ANALYSIS OF WEP PERFORMANCE ON MOBILE DEVICES

Arnulfo Ochoa Indart [1], Jesús Arturo Pérez Díaz [2],

1 Informatic Graduate Program, ITESM Campus Cuernavaca, Paseo de la Reforma 182-A, Cuernavaca, México

2 Electronic and Communications Department, ITESM Campus Cuernavaca, Paseo de la Reforma 182-A, Cuernavaca, México

Keywords. Wireless Networks, 802.11b, WEP, Performance, Mobile Devices

Abstract. Mobile devices are becoming more popular every day; they must keep up with security implemented by desktop computers. This paper tries to evaluate performance of data transmission with and without ciphering techniques. WEP is not the best way of securing a network but it is widely used, that is why we used WEP on these tests. This article tries to define how much performance is lost with WEP, so we can estimate the loss of performance on mobile devices when TKIP and WPA's MIC protocols are implemented. We observed in the results that decrease on performance was more noticeable on PDAs than other devices such as laptops

1 Introduction

Ever since wireless networks appeared, many questions concerning security issues were made. WEP (Wired Equivalent Privacy) was part of IEEE's 802.11 standard, and it attempted to provide secure wireless communications.

In 802.11 WEP uses a secret 40 bit key (weak) or 128 bit key (strong) in 802.11b and a pseudorandom number generator (RC4). Two processes are applied to clear text; one of them ciphers data and the other one protects it from unauthorized modifications while in transit. The secret key is concatenated with a random initialization vector (IV) that adds 24 bits to the resulting key. This key is processed in the pseudorandom number generator that outputs a large pseudorandom key stream. The transmitter combines it with the clear text using an XOR operation, creates the ciphered text and sends it to the receiver along with the IV. When the receiver gets the ciphered text, it uses the IV and its own copy of the secret key to generate the same key stream as the transmitter. The receiver combines them with the XOR operation and generates the original clear text.

Ochoa Indart A. and Arturo Pérez Díaz J. (2004).
ANALYSIS OF WEP PERFORMANCE ON MOBILE DEVICES.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 324-330
DOI: 10.5220/0002686203240330

In order to protect the ciphered text against modifications while it is in transit, WEP applies an integrity checking algorithm (CRC-32) to the clear text and generates an integrity check value (ICV).

The ICV is concatenated to the text before it is encrypted with the key and is sent to the receptor along with the IV. When the checking algorithm is applied to the clear text and is compared with the output with the ICV value received, it can be verified if there has been any modification. [1]

However as Nikita Borisov et. al demonstrated, the WEP checksum is a linear function of the message. One consequence of the above property is that it becomes possible to make controlled modifications to a ciphertext without disrupting the checksum. [2].

Description	Processor	RAM	WLAN NIC	OS
Laptop Client 1 – HP ze5785 us	Intel Pentium 4 2.4 Ghz.	512 MB	LAN-Express IEEE 802.11b NIC	Windows XP Home Edition
Laptop Client 2 – IBM Think Pad 2655	Intel Pentium 3 1 Ghz.	128 MB	Proxim IEEE 802.11 b/g PC Card.	Windows 2000 Professional
PDA Client – HP iPAQ 4155	Intel XScale 400 Mhz.	64 MB	Embedded	Windows Mobile 2003
Server Laptop – HP ze5385 us	Intel Pentium 4 2.66 Ghz.	512 MB	LAN-Express IEEE 802.11b NIC	Windows XP Home Edition

WEP uses the RC4 symmetric stream cipher for encryption and decryption purposes. Symmetric means that the sender and receiver must use the same key for proper encryption and decryption functions. [3]

There are other key lengths for WEP, such as 64 bits, which was used in our tests.

There are various types of known attacks against WEP, and it is not considered secure. Although there are other ciphering techniques, WEP is implemented natively in many OS such as Windows XP, Windows Mobile and Palm OS. This is why WEP is still widely used.

Design of secure protocols is difficult, and fraught with many complications. It requires special expertise beyond that acquired in engineering network protocols. A good understanding of cryptographic primitives and their properties is critical. From a purely engineering perspective, the use of CRC-32 and RC4 can be justified by their speed and ease of implementation. [2]
Mobile devices such as PDA's are being increasingly used in Wireless LANs (WLANs); these devices have limited processing resources; and therefore, the impact on data transfer performance is of particular interest because of the processing overhead it causes.

There are other security protocols such as PEAP or LEAP, which promise better protection, however, it has been proofed that there are other attacks that could affect them such as the ones published by Mishra and Arbaugh, which explains that 802.11 frames, including 802.1X messages, are easily sniffed. For this reason, IEEE 802.11 Task Group I recommends EAP methods resistant to dictionary attack.

It's worth heeding this advice, since dictionary attacks enable an attacker to recover the user password, which often can provide access to more than just the 802.11 network. Therefore these attacks are more serious than the previously documented WEP attacks and customers using 802.1X should strongly consider adopting dictionary attack-resistant authentication methods such as EAP TLS, SRP, TTLS and PEAP. [4]

LEAP is a type of Radius EAP. It is used to authenticