Wireless Hacking Tools

Author: Michael Roche mroche@wustl.edu

Abstract:

This paper is a survey of wireless attack tools focusing on 802.11 and Bluetooth. It includes attack tools for three major categories: confidentiality, integrity, and availability. Confidentiality attack tools focus on the content of the data and are best known for encryption cracking. Integrity attacks tools focus on the data in transmission and include frame insertion, man in the middle, and replay attacks. Finally, availability attack tools focus on Denial of Service (DoS) attacks.

Table of Contents

1.0 Introduction

There are three main principles to computer network security. They are confidentiality, integrity, and availability. All three concepts are needed, to some extent, to achieve true security. Not using all three concepts in the security of the network will leave it vulnerable to attacks. Attackers strive to compromise one or more of the three main security principles. [1]

The basic definition of confidentiality is assuring that sensitive information will be kept secret and access limited to the appropriate persons. In network security, confidentiality can be achieved with data encryption. Data encryption scrambles plaintext data into unreadable cipertext data.

Integrity can be defined as unimpaired, complete, undivided, or unbroken. In network security this means that the message has not been tampered. No portion of the message has been removed, rearranged, or changed. The basic security measure to ensure integrity is to generate a cryptographic checksum of some sort to guarantee the message is unaltered.

Finally, availability means that data should be accessible and usable upon demand by an authorized user or process. An availability attack consists of some sort of Denial of Service (DoS) attack. A DoS attack prevents the user or device from accessing a particular service or application.

Having strong network security does not mean one can prevent the network from being attacked. It simply means that the security mechanisms implemented are just that secure and have not been broken yet. Computer and network security is constantly evolving. Strong security mechanisms must also evolve. As older mechanisms are broken or cracked, new ones must be developed.

1.1 Wireless Attack Tools

Many of the wireless attack tools are developed to compromise 802.11 networks. The popularity and widespread use of Wi-Fi gives the attacker a platform in which they can cause the most disruption. As other technologies gain popularity and usefulness, the more attack tools are developed for those technologies.

The wireless attack tools can be categorized, for the most part, as one that attacks the confidentiality, integrity, or availability of a network. This paper is organized as follows: first confidentiality attacks will be discussed and examples of wireless hacking tools will be given in section two. Then integrity attacks and availability attacks will follow in sections three and four. Specific Bluetooth attacks and hacking tools will be discussed in section five.

Back to Table of Contents

2.0 Confidentiality Attacks

The confidentiality attacks attempt to gather private information by intercepting it over the wireless link. This is true whether the data is encrypted or sent in the clear. If the data is encrypted, these attacks would include breaking the encryption and finding the key. Additionally, eavesdropping, key cracking, access point (AP) phishing, and man in the middle attacks are including in this category.

Eavesdropping is intercepting or sniffing the transmitted network traffic. This is capturing the bits transmitted on the physical layer, but many commercial programs will format the data into a user friendly way. This makes understanding the data much easier. If encryption is used, one will only see the encrypted data while sniffing. There are other tools available to crack certain encryption techniques. These tools also are considered confidentiality attack tools.

Beyond simply capturing and displaying the packets from the physical layer, many of the sniffing programs have filters and plugins installed that have the ability to manipulate the data creating a man in the middle attack. For example, a sniffing program can have a filter running that will replace the https (secure website) with http (non-secure). As a result, the victim's authentication would appear in the clear across the physical layer. The eavesdropper would be able to see both the username and password for the login.

Another example of a man in the middle attack would be to downgrade the encryption used. It is possible to rollback the Microsoft Challenge-handshake Authentication Protocol (MSCHAP2) encryption to MSCHAP1, which is a weaker encryption, and then rollback further to plain text for Microsoft's Point to Point Tunneling Protocol over a Virtual Private Network. This involves using a man in the middle attack tools to alter the handshake messages between the client and server. [36]

