

Evaluation of current security mechanisms and lacks in wireless and Bluetooth networks

Dr. Kai-Oliver Detken
DECOIT GmbH

Fahrenheitstraße 9, D-28359 Bremen
e-mail: detken@decoit.de, phone: +49-421-596064-01, fax: +49-421-596064-09

Prof. Dr. Evren Eren

University of Applied Sciences Dortmund
Emil-Figge-Str. 42, D-44227 Dortmund
e-mail: eren@fh-dortmund.de, phone: +49-231-755-6776, fax: +49-231-755-6776

Abstract

This paper deals with the subject of security of wireless technologies such as Wireless LAN (WLAN) and Bluetooth. It deals with WLAN technologies and their different characteristics and focuses on security mechanisms. These include WEP, dynamic WEP, WPA-PSK, WPA-RADIUS, WPA2, 802.1X, EAP, TKIP, and Robust Secure Networks (802.11i). These mechanisms have been examined and evaluated to identify weaknesses. The target of this contribution is to evaluate current WLAN technologies with regards to security and present solutions to prevent wireless hacking attacks. It is necessary to integrate wireless technologies into the security platform of a company as an integral part. We suggest aspects to transform these points into the global security policies of a company or other institution.

Furthermore, this paper deals with the subject of Bluetooth security. Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth offers a way to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, digital cameras and video game consoles via a secure, globally unlicensed short-range radio frequency. Bluetooth is not the first wireless technology, however, it is easier to handle than e.g. WLAN. Furthermore, this technology does not require line of sight conditions like infrared solutions. Although the application layer includes many security mechanisms which involve an interaction with the user the protocol lacks security. In this paper the possible security lacks of Bluetooth will be examined, i.e. design and implementation weakness will be assessed and security lacks will be shown. Additional attack variants will be described.

WLAN technology

A wireless LAN or WLAN is a wireless local area network, which connects two or more computers not by using wires, but radio communication. WLAN utilises spread-spectrum technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network. This technology is becoming increasingly popular, especially with the rapid emergence of

small portable devices such as PDAs (personal digital assistants).

One big issue with wireless networks in general, and WLANs in particular, involves the need for security. Many early access points could not discern whether a particular user had authorisation to access the network or not. Although this problem reflects issues that have troubled many types of wired networks for a long time, it did not usually pose a significant problem, since many organisations had reasonably good physical security. However, the fact that radio signals bleed outside of buildings and across property lines makes physical security largely irrelevant to war drivers.

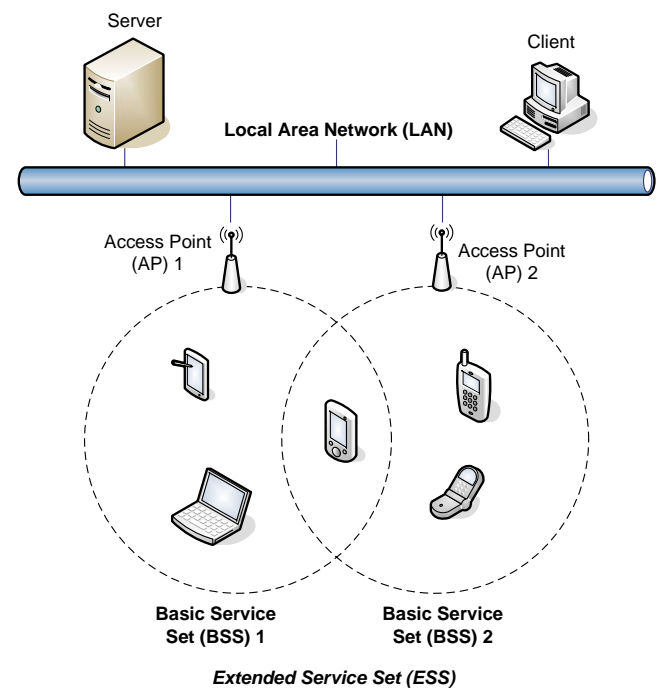


Figure 1: WLAN architecture

Anyone within the geographical network range of an open, unencrypted wireless network can sniff on traffic, gain unauthorised access to internal network resources as well as to the Internet, allowing him or her to send spam or even acting illegally while using the owner's IP address. The lack of default security in wireless connections is quickly becoming an issue, where many broadband (e.g. ADSL) connections are now offered together with a wireless base station access point. Furthermore, many laptop PCs now have in-built wireless networking (e.g.

