Security Protocols

1. Data Link Layer Security: Focusing on WLAN

The **Datalink** lyaer of the OSI Model, deals with the transfer of data between adjacent network nodes within a wide area or local area network. The most common example of a protocol operating on the layer is that of **Ethernet**. This chapter, however will be concerned with the protection of wireless networks also known as **Wireless LAN Security**, this incorporates the use of the**IEEE 802.11i** standard. The goal of this chapter is to understand the current and future Wireless LAN security vulnerabilities and solutions.

1.1. Wireless LAN: An introduction

The `IEEE` ratified 802.11 (Wi-Fi) in 1997. Its primary focus is to provide protocols for Wireless LANS on both the first and second layers of the OSI model, the **Physical** and **Datalink** layers respectively. Such WLANS could transmit at either 1 Mb/s and 2 Mb/s. In order to promote interoperability between the different implementations of these protocols the Wi-Fi Alliance (Wireless Ethernet Compatibility Alliance) was set up to ensure that a certain degree of interoperability was achieved.

1.1.1. Components

There are two main pieces of equipment defined:

Wireless Station

> This is just a desktop, laptop or other wireless device that carries and uses a wireless **Network Interface Card** (NIC).

Access Point

> This is a bridge between the wireless and wired networks and is composed of an antenna, bridging software and a wired network interface, usually 802.3. It aggregates access for multiple wireless stations wired to the network.

1.1.2. Modes

There are two modes available:

Infrastructure

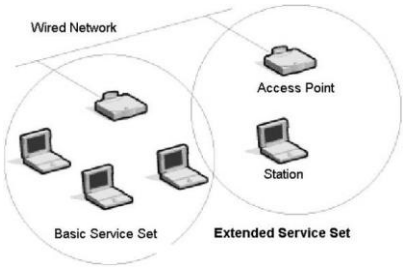

Figure 3. Adhoc Mode

Used to attach wireless nodes to an existing wired network via an access point. Each packet has attached the **Service Set Identifier** (SSID) for the **Basic Service Set** (BSS) that the station is attached to. Multiple access points with the same SSID form an **Extended Service Set** (ESS). See the figure above. Original image from http://www.acm.org/crossroads/xrds9-4/gfx/wlan_abc1.jpg

Adhoc

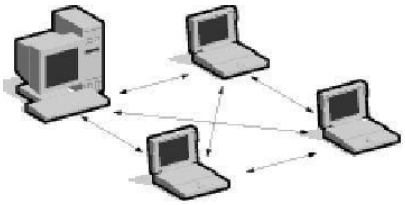

Figure 4. WLAN Modes

When no existing network service is available, ad-hoc mode, is used to facilitate the creation of a network between the stations. This is also known as an **Independent Basic Service Set** (IBSS). See the figure above. Original image fromhttp://www.acm.org/crossroads/xrds9-4/gfx/wlan_abc2.jpg

1.1.3. IEEE Protocol Standards

Here is a list of **some** of the existing protocol standards for Wireless LAN:

`IEEE 802.11`	Original standard in 2.4 GHz: 1 Mb/s or 2 Mb/s
`IEEE 802.11a`	PHY Standard in 5 GHz 8 channels 54 Mb/s possible
`IEEE 802.11b`	PHY Standard in 2.4 GHz 3 channels 11 Mb/s possible
`IEEE 802.11e`	MAC Standard QoS support

`IEEE 802.11f`	Inter-Access Point Protocol
`IEEE 802.11g`	PHY Standard in 2.4 GHz 3 channels 54 Mb/s possible
`IEEE 802.11n`	Higher throughput improvements 100+ Mb/s
`IEEE 802.11p`	vehicular networks
`IEEE 802.11u`	Inter-working with non-802 networks

1.2. Security History

1.2.1. Practicalities

Wireless LAN operates using radio signals, all an attacker needs to perform any attacks is equipment capable of monitoring and transmitting encrypted traffic. Passive attacks (monitoring) can be achieved through off-the-shelf equipment and modification of driver settings. The active attacks (transmission), are more difficult but through upgrades to the firmware of the PCMCIA cards, it is easier to achieve.

> **Note** Always assume that motivated attackers have full access to the link layer for passive and active attacks.