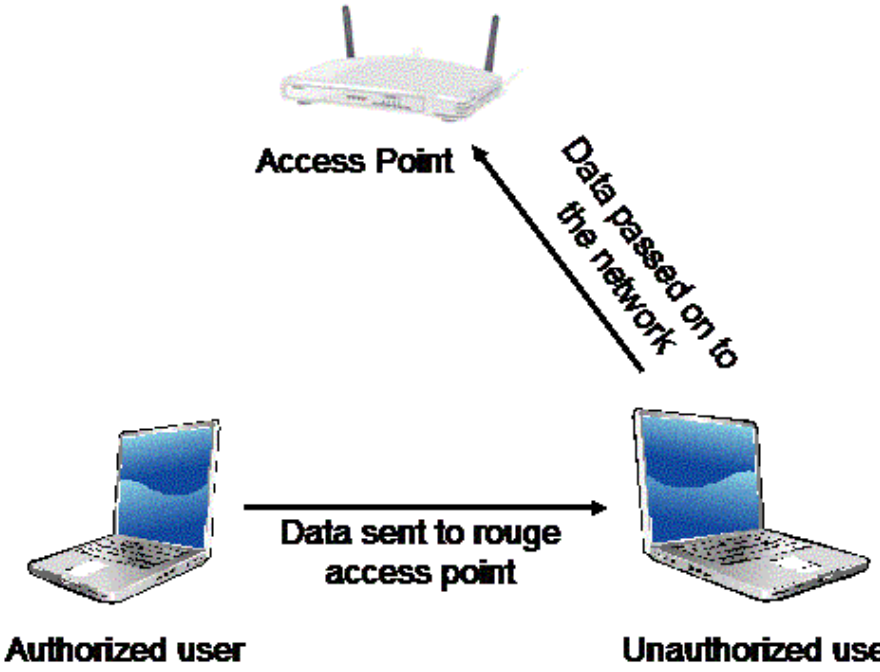

Figure 1 - Man in the Middle Attack

Figure 1 illustrates a man in the middle attack. The authorized user will be faked into connecting to the unauthorized user instead of the AP. The unauthorized user will be able to alter the message sent between the authorized user and the AP in order to attack the security.

AP phishing or "Evil Twin" is a confidentiality attack where the user is tricked into trying to logon to fake APs thus providing their credentials to the attacker. Attackers will setup these phony APs and create fake logon pages in hopes to collect users' personal information including credit card information. The user may also be coerced into downloading a series of trojan horses. They may also use these fake APs to invoke man in the middle attacks. [34]

There are a variety of confidentiality attacks, but they all have one common goal - to gather the private information of a user. One or more of the attacks can be used. These include eavesdropping or sniffing, man in the middle attacks, and AP phishing.

2.1 Confidentiality Attack Tools

For eavesdropping a commonly used tool is Wireshark, formally Ethereal. It is a basic sniffing program that will display all network traffic both wired and wireless. It is a multi-platform, multi-protocol analyzer with hundreds of protocols supported. It includes support for 802.11 and Bluetooth and also includes decryption support for many popular wireless security protocols including IPsec, Internet Security Association and Key Management Protocol (ISAKMP), Kerberos, Secure Sockets Layer, Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA)/WPA2. [10]

Wireshark will display the captured data in an easy to read and easy to follow form. It also has many built in filters and the ability for the user to design their own filters. These filters can be used to only capture specific data such as a certain IP address, protocol, port number, etc.

Figure 2

Figure 2 - Wireshark Screenshot

Figure 2 shows a screenshot of Wireshark. Each different color indicates a different protocol identified. When the user selects a packet, the details of that packet are displayed below.

The sniffing programs work well for information that is sent in the clear. For encrypted information, an encryption key cracker is necessary. For 802.11, WPA2 is the latest wireless encryption standard that has not been broken yet. WPA and WEP are two previous encryption schemes with many tools available that will crack their encryption keys. AirSnort [6] is a well known for WEP and AirCrack [7] is an attack tools for WPA.

Ettercap [8] and dsniff [9]
are two popular man in the middle attack tools. They both provide sniffing capabilities similar to Wireshark, but go beyond that with the ability to modify the data in transmission. Again these are available for many platforms. Ettercap even has a tutorial on how to write your own plugin.

