**Syrian Arab Republic**

**Ministry of Education**

**National Center for the Distinguished**

**A Seminar Named:**

**Wireless Securities**

**Presented by: Amir Najjar**

**Supervised by: Mr. Amjad Taha**

**11th grade**

**2015-2016**

Contents

[Modes of unauthorized access: 2](#_Toc437837545)

[Accidental association: 2](#_Toc437837546)

[Malicious association: 2](#_Toc437837547)

[Ad hoc networks: 3](#_Toc437837548)

[Identity theft (MAC spoofing): 4](#_Toc437837549)

[Man-in-the-middle attacks: 4](#_Toc437837550)

[Denial of service: 5](#_Toc437837551)

[Network injection: 5](#_Toc437837552)

[Caffe Latte attack: 5](#_Toc437837553)

[Wireless intrusion prevention concepts: 6](#_Toc437837554)

[A wireless intrusion prevention system: 7](#_Toc437837555)

[Security measures: 7](#_Toc437837556)

[SSID hiding: 7](#_Toc437837557)

[MAC ID filtering: 7](#_Toc437837558)

[Static IP addressing: 8](#_Toc437837559)

[802.11 security: 8](#_Toc437837560)

[Regular WEP: 8](#_Toc437837561)

[WPAv1: 8](#_Toc437837562)

[Additions to WPAv1: 9](#_Toc437837563)

[TKIP: 10](#_Toc437837564)

[EAP: 10](#_Toc437837565)

[EAP-versions: 10](#_Toc437837566)

[LEAP: 10](#_Toc437837567)

[PEAP: 11](#_Toc437837568)

[Other EAPs: 11](#_Toc437837569)

[Restricted access networks: 11](#_Toc437837570)

[End-to-end encryption: 11](#_Toc437837571)

[802.11i security: 12](#_Toc437837572)

[WPAv2: 12](#_Toc437837573)

[Additions to WPAv2: 13](#_Toc437837574)

[WAPI: 13](#_Toc437837575)

[Smart cards, USB tokens, and software tokens: 13](#_Toc437837576)

[RF shielding: 14](#_Toc437837577)

[Conclusion: 15](#_Toc437837578)

[References: 16](#_Toc437837579)

**Introduction:**

**What are wireless securities? And why do we use them?**

**What modes of unauthorized access are there?**

**How do we prevent intrusion to our wireless network?**

**What are the security measures that we should take?**

**Could we come up with a new type of wireless security? Or we would be just developing current security types?**

**We’re going to discuss all this in this Seminar.**

# **Modes of unauthorized access:**

## **Accidental association[[1]](#footnote-1):**

Violation of the security perimeter of a corporate network can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

Accidental association is a case of wireless vulnerability called as "mis-association".[[2]](#footnote-2) Mis-association can be accidental, deliberate (for example, done to bypass corporate firewall) or it can result from deliberate attempts on wireless clients to lure them into connecting to attacker's APs.

## **Malicious association[[3]](#footnote-3):**

“Malicious associations” are when wireless devices can be actively made by attackers to connect to a company network through their laptop instead of a company access point (AP). These types of laptops are known as “soft APs” and are created when a cyber-criminal runs some software that makes his/her wireless network card look like a legitimate access point. Once the thief has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with some protection but are still vulnerable to hacking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level.

## **Ad hoc networks[[4]](#footnote-4):**

Ad hoc networks can pose a security threat. Ad hoc networks are defined as [peer to peer] networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.[[5]](#footnote-5)

