Chapter 1

WLAN

1.1 Introduction

Definition 1.1.1 ▸ Wireless Local Area Network (WLAN)

WLAN

WLANs are accessed using the Wi-Fi[1] protocol. Wi-Fi itself is a data link layer protocol like ethernet (layer 2).

Components The mobile station (STA) connects to a network using Wi-Fi. The STA connects to the network by way of an ***access point***, often part of the router. The access point is identified by a ***service set identifier*** (SSID) which appears as the network name. These are not intended to be secret.

Connecting to an Access Point In this context, we can think of the mobile station (STA) as the "client" and the access point as the "server".

1. The STA probes nearby access points; this is used by the STA to determine which AP they will connect to.
2. Low-level authentication, which has since been deprecated but is still engrained in the standard. Devices now just send null responses, making this step more of a handshake than any form of authentication.

[1]Wi-Fi isn't an acronym, but rather a reference to the IEEE 802.11 standard

3. Association with the AP to establish the connection, so both devices know to listen for each other's communications.
4. High-level authentication: Authenticates the STA to the PA. It may also authenticate the AP to the STA. This step is omitted for open networks.

Frame Types

- ***Data Frames*** carry upper-layer protocol data, similar to an ethernet frame.
- ***Management Frames*** ensure connections maintain basic service guarantees. They handle new connections between STA and AP, handle handovers between APs as STAs physically move, and handle disconnections.
- ***Control frames*** communicate data and management frames and are the lowest-layer frames

1.2 WLAN Threats

WLAN has many of the same vulnerabilities as a physical LAN. However, it is more vulnerable as an attacker does not need physical access to the network. They would only need to be within proximity and attack devices. The issue is further exacerbated as Wi-Fi is a Broadcast Protocol—any device within proximity can receive, record, and inject Wi-Fi packets. Modern Wi-Fi supports beam forming (one-way communication), but this is only designed as an efficiency benefit and should not be relied on for security.

Rogue AP A rogue AP attack establishes a copycat AP used to create a man-in-the-middle connection. This attack is only possible when there is no mutual authentication between the STA and AP.

1. The attacker sets up an AP with the same SSID as the legitimate AP. Ideally, the STA should see that the rogue AP should have a stronger signal than the legitimate AP.
2. The attacker interrupts the STA's connection. This can be done by sending a `disassociate` frame to the STA. The broadcast nature of Wi-Fi makes this easy to perform.
3. The STA probes the APs and finds the rogue AP that has stronger signal than the legitimate AP.
4. The STA connects to the rogue AP, and a man-in-the-middle connection is established.

Session Hijacking This attack is only possible when session encryption is not used.

1. The attacker interrupts the STA's connection, but the attacker ensures the message isn't seen by the AP.
2. The attacker spoofs the MAC address of the STA and takes over the legitimate STA's session.

War Driving War driving involves scanning radio channels for in-range wireless networks. The attacker often uses high-power omnidirectional antenna while literally driving around to maximize the search radius. This can be used for:

- ***Reconnaissance:*** SSIDs may reveal a lot about a building's occupants, or they can be used to steal material to perform a brute force attack for the AP's authentication credentials.
- ***Monitoring communication***, which is especially easy if the networks are unencrypted.
- ***Manipulating packets:*** It's possible to override a client's packet with an attacker's packet if the attacker can generate a stronger signal. It is also easy to perform a denial of service to the WLAN.

Connecting to AP The authentication server () dothis

Open Networks Open networks omit any form of authentication, allowing for any device to connect. As such, packets are neither encrypted nor authenticated. Any confidential communication over an open network has to rely on end-to-end encryption such as TLS. In addition, open networks are highly susceptible to rogue AP attacks.

Some open networks authenticate users by a login page (e.g. hotel Wi-Fi). However, this happens over the HTTP protocol and is not part of the Wi-Fi protocol itself. Packets are still neither encrypted nor authenticated. This kind of authentication is also susceptible to session hijacking.

Note that, even with end-to-end encryption, the DNS protocol is still plaintext and thus highly vulnerable.