Tools such as Hotspotter [11], APsniff [12], APhunter [13], and KNSGEM [14] will scan for wireless AP beacon signals. Although they are not necessarily attack tools, they can be used to find the wireless APs. KNSGEM will even place the APs on a Google Earth map. Attackers will then setup their "Evil Twin" AP near these legitimate ones. HermesAP [15] and OpenAP [16]
are two Linux based tools that allow the user to setup phony APs. OpenWRT [17] and HyperWRT [18] are two open source projects that replace the factory firmware for Linksys's popular WRT line of APs. Attackers can use these distributions to create fake APs.

Table 1 - Summary of confidentiality attack tools

Tools	**Description**	**Type of Attack**
AirSnort	Brute force WEP cracker	Encryption Cracker
AirCrack	WPA cracker	Encryption Cracker
Ettercap, dsniff, and Wireshark	Packet sniffers with traffic analysis. These also include tools to break encryption.	Packet sniffing
Hotspotter, APsniff, APhunter, and KNSGEM	Discovers WLANs by listening for beacon signals transmitted from APs.	AP locator
HermesAP and OpenAP	Used to setup an rogue AP	Evil Twin
OpenWRT and HyperWRT	Replacement firmware so APs can be programmed to execute attacks.	Fake AP creation

Back to Table of Contents

3.0 Integrity Attacks

The idea of an integrity attack is to alter the data while in transmission. Remember the integrity of the data means that it has not been altered in any way. This includes data deletion or addition, frame deletion or addition, or replay

attacks.

One integrity attack is frame injection. This is when an attacker will inject their own Ethernet frames in the middle of the transmission. This can be used in a variety of ways to attack the user. The user can be misled into accepting frames that it did not intend. All the major Internet browsers were vulnerable to a frame injection attack. This vulnerability has been fixed, but it does give an example on how this can be used as an attack. An attacker could inject frames into a transmission to display their content with the legitimate outer web page frames of another company. For example, a user would access their banking web page and it would look like their legitimate web page, but the attacker has injected Ethernet frames so that even though the web page looks legitimate it is not. When the user attempts to login all the login information can be recorder by the attacker.

It is relatively easy to inject spoofed packets in a wireless network. When communicating with a web server there is a delay of tens of milliseconds while waiting for a reply. This is plenty of time for spoofed packets to be injected and the legitimate packets to be deleted. This is similar, but not exactly the same as the man in the middle attacks.

Packet injection can be used to generate a DoS attack as well. In 802.11, the AP and wireless device attempting to connect to it will trade associate and authenticate messages. When disconnecting, they will exchange deauthenticate messages. Packet injection tools can be used to issue deauthenticate messages for the IP addresses in the network, that could easily be obtain from sniffing the traffic. This would cause the valid device to be disconnected from the AP.

Similarly an attacker can delete or jam the data being transmitted. For example, an attacker could jam the wireless signal from reaching its intended target and also provide acknowledgments (ACKs) back to the source. The data would never reach the intended target, but the sender would have no idea, since it would see the ACKs.

Data replay is yet another attack on data integrity. This involves the attacker capturing authentication information and saving it for later use. This can be used for 802.1X Extensible Authentication Protocol (EAP) or for 802.1X Remote Authentication Dial-In User Service (RADIUS) authentications. Once the attacker has captured and saved the authentication information, it will monitor the traffic for another authentication. Then it will inject those frames instead of the legitimate authentication frames and essentially gaining access to a system.

3.1 Integrity Attack Tools

The list of integrity attack tools is not as extensive as the confidentiality attack tools. It is more common for sniffing and encryption cracking than it is for frame injection and replay attacks. Nonetheless, there are tools for frame manipulation (addition and deletion) and replay. .

Airpwn [19]
is a wireless attack tool for 802.11 packet injection. It listens for specific patterns of the incoming packets. If there is a match with what is specified in the config file, then custom spoofed packets are injected from the AP. The valid packet that the spoofed packet replaced will be intercepted by airpwn and not allowed to reach the user.