Usually attackers perform WarDriving, that is driving around a city searching for existing WLAN 802.11 networks. When one is found it is often the case that the attacker takes note of the: MAC Address, Network Name, SSID, Manufacturer, Channel, Signal Strength, Noise and possibly the location via GPS. There are various ways in which one can protect oneself from WarDriving, some of which are discussed during this chapter. However it is important that users be authenticated using protocols such as `EAP`and `RADIUS` or `DIAMETER`.

1.2.2. 802.11b Security Services

The security services offered by 802.11b are:

Authentication

Open System and Shared Key

Confidentiality, Access Control and Data Integrity

Wired Equivalence Privacy (WEP).

1.2.3. Access Control

Access Control is achieved in two ways. First, through the use of WEP encryption, an optional feature is used to discard packets that are not properly encrypted. Secondly, SSID can be used when: the access point does not broadcast the SSID, the station and access point use the same pre-configured SSID and the the station must specify the SSID (in management frames) to the access point when requesting association.

1.2.4. Ron's Code Number 4

Ron's Code Number 4 (RC4), is a symmetric key stream cipher developed by **Ron Rivest** in 1987 at RSA Security Inc. , it was a trade secret until it was leaked in 1994. RC4 uses keys in size ranging from 8 bits to 2048 bits. It uses the key to generate a stream of pseudo-random bits that are XORed with the plaintext to generate the cipher text.

1.2.5. Wired Equivalence Privacy

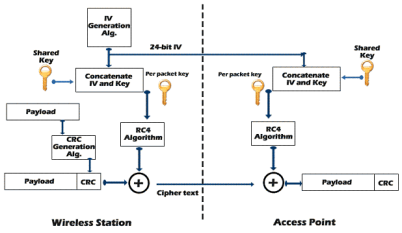

Figure 5. WEP

When using WEP, there is a shared key between all the stations and access points. In an ESS all the access points will usually have the same key. Usually there is no key management and keys are entered manually into the stations and action points. In a large WLAN this is stupid. Image from: http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_security/fig14.gif

Sending

When sending data using WEP, a **Integrity Check Vector** (ICV) is generated, its a 32bit Cyclic Redundancy Check code, that is appended to the message to form the plaintext. This CRC-code provides integrity. The resulting plaintext is encrypted (providing confidentiality) using RC4 by XORing the plaintext with a long key stream of pseudo-random bits. This key stream is a function that takes a 40-bit secret key and a 24-bit initialisation Vector (IV) as its input. This encryption is summarised in the left hand side of Figure wlan:wep. The resulting ciphertext is then transmitted.

Receiving

On receipt of a ciphertext, it is first decrypted using RC4, this involves the XORing of the ciphertext with a long key stream of pseudo-random bits. The key stream uses the same input as with the encryption. Once the plaintext has been obtained, the ICV is then checked by first extracting the sent ICV from the plain text and checking that against a newly computed ICV over the sent message. This decryption is summarised in the right hand side of Figure wlan:wep.

Safeguards

The shared key in WEP is used to connect to an access point and the sending and receiving of data. Though the distribution of keys is not defined, an external mechanism is required to populate a globally shared array of four keys. Each message sent will contain an key identifier field that specifies the index in the key array. Typically a single key is used for an entire network. Given that the messages are encrypted, this provides confidentiality. Integrity is achieved via a check-sum. However management traffic is still broadcasted in the clear and contains the SSID.

1.2.6. Initialisation Vector

The IV must be different for every message transmitted, this is optional. The 802.11 standard does not specify how this IV is calculated. Wireless cards can use several methods: **Ascending Counter**, **Alternate Ascending, Descending** or a **Pseudo random IV generator**. Though Ascending order is preferable.

1.3. Vulnerabilities

WEP is vulnerable to number of attacks.

1.3.1. Passive WEP

One passive attack can be performed by the attacker either collecting all traffic and analysing it or an attacker can collect two messages that are encrypted with the same key and same IV and perform a statistical analysis to reveal the plaintext. XORing the ciphertexts causes the key stream to cancel out and the result is an XOR of the two plaintexts. Then each of the XORed plaintexts can be calculated when there is partial knowledge of some part of the plaintexts.