The security hole provided by Ad hoc networking is not the Ad hoc network itself but the bridge it provides into other networks, usually in the corporate environment, and the unfortunate default settings in most versions of Microsoft Windows to have this feature turned on unless explicitly disabled. Thus the user may not even know they have an unsecured Ad hoc network in operation on their computer. If they are also using a wired or wireless infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad hoc connection. Bridging is in two forms. A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and an indirect bridge which is the shared resources on the user computer. The indirect bridge provides two security hazards. The first is that critical organizational data obtained via the secured network may be on the user's end node computer drive and thus exposed to discovery via the unsecured Ad hoc network. The second is that a computer virus or otherwise undesirable code may be placed on the user's computer via the unsecured Ad hoc connection and thus has a route to the organizational secured network. In this case, the person placing the malicious code need not "crack" the passwords to the organizational network, the legitimate user has provided access via a normal and routine log-in. The malefactor simply needs to place the malicious code on the unsuspecting user's end node system via the open (unsecured) Ad hoc networks.[[6]](#footnote-6)

## **Identity theft (MAC spoofing)[[7]](#footnote-7):**

Identity theft (or MAC spoofing) occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the hacker desires,[[8]](#footnote-8) and the hacker can easily get around that hurdle.

MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

## **Man-in-the-middle attacks:**

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a “de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the hacker’s soft AP (disconnects the user from the modem so they have to connect again using their password which one can extract from the recording of the event). Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

## **Denial of service:**

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various cracking tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

## **Network injection:**

In a network injection attack, a hacker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP. The hacker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

## **Caffe Latte attack:**

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client.[[9]](#footnote-9) By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.[[10]](#footnote-10)

# **Wireless intrusion prevention concepts:**

There are three principal ways to secure a wireless network.

* For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.
* For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
* Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However, there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. The system of qualifying is an international consensus as specified in ISO/IEC 15408.

## **A wireless intrusion prevention system:**

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks.[[11]](#footnote-11) However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is considered so important to wireless security that in July 2009, the Payment Card Industry Security Standards Council published wireless guidelines[[12]](#footnote-12) for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

# **Security measures[[13]](#footnote-13):**

There are a range of wireless security measures, of varying effectiveness and practicality.

## **SSID hiding:**

A simple but ineffective method to attempt to secure a wireless network is to hide the SSID (Service Set Identifier).[[14]](#footnote-14) This provides very little protection against anything but the most casual intrusion efforts.

## **MAC ID filtering:**

One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this address.

## **Static IP addressing:**

Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.[[15]](#footnote-15)

## **802.11 security:**

IEEE 802.1X is the IEEE Standard authentication mechanisms to devices wishing to attach to a Wireless LAN.

## **Regular WEP:**

The Wired Equivalent Privacy (WEP) encryption standard was the original encryption standard for wireless, but since 2004 with the ratification WPA2 the IEEE has declared it "deprecated",[[16]](#footnote-16) and while often supported, it is seldom or never the default on modern equipment.

Concerns were raised about its security as early as 2001,[[17]](#footnote-17) dramatically demonstrated in 2005 by the FBI,[[18]](#footnote-18) yet in 2007 T.J. Maxx admitted a massive security breach due in part to a reliance on WEP[[19]](#footnote-19) and the Payment Card Industry took until 2008 to prohibit its use - and even then allowed existing use to continue until June 2010.[[20]](#footnote-20)

## **WPAv1:**

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address the problems with WEP. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password (e.g. 14 random letters) or passphrase (e.g. 5 randomly chosen words) makes pre-shared key WPA virtually uncrackable. The second generation of the WPA security protocol (WPA2) is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance. With all those encryption schemes, any client in the network that knows the keys can read all the traffic.

Wi-Fi Protected Access (WPA) is a software/firmware improvement over WEP. All regular WLAN-equipment that worked with WEP are able to be simply upgraded and no new equipment needs to be bought. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP. The TKIP encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices. The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

WPA Enterprise provides RADIUS based authentication using 802.1x. WPA Personal uses a pre-shared Shared Key (PSK) to establish the security using an 8 to 63 character passphrase. The PSK may also be entered as a 64 character hexadecimal string. Weak PSK passphrases can be broken using off-line dictionary attacks by capturing the messages in the four-way exchange when the client reconnects after being deauthenticated. Wireless suites such as aircrack-ng can crack a weak passphrase in less than a minute. Other WEP/WPA crackers are AirSnort and Auditor Security Collection.[[21]](#footnote-21) Still, WPA Personal is secure when used with ‘good’ passphrases or a full 64-character hexadecimal key.

