Network Security

Wireless

Johannes Schmidt

Institutionen för Datavetenskap (IDA)

Avdelningen för Databas- och Informationsteknik (ADIT)

Disclaimer

- Wireless networks come with so much security related issues that an entire 6 credit course could be dedicated to it.
- In this course we want to make you understand only a small fraction of the issues.
- The important part is that you remember that *“adding wireless”* should be taken very serious, and it may be the case that *“adding wireless”* adds so much uncertainty to a security policy that business needs do not make up for it.

Some general terminology

- DoS attack = Denial of Service attack: make some machine or service unavailable to its users
- MITM attack = Man In The Middle attack: the attacker secretly sits between two communicating parties and controls the whole communication (either just listening or even altering content)
- Replay attack = intercept a message in order to repeat/resend it

Wireless networks

- WLAN (e.g. IEEE 802.11)
  - Medium range communication
- WPAN – Wireless personal area networks (e.g. Bluetooth)
  - Short range communication
- Other wireless technologies
- Wireless networks are an important consideration, as businesses today use them extensively.

IEEE 802.11

- A family of standards, security was top concern when 802.11 was defined. The standard includes an optional protocol called WEP that is designed to give the same level of security as wired networks.

Standard	Band	Speed	Notes
802.11	2.4GHz	1Mbit/s	1997
802.11a	5GHz	54Mbit/s	1999
802.11b	2.4GHz	11Mbit/s	1999
802.11g	2.4GHz	54Mbit/s	2003
802.11n	2.4GHz+5GHz	max 600Mbit/s	2009
802.11ac	5GHz	min 1Gbit/s	Approved 2014

Data taken from https://en.wikipedia.org 2016-01-20

Infrastructure

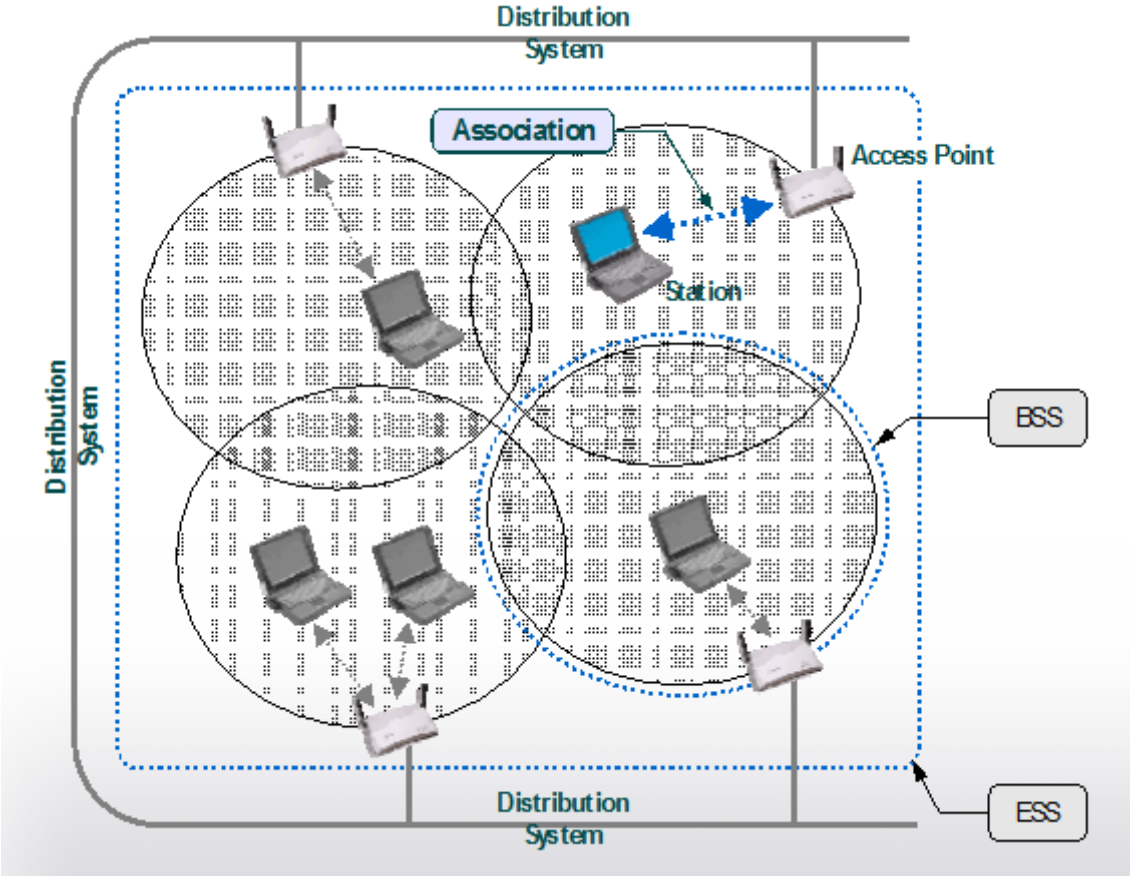
AP = Access point – Bridge between wired and distributed systems. Responsible for relaying traffic between wired and wireless, manages associations and authenticating stations.