This problem stems from a Birthday Paradox in relation to the IV. Given that the 24 bit IV is calculated from an ascending counter, it would take an access point transmitting at 11 Mb/s with a packet length of around 1500 bytes, around five hours to cycle i.e. unique IV's are exhausted. If a pseudo random generator was used the time taken is lessened. For

instance due to the Birthday paradox, assuming a probability of sequence number matching being 50% then collisions start to occur after around 5000 packets. Thus the IV can be recovered within a few minutes.

1.3.2. Example: Calculating time taken to break WEP

Question

> How many seconds should a receiving wireless node observe the traffic such that it can be 40% certain that it observes a collision? Explain your answer.

In order to determine the number of seconds, one must first calculate (using the birthday paradox) the number of packets that must be had in order to be sure that a collision has occurred. This will give us a worst case scenario and the number of packets can then be used to determine the time needed to transmit said packets. This number of packets is calculated as follows:

$$\mathbf{n} \approx \sqrt{(-2\ln(1-\mathbf{m}))} \times \sqrt{\mathbf{t}}$$

where:

n	is the number of packets before a collision
m=0.4	is the probability of a collision
$t=2^{24}$	total number of permissible IV

This ultimately results in:

$$\mathbf{n} \approx \sqrt{(-2\ln(1-0.4))} \times \sqrt{2^{24}} \approx 4140 \text{ packets}$$

Given the number of packets this will result in a total of:

$$4140 \times 1500 = 6210000 \text{ bytes}$$

being sent over the network. Given the maximum rate of `802.11a` being 54 Mbit/s (with error correction), then this will take:

$$\frac{6210000 \text{ bytes}}{54 \times 125000 \text{ bytes}} = \frac{6210000}{6750000} = 0.92 \text{ seconds}$$

to occur. Hence the station needs to wait 0.92 seconds.

1.3.3. Active WEP

If the attacker knows the plaintext and ciphertext pair, then the Keystream for the IV values are known, thus an attacker can build a decryption dictionary of tables indicating Keystream

IV value pairs. The attacker can now generate correctly encrypted messages by XORing the keystream against the plaintext. The subsequent ciphertexts are sent together with the known IV. As a result the Access point can be deceived into accepting messages.

Even still message authentication using CRC checksum is not secure enough as it is susceptible to bit flipping attacks, as a bit can be flipped in the ciphertext and the difference in the CRC-32 is computed. Hence integrity fails.

1.3.4. Limited WEP Keys

Some vendors allowed limited WEP keys. The user types in a passphrase and this is used to generate the WEP key. Passphrases facilitate only 21 bits of entropy in a 40 bit key. This reduces the key strength to 21 bits i.e. `2,097,152`, which can be brute forced in minutes. Even more so the remaining 19 bits are predictable. More information can be easily obtained Online.

1.3.5. Brute Force

Imagine that a ciphertext has been captured, the IV is included within this message. An attacker can search through all 40 bit combinations for possible secret keys i.e. `1,099,511,627,776` keys. On a modern laptop this takes approximately 170 days. The attacker simply finds the key that can decrypt the ciphertext. Vendors have extended WEP to use 128 bit keys, this is 104 bit secret key and 24 bit IV. Using a bruteforce technique it would take an attacker 10^{19} years to get the 104 bit key. This effectively safeguards against brute force attacks.

1.3.6. IV Weaknesses

[Fluher2001] presented a passive attack on WEP in which they were able to retrieve an entire secret key using four million packets, this is a relatively short amount of time. This works by retrieving information about all the key bytes when the pseudo-random number generator input is known.

WEP exposes part of the pseudo-random number generator input, the IV is transmitted with each message. Every wireless frame has a reliable and known first byte. This is from the **Sub-network Access Protocol** (SNAP) header as used in the logical link control layer, upper sub-layer of the data link layer. It is `0xAA`. An attacker can capture the packets with a weak IV (specific IV values that easy calculation of a key byte when previous key bytes are known). Determine the first byte of the ciphertext i.e. XOR`0xAA` with the first byte of the key stream, and then determine the key from the initial byte key stream. This is practical fro

40 bit and 104 bit keys. Software has also been developed to make this attack easier to perform:

Wepcrack

> First tool to demonstrate the attack using IV weaknesses, it is open source. It consists of: Weaker IV Generator, Search sniffer and Cracker. The search sniffer looks for the weaker IV's and records the first byte. The cracker, combines the weaker IV's and selected first bytes. This tool is cumbersome. http://wepcrack.sourceforge.net