There was information, however, that Erik Tews (the man who created the fragmentation attack against WEP) was going to reveal a way of breaking the WPA TKIP implementation at Tokyo's PacSec security conference in November 2008, cracking the encryption on a packet in between 12–15 minutes.[[22]](#footnote-22) Still, the announcement of this 'crack' was somewhat overblown by the media, because as of August, 2009, the best attack on WPA (the Beck-Tews attack) is only partially successful in that it only works on short data packets, it cannot decipher the WPA key, and it requires very specific WPA implementations in order to work.[[23]](#footnote-23)

### Additions to WPAv1:

In addition to WPAv1, TKIP, WIDS and EAP may be added alongside. Also, VPN-networks (non-continuous secure network connections) may be set up under the 802.11-standard. VPN implementations include PPTP, L2TP, IPsec and SSH. However, this extra layer of security may also be cracked with tools such as Anger, Deceit and Ettercap for PPTP;[[24]](#footnote-24) and ike-scan, IKEProbe, ipsectrace, and IKEcrack for IPsec-connections.

## **TKIP:**

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

## **EAP:**

The WPA-improvement over the IEEE 802.1X standard already improved the authentication and authorization for access of wireless and wired LANs. In addition to this, extra measures such as the Extensible Authentication Protocol (EAP) have initiated an even greater amount of security. This, as EAP uses a central authentication server. Unfortunately, during 2002 a Maryland professor discovered some shortcomings. Over the next few years these shortcomings were addressed with the use of TLS and other enhancements.[[25]](#footnote-25) This new version of EAP is now called Extended EAP and is available in several versions; these include: EAP-MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP, EAP-FAST, EAP-TLS, EAP-TTLS, MSCHAPv2, and EAP-SIM.

## **EAP-versions:**

EAP-versions include LEAP, PEAP and other EAP's.

### LEAP:

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not secure; THC-LeapCracker can be used to break Cisco’s version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. Anwrap and asleap finally are other crackers capable of breaking LEAP.[[26]](#footnote-26)

### PEAP:

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

Other EAPs:

There are other types of Extensible Authentication Protocol implementations that are based on the EAP framework. The framework that was established supports existing EAP types as well as future authentication methods.[[27]](#footnote-27) EAP-TLS offers very good protection because of its mutual authentication. Both the client and the network are authenticated using certificates and per-session WEP keys. EAP-FAST also offers good protection. EAP-TTLS is another alternative made by Certicom and Funk Software. It is more convenient as one does not need to distribute certificates to users, yet offers slightly less protection than EAP-TLS.[[28]](#footnote-28)

## **Restricted access networks:**

Solutions include a newer system for authentication, IEEE 802.1x, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

## **End-to-end encryption:**

One can argue that both layer 2 and layer 3 encryption methods are not good enough for protecting valuable data like passwords and personal emails. Those technologies add encryption only to parts of the communication path, still allowing people to spy on the traffic if they have gained access to the wired network somehow. The solution may be encryption and authorization in the application layer, using technologies like SSL, SSH, GnuPG, PGP and similar.

The disadvantage with the end-to-end method is, it may fail to cover all traffic. With encryption on the router level or VPN, a single switch encrypts all traffic, even UDP and DNS lookups. With end-to-end encryption on the other hand, each service to be secured must have its encryption "turned on", and often every connection must also be "turned on" separately. For sending emails, every recipient must support the encryption method, and must exchange keys correctly. For Web, not all web sites offer https, and even if they do, the browser sends out IP addresses in clear text.