Intel's Centrino technology) thus eliminating the need for an additional plug-in (PCMCIA) card. These features might be enabled by default and unnoticed by the owner, and broadcasting the laptop's accessibility to any computer nearby.

Modern operating systems such as Linux, Mac OS, or Microsoft Windows XP, representing the „standard” in home PCs, make it very easy to set up a PC as a WLAN base station and using Internet connection. Sharing allows all PCs at home to access the Internet via the PC. However, lack of knowledge about the security issues in setting up such systems often means that someone nearby, such as a next-door neighbour, may also use the Internet connection. This is typically done without the wireless network owner's knowledge; it may even be without the intruder's knowledge if his or her computer automatically selects a nearby unauthorised wireless network to use as an access point.

In our opinion this is unfortunate as there should be sufficient experience in the area of traditional IT to avoid such user mistakes or hesitant actions. Not protected WLAN connections and unsecured configurations are easily abused by hackers and e.g. a company runs risk to lose its integrity of their confidential data. Mobile devices using WLAN connectivity are also relatively unsafe and are attacked more often than fixed computer equipment in companies. Uncontrolled private usage of mobile devices (e.g. downloads, e-mails) and the lack of security will lead to dangerous trapdoors inside a security policy-based network.

The spread of security risks and attacks is not sufficient for either private persons, companies or institutions to adapt a new thinking about security concepts. Currently the sensibility is not high enough to establish new security concepts and policies which involve mobile devices. In most cases this is due to a lack of knowledge or uncertainty. Partly people are of the opinion that mobile security these days is sufficient. However, this is not the case as we will show in the following.[6]

Bluetooth technology in comparison to WLAN

Bluetooth is a radio standard and communications protocol primarily designed for low power consumption, with a short range (power class dependent: 1 meter, 10 meters, 100 meters) based around low-cost transceiver microchips in each device. Bluetooth lets these devices communicate with each other when they are in range. The devices use a radio communications system, so they do not have to be in line of sight of each other, as long as the received transmission is powerful enough. As a result of different antenna designs, transmission path attenuations, and other variables, observed ranges are variable. However, transmission power levels must fall into one of three classes:

Class	Maximum Permitted Power	Range
Class 1	100 mW / 20 dBm	~100 meters
Class 2	2.5 mW / 4 dBm	~10 meters
Class 3	1 mW / 0 dBm	~1 meter

Table 1: Bluetooth classes and ranges

Both, Bluetooth and WiFi are established devices in today's offices, homes and on the move: setting up networks, printing, or transferring presentations and files from PDAs to computers.

Bluetooth ranks within a variety of new products such as phones, printers, modems, and headsets, to name a few. Bluetooth is suitable for situations in which two or more devices are in close proximity to each other, and doesn't require high bandwidth. Bluetooth is most commonly used with cell phones and handheld computing devices, either using a Bluetooth headset or transferring files from phones/PDAs to computers. Since Bluetooth uses short-range radio frequencies, it is not as effective as WiFi for setting up networks that can be accessed from remote locations.

Bluetooth also simplifies the discovery and setup of services. WiFi is more analogous to the traditional Ethernet network and requires configuration to set up shared resources, transmit files, set up audio links (e.g. headsets and hands-free devices), whereas Bluetooth devices advertise all services they actually provide; it makes the utility of the service that much more accessible, without the need to worry about network addresses, permissions and all the other considerations that go with typical networks.

- Up to 7 Slaves are supported from a Master within one Piconet
- Master controls the Piconet
- Slaves communicates every time via the Master

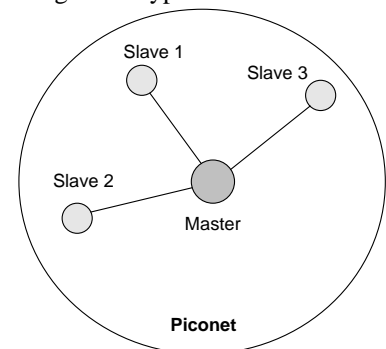


Figure 2: Bluetooth Piconet

WiFi uses the same radio frequencies as Bluetooth, but with higher power consumption resulting in a stronger connection. WiFi is sometimes, but rarely, called „wireless Ethernet“. Although this description is inaccurate, it provides an indication of WiFi's relative strengths and weaknesses. WiFi requires more setup but is better suited for operating full-scale networks as it enables a faster connection, better range from the base station, and better security than Bluetooth. WiFi is also becoming increasingly popular and widespread; it is a standard feature of most new laptop computers, and is a straightforward expansion to desktop computers not already WiFi enabled (e.g. through the use of a USB dongle).