Wired Equivalent Privacy (WEP) WEP encrypts all traffic using the RC4 stream cipher with a 40-bit key and 24-bit IV. This is limited due to export restrictions, where the United States didn't want to give away strong cryptographic schemes. However, in this configuration, it is highly insecure.

WEP verifies integrity by using CRC-32 checksum. This protocol is highly susceptible to collisions, so it isn't a cryptographically secure protocol.

WEP uses Open System Authentication (OSA) which allows anyone to finish

A pre-shared key between the STA and AP may be used for authentication (usually just a password). RC4 key is based on the pre-shared key, which is the same for all clients. This renders it less secure than just using OSA!

> Ultimately, WEP is extremely insecure and should not be used.

1.3 EAP, Radius, WPA3

Definition 1.3.1 ▸ Authentication Server (AS)

Definition 1.3.2 ▸ Extensible Authentication Protocol (AEP)

EAP provides a framework for implementing Wi-Fi authentication between STA and AP, and between AP and the AS. It does not specify how authentication happens, rather only facilitates how the communication happens between devices.

EAP can be used to implement many authentication protocols. It is now considered broken, so most networks now use Protected EAP (PEAP).

Definition 1.3.3 ▸ Remote Authentiation Dial-In User Service (RADIUS)

RADIUS is a client/server protocol that:

- can tunnel EAP messages,
- provides authentication, authorization, and auditability,
- access request outcomes (accept, reject, challenge)

For example, Eduroam can use a specific university's RADIUS server to implement arbitrary authentication methods, and decouple authentication from the access points themselves.

Definition 1.3.4 ▸ Wi-Fi Protected Access (WPA)

WPA integrates PEAP and RADIUS to create a protocol more secure than WEP, by:

1. significantly increasing the key length,
2. giving each packet a different key (called ***key rotation***), and
3. using a MAC to protect integrity.

Explain why WPA1 and WPA2 are broken, and how good WPA3 is

Chapter 2

Blockchain

Nowadays, we typically associate the term "blockchain"

Definition 2.0.1 ▸ Blockchain

Blockchain is a database technology with three key properties:

1. Cryptographic append-only ledger, which stores the full history of all transactions
2. Replication
3. Distributed operation (i.e. decentralized)

2.1 Cryptographic, append-only ledger

A blockchain's ledger uses cryptography to guarantee its integrity. It does so via an ***Authenticated Data Structure (ADS)***, where modifications to the data can be detected (but does not necessarily prevent modification of the ADS). An ADS produces a ***verifier*** that can be used to verify the data hasn't been changed since the verifier was produced. This requires access to the ADS to verify its integrity. In some ADS systems, the verifier can also be used to create proofs of inclusion and non-inclusion. In this case, access to the ADS is not required.

Definition 2.1.1 ▸ Hash Chain

A ***hash chain*** is an authenticated data structure based on singly linked lists. Each item stores the following:

- Its data
- A pointer to the previous item

- A hash value calculated based on the value of the current item and the hash value of the previous item; the first item uses a hard-coded value, and is sometimes called the ***genesis item***

Items in the hash chain that store transactions are referred to as ***blocks***, hence the term ***blockchain***.

2.2 Replication

Multiple entities store the blockchain ledger in its entirety as well as the verifier. If one entity modifies their ledger, the others can detect that change because their verifier values will no longer match. If the modification was malicious, the modified ledger can be restored from the replicated copies.

2.3 Distributed Operation

Multiple entities operate the system, often referred to as ***miners***. Each miner replicates the full blockchain, operating individually but verify and replicate each other.

To add a new block, miners undergo the following procedure:

1. An individual miner will first add a new block to their personal copy of the blockchain. The miner generates a list of transactions to add to a blockchain. They verify the legitimacy of those transactions and then create a block with those transactions. That miner adds the block to their copy of the blockchain.

2. Next, that miner announces the new block to the other miners. Each other miner verifies the legitimacy of the transactions in the new block. The other miners then add the new block to their copy of the blockchain.

In public blockchains, anybody can be a miner. Each miner votes on which blocks should be added. This requires a mechanism to fairly allocate votes.

In permissioned blockchains, the identities of the miners are defined by the system. Blocks are added directly without voting. Hence, it is more efficient than open operation.