encryption algorithm and encrypting data blocks individually. These improvements are implemented in the successor of WPA2, which is WPA3. WPA3 uses a new key exchange protocol called Simultaneous Authentication of Equals (SAE) to better protect against password guessing attacks, as well as to provide forward secrecy. Although security is improved, the data encryption and decryption algorithm remains the same, which implies that the efficiency of data transmission remains the same. This problem can be tackled from a few angles. By using specialized hardware that can accelerate the encryption and decryption processes, throughput can be increased. Another way is to optimize the security protocol to reduce the amount of processing required, such as using more efficient encryption algorithms or reducing the number of round trips required for key exchange. Optimizing the key management process and certificate management can also improve network throughput.

Generally, to set up a WPA2 wireless network, one will need a WIreless Access Point (WAP), a Wireless Network Adapter, a Router and an Ethernet Cable. A WAP is a device that allows wireless devices to connect to a wired network, which has a cost range from RM100 to RM1000, depending on the features and capabilities of the device. A Wireless Network Adapter is a device that allows devices to connect to a wireless network, with a cost ranging from RM40 to RM400. A Router is a device that connects multiple networks together and also provides wireless connectivity. It may cost from anywhere between RM200 to RM1000. Last but not least, an Ethernet Cable is a wired connection that connects the WAP to the router, where its cost can range from RM20 to RM80, depending on the length of the cable. These price ranges are estimates and can vary depending on the specifications of the hardware, as well as the place and time of purchase.

References

DataReportal. (2023) Retrieved from
Digital Around the World — DataReportal – Global Digital Insights

Adnan, A. H., Abdirazak, M., Sadi A. B. M. S., Anam, T., Khan, S. Z., Rahman, M. M. & Omar, M. M. 2015 A comparative study of WLAN security protocols: WPA, WPA2
IEEE Xplore Full-Text PDF:

Bellare, M., Kilian, J.& Rogaway, P. (2000) The Security of the Cipher Block Chaining Message Authentication Code
https://www.sciencedirect.com/science/article/pii/S002200009991694X

Camenisch, J., Fischer-Hübner, S., & Rannenberg, K. (2011) Privacy and Identity Management for Life
https://books.google.com.my/books?id=vYxzh3C6OPUC&pg=PA185&redir_esc=y#v=onepage&q&f=false

Vanitha, K., Anitha, K., Zubair Rahaman A. M. J. Md, & Mohamed Musthafa M. (2018) Analysis of Cryptographic Techniques in Network Security Vol. 5 Issue 8 p. 155
(PDF) Analysis of Cryptographic Techniques in Network Security (researchgate.net)

D. J. Fehér and B. Sandor, "Effects of the WPA2 KRACK Attack in Real Environment," *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, Subotica, Serbia, 2018, pp. 000239-000242
Effects of the WPA2 KRACK Attack in Real Environment | IEEE Conference Publication | IEEE Xplore

Noman, H. A., Noman, S. A. & Al-Maatouk, Q 2020 “Wireless Security in Malaysia, A Survey Paper
(PDF) WIRELESS SECURITY IN MALAYSIA: A SURVEY PAPER (researchgate.net)

Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A. & Shrawne, S “Vulnerabilities of Wireless Security Protocols (WEP and WPA2)” 2012
Vulnerabilities-of-Wireless-Security-protocols-WEP-and-WPA2.pdf (researchgate.net)

Sari A., and Karay M., “Comparative Analysis of Wireless Security Protocols: WEP vs WPA” 2015
https://www.researchgate.net/publication/287197979_Comparative_Analysis_of_Wireless_Security_Protocols_WEP_vs_WPA

Tucker A. “WPA2-Enterprise Authentication Protocols Comparison”
https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison

Li P., Kolahi S.S., Safdari M., & Argawe M., “Effect of WPA2 Security on IEEE 802.11n Bandwidth and Round Trip Time in Peer-Peer Wireless Local Area Networks”
https://ieeexplore.ieee.org/abstract/document/5763598/authors#citations

Mtroi, “4-Way Handshake”
https://wlanınde.wordpress.com/2014/10/27/4-way-handshake/

Lashkari A.H., Danesh M.M.S., & Samadi B., “A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)”
https://ieeexplore.ieee.org/abstract/document/5234856/authors#authors