OWASP
Open Web Application Security Project

Wireless Security and its Discontents

OWASP

Open Web Application Security Project

Introduction

OWASP

Open Web Application Security Project

The purpose of this presentation is to provide an overview of the strengths and weaknesses of Wireless Security solutions. We will cover:

- Real-world examples of Wireless Security application
- IEEE 802.11 standards for WiFi security
- WiFi encryption protocols
- Ways in which Cyber-criminals exploit vulnerabilities in Wireless Security standards
- Best practices in preventing WiFi hacking attacks

OWASP

Open Web Application Security Project

About the presenter:

Name: Boyan Lazarevski

Profession: IT Operations Specialist

Experience: System Administration, Network Security

Interests: Cybersecurity, Computer Hardware, Retro-computing

OWASP

Open Web Application Security Project

Application of Wireless Technology

OWASP
Open Web Application Security Project

F-35 is a single-seat, single-engine, stealth, 5th-generation, multi-role combat aircraft.

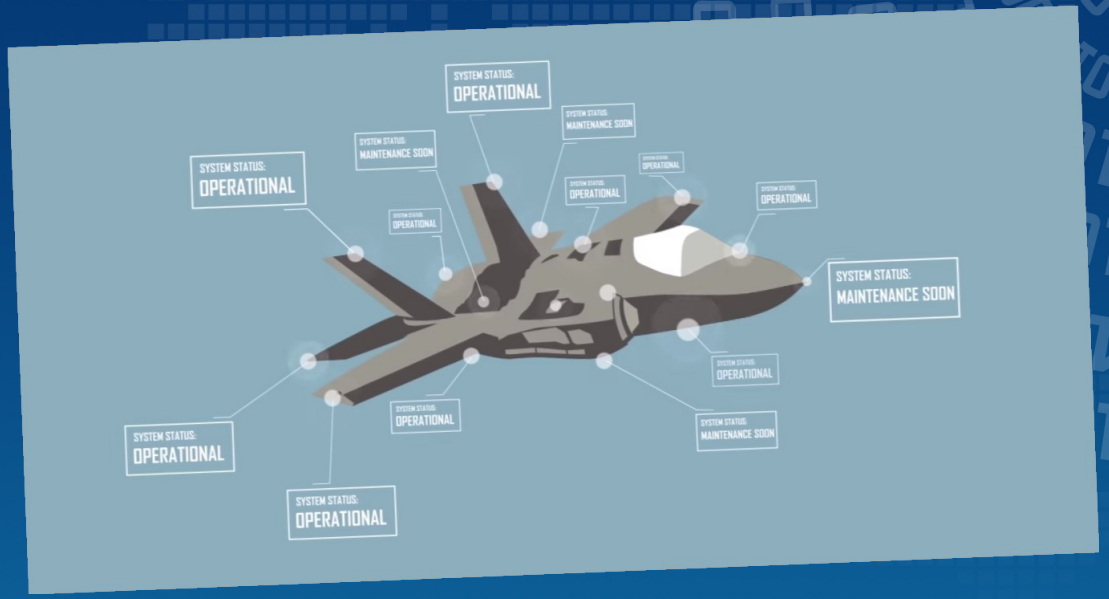
Three main models: F-35A, F-35B and F-35C.

Development began in 1992; first flight in 2006; first deployment in 2015; mass production in 2018.

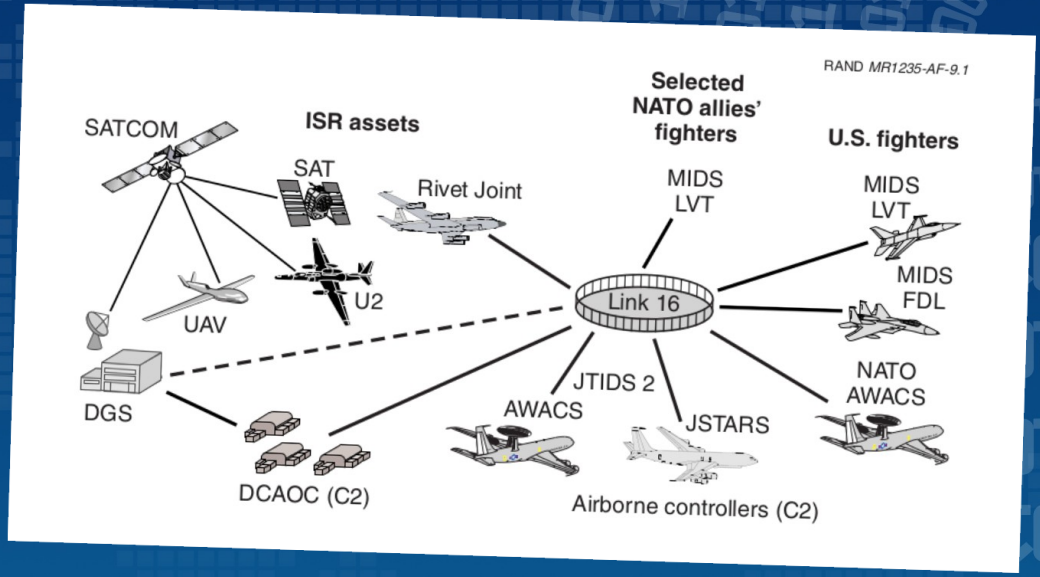
OWASP
Open Web Application Security Project

Nicknamed “Flying Computer”:

- Stealth capabilities,
- Advanced sensors
- Integrated computer system with a powerful core processor (400 billion ops p/s)
- 8 million lines of code that run the on-board systems
- Networking capabilities with other elements within the battle-space for situation awareness.



F-35 has a powerful integrated sensor system that gives pilots 360-degree access to battlefield information. Data gathered by F-35 sensors can be securely shared with commanders at sea, in the air or on the ground.



F-35 communicates situational awareness information via a military tactical data link network known as “Link 16”.

Link 16 is based on MIL-STD 6016 and STANAG 5516 transmission protocols, and is capable of:

- Encrypting voice or data.
- Using error detection and correction coding.

OWASP
Open Web Application Security Project

The worldwide F-35 fleet is connected to two secure networks designed to maximize efficiency:

- Autonomic Logistics Information System (ALIS): keeps track of individual aircraft issues, worldwide location of spare parts and equipment.

- Joint Reprogramming Enterprise (JRE): maintains a shared library of potential adversary sensors and weapon systems that is distributed to the worldwide F-35 fleet.

OWASP

Open Web Application Security Project

F-35 blurs the line between a 5th-gen fighter (stealth and sensor fusion) and a **6th-gen** one (advanced network capabilities that give the pilot control over external weapons, drones and sensors).

The F-35 is by far the most advanced piece of equipment ever made by humans!

However, it has one major vulnerability ...

OWASP

Open Web Application Security Project

… it is, reportedly, *susceptible to hacking*.

Just like any device with networking capabilities, such as a home computer, phone, tablet, etc.

POPULAR MECHANICS TECHNOLOGY CARS TOOLS DEFENSE CAMPING GUIDE SUBSCRIBE NEWSLETTER

The F-35's Greatest Vulnerability Isn't Enemy Weapons. It's Being Hacked.

The high-tech fighter can hide from radar, but hackers are a different matter.

By Kyle Mizokami Nov 14, 2018

UNITED STATES MARINE CORPS / GETTY IMAGES

OWASP
Open Web Application Security Project

The F-35 program along with all of its elements constitutes a vast attack surface. However, it is always most convenient for hackers to attack the weakest link.

In a recent interview with *Defense News*, Brig. Gen. Stephen Jost, the director of the Air Force F-35 Integration Office, identified the weakest link of the program when he mentioned that wireless systems used to support the F-35 could also be points of entry for hackers.

OWASP
Open Web Application Security Project

In the following section we will provide an overview of the most popular family of wireless network technologies – the 802.11 WiFi.

We will explore how WiFi standards and associated encryption protocols work; and will illustrate how hackers use vulnerabilities in the protocols to launch their attacks.

OWASP

Open Web Application Security Project

WiFi Network Standards (802.11)

OWASP
Open Web Application Security Project

Wireless Fidelity (WiFi) is a family of radio technologies used for connecting computational devices into wireless local area networks. WiFi is regulated by the 802.11 protocol standards, governed by the Institute of Electrical and Electronics Engineers (IEEE).

The different 802.11 Wi-Fi standards incorporate different radio technologies that determe the range, data transfer rates, frequency, and modulation that may be achieved. These include:

- 802.11a: 54 Mb/s, 5 GHz
- 802.11b: 11 Mb/s, 2.4 GHz
- 802.11g: 54 Mb/s, 2.4 GHz
- 802.11n: 300/600 Mb/s, 5 and 2.4 GHz
- 802.11ac: 1.7 Gb/s and beyond, 5 GHz

OWASP
Open Web Application Security Project

The following encryption protocols are used to secure the various 802.11 WiFi networks:

- WEP (Wired Equivalent Privacy)
  - RC4
- WPA/WPA2 (Wi-Fi Protected Access)
  - TKIP (Temporal Key Integrity Protocol)
  - AES (Advanced Encryption Standard)

OWASP

Open Web Application Security Project

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was designed to protect the data-link layer frames during wireless transmission. Without it, anyone could read a packet or message sent on the Internet. It was first introduced in 1997.

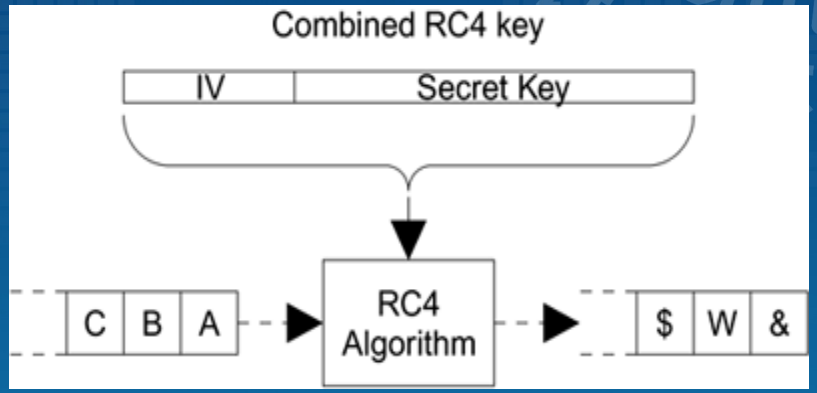
WEP uses an algorithm called “RC4 Stream Cipher” to encrypt the data packets. The standard originally specified a 40-bit, pre shared encryption key (a 104-bit key was later made available).

RC4 takes in one byte from a stream of ordinary data (plain-text) at a time and produces a corresponding byte of encrypted data (cipher-text) for the output stream. Decryption is the reverse process and uses the same keys (symmetric).

All data packets are encrypted using the same key value - so, if one spots the same encrypted bytes in a given position, they know that the original plain-text is being repeated (the IP address always falls in the same place in a packet).

The solution to this problem was the Initialization vector (IV). Instead of only using the fixed secret key to encrypt the packets, we now combine the secret key with a 24-bit number that changes for every packet sent. This extra number is the IV and converts the 104-bit key into a 128-bit key.

To prevent the use of a fixed key for encryption, the actual key used to initialize the RC4 algorithm is the combination of the secret key and the IV.



OWASP

Open Web Application Security Project

IV value changes changes for every packet transmitted, as does the encryption key – so, even if the plain-text is the same, the cipher-text is always different.

The initialization vector is sent openly as part of the transmission so the receiver knows which IV value to use in decryption. Any attacker can read the IV as well. In theory, however, knowledge of the IV is useless without knowledge of the secret part of the key.

For WEP to be effective, the same IV value should never be used twice with a given secret key. Since the attacker can read the IV value, they could keep a log of the values used and notice when a value is used again. This would be the basis for an attack.

Unfortunately, the IV in WEP is only 24 bits long: it has values from 0 to 16,777,216. This means that access points that transmit/receive hundreds of packets a second will exhaust all of the 16 million IV value combinations in a matter of hours. When this happens, IV values are bound to be reused. This, in turn, provides a basis to launch an attack.

WEP Cracking Demo

OWASP

Open Web Application Security Project

Cybersecurity experts identified several severe flaws in WEP in 2001.

Nevertheless, according to a research conducted by *WIGLE* - a site where individuals submit both the location and properties of wireless networks from around the world - WEP encrypted access points make up to 20% of all wireless networks observed to date.

In other words, 1 in 5 wireless networks globally are still using a flawed encryption solution.

OWASP

Open Web Application Security Project

WiFi Protected Access (WPA/WPA2)

OWASP
Open Web Application Security Project

In 2003, the Wi-Fi Alliance released The **WiFi Protected Access (WPA)** as an interim standard, while the IEEE worked to develop a more advanced, long-term replacement for WEP.

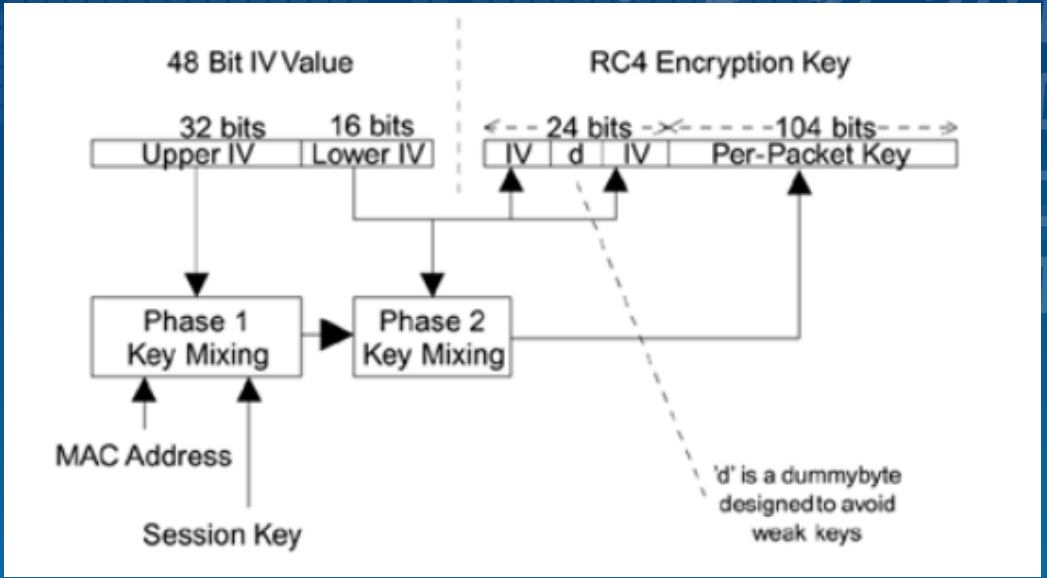
WPA has modes for enterprise users and for personal use. The enterprise mode uses more stringent authentication with the Extensible Authentication Protocol (EAP). The personal mode, WPA-PSK, uses pre-shared keys for simpler implementation (homes and small offices). Enterprise mode requires the use of an authentication server.

Although WPA is also based on the RC4 cipher, it introduced enhancements to encryption: the Temporal Key Integrity Protocol (TKIP).

TKIP is a suite of algorithms that works as a "wrapper" to WEP. Like WEP, TKIP uses the RC4 stream encryption algorithm as its basis.

The protocol uses a set of functions to improve wireless LAN security: use 256-bit keys, per-packet key mixing (the generation of a unique key for each packet), a message integrity check, a larger IV size (48 bits) and mechanisms to reduce IV reuse.

This protocol, however, did not provide the robust security that it needed to.



OWASP
Open Web Application Security Project

Wi-Fi Protected Access 2 (WPA2) came as the successor to WPA in 2004, when ratified by IEEE. WPA2 also offers enterprise and personal modes. Although WPA2 has vulnerabilities, it is considered the most secure wireless security standard available.