As a traditional networking medium, WiFi is more versatile, but harder to configure. Most users need good know-how (or an IT department) to get things set up, especially when using more obscure services such as audio and HID. For this reason, WiFi falls well short of the standard for ad-hoc networking, one of the basic tenets of the Bluetooth framework.

On the other hand Bluetooth uses the SAFER+ algorithm for authentication and key generation. The E0 stream cipher is used for encrypting packets. This makes

eavesdropping on Bluetooth-enabled devices more difficult. But there are other possibilities to attack Bluetooth networks. It basically has two weakness points:

- a. Weakness in the design of Bluetooth regarding the security concept
- b. Lacks within the implementation and possible risks which arise in the context of several Bluetooth applications

Therefore this paper will show and discuss possible design lacks, attacks, and assess the Bluetooth technology. [5]

Wireless security problems

Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Furthermore, due to space and costs, the „antennas“ typically present on wireless networking cards in the end computers are generally merely "naïve" reception devices. In order to properly receive signals using such limited antennas within even a modest area, the wireless LAN transceiver utilises a considerable amount of power. This means not only can wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, those who engage in the activity of locating (and sometimes, exploiting for profit) wireless LAN networks are known as war drivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires; this is not an issue with wireless packets. To combat this possibility, wireless networks may choose to utilise some of the various encryption technologies available. However, some of the more commonly utilised encryption methods are known to have weaknesses that can be compromised by a dedicated adversary.

There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure. The best strategy is to combine a number of security measures. [6]

There are three steps to take when securing a wireless network:

- a. All wireless LAN devices need to be secured
- b. All users of the wireless network need to be educated in wireless network security
- c. All wireless networks need to be actively monitored for weaknesses and breaches

Security mechanisms and lacks of WLAN

A number of WLAN_security mechanisms are available. The most important and most user-friendly are:

- a. **MAC ID filtering:** Most wireless access points contain some type of MAC ID filtering that allows the administrator to only permit access to computers that have wireless functionalities which contain certain MAC IDs. This can be helpful; however, IT personnel must remember that MAC IDs over a network can be faked. Cracking utilities

such as SMAC are widely available, and some computer hardware also gives the option in the BIOS to select any desired MAC ID for it's built in network capability.

- b. **Static IP Addressing:** Disabling at least the IP assignment function of the network's DHCP server, with the IP addresses of the various network hosts then set manually, will also make it more difficult for a casual or unsophisticated intruder to log into the network., especially if the subnet size is also reduced from one of the standard default settings to a minimum and if permitted but unused IP addresses are blocked by the access point's firewall. In this case, in which no unused IP addresses are available, a new user can log in without detection using TCP/IP only if he or she stages a successful Man in the Middle Attack using appropriate software.
- c. **WEP encryption:** WEP stands for Wired Equivalency Privacy. This encryption standard was the original encryption standard for WLANs. As it's name implies, this standard was intended to make wireless networks as secure as wired networks. Unfortunately, this never happened as flaws were quickly discovered and exploited. There are several open source utilities like aircrack-ng, weplab, WEPCrack or airtsnort which can be used by crackers, examining packets and looking for patterns in the encryption. WEP comes in different key sizes. The common key lengths is currently 128 and 256 bit. The longer the key length the better as it increases the difficulty for crackers. However, this type of encryption has seen its day come and go. In 2005 a group from the FBI demonstrated that it is possible to break a WEP encrypted network within three minutes using publicly available tools. WEP protection is preferable to no protection at all but generally not as secure as the more sophisticated WPA-PSK encryption. If a cracker is able to get a lock on a network, it is easy to crack the code.
- d. **WiFi Protected Access (WPA):** WPA is an early version of the 802.11i security standard which was developed by the WiFi Alliance in order 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 which 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 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 an off-line dictionary attack 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 one minute. Providing a 'good' passphrases or a full 64-character hexadecimal key is used WPA Personal can be regarded secure.