BSS – Basic service set – The service provided by a single access point.

ESS – Extended service set – Service provided by several APs connected by a distribution system. Stations can roam between the BSSes that make up the ESS.

Distribution system – Used to relay traffic between a station in one BSS to a station in another BSS. Also to relay traffic to and from external networks. Also used for APs to communicate with each other, e.g. when a station moves from one BSS to another.

An association is a logical connection between a station and an AP. Traffic between a station and hosts outside the BSS will go through the AP to which the station is connected.



Management frames

- 802.11 management frames are used by stations to establish and maintain communications. There exist different types. Some important ones are:
  - **Association frame:** A station sends an association request to an access point. This frame carries information about the station and the SSID of the network it wishes to connect with. The AP can accept or reject.
  - **Disassociation frame:** A station sends a disassociation frame when it no longer wants to be connected to the AP.
  - **Reassociation frame:** A station moves away from the currently associated AP and finds another with a stronger signal. The new AP coordinates forwarding of data frames that may still be in the buffer.
  - **Beacon:** A broadcast from an AP saying that it exists, displays the SSID.

Management frames

- Management frames can be forged, because there is no security placed on them.
- This opens up for attacks.
- One of the arguments why these frames are not protected is that *“whatever you can do by manipulating these frames you also can do by manipulating radio waves”* – Even if that is true it is a lazy excuse, it is much harder manipulating radio waves.
- The IEEE 802.11w attempts to secure management frames, but it is far from broadly implemented and requires new hardware.
- **Conclusion:** Assume management frames are unprotected.

Stupid trick

- Does your router allow you to “hide” the SSID (the *name*) of your network?
- Then only those who know the SSID of the network can find it and connect to it, right?

  - 1. I can sit and listen to all management frames that go through the air, and wait for someone to send a Associate Request management frame, this is unencrypted and I can read your SSID.

Stupid trick

- Does your router allow you to “hide” the SSID (the *name*) of your network?
- Then only those who know the SSID of the network can find it and connect to it, right?

  - 2. I actually don’t even have to wait for that to happen: There are management frames called ***probe request*** that I can send, these are sent on all frequencies asking for AP’s to connect to. AP’s will respond that they exist including their SSID.

Stupid trick

- Does your router allow you to “hide” the SSID (the *name*) of your network?
- Then only those who know the SSID of the network can find it and connect to it, right?

  - 3. But I can turn this off on my router, so that they do not even respond to probes.

    Does not matter. If I can figure out a station that is connected to an AP, I will send a ***disassociation*** frame to it, it will disconnect but immediately send a ***reassociation*** request to the AP (which exposes the SSID).

Wi-Fi security standards

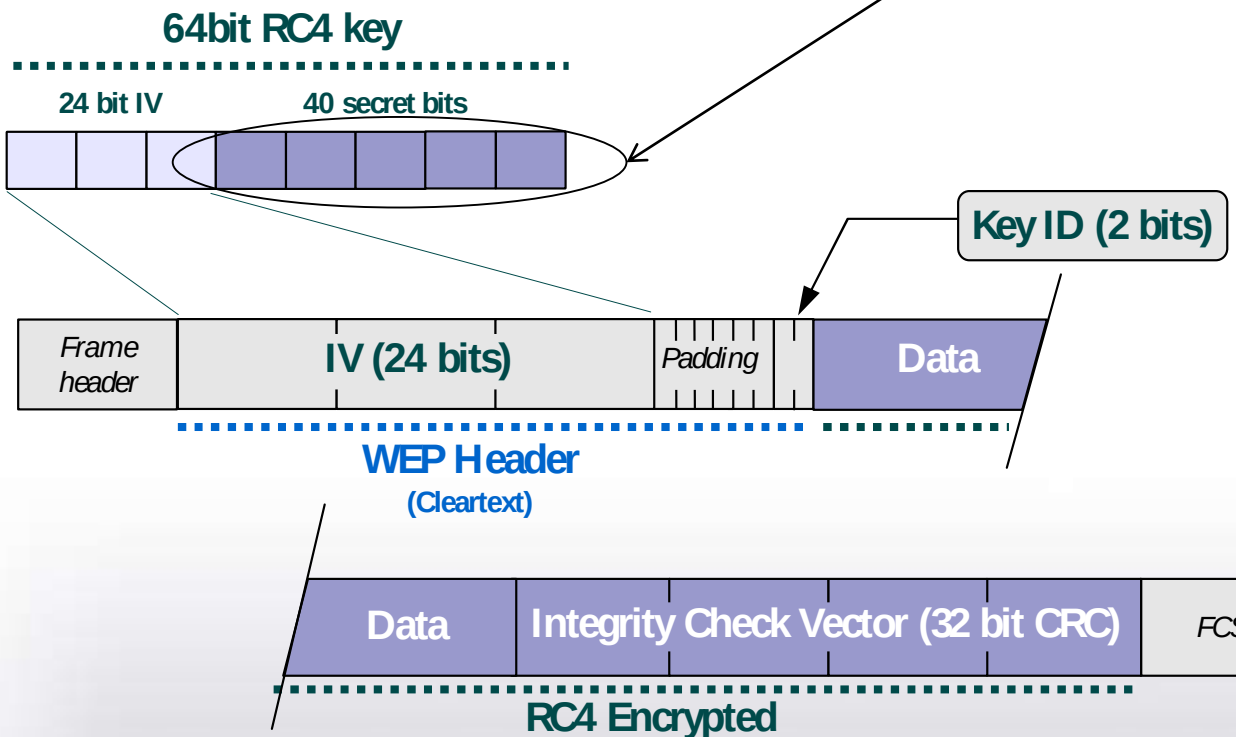
- WEP (Wired Equivalent Privacy)
  - First security standard – Broken by design
  - Today: only seconds to break into a WEP network (2016)
- WPA (Wi-Fi protected Access)
  - Probably secure by design – may be vulnerable to DoS
  - Really a patch for WEP, can use the same hardware, big win!
- WPA2/IEEE 802.11i
  - Probably most secure by design – new everything (including hardware)
  - Still has issues with forged management frames.

WEP

- Wired Equivalent Privacy
  - Goal was to offer same security as wired networks
  - Features authentication, confidentiality, integrity
  - Does not attempt to ensure availability

Secret key shared between AP and station.

RC4 = a stream cipher



Ok, does not look too bad. Encryption using a pretty good algorithm, an encrypted checksum ensures data has not been tampered with. An IV ensures that not every frame will be encrypted with the same key.

RC4 = a stream cipher

IV = Initialization Vector

RC4

- RC4 is the most widely used stream cipher and is used in popular protocols such as TLS and WEP. (In simple terms it is a bitwise *xor* between a key and plaintext, no need to worry about the details for this course).

- RC4 generates a pseudorandom key-stream using as input a key (typically 40-256 bits).
  - It is however vulnerable if the keys used are non-random or if they are related.
  - Under correct usage RC4 is "*secure" (remember that nothing is secure),* but used incorrectly RC4 is vulnerable.

- Speculative: It has been suggested that NSA can reliably crack RC4, and thus SSL/TLS network communication.