File2air [20] is a similar injection tools except it allows the user to specify a file that will be used for the payload of the injected packets. It uses another tool called AirJack [21] to perform the actual frame injection. File2air runs on top of AirJack and reads in a binary file and transmits its contents onto a wireless network.

Simple-replay [22]
is an attack tool that does exactly as the name implies. It allows for 802.11 packets that were previously captured to be injected back into the network.

Frame injection and frame replay tools can be used to attack the integrity of the data. Data integrity ensures that the transmitted data arrives at the destination unchanged. The attack tools focus on frame manipulation, so that an attacker can cause the user to receive the information it chooses.

Table 2 - Summary of integrity attack tools

Tools	Description	Type of Attack
Airpwn	Allows for generic 802.11 packet injection	802.11 packet injection
File2air	Allow the specified file be used as packet payload.	802.11 replay
AirJack and Simple-replay	Allows previously captured packets to be injected back into the network.	802.11 replay

Back to Table of Contents

4.0 Availability Attacks

Availability attacks are most simply described as DoS attacks. DoS focuses on attacking a specific part of the network so that it is unreachable. Network availability means that any point the network is able to provide the requested information to the authorized user. DoS attacks prevent this information from reaching the user.

There are several types of DoS attacks; one is flooding. Flooding is overloading the network with a certain type of packet so that the wireless AP is busy serving all the flooding packets that it cannot serve any legitimate packets. For example, an 802.11 beacon flood is where thousands of illegitimate beacons are generate to make it difficult for individual machine to find the legitimate AP. Another is an 802.11 authentication flood where thousands of authentications are sent from random Media Access Control (MAC) addresses filling up the AP's authentication table and making it hard for a legitimate user to gain access. This gives a small example of the types of flooding attacks someone could execute on a wireless network.