WPA2 replaces the RC4 cipher and TKIP with two stronger encryption and authentication mechanisms:

- Advanced Encryption Standard (AES) and
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

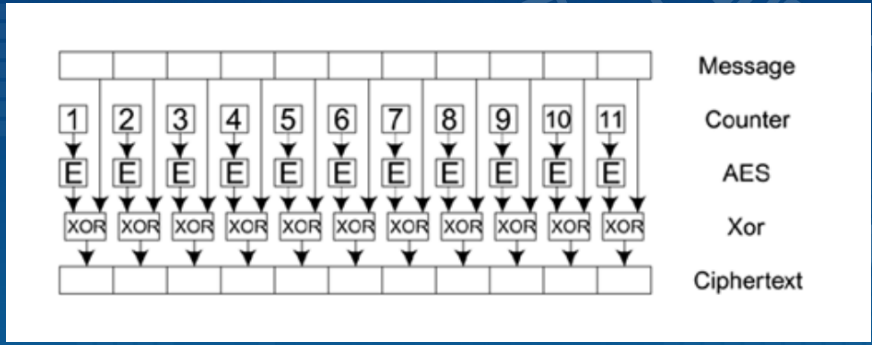
Also meant to be backward-compatible, WPA2 supports TKIP as a fall-back if a device cannot support CCMP.

OWASP

Open Web Application Security Project

Unlike WEP, which is based on the RC4 stream cypher as the encryption method, WPA2 uses a block cipher encryption method called Advanced Encryption Standard (AES). AES encrypts and decrypts data in blocks of 128 bits using 128, 192 and 256-bit keys.

The format in which the data is sent by the network card, via the WiFi radio antenta, to the AP (and vice-versa) is known as MAC Protocol Data Unit, or MPDU.



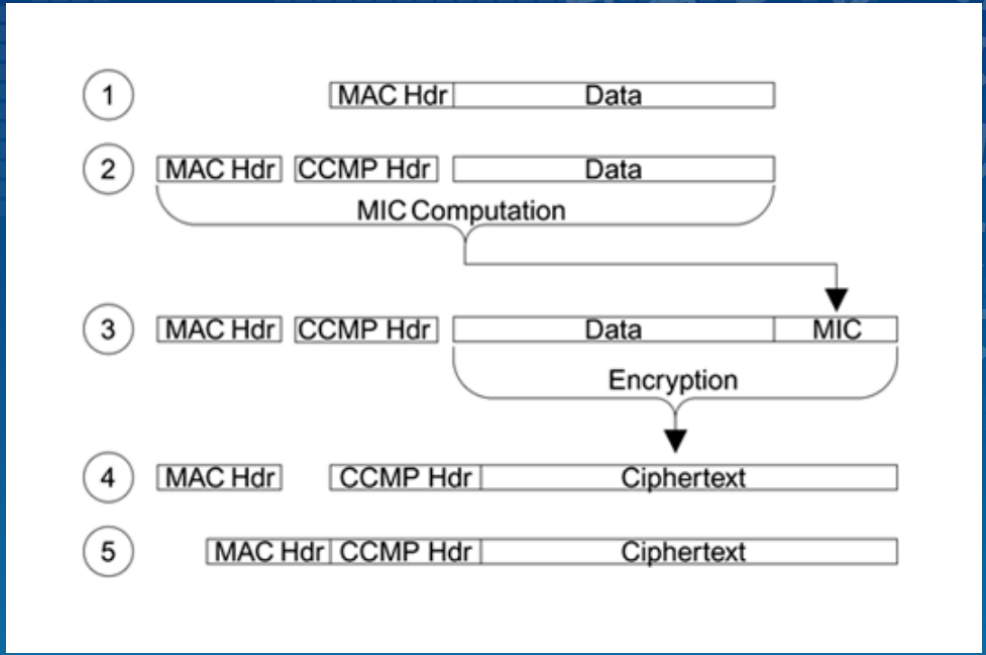
AES operates in several modes, but the most secure and advanced is the **Counter Mode (CTR)**. With CTR encryption, the system produces random values (that are unique for each block of plain-text); the random values are then encrypted with AES encryption algorithm, and the output (of the encryption of the random counter value) is them XOR-ed against the block of plain-text to produce the corresponding block of cypher-text.

OWASP

Open Web Application Security Project

The Counter Mode (CTR) is the algorithm that provides data privacy. However, this is not enough in itself. In addition to CTR, WPE2 utilizes a mechanism that provides data integrity and authentication – known as Cipher Block Chaining Message Authentication Code (CBC-MAC).