WEP is broken

- The big problem is that WEP uses RC4 in a non standard way:
  - The keys used as input are related, the base key is the same for all of them.
  - The IV is available for the attacker, as it is sent in the clear.
  - The first byte of a frame are almost always the same, giving the attacker knowledge about the first byte in the key-stream as well.
  - Using crypto analysis one can find the base key.
  - (How this is actually done is outside the course scope)
- There are other problems as well,
  - Key is too short, total storage for all key-streams for a frame apprx. 24GB.
  - Standard WEP authentication is susceptible to *replay* attacks.
  - Does nothing to prevent *DoS*.

So why should we bother studying WEP?

- If it is broken why do we bother studying it, shouldn't we just move on and study the working protocols?
- Well … one of the driving forces behind new and better security standards and protocols is the study of what has been done incorrectly in the past.
- It may seem a bit morbid, but to some degree we live of others mistakes.
- Even if we have only glanced at the WEP weaknesses we have already learnt one major lesson: **Do not use encryption algorithms in non-standard ways**.

WPA and IEEE 802.11i

WPA

- Longer RC4 keys
- Avoid *weak keys* (this is what is exploited in the attack)
- Hide keys better
- New integrity check
- Replay protection
- Can be implemented on WEP hardware

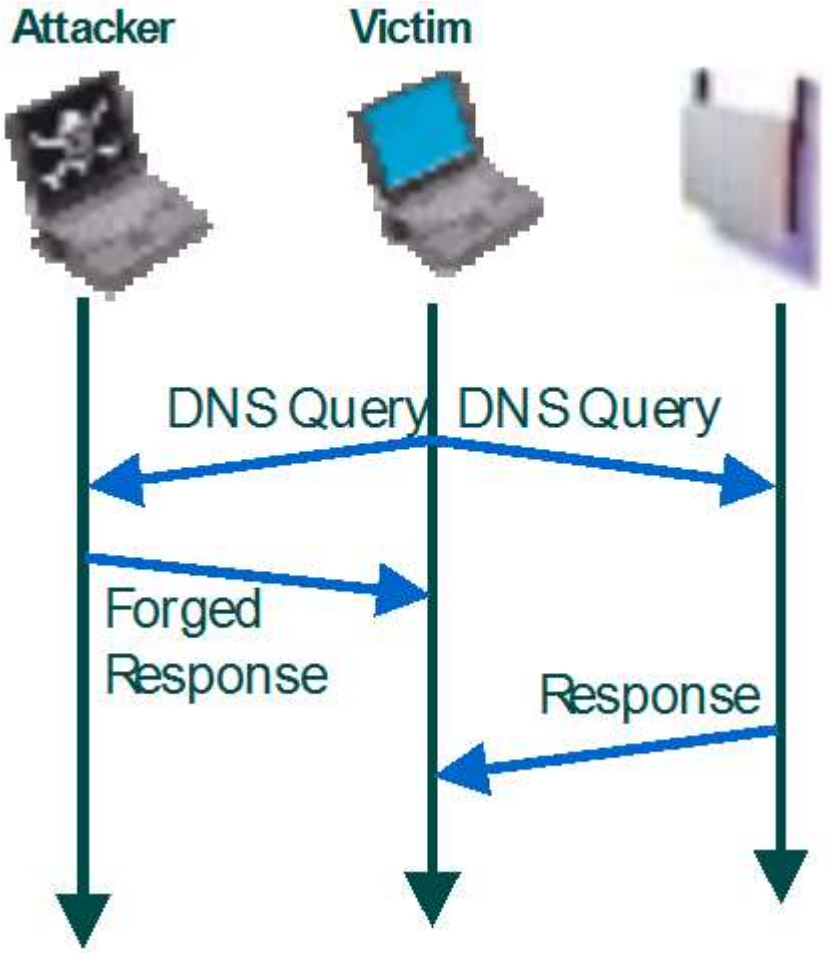
Has some problems, including if passwords or SSID are easy to guess.