The most prized resource is often access to Internet. An office LAN owner seeking to restrict such access will face the nontrivial enforcement task of having each user authenticate themselves for the router.

## **802.11i security:**

The newest and most rigorous security to implement into WLAN's today is the 802.11i RSN-standard. This full-fledged 802.11i standard (which uses WPAv2) however does require the newest hardware (unlike WPAv1), thus potentially requiring the purchase of new equipment. This new hardware required may be either AES-WRAP (an early version of 802.11i) or the newer and better AES-CCMP-equipment. One should make sure one needs WRAP or CCMP-equipment, as the 2 hardware standards are not compatible.

## **WPAv2:**

WPA2 is a WiFi Alliance branded version of the final 802.11i standard.[[29]](#footnote-29) The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and preshared key (PSK).

The number of WPA and WPA2 networks are increasing, while the number of WEP networks are decreasing,[[30]](#footnote-30) because of the security vulnerabilities in WEP.

WPA2 has been found to have at least one security vulnerability, nicknamed Hole196. The vulnerability uses the WPA2 Group Temporal Key (GTK), which is a shared key among all users of the same BSSID, to launch attacks on other users of the same BSSID. It is named after page 196 of the IEEE 802.11i specification, where the vulnerability is discussed. In order for this exploit to be performed, the GTK must be known by the attacker.[[31]](#footnote-31)

### Additions to WPAv2:

Unlike 802.1X, 802.11i already has most other additional security-services such as TKIP. Just as with WPAv1, WPAv2 may work in cooperation with EAP and a WIDS.

## **WAPI:**

This stands for WLAN Authentication and Privacy Infrastructure. This is a wireless security standard defined by the Chinese government.

## **Smart cards, USB tokens, and software tokens:**

This is a very strong form of security. When combined with some server software, the hardware or software card or token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will very frequently generate a new encryption code. The server will be time synced to the card or token. This is a very secure way to conduct wireless transmissions. Companies in this area make USB tokens, software tokens, and smart cards. They even make hardware versions that double as an employee picture badge. Currently the safest security measures are the smart cards / USB tokens. However, these are expensive. The next safest methods are WPA2 or WPA with a RADIUS server. Any one of the three will provide a good base foundation for security. The third item on the list is to educate both employees and contractors on security risks and personal preventive measures. It is also IT's task to keep the company workers' knowledge base up-to-date on any new dangers that they should be cautious about. If the employees are educated, there will be a much lower chance that anyone will accidentally cause a breach in security by not locking down their laptop or bring in a wide open home access point to extend their mobile range. Employees need to be made aware that company laptop security extends to outside of their site walls as well. This includes places such as coffee houses where workers can be at their most vulnerable. The last item on the list deals with 24/7 active defense measures to ensure that the company network is secure and compliant. This can take the form of regularly looking at access point, server, and firewall logs to try to detect any unusual activity. For instance, if any large files went through an access point in the early hours of the morning, a serious investigation into the incident would be called for. There are a number of software and hardware devices that can be used to supplement the usual logs and usual other safety measures.

## **RF shielding:**

It’s practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility. This can significantly improve wireless security because it’s difficult for hackers to receive the signals beyond the controlled area of an enterprise, such as within parking lots.[[32]](#footnote-32)

Despite security measures as encryption, hackers may still be able to crack them. This is done using several techniques and tools. An overview of them can be found at the Network encryption cracking article, to understand what we are dealing with. Understanding the mindset/techniques of the hacker allows one to better protect their system.

For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.

For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN. Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

# **Conclusion:**

**Wireless security** is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

There are too many ways to protect our networks, like:

* Using encryption and MAC Checks.
* Hide the network’s SSID.
* ­­­­­­­­­­­Use MAC ID Filtering and prevent MAC Spoofing by protecting the clients’.
* Use 802.11x or 802.11i security concepts.
* Use wireless encryption methods like (WEP, WPA1, WPA2**(recommended)**).
* Don’t use wired-networks, but use wireless networks.
* You can keep your network open, but use a proxy server and port to be able to access the network.
* Protect your network using methods like TKIP, WIPS, AES-CCMP.