Airsnort

> An automated tool that does everything until the key has been derived i.e. Sniffing, Searching for weaker IV and recording encrypted data. It takes around three to four hours to derive a key using anything from 100 Mb to 1 Gb of transmitted data.http://airsnort.shmoo.com/

One way to limit the number of IV based attacks is to avoid the weak IVs. **Fluher** described a simple method for finding weak IV. Manufacturers have avoided such IVs since 2002. Thus tools such as airsnort and others may not work on recent hardware. However, David Hulton has shown that a properly implemented attack can identify more weak IV. These are IV that leak into the second by of the key stream. The second byte of the SNAP header is also `0xAA`. As a result this attack also works on recent hardware and is faster on older.
See Aircrack-ng and WEP Lab for further details.

1.4. 802.11 Safeguards

Here several common safeguards for use with 802.11 and at times other wireless networks are given and described.

Security Policy and Architecture

> Be tough on usage policy, there should be clear definitions as to **what is allowed** and **what is not allowed**. Moreover one should also consider all threats and design the entire architecture to minimise risk.

Wireless as Untrusted LAN

> Ideally one should treat the wireless network as untrusted by default. This may dictate the inclusion of a firewall between the wireless and wired networks. Extra authentication for wireless users i.e. `EAP` as well as `RADIUS`. Addition of IDS system at the wireless/wired junction and vulnerability assessments.

Discover unauthorised use

Active searches for unauthorised access points, adhoc networks and clients is encouraged. This can be achieved through port scanning for unknown SNMP agents and unknown web/telnet interfaces. Wireless Intrusion Detection can also be useful e.g. AirMagnet, AirDefense, Trapeze… . Moreover **WarWalking** should be performed regularly. This is when WarDriving tools are used to sniff packets, identify IP addresses etc.

Access point audits

Access points should be subjected to frequent reviews. Such reviews can highlight insecure passwords and community strings. Ensure that firewalls and ACL's are maintained and implemented, and that there is a standard configuration on all access points i.e. SSID, WEP Keys etc, and the level of security is kept consistent.

Station protection

One should also protect the station. Personal firewalls defend against attackers. VPN's provide end-to-end security into a trusted network, but can suffer from roaming issues. Intrusion detection schemes can provide early warning of certain attacks. Configuration scanning, allows for a numpty check of the stations settings. Moreover strong encryption protocols such as `SSH` and `TLS/SSL` should be considered.

Access point location

Ideally the access points should be located in the centre of buildings. This allows not only for efficient use of the signal within the building but access points placed by windows, on external walls or with line of sight to the outside, improve the attackers chances.

Antenna design

It is best to utilise a directional antenna to point the radio signal instead of a normal broadcast antenna.

1.5. WLAN Security Enhancements

1.5.1. IEEE 802.1x

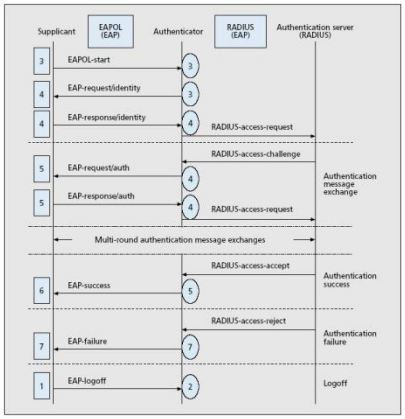

Figure 6. IEEE 802.1x Authentication Enhancements

Due to the problems encountered with authentication 802.11, `IEEE 802.1x` was created. It defines a security framework in the upper OSI layers to provide compatible authentication and authorisation for IEEE 802 LAN. It distributed the keys for 802.11 and enables authentication and encryption between Access Points and wireless stations. Its main components are: **Supplicant**(wireless station), **Authenticator** (access point), **Authentication Server**, `EAP RFC2284` and `EAPOL` (EAP over lans). Figure wlan:wep:enhance:8021x contains a summary. `IEEE 802.1x` adds more roaming support for supplicants in terms of:

Authentication

> A supplicant should re-authenticate with the Authenticator or the Authentication Server when roaming to another 802.1X-enabled network.

Intra-subnet roaming

> Facilitates movement from one Authenticator to another within the same IP subnet.