IEEE 802.11i (WPA2)

- Uses AES not RC4
- Longer keys
- New integrity check
- Replay protection
- Requires new hardware

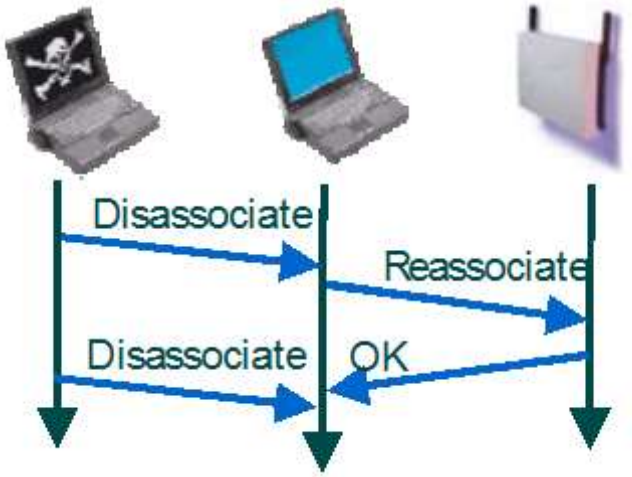
Wireless attacks

- Assume the attacker knows the encryption key used by a station (this can be found in numerous ways, including stealing a station that is already associated).
- The attacker can then usually respond quicker than anything that is on a different network.
- A DNS query from the victim is responded to by the attacker, the attacker sends the victim to a malicious website instead of the one requested.



Wireless attacks

- Wireless networks are exceptionally vulnerable to DoS attacks. There are two particularly effective methods.
  - Management frames are not protected, attacker can forge disassociation frames from the AP to any station. A station will, upon receiving the frame, have to reassociate, but the attacker continues sending disassociation frames for as long as required.
  - An attacker can send ACK frames every half second to reserve radio channels.
- Finally, wireless networks can be disrupted using radio signals. (Some say a microwave is enough).



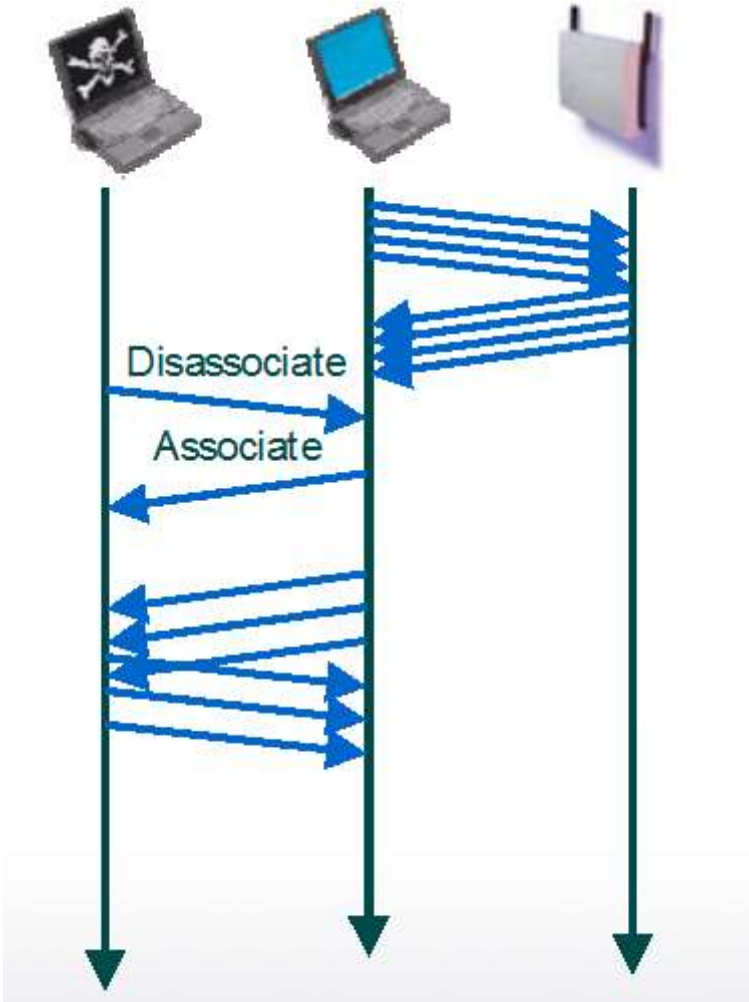
Evil Twins

- Procedure
  - Attacker disassociates victim
  - Victim re-associates to attacker

The attacker has a really good signal to victim, so the victim re-associates with the attacker instead of the real AP.