CBC-MAC achievs this by adding a unique value to the original plain-text block message, called the Message Integrity Code (MIC). The original plan-text is then encrypted along with the MIC by the Counter Mode encryption of AES, to produce a cypher-text that provides data confidentiality and data integrity.



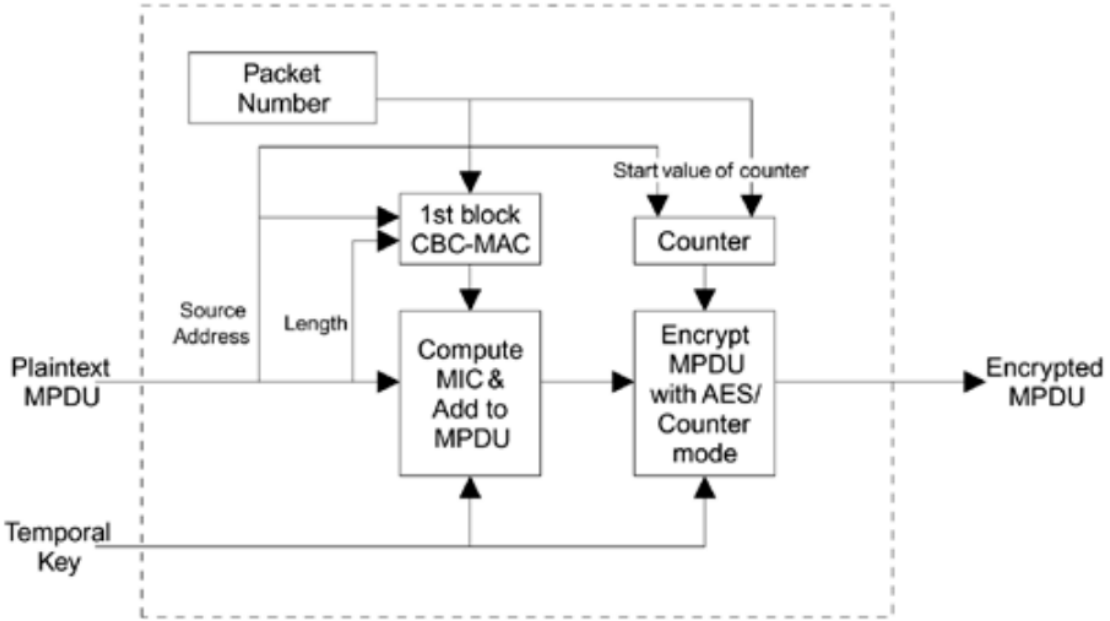
OWASP

Open Web Application Security Project

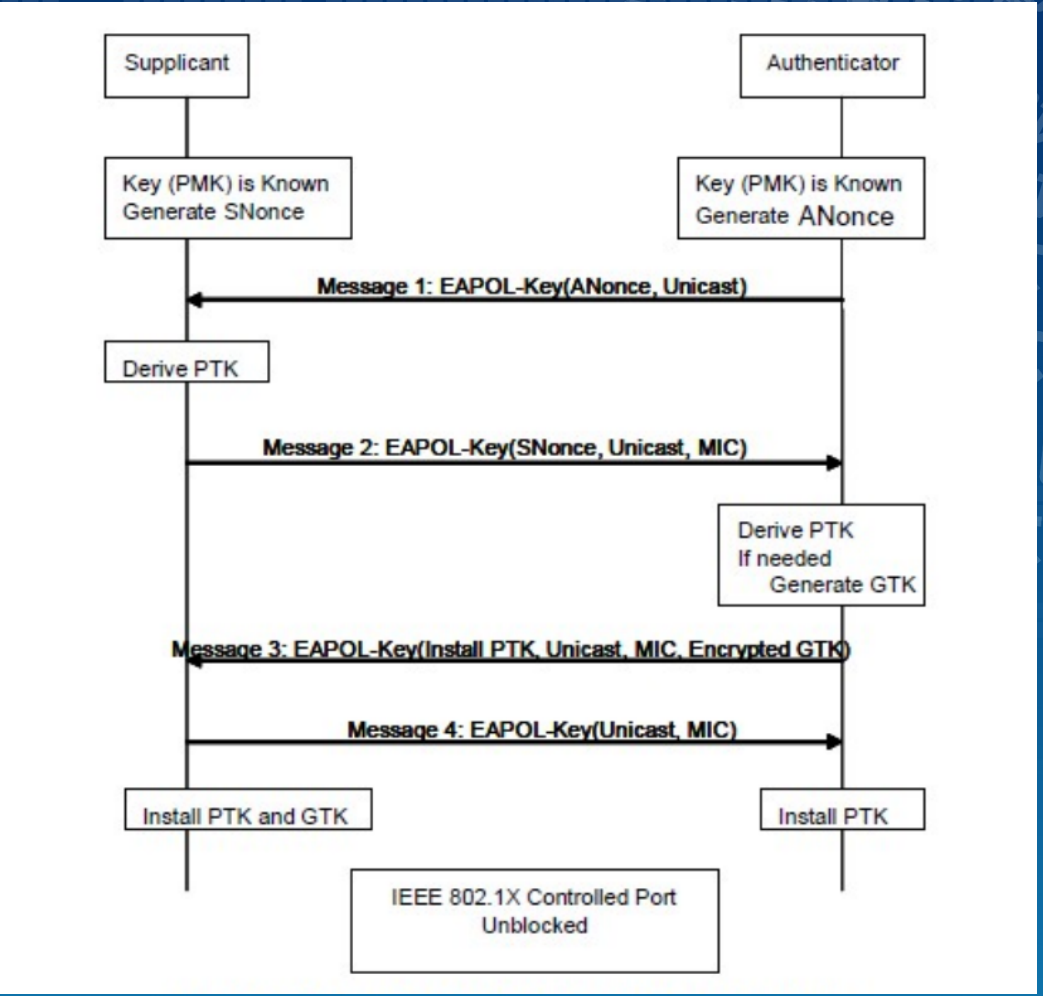
CTR together with CBC-MAC are the two components of the **CCM Protocol** (CCMP - Counter Mode - Cipher Block Chaining - Message Authentication Code Protocol).

AES-CCMP is proven to provide superior encryption and, to date, has not been cracked.

Implementation of the CCMP encryption block is represented on the following graph.



WPA2 uses a 4-way handshake as a authentication protocol for establishing a wireless connection between an AP and a client device – known as the Extensible Authentication Protocol [EAP] over LAN (EAPOL).



OWASP
Open Web Application
Security Project

EAPOL 4-way Handshake:

- To connect to an AP, the client enters a Pre-Shared Key (PSK), which maches the one set for the AP. The PSK is used to generate a PMK (Pairwise Master Key) for the 4-way handshake.
- The PMK is derived by hashing the PSK. The PMK generated in such a way is not an encryption key but forms the input to generate further temporal keys that can be used to encrypt data. (The Master key is termed “Pairwise” since it is the same between the station and the Access Point. The purpose of the 4-way handshake is to turn the PMK into data encryption keys).
- The AP sends the client a pseudo-randomly generated number called ANonce (A Number used Once).

The client device uses the ANonce together with the PMK to create PTK (Pairwise Transient Key). The PTK is a set of encryption keys used for different functions for Unicast data protection.

- The client then sends the AP its SNonce (Supplicant [client] Number used Once), and adds a MIC (Message Integrity Code) to it for protection.
- The AP receives the SNonce and uses it to calculate the PTK – which is used to validate the MIC and make sure that the SNonce was not manipulated in transit. (The AP also creates a GTK - Group Temporal Key - and sends it to the client with an added MIC for protection).
- The client device receives and installs the GTK alongside the PTK – and sends back the AP a ACK message.

OWASP

Open Web Application Security Project

The only weakness in WPA2 is the 4-way handshake. That is, the weakness is in the encrypted password can be derived from the information shared during the handshake. If we can grab the hashed password (PMK) during the client to AP authentication process, then we can as a basis for the cracking exercise.

The way AirCrack-ng (AeroDump-ng) works is to collect the Nonce info, the MAC header information, and several other values that are transmitted openly over the connection as part of the handshake – and use this data to derive the hashed PMK out of the MIC.