Inter-subnet roaming

> Facilitates movement from one Authenticator to another Authenticator located in another IP subnet (Supplicant has to change its IP address). It uses IETF Mobile IP to support mobility management in the IP layer.

More info on IEEE 802.1X can be found at http://www.ieee802.org/1/files/public/docs2000/8021xSecurity.PDF

1.5.2. Wi-Fi Protected Access

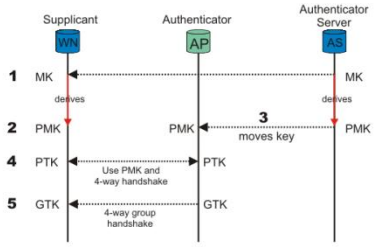

Figure 7. WPA Communication Enhancement

WPA is a successor to WEP, it has been designed to used more robust techniques to ensure the security of WLAN. Operates in two modes: **Home** — pre-shared keys are used; and **Enterprise**-- either `802.1x` authentication and key management or EAP and either `DIAMETER` or `RADIUS`.

Encryption

In WPA, a choice can be made between either **Temporal Key Integrity Protocol** (TKIP) or `WEP2`. Each utilise a 128-bit secret key. RC4 is now session based and utilises dynamic encryption keys. The IV has been increased to 48 bit with a new sequencing method. During operation, a **Temporal Key** is used and updated before the IV space is exhausted. Moreover `Michael` an 8 byte message integrity code is used instead of CRC-32.

Key Management

Key management can either be manual or automatic. If automatic, `IEEE 802.1X` is used. This implies that the supplicant and authentication server utilise both a Master Key and a Pairwise Master Key for communication. The authentication server sends the pairwise master key to the authenticator. The Supplicant and Authenticator use PMK and others, to generate each: Pairwise Transient Key (PTK) using four way handshake, and Group Transient Key (GTK) for encrypting broadcast messaging. The PTK consists of a EAPOL-Key Confirmation Key (KCK), EAPOL-Key Encryption Key (KEK) and the Temporal Key (TK 1 and 2) used for encrypting wireless traffic; TK is further computed using MAC address and 16 bit of IV to produce unique security key per wireless station. Figure wlan:wep:enhance:wpa:enc summarises this interaction.

Practical WPA Attacks

There are currently two known attacks on WPA.

Dictionary Attack

Attacks the pre-shared key
mode. http://www.securiteam.com/tools/6L00F0ABPC.html

DOS

If WPA equipment sees two packets with an invalid MiC in one second, all clients are disassociated and activity is stopped for a minute. Two malicious packets can be used to stop a wireless network for a minute.

WPA over WEP

In `WEP` the RC4 stream cipher was used with an Initialisation Vector (IV) length of 24-bits. The IV is used in conjunction with the Secret Key to generate a **Pseudorandom stream of bits** (the keystream) that is used to encrypt the data and is seen as an integral part of the RC4 Cipher. The IV is also appended to the Ciphertext during transmission. However as the IV is 24-bits in length the possible values for the IV will be repeated within a predetermined length of time. Together with a fixed secret key, an attacker can perform a passive attack that involves using messages that have been encrypted with the same key and the same IV. These messages will then be subjected to a statistical analysis that can be used to determine the plaintext. Furthermore an attacker with knowledge of known plaintext ciphertext pairs they use these pairings to build a **Rainbow-esque** Table for known Keystream and IV values. This can subsequently be used to produce {authentic messages}i.e. spoofing, that can be accepted by the ciphertext sufficiently that the `CrC` checksum value can be updated accordingly.

These attacks are possible as the data that can be collected contains enough linked information i.e. has high entropy, such that the the missing information e.g. plaintext and keystream, can be deduced. `WPA` has addressed the entropy question through:

- Increased RC4 Initialisation Vector (IV) Length
- Inclusion of Temporary Secret Keys; and
- New Message Integrity Check (MiC) Algorithm named **Michael**

In `WPA` the IV length has been increased to 48-bits, this increases the length of the cycle through which the IV is calculated. This will increase the number of messages that will be sent with a different IV. Also introduced in `WPA` is dynamic session keys (TKIP) that are 128-bits in length for the RC4 algorithm that stipulates a new key must be generated per session. Again this increases the amount of messages that will have differening IV and Secret Keys. In the case that the IV will become exhausted during the session a new secret key will be generated again increasing the amount of data. Finally the message authentication code has been supplmented with a new MiC called **Michael** that generates a 8-byte checksum rather than the 32-bit checksum given by `CRC-32`.