- e. **WPA2:** WPA2 is a WiFi Alliance branded version of the final 802.11i standard. The primary improvement is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support Extensible Authentication Protocol (EAP) authentication methods using RADIUS and preshared key (PSK) based security.
- f. **802.1X:** This is an IEEE standard for port-based access of wireless and wired LANs. It provides for authentication and authorisation of LAN nodes. This standard defines the Extensible Authentication Protocol (EAP) which uses a central authentication server. Unfortunately, during 2002 there were discovered some shortcomings, which can be solved by PEAP.
- g. **LEAP:** This stands for Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimising original security flaws by using WEP and a sophisticated key management system. This also uses MAC address authentication. LEAP is not safe from crackers. THC-LeapCracker can be used to break Cisco's version of LEAP and can be used against computers connected to an access point in the form of a dictionary attack.
- h. **PEAP:** This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without requiring a certificate server. It was developed by Cisco, Microsoft, and RSA Security.
- i. **TKIP:** This stands for Temporal Key Integrity Protocol, 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. It also provides a message integrity check called MICHAEL. These avoid the problems of WEP.
- j. **RADIUS:** This stands for Remote Authentication Dial In User Service, an AAA (authentication, authorisation and accounting) protocol used for remote network access. This service provides an excellent countermeasure against crackers. RADIUS was originally proprietary but was later published under ISOC documents RFC 2138 and RFC 2139. The idea is to have an inside server acting as a gatekeeper by using verifying identities through a username and password that is already pre-determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as recording accounting information such as time connected for billing purposes. RADIUS offers great flexibility in authentication if combined with Extensible Authentication Protocol (EAP).

Additionally, it is possible to increase the security level by using smart cards, USB tokens, or software tokens which leads to a very high level of security. In combination with server software, the hardware or software card/ token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will frequently generate a new encryption code. The server is time synced to the card or token. This is an extremely secure way to conduct wireless transmissions. Companies allocated within this area produce USB tokens, software tokens, and smart cards. They even produce hardware versions that serve as an employee picture badge. Currently smart cards / USB tokens can be regarded the safest security measures on the market, at the same time though, they are very expensive. Other safe methods are WPA2 or WPA using a RADIUS server. Any of these three devices will provide an acceptable security-level. The third suggestion is to educate both employees and contractors about security risks and personal measures for prevention. Furthermore, it is IT-personnel's responsibility to inform employees about latest developments and to make them aware of security risks and dangers. If employees are educated appropriately, it will reduce the risk of security "accidents" such as not locking down their laptop or bring in a wide open home access point to extend their mobile range. Employees need to be aware of the fact that company laptop security applies to areas across their work site as well. This includes locations such as cafes etc. where employees are most vulnerable. The last suggestion deals with 24/7 active defense measures. which ensure that the company network is secure and compliant. This can take form by regularly checking on access points, servers, and firewall logs for unusual activities. For instance, large files going through an access point during non-working hours demand for further attention. There are a number of software and hardware devices that can be used to supplement the usual logs and usual other safety measures. [1]

Unauthorised access via wireless

Unauthorised access to company wireless and wired networks can be gained through and for a number of different methods and intents. One of these methods is referred to as „**accidental association**“: a user turns on his or her computer and the latter latches on to a wireless access point from a neighbouring company's overlapping network. The user may not even be aware that this has occurred. However, it represents a security breach in that proprietary company information is exposed and the possibility for a link from one company to the other arises. This is particularly the case if the laptop is also hooked to a wired network.

„**Malicious associations**“ describes situations in which wireless devices are used by crackers to connect to a company network via their cracking laptop instead of a company access point (AP). These types of laptops are known as „rogue APs“ and are created when crackers run special software which makes his/her wireless network card

appear to be a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant Trojans. Since wireless networks operate in the Layer-2 world, Layer-3 protections such as network authentication and virtual private networks (VPNs) offer no protection. Wireless 802.1x authentications help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the cracker is aiming to take over the client at layer-2 level.

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. While these types of networks usually have little security, encryption methods can be used to provide security, e.g. WPA2 (802.11i and RSN).

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even bar code scanners, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel which is predominantly focused on laptops and APs.

Identity theft (or **MAC Spoofing**) occurs when a cracker is able to eavesdrop 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 authorised computers with specific MAC IDs to gain access to and utilise the network. However, a number of programs exist that have network „sniffing” capabilities. If combined with other software that allows a computer to pretend it has any MAC address that the cracker desires, the cracker can easily avoid this barrier.