**But could we really invent a new security method? Or would we be just developing the current ones?**

If we’re speaking about encryption, then just reversing our phrase would be a new encryption method, you can refer back to my project in the 10th grade about text cryptography, and find out that me and my “project-mates” did invent new encryption algorithms.

We can also fix the breaches that were found in WEP, and those who were in WPA2 (Such as Hole196)

So we would be inventing a new security method.

# **References:**

-<http://searchmobilecomputing.techtarget.com/tip/Guilt-by-accidental-association-The-distinctions-between-rogue-and-unapproved-access-points>

-"Top reasons why corporate WiFi clients connect to unauthorized networks". InfoSecurity. Retrieved 2010-03-22.

<http://www.infosecurity-us.com/view/7410/comment-top-reasons-why-corporate-wifi-clients-connect-to-unauthorized-networks-/>

-<http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/bournejc/wireless_security.html>

-Margaret Rouse. "Encryption". TechTarget. Retrieved 26 May 2015.

<http://searchsecurity.techtarget.com/definition/encryption>

-<http://www.journals.elsevier.com/ad-hoc-networks/>

- Bradely Mitchell. "What is Ad-Hoc Mode in Wireless Networking?". about tech. Retrieved 26 May 2015.

<http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm>

-"SMAC 2.0 MAC Address Changer". klcconsulting.com. Retrieved 2008-03-17.

<http://www.klcconsulting.net/smac/>

-Lisa Phifer. "The Caffe Latte Attack: How It Works—and How to Block It". wi-fiplanet.com. Retrieved 2008-03-21.

<http://www.wi-fiplanet.com/tutorials/article.php/10724_3716241_1>

-"Caffe Latte with a Free Topping of Cracked WEP: Retrieving WEP Keys from Road-Warriors". Retrieved 2008-03-21.

<http://www.airtightnetworks.com/home/news/pr/select_category/14/article/123/airtight-wireless-security-researcher-reveals-wep-can-be-cracked-without-an-access-point.html>

-"Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards".

<https://www.pcisecuritystandards.org/>

-*"PCI DSS Wireless Guidelines" (PDF). Retrieved 2009-07-16.*

<https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf>

-"The six dumbest ways to secure a wireless LAN", George Ou, March 2005, ZDNet

<http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43>

-*"What is a WEP key?". lirent.net. Retrieved 2008-03-11.* <http://lirent.net/wifi/what-is-a-wep-key.html>

-[e.g. “Weaknesses in the Key Scheduling Algorithm of RC4” by Fluhrer, Mantin and Shamir.

-"FBI Teaches Lesson in How to Break into Wi-Fi Networks", informationweek.com. <http://www.informationweek.com/news/160502612>

-"Analyzing the TJ Maxx Data Security Fiasco", New York State Society of CPAs.

<http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm>

*-"PCI DSS 1.2".* [*http://www.infosecstuff.com/pci-dss-12/*](http://www.infosecstuff.com/pci-dss-12/)

*-Hacking Wireless Networks for Dummies*

*-Robert McMillan. "Once thought safe, WPA Wi-Fi encryption is cracked".* [*IDG*](https://en.wikipedia.org/wiki/International_Data_Group)*. Retrieved 2008-11-06.* [*http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258*](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258)

-Nate Anderson (2009). "One-minute WiFi crack puts further pressure on WPA". Ars Technica. Retrieved 2010-06-05.

<http://arstechnica.com/tech-policy/news/2009/08/one-minute-wifi-crack-puts-further-pressure-on-wpa.ars>

-Kevin Beaver, Peter T. Davis, Devin K. Akin. Hacking Wireless Networks For Dummies. Retrieved 2009-02-09.