However it must be noted that `WPA` using TKIP is known to be vulnerable and that it has been suggested that networks must either use `WPA` with CCMP or `WPA2` that used CCMP by default.

1.5.3. IEEE 80211i

`IEEE 802.11i` defines **Robust Security Network** (RSN) used to create a RSN Associations (RSNAs) that include four way handshake mechanisms for robust security key management. It depends on 802.1x for authentication services and `802.1x` offers key management services. There are two modes:

RSN

> This is compatible with WPA2 as ratified by the Wi-Fi Alliance, supports RSNA and extends upon WPA.

Pre-RSN

> This is a combination of `IEEE 802.11` entity authentication and WEP.

Other enhancements include the **RSN Authentication**, this is similar to WPA in that it utilises `IEEE 802.11x` for authentication and key management. Also Key establishment and management is similar for both manual and automatic modes. However in automatic mode `AES` is used instead of `TKIP`. For encryption there are two modes of operation:

Transient Security Network

> Short term and optional, it uses `TKIP` and is based upon a mode of RC4, that uses 128 bit key and 48 bit IV, also Michael is used.

Mandatory

> Long term. Operation is based upon AES, with a 128 key and 128 bit block size. AES is configured to use **Counter Mode with Cipher Block Chaining Messenger Authentication Code Protocol** (CCMP) `RFC3610`. Counter mode (CTR) is for encryption and CBC-MAC is for calculation of the MiC. Moreover a temporal key for AES is generated for every session and packet number repetition.

More information can be found: Online

1.5.4. Similarities between WPA and IEEE 802.11i

`IEEE 802.11i` is a security enhancement to the `IEEE 802.11` standard dealing primarily with encryption and authentication. `WPA2`(an enhancement/solidifcation of WPA) is a standard from the Wifi-Alliance based upon the `IEEE 802.11i`. Hence it can be said that

there is a multitude of similarities between the two. With three of the important similarities being in relation to encryption and message integrity, key establishment and management, and finally authentication.

Encryption and Message Integrity

Both standards require that the more secure AES derived **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol** (CCMP) be used for encryption and message integrity, instead of the TKIP Protocol. The Counter Mode Protocol is for encryption and the **Cipher Block Chaining Message Authentication Code** is used for message integrity. However in `IEEE 802.11i` TKIP can be used as an alternative while in `WPA2` TKIP has been deprecated. Interestingly the situation is reversed for `WPA` in that TKIP is mandatory and CCMP is optional.

Authentication

As mentioned in **Key Establishment and Management** the `IEEE 802.1x` standard is stipulated for authentication. This standard stipulates a **four-way handshake** and **group-key handshake** for the authentication and authorisation of stations.

Key Establishment and Management

Finally n both standards there are two operating modes an **Enterprise Mode** aimed at Business and Government Networks and also a **Personal Mode** that is suitable for Small Business and Personal Networks. The Personal Mode in both stipulates the use of pre-shared keys and the CCMP encryption. Whereas the **Enterprise Mode** stipulates that the `IEEE 802.1x` standard for authentication be used to obtain the required cryptographic keys. A **four-way handshake** is used to obtain the **Pairwise Transient Key** that is used for communication between the device and the Access Point. A **group key handshake** is used to obtained the **Group Transient Key** that is used decrypt messages that have been broadcasted to the network.

1.6. Summary

In this chapter we have discussed various WLAN security concepts. Discussed currently deployed WLAN security vulnerabilities and enhancements that can be made.

1.7. Recommended Reading

The information in this chapter has been based upon the following material:

- **Wireless LAN Security**, a presentation by **Matthew Joyce** of Rutherford Appleton Laboratory, Council for the Central Laboratory of the Research Councils (CCLRC), UK
- **Wireless LAN Security and IEEE 802.11i**, IEEE Wireless Communications, February 2005.
- **Intercepting Mobile Communications: The Insecurity of 802.11**, Mobile Computing and Networking, July 16-21, 2001

Source: http://jfdm.host.cs.st-andrews.ac.uk/notes/netsec/#_security_attacks