A **man-in-the-middle** attack is one of the more sophisticated attacks. This attack revolves around the attacker enticing computers to log into his/her computer which is set up as a rogue AP (Access Point). Once this is accomplished, the cracker connects to a real access point through another wireless card, offering a steady flow of traffic through the transparent cracking computer to the real network. In consequence, the cracker is able to sniff the traffic for user names, passwords, credit card numbers, etc. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols. It is called a „de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the cracker’s rogue AP. Man-in-the-middle attacks are getting easier to pull off due to freeware such as LANjack and AirJack automating multiple steps of the process. What once was only possible for cutting edge crackers can now be managed by script kiddies, less knowledgeable and skilled crackers sitting around public and private hotspots. Hotspots are particularly vulnerable to any attack since there is little or no security offered.

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 being able

to access 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 final attack to be covered is the **network injection** attack. A cracker can make use of access points that are exposed to non-filtered network traffic. Specifically broadcast network traffic such as Spanning Tree (802.1D), OSPF, RIP, HSRP, etc. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and requires rebooting or even reprogramming of all intelligent networking devices. [6]

Weaknesses of Bluetooth

The first security cracks with regards to this technology came about in November 2003: some of the Bluetooth protocol implementations seemed to allow access to data and information to unauthorised individuals.

In April 2004, the news of a relative possibility to force some of the Bluetooth implementations in order to access personal data, started to circulate: this was done by analysing Bluetooth devices and retrieving the code used to encode data transmission.

A few months later, in Summer 2004, the possibility to intercept the Bluetooth signal from the 11th floor of a Las Vegas hotel was demonstrated by capturing 300 phone books from the cellular phones of unaware passerbys with the help of a directional antenna connected to a lap top computer: a discovery that has significantly extended the action range of potential aggressors.

Therefore, a series of weaknesses, has brought about the need to reflect on the existence of a problem that, also in consideration of the rapid diffusion of Bluetooth technology, cannot be undermined.

When considering latest generation cellular phones, four types of threats can be identified for these types of devices:

1. Damaging content such as viruses, worms or Trojan horses, which can be transmitted to user terminals via Bluetooth, SMS or MMS or through WAP pages. Taking advantage of their vulnerability (for instance through attacks to the Bluetooth protocol or through specially „deformed” SMS or MMS messages) such applications can also be installed on the device;
2. Episodes of denial of service (DoS) attacks or system interruption, caused by the propagation of malware or other types of attacks;
3. Unauthorised access to information using Trojan horse, spyware and eavesdropping attacks, etc.
4. Deletion, corruption or modification of data kept on the device

This means that, on top of the propagation of malware and viruses, an unaware user could become the victim of phone book and agenda theft with all the relative contact numbers and appointments. This as long as the thief does not take any further steps such as taking control of the device and making phone calls or sending messages charged to the victim.

Among existing attacks that damage devices using Bluetooth technology - classified by security experts

worldwide – some are particularly known and widespread: [4]

- a. **BlueSnarf:** This type of attack is based on the OBEX Push service, which is the type of service that is commonly used to exchange electronic business cards. Easy to set in place when a cellular has Bluetooth set on visible mode, BlueSnarf allows connecting to a cellular phone and accessing the phone book and agenda without authorisation.
- b. **Bluejacking:** Taking advantage of the IDs that devices exchange at the beginning of a connection – e.g. when a cell phone associates to a computer - short deceitful text messages can be transmitted. For instance, a user could be invited to dial a code to solve network problems and, unknowingly, authorises an aggressor to acquire all the necessary privileges to access a phone book, agenda or file and potentially compromise information and data residing on the device.
- c. **BlueBug:** This vulnerability allows to access the AT Commands of the cellular phone – a set of commands that give instructions to the cellular phone – allowing the aggressor to use the phone services without the user’s knowledge: this includes incoming and outgoing phone calls, sent, received or deleted SMS messages and many more intrusive operations as well as the possibility to modify the device’s configuration parameters.
- d. **BlueBump:** A type of attack that takes advantage of the vulnerability linked to the Bluetooth connection type that is always active giving the possibility to unauthorised cellular phones to continue accessing as if they were still part of the list of authorised cell phones. This type of attack, allows theft of data present on the cellular phone and allows aggressors to use WAP and GPRS services without the owner’s knowledge.