At this point, we can use a dictionary-based off-line brute-force attack on the PMK value (the hashed output of the password). We achieve by using dictionary files – text files of billions of permutations of words and phrases. AirCrarck-ng hashes each phrase and compares it to the signature of the PMK. Once two hashes match, the password is cracked.

WPA/WPA2 Cracking Demo

OWASP

Open Web Application Security Project

Hardening WiFi Security

OWASP

Open Web Application Security Project

There are ways to (try to) prevent Wi-Fi Cracking of home WiFi networks, and they involve measures based on everyday vigilance:

- Changing the name of the default home network
- Changing default IP address on the Wireless router
- Using a strong network administrator password
- Making sure we set a strong and unique SSID password
- Increasing Wi-Fi security by activating network encryption
- Turning off the wireless home network when not at home
- Turning off the DHCP functionality on the router
- Disabling Remote Access
- Always keeping AP/router software up-to-date
- Enhancing protection for the devices most frequently connected to the home network

OWASP

Open Web Application Security Project

As for enterprise WiFi networks, we can use the following measures that are considered best practice:

- Establish multi-factor authentication for access to the network (such as Active Directory service authentication, utilizing tokens, etc.)
- Deploy a wireless intrusion detection system (WIDS) and/or wireless intrusion prevention system (WIPS).
- Use Extensible Authentication Protocol-Transport Layer Security certificate-based methods to secure the entire authentication transaction and communication.
- Implement a guest Wi-Fi network that is separate from the main network (involving routers that support multiple SSIDs)
- Ensure equipment is regularly patched and free from known vulnerabilities by updating all software in accordance with developer service pack issuance.
- Ensure compliance with the most current National Institute of Standards and Technology guidelines.

OWASP
Open Web Application Security Project

Questions?

OWASP
Open Web Application
Security Project

References

Articles

https://www.defensenews.com/digital-show-dailies/paris-air-show/2019/06/21/lockheed-hypes-f-35s-upgrade-plan-as-interest-in-sixth-gen-fighters-grows/
https://www.popularmechanics.com/military/aviation/a25100725/f-35-vulnerability-hacked/
https://www.f35.com/about/capabilities
https://www.fifthdomain.com/air/2018/11/14/us-air-force-moves-to-fortify-f-35-weak-points-against-hacking/
https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/
https://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/
https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2
http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+6.+How+IEEE+802.11+WEP+Works+and+Why+It+Doesn+t/Privacy/
http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+11.+TKIP/TKIP+Overview/
http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+12.+AES+CCMP/AES+Overview/
https://heimdalsecurity.com/blog/home-wireless-network-security/
https://www.us-cert.gov/ncas/tips/ST18-247

Photos

https://breakingdefense.com/2019/08/lockheed-launches-new-weapons-cybersecurity-strategy/
https://nationalinterest.org/blog/buzz/just-2-out-23-us-f-35-test-planes-are-fully-operational-72326
https://defensesystems.com/articles/2017/09/29/electromagnetic-weapons-air-force.aspx
https://www.luminantsecurity.com/wp-content/uploads/2015/12/data-encryption-vector-294x300.png
https://static-vectorplace-com.ams3.digitaloceanspaces.com/uploads/works/15258/thumb_15258.jpg
https://process.fs.teachablecdn.com/ADNupMnWyR7kCWRvm76Laz/resize=width:705/https://www.filepicker.io/api/file/XERODrGuSPCTFCgfEtmd
https://usa.kaspersky.com/blog/dangerous-public-wi-fi/6377/
https://1.bp.blogspot.com/-QkWOt9zvIIA/WBxK1MdgADI/AAAAAAAAqGg/QR8JZu9BrpEYX-2n-XFuUXQn6fFKnfuPACLcB/s728-e100/track-cellphone.png
https://image.freepik.com/free-vector/flat-design-wifi-network-concept_23-2148219689.jpg
http://www.tech-faq.com/wp-content/uploads/CCMP.gif
https://www.agileit.com/wp-content/uploads/2017/01/data-encryption-cloud.jpg