<http://books.google.com/books?id=i0Edxmcly1oC&pg=PA295&lpg=PA295&dq=deceit+pptp&source=bl&ots=nY2yJjStHU&sig=mYiCPZWaSzgY6L9e4m6CzZFP-Y8>

-"Extensible Authentication Protocol Overview". TechNet. Retrieved 26 May 2015.

<https://technet.microsoft.com/en-us/library/bb457039.aspx>

-"Extensible Authentication Protocol Overview". *Microsoft TechNet*. Retrieved2008-10-02. <http://www.microsoft.com/technet/network/eap/eap.mspx>

- George Ou. "Ultimate wireless security guide: A primer on Cisco EAP-FAST authentication". *TechRepublic*. Archived from the original on 2012-07-07. Retrieved2008-10-02.

<http://archive.is/Htb0>

- "WiGLE - Wireless Geographic Logging Engine - Stats".

<https://wigle.net/gps/gps/main/stats>

- "WPA2 Hole196 Vulnerability".

<http://www.airtightnetworks.com/WPA2-Hole196>

- "How to: Improve Wireless Security with Shielding". Retrieved 2008-10-09.

<http://www.wireless-nets.com/resources/tutorials/rf_shielding.html>

1. <http://searchmobilecomputing.techtarget.com/tip/Guilt-by-accidental-association-The-distinctions-between-rogue-and-unapproved-access-points> [↑](#footnote-ref-1)
2. [*"Top reasons why corporate WiFi clients connect to unauthorized networks"*](http://www.infosecurity-us.com/view/7410/comment-top-reasons-why-corporate-wifi-clients-connect-to-unauthorized-networks-/)*. InfoSecurity. Retrieved 2010-03-22.* [↑](#footnote-ref-2)
3. <http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/bournejc/wireless_security.html> [↑](#footnote-ref-3)
4. <http://www.journals.elsevier.com/ad-hoc-networks/> [↑](#footnote-ref-4)
5. *Margaret Rouse.* [*"Encryption"*](http://searchsecurity.techtarget.com/definition/encryption)*. TechTarget. Retrieved 26 May 2015.* [↑](#footnote-ref-5)
6. *Bradely Mitchell.* [*"What is Ad-Hoc Mode in Wireless Networking?"*](http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm)*. about tech. Retrieved 26 May 2015.* [↑](#footnote-ref-6)
7. <http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/bournejc/wireless_security.html> [↑](#footnote-ref-7)
8. [*"SMAC 2.0 MAC Address Changer"*](http://www.klcconsulting.net/smac/)*. klcconsulting.com. Retrieved 2008-03-17.* [↑](#footnote-ref-8)
9. *Lisa Phifer.* [*"The Caffe Latte Attack: How It Works—and How to Block It"*](http://www.wi-fiplanet.com/tutorials/article.php/10724_3716241_1)*. wi-fiplanet.com. Retrieved 2008-03-21.* [↑](#footnote-ref-9)
10. [*"Caffe Latte with a Free Topping of Cracked WEP: Retrieving WEP Keys from Road-Warriors"*](http://www.airtightnetworks.com/home/news/pr/select_category/14/article/123/airtight-wireless-security-researcher-reveals-wep-can-be-cracked-without-an-access-point.html)*. Retrieved 2008-03-21.* [↑](#footnote-ref-10)
11. [*"Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards"*](https://www.pcisecuritystandards.org/)*.* [↑](#footnote-ref-11)
12. [*"PCI DSS Wireless Guidelines"*](https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf) *(PDF). Retrieved 2009-07-16.* [↑](#footnote-ref-12)
13. <http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/bournejc/wireless_security.html> [↑](#footnote-ref-13)
14. ["The six dumbest ways to secure a wireless LAN"](http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43), George Ou, March 2005, ZDNet [↑](#footnote-ref-14)