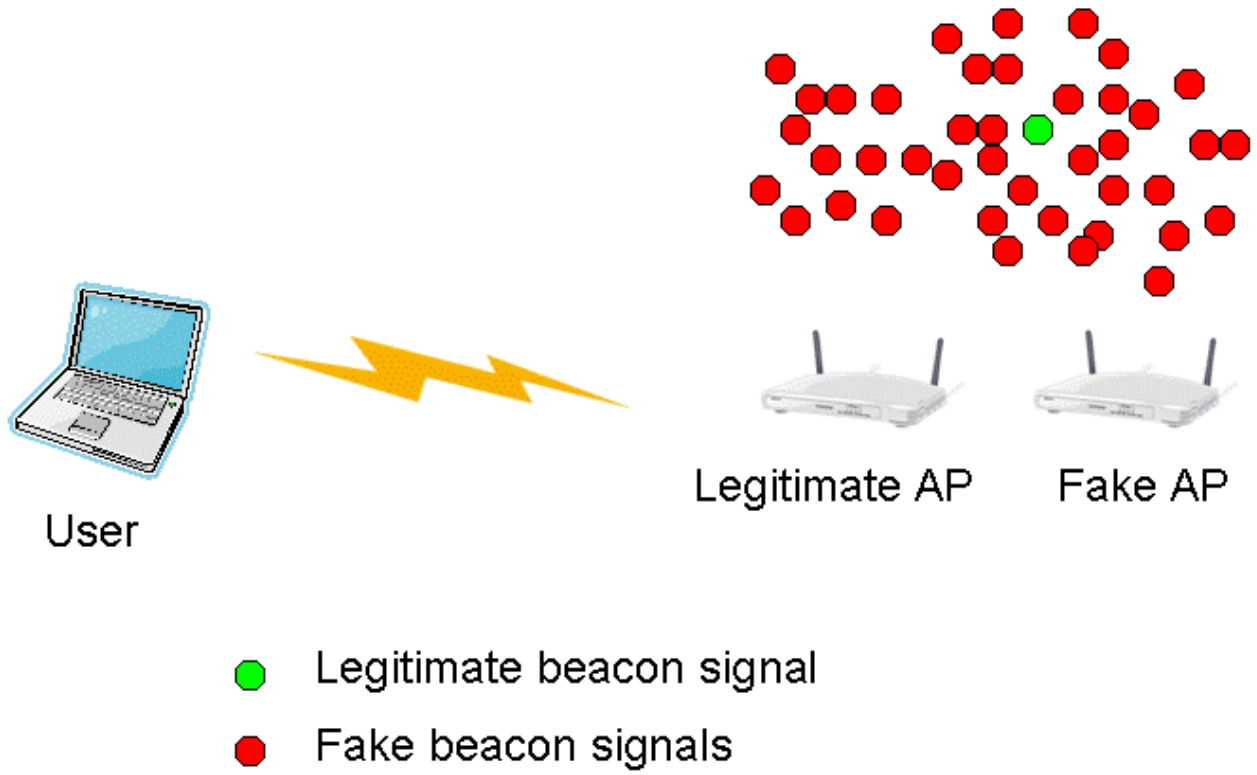

Figure 3 - Beacon Flooding

Figure 3 shows an example of the beacon flooding attack. The legitimate AP emits a legitimate beacon signal that the user will look for. The fake AP is emitting many fake beacon signals. The user has a much better chance of trying to connect to one of the fake beacon signals rather than the one legitimate one. This leads to a DoS since the user cannot connect to the legitimate AP.

Another type of DoS attack is radio frequency jamming. In this case the attacker jams the frequency of the Wireless Local Area Network (WLAN); most likely with a much higher power level allowed by the regulation. This will not allow anyone access to the WLAN.

Again the idea of a DoS attack is to prevent the user from gaining access to the network. This is done by attacking certain pieces of the network usually those needed to connect to the network. Flooding and RF jamming are two examples of DoS attacks.

4.1 Availability Attack Tools

The list of attack tools for availability is similar to that of integrity. Many of the same tools can be used because of the similarity in the attacks. Many of the flooding attacks can be accomplished by using the injection attack tools on top of the flooding tools. To execute an authentication flooding attack, you could use frame injection to inject many authentication frames from different MAC addresses. This will fill up the authentication table of the AP and make it difficult for a legitimate user to connect.

There are, however, some specific tools available to launch these attacks that are separate from the integrity attack tools. FakeAP [23]
generates thousands of 802.11 APs or more specifically it generates thousands of 802.11 beacon signals that can be used for the beacon signal flooding attack.

Void11 [24]

is another flooding attack tool. It has the ability to implement three different flooding attacks: deauthenticate clients, authentication flood, and association flood. The deauthenticate attack floods the WLAN with deauthenticate packets for random MACs. Those legitimate users connected with matching MAC address will close their connection upon receiving the deauthenticate packet. The authentication attack again floods the network with authentication packets so legitimate user cannot connect. The same is with the association packets.

There are a variety of availability attacks. All of them implement a DoS attack of some sort whether it is radio frequency (RF) jamming or network flooding. There also are many different flooding attacks with just a few examples given here. Flooding attacks promote the vulnerabilities of the protocols.

Table 3 - Summary of availability attack tools

Tools	**Description**	**Type of Attack**
FakeAP	Generate thousands of 802.11 beacon signals.	Flooding DoS
Void11	Can be used to execute deauthenticate, authenticate, and association flooding attack.	Flooding DoS
Many commercial tools available	Jams the RF signal so that it cannot be distinguished by a legitimate device.	RF jamming

Back to Table of Contents

5.0 Bluetooth Attacks

Recently more Bluetooth attacks have emerged with Bluetooth technology gaining popularity. The two most well known attacks are DoS, bluesnarfing, and a key bump attack. The key bump attack involves obtaining the pairing key and then having full access to the victim's system.

One Bluetooth DoS attack involves a device that is not part of a piconet disrupting the established piconet of other devices. A Bluetooth piconet is the ad hoc network created with two or more Bluetooth devices that includes one master device and a number of slaves. The attacking device that is not participating in the piconet spoofs a slave out of the piconet and then contacts the master of the piconet. This will confuse the master device and lead to a disruption of the piconet.