Most of the attacks are using typical interfaces of Bluetooth. Here attacks use security lacks in the implementation of the protocol stack of Bluetooth. Table 2 shows the current design weakness of the Bluetooth technology.

Attacks	C	I	A	L	AU	R
E ₀	X	X		X	X	
Generator	X	X		X	X	
Key strength	X	X		X	X	
PIN code	X	X		X	X	
Unit Key	X	X		X	X	
FH method	X			X	X	
Security modes	X	X		X	X	
Receive area			X			X

Table 2: Design weakness (C=Confidence; I=Integrity; A=Availability; L=Liability; A=Authenticity; R=Reliability)

Further attacks for Bluetooth are available, like PIN hacking, Bluesniping, spoofing, war driving, location

tracking, DoS, man in the middle, re-pairing, brute force, etc. Therefore, the standard configuration of Bluetooth equipment is not secure and has to be improved from the user itself. [5]

Steps to secure a WLAN

The following are some basic steps that should be taken to secure a wireless network, in order of importance:

- a. Turning on encryption. WPA2 encryption should be used if possible. WPA encryption is the next best alternative, and WEP is better than nothing.
- b. Changing the default password needed to access a wireless device — Default passwords are set by the manufacturer and are known by crackers. By changing the password crackers can be prevented from accessing and changing network settings.
- c. Changing the default SSID, or network name — Crackers know the default names of the different brands of equipment, and use of a default name suggests that the network has not been secured. It should be changed to something that will make it easier for users to find the correct network. It is useful to use a name that will not be associated with the owner in order to avoid being specifically targeted.
- d. Disabling File and Print Sharing if it is not needed — this can limit a cracker's ability to steal data or commandeer resources in the event that they get past the encryption.
- e. Access points should be arranged to provide radio coverage only to the desired area if possible. Any wireless signal that spills outside of the desired area could provide an opportunity for a cracker to access the network without entering the premises. Directional antennas should be used, if possible, at the perimeter directing their broadcasting inward. Some access points allow the signal strength to be reduced in order to minimise such signal leakage.
- f. Wired and wireless portions of the network should be divided into different segments, with a firewall in between. This can prevent a cracker from accessing a wired network by breaking into the wireless network.

There are some often-recommended security steps that are usually not of any benefit against experienced crackers (they will however prevent the larger group of inexperienced users from gaining access to your network easily, should they find your password). These are:

- a. Disabling the SSID broadcast option — theoretically, hiding the SSID will prevent unauthorised users from finding the network. In fact, while it will prevent opportunistic users from finding the network, any serious cracker can simply scan other network traffic to find the SSID. It will also make it harder for legitimate users to connect to the network, since they must know the SSID in advance and type it in to their equipment. Hiding the SSID will not prevent

anyone from reading the data that is transmitted; only encryption will do that.

- b. Enabling MAC address filtering — MAC address filtering will prevent casual users from connecting to your network by maintaining a list of MAC addresses that are allowed access, (or not) but a professional cracker will simply scan the network traffic to find a MAC address that is allowed access, then change their equipment to use that address. Any new equipment will require another MAC address to be added to the list before it can be connected. Again, enabling MAC address filtering will not prevent anyone from reading the data that is transmitted without encryption.