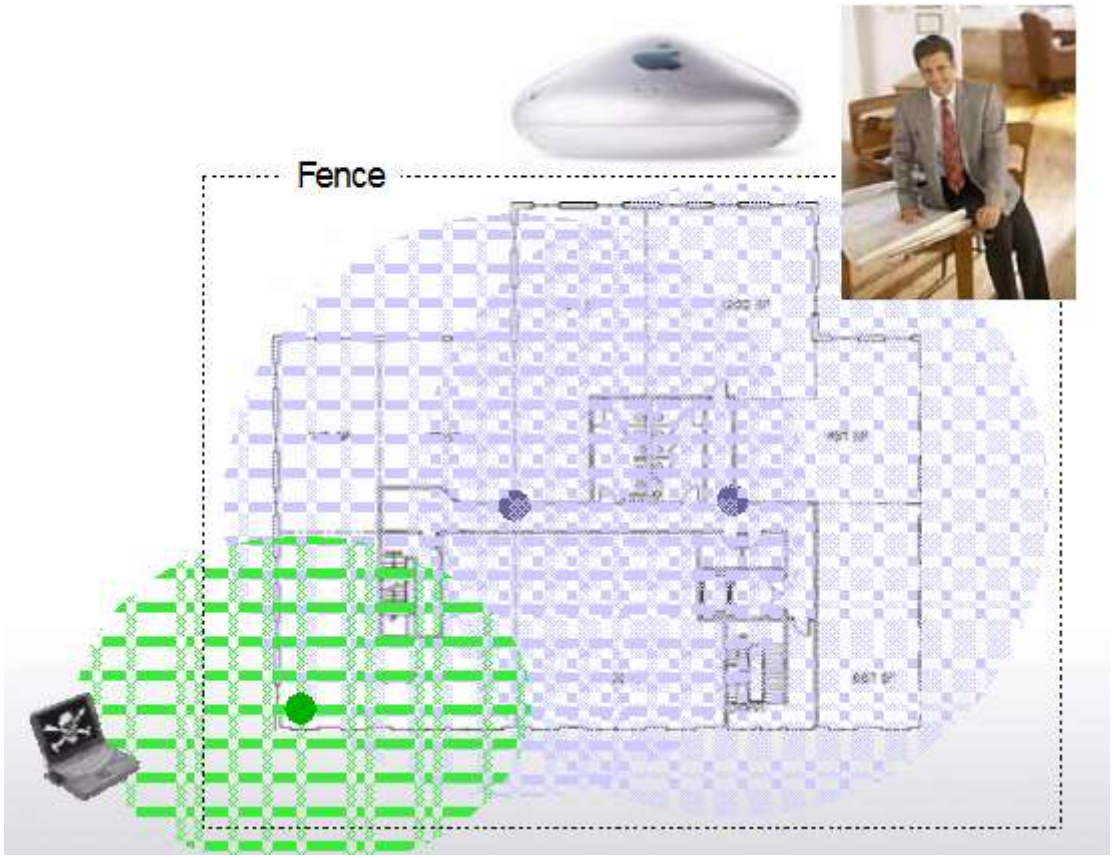
The attacker could relay traffic to the real AP, or use its own Internet connection to stage an MITM.

Even in encrypted networks this is a problem (even in WPA).



Rogue access points

- A huge problem for both wired and wireless networks are *rogue access points*.
- These are access points put into place without those managing the network being aware of them.
  - **They are usually not configured according to network policy**
- Setting them up is trivial and cheap, detecting them is difficult.



Wireless range

- Specification
  - 802.11b/g: 100m indoors
  - Bluetooth: 10m (or 100m)
- Reality
  - WiFi Yagi Rifle: 16km (WiFi)
  - BlueSniper: 1.6km (Bluetooth)
  - More if devices cooperate

BlueSniper in action

- Never base security on the range of the radio!
  - Assume that the attacker has a stronger transmitter and antenna than you do.

Conclusions on wireless

- Immature security mechanisms
  - Early versions have proven completely broken
  - New versions look good on paper
- Changes the extent of the network
- Challenge for completely wired networks
  - Rogue access points,
  - Laptops with ad-hoc networks
- Be aware of risks, use wireless with care.

Linköpings universitet

expanding reality

www.liu.se