Another DoS attack on Bluetooth devices involves a buffer overrun. This is when data is copied into a buffer, but the amount of data copied into the buffer exceeds the size of the buffer. This will cause the data to be copied into memory where it is not intended. The resulting status of the system depends on where in memory the data is copied.

Bluesnarfing is a term that means an attacker has obtained unauthorized information through a Bluetooth connection. The Object Exchange (OBEX) Push Profiler (OPP) has been identified as an easy mechanism for exchange of business cards, calendar entries, and other similar items. In most cases it does not require authentication. Bluesnarfing involves connecting to the OBEX Push target and issuing an OBEX GET request for common known filenames. In some cases, depending on the victim device's firmware, the attacker will be able to obtain all the files that were requested.

In the key bump attack the attacker gets the victim to accept a connection for some trivial data transfer, such as a picture, calendar notice, or a business card on a PDA. After the data is sent, the attacker keeps the connection open. This allows the attacker to request a key regeneration after the victim has deleted the pairing between the two

devices. Once the key regeneration is done, the attacker has full access to any services provided by the victim's device.

5.1 Bluetooth Attack Tools

The number of tools available to attack Bluetooth devices is also growing with the growing popularity of Bluetooth devices. For DoS attacks, the BlueSmack [25]
tool can be used to launch the ping of death attack on Bluetooth devices. It works by requesting an echo from a Bluetooth device. When thousand of these echoes are requested, the device cannot service anything but the echoes and causes a DoS. Other DoS tools include BlueChop [26] and BluePass [27]. BlueChop can be used to disrupt the established piconet and BluePass can be used to create Bluetooth packets to cause the buffer overflow attack.

BlueSnarf [28]
is a tool that can be used for bluesnarfing. Again means obtaining unauthorized files from a Bluetooth device by keeping the connection open and requesting those file. BlueBump [29] is a tool that can be used to obtain the victim's key. Some PDAs will allow an attacker to request a key regeneration that can be used later to gain full access to the system. The table below summarizes the Bluetooth attack tools presented.

As Bluetooth technology becomes more prevalent in user's everyday lives and as more product become available, more attack tools will emerge. There are several DoS attacks that can be used to disrupt normal Bluetooth communication. Also there are attacks to gain full access to a victim's device. All of which can cause major problems for the user.

Table 4 - Summary of Bluetooth attack tools

Tools	**Description**	**Type of Attack**
BlueSmack	Issues ping of death attack	DoS
BlueChop	Disrupts and existing piconet	DoS
BluePass	Causes a buffer overflow attack	DoS
BlueSnarf	Obtain unauthorized access to files.	Bluesnarfing
BlueBump	Obtains the piconet key	Key bump

Back to Table of Contents

Summary

In this paper we discussed several attack tools for 802.11 and Bluetooth systems. Since both of these protocols are a major part of everyday lives, many attack tools exist. The attacks can be categorized into three major categories: confidentiality, integrity, and availability. Confidentiality attacks include sniffing, encryption cracking, and AP attacks. Integrity attacks include attacks on the data while in transmission. This includes frame manipulation, addition, and subtraction. Finally, the availability attacks in all DoS attacks.

Presented were wireless hacking tools and possible attacks on wireless networks. Although wireless networks will probably never be completely secure because research on protocol vulnerabilities will always continue, one can keep their network as secure as possible. Staying educated on the latest encryption schemes and other network security related items is probably the best way to keep your network secure. You will not be able to stop the sniffing of your traffic; however, you can prevent the attacker from being able to decipher the traffic. The protocols

will continue to evolve to keep unauthorized devices from connecting to a wireless network. However, even the latest security methods have their weaknesses. For example, WPA2, the latest encryption method, does not address the problem of dissociation and deauthentication attacks, but does address many of the issues with WEP.

The attack tools are easy to obtain, easy to install, and have detailed web pages or forums that include directions on how to obtain, install and use. Many of the tools are multi-platform which makes it even easier to use. As the network security field grows in complexity, the attack tools will evolve.

Back to Table of Contents

References

These reference are ordered approximately in usefulness and relevance to this survey paper.