15. ["The six dumbest ways to secure a wireless LAN"](http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43), George Ou, March 2005, ZDNet. [↑](#footnote-ref-15)
16. [*"What is a WEP key?"*](http://lirent.net/wifi/what-is-a-wep-key.html)*. lirent.net. Retrieved 2008-03-11.* [↑](#footnote-ref-16)
17. [e.g. “Weaknesses in the Key Scheduling Algorithm of RC4” by Fluhrer, Mantin and Shamir [↑](#footnote-ref-17)
18. ["FBI Teaches Lesson In How To Break Into Wi-Fi Networks"](http://www.informationweek.com/news/160502612), informationweek.com [↑](#footnote-ref-18)
19. ["Analyzing the TJ Maxx Data Security Fiasco"](http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm), New York State Society of CPAs [↑](#footnote-ref-19)
20. [*"PCI DSS 1.2"*](http://www.infosecstuff.com/pci-dss-12/)*.* [↑](#footnote-ref-20)
21. Hacking Wireless Networks for Dummies [↑](#footnote-ref-21)
22. Robert McMillan. ["Once thought safe, WPA Wi-Fi encryption is cracked"](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258). [IDG](https://en.wikipedia.org/wiki/International_Data_Group). Retrieved 2008-11-06. [↑](#footnote-ref-22)
23. Nate Anderson (2009). ["One-minute WiFi crack puts further pressure on WPA"](http://arstechnica.com/tech-policy/news/2009/08/one-minute-wifi-crack-puts-further-pressure-on-wpa.ars). [Ars Technica](https://en.wikipedia.org/wiki/Ars_Technica). Retrieved 2010-06-05. [↑](#footnote-ref-23)
24. Kevin Beaver, Peter T. Davis, Devin K. Akin. [Hacking Wireless Networks For Dummies](http://books.google.com/books?id=i0Edxmcly1oC&pg=PA295&lpg=PA295&dq=deceit+pptp&source=bl&ots=nY2yJjStHU&sig=mYiCPZWaSzgY6L9e4m6CzZFP-Y8). Retrieved 2009-02-09. [↑](#footnote-ref-24)
25. ["Extensible Authentication Protocol Overview"](https://technet.microsoft.com/en-us/library/bb457039.aspx). TechNet. Retrieved 26 May 2015. [↑](#footnote-ref-25)
26. Hacking Wireless Networks for Dummies [↑](#footnote-ref-26)
27. ["Extensible Authentication Protocol Overview"](http://www.microsoft.com/technet/network/eap/eap.mspx). [*Microsoft TechNet*](https://en.wikipedia.org/wiki/Microsoft_TechNet). Retrieved2008-10-02. [↑](#footnote-ref-27)
28. George Ou. ["Ultimate wireless security guide: A primer on Cisco EAP-FAST authentication"](http://archive.is/Htb0). *[TechRepublic](https://en.wikipedia.org/wiki/TechRepublic" \o "TechRepublic)*. Archived from [the original](http://articles.techrepublic.com.com/5100-10878_11-6148557.html) on 2012-07-07. Retrieved2008-10-02. [↑](#footnote-ref-28)
29. ["Wi-Fi Protected Access"](https://web.archive.org/web/20070521092851/http:/www.wifialliance.org/knowledge_center_overview.php?docid=4486). [*Wi-Fi Alliance*](https://en.wikipedia.org/wiki/Wi-Fi_Alliance). Retrieved 2008-02-06. [↑](#footnote-ref-29)
30. ["WiGLE - Wireless Geographic Logging Engine - Stats"](https://wigle.net/gps/gps/main/stats). [↑](#footnote-ref-30)
31. ["WPA2 Hole196 Vulnerability"](http://www.airtightnetworks.com/WPA2-Hole196). [↑](#footnote-ref-31)
32. ["How to: Improve Wireless Security with Shielding"](http://www.wireless-nets.com/resources/tutorials/rf_shielding.html). Retrieved 2008-10-09. [↑](#footnote-ref-32)