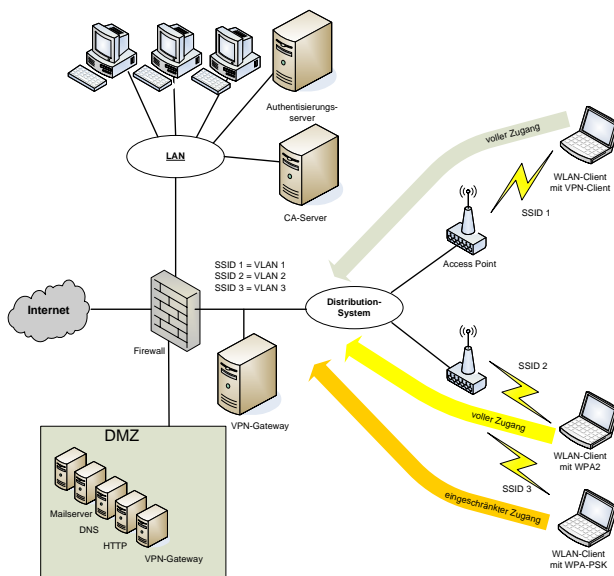


Figure 3: WLAN mixed operation

Moreover, it is important which security mechanisms are used or combined. As basis mutual authentication, dynamical session key, message integrity check (MIC), TKIP, and fast re-keying are needed. This is defined within the 802.11i Security Task Group and the WiFi WPA standard. To reach this standard 802.1x, 802.11i (WPA, WPA2), EAP and RADIUS are required. However, it is important which kind of EAP protocol is used. EAP-TLS is useful, but demands a very high effort regarding infrastructure. Additionally, PKI mechanisms are required. If PKI is not available, EAP has to be combined with TTLS or PEAP. This combination only needs server certificates and is depends on the authentication. EAP-TTLS is more flexible regarding the authentication methods. PEAP is also secure for most applications and the implementation effort is little. But PEAP only supports EAP. Ideally 802.1x is combined with EAP, see also Figure 3, because of [6]

- a. uniform authentication method with EAP
- b. flexible access technology, because AAA infrastructure is also for LAN and VPN useable
- c. Changes of the authentication method has no effects on clients or network infrastructure

Steps to secure a Bluetooth network

From an initial analysis of the results gained during the course of the experiments, a broad diffusion of devices based on Bluetooth technology can be noted: at first sight, this technology appears to be within everyone's reach and to be an integrated part of everyone's life, not only in a professional context but also for personal use. This makes user awareness of both the advantages and the risks of this technology all that more important.

Moreover, it must not be forgotten that latest generation devices often represent a daily work tool that many people with a medium/high level of responsibility use within their companies. This implies that often trendy or innovative cellular phones or palm pilots hold particularly tempting information for potential aggressors interested in industrial espionage or looking for sensitive data.

Without creating useless alarmism, it is important to understand how some simple tricks – such as keeping the Bluetooth connection on hidden mode as opposed to visible – can contribute in increasing the security level of the device, discouraging possible attacks on part of potential aggressors.

It is important to point out that some cellular phones are launched with a configuration ensuring that if the Bluetooth connection is activated the visible mode is set as default: the user has to manually modify the setting, enabling the „hidden” mode. In other cases, the visible mode must be explicitly requested by the user and is re-set automatically as invisible after a short period of time. This was shown to be effective: many users wouldn't otherwise perform this short and easy operation, leaving their device visible to everyone.

Furthermore, it is of importance to know with regards to default settings on cellular phones, deals with the ID name of the device: our survey has shown that, in most cases, the users do not change the configuration parameters set by the producer, hence, allowing immediate identification of the telephone model. This apparently trivial information allows to associate potential weaknesses known to the different device models giving potential aggressors the chance to conduct a targeted attack with high success probabilities. [5]

The following points are recommendations for using Bluetooth on a secure way to avoid attacks: [4]

- a. Be careful when downloading new software or applications from the Internet: before proceeding with the installation of new software or downloading new applications from the Internet, always verify the reliability of the source.
- b. Pay attention to possible anomalies in the functioning of the device: considering that without an installed security application it is rather difficult to identify a virus, there are nonetheless situations that can alarm the user. Generally, in fact, viruses cause anomalies on the telephone like for instance a sudden increase in communication activity, an unusual consumption of the battery, the reception of undesired

messages, the deletion of icons or the modification of the latter.

- c. Remember to deactivate Bluetooth after use and if this is not possible, at least set the device on „hidden” mode. This precaution ensures at least a minimal level of security since it elongates the time necessary for a potential aggression.
- d. Modify the cellular phone’s ID name: Many users tend to maintain the default ID name of their cell phones set by the producer which is usually associated with the specific model of the device. This simple information can allow an aggressor to associate to the device well-know weaknesses that can therefore be taken advantage of.
- e. Always update security and antivirus software: to successfully counteract attacks, all security software must be updated. Software that is not updated is not useful since computer insecurity is in constant evolution and old software is not designed to face new issues. It is important to underline that „old” refers to software that can be only one month old since software updated are made weekly.
- f. Be careful when choosing PIN numbers to associate devices: too often the codes given by the manufacturer are maintained or, even worse, easily traceable information is used (birthdates for instance).

Conclusions

The risks to users of wireless technology have increased exponentially as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. Currently, however; there is a great number of security risks associated with wireless technology. Some issues are obvious and others are not. At a corporate level, it is the IT department’s responsibility to keep up to date with the types of threats and appropriate counter measures to deploy. Security threats are growing in the wireless arena. Crackers have learned about the vulnerability of current wireless protocols, encryption methods, and are aware of the carelessness and ignorance shown by users and by corporate IT departments. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has become much easier and more accessible with easy-to-use Windows-based and Linux-based tools available on the web at no charge. IT personnel should be familiar with the potential of these tools and the possibilities to counteract the cracking that stems from them.

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by Fluhrer, Mantin, and Shamir’s paper entitled

„Weaknesses in the Key Scheduling Algorithm of RC4”. Not long after, Adam Stubblefield and AT&T publicly announced the first verification of the attack. In the attack they were able to intercept transmissions and gain unauthorised access to wireless networks.

The IEEE set up a dedicated task group to create a replacement security solution, 802.11i (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The WiFi Alliance announced an interim specification called WiFi Protected Access (WPA) based on a subset of the then current IEEE 802.11i draft. These started to appear in products in mid-2003. IEEE 802.11i (also known as WPA2) itself was ratified in June 2004, and uses the Advanced Encryption Standard, instead of RC4, which was used in WEP and WPA. In January 2005, IEEE set up yet another task group TGw to protect management and broadcast frames, which previously were sent unsecured. Therefore, today the WLAN standard has reached a relative high security level. It is a question of security combinations to get a secure wireless network. Further standards will be developed to compensate the WLAN weaknesses.

On the other hand, the next version of Bluetooth also includes a number of features to increase security, usability and value of Bluetooth. The following features are defined:

- a. **Atomic Encryption Change:** allows encrypted links to change their encryption keys periodically, increasing security, and also allowing role switches on an encrypted link.
- b. **Extended Inquiry Response:** provides more information during the inquiry procedure to allow better filtering of devices before connection. This information includes the name of the device, and a list of services, with other information.
- c. **Sniff Subrating:** reducing the power consumption when devices are in the sniff low-power mode, especially on links with asymmetric data flows. Human interface devices (HID) are expected to benefit the most, with mice and keyboards increasing the battery life from 3 to 10 times of those currently used.
- d. **QoS Improvements:** these will enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.
- e. **Simple Pairing:** this improvement will radically improve the pairing experience for Bluetooth devices, while at the same time increasing the use and strength of security. It is expected that this feature will significantly increase the use of Bluetooth.

Bluetooth technology already plays a part in the rising Voice over IP (VoIP) scene, with Bluetooth headsets being used as wireless extensions to the PC audio system. As VoIP becomes more popular, and more suitable for general home or office use than wired phone lines, Bluetooth may be used in Cordless handsets, with a base station connected to the Internet link.

For both technologies there are enough security mechanisms available to make these techniques secure, but in most cases these mechanisms are not well tuned. Additionally, many companies do not implement wireless security requirements in their common security policy for the wired network. However, this is essential, because the attacks to wireless equipment will increase in the future and will reach a higher level. To protect company's networks in an efficient way, the wireless environment has to be an integral part of the existing security concept with defined user and communication profiles.

References

1. Detken, Kai-Oliver; Eren, Evren: Mobile Security – Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit; 672 pages; hardcover; Hanser Verlag; ISBN 3-446-40458-9; Munich 2006
2. Wireless LAN Security: What Hackers Know That You Don't; A white paper by AirDefense, Inc.; 2002-2005 AirDefense, Inc.
3. John K. Sturm, Lahela Corriagn, Kevin Carley: Security Aspects of Wireless Networking; a college report
4. Secure Report Bluebag Brochure: Going around with Bluetooth in full safety; F-Secure in collaboration with Secure Network; May 2006
5. Detken, Eren: Bluetooth-Sicherheit – Schwachstellen und potenzielle Angriffe; D.A.CH Mobility 2006: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven; Herausgeber: Patrick Horster; syssec Verlag; 3-00-019635-8; München 2006
6. Detken, Eren: WLAN Sicherheit – von WEP bis CCMP; D.A.CH Security 2006: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven; Herausgeber: Patrick Horster; syssec Verlag; ISBN 3-00-018166-0; Düsseldorf 2006
7. Bluetooth Special Interest Group; SIG public pages; URL: <http://www.bluetooth.com/bluetooth/>
8. The Official Bluetooth Membership Site: URL: <https://www.bluetooth.org/>
9. Enhanced Wireless Consortium; URL: <http://www.enhancedwirelessconsortium.org>