[1] "Wireless Attacks A to Z", http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1167611,00.html March, 2006

[2] "Top 5 Wireless Tools", http://sectools.org/wireless.html, 2006

[3] "The Top 10 Hacker Attack Tools", http://www.thenetworkadministrator.com/2005tophackingtools.htm

[4] "Recon and Attack Tools", http://www.wi-foo.com/index-3.html

[5] "Wireless Attack Primer", http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html, July 2004

[6] "AirSnort", http://airsnort.shmoo.com/, The Schmoo Group

[7] "AirCrack", http://www.wirelessdefence.org/Contents/AircrackMain.htm

[8] "Ettercap", http://ettercap.sourceforge.net/

[9] Song, D., "dsniff", http://monkey.org/~dugsong/dsniff/

[10] Combs, G., "Wireshark", http://www.wireshark.org/

[11] Moser, M., "Hotspotter - Automatic wireless client penetration", http://www.remote-exploit.org/codes_hotspotter.html

[12] "APsniff", http://www.zdnet.de/downloads/prg/w/i/de0DWI-wc.html, April 2004

[13] "APhunter", http://www.attackprevention.com/article/aphunter-2618.html

[14] "KNSGEM", http://www.rjpi.com/knsgem.htm

[15] "HermesAP", http://hunz.org/hermesap.html

[16] "OpenAP", http://www.seattlewireless.net/OpenAP

[17] "OpenWRT", http://openwrt.org/

[18] "HyperWRT", http://hyperwrt.org/

[19] "Airpwn", http://airpwn.sourceforge.net/Airpwn.html July, 2006

[20] "File2air", http://www.wolfslair.nl/php/modules.php?name=News&file=article&sid=62

[21] "AirJack", http://sourceforge.net/projects/airjack/

[22] "Simple-replay", http://www.802.11mercenary.net/simple-replay/

[23] Black Alchemy Enterprises, "FakeAP", http://www.blackalchemy.to/project/fakeap/

[24] Floeter, R., "Void11", http://www.wirelessdefence.org/Contents/Void11Main.htm

[25] Laurie, A., Holtmann, M., Herfurt, M., "BlueSmack", http://trifinite.org/trifinite_stuff_bluesmack.html

[26] Laurie, A., Holtmann, M., Herfurt, M., "BlueChop", http://trifinite.org/trifinite_stuff_bluechop.html

[27] Gianluigi Me, "Exploiting buffer overflows over Bluetooth: the BluePass tool", WOCN 2005, March 2005

[28] Laurie, A., Holtmann, M., Herfurt, M., "BlueSnarf++", http://trifinite.org/trifinite_stuff_bluesnarfpp.html

[29] Laurie, A., Holtmann, M., Herfurt, M., "BlueBump", http://trifinite.org/trifinite_stuff_bluebump.html

[30] "Bluetooth Attacks", http://www.viruslist.com/en/analysis?pubid=181198286

[31] "Top 3 Attack Tools Threatening Wireless LANs", http://whitepapers.techrepublic.com.com/webcast.aspx?docid=161061

[32] "Wardriving Tools", http://www.wardrive.net/wardriving/tools

[33] "Widely Used Attack Tools", http://www.networkdictionary.com/security/Widely.php

[34] Phifer, L "Anatomy of a Wireless "Evil Twin" Attack (Part 1)", http://www.corecom.com/external/livesecurity/eviltwin1.htm 2005

[35] "Wi-Foo, The Secrets of Wireless Hacking", http://www.wi-foo.com/index-2.html

[36] Wilds, B., "Wireless Man in the Middle Attack Part 2", http://blogs.ittoolbox.com/wireless/networks/archives/wireless-man-in-the-middle-attack-part-ii-7421

Back to Table of Contents

List of Acronyms

ACK	Acknowledgment
AP	Access Point
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ISAKMP	Internet Security Association and Key Management Protocol
MAC	Medium Access Control
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
OBEX	Object Exchange
OPP	OBEX Push Profiler
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency

WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Back to Table of Contents

Last Modified: December 02, 2007.

Note: This paper is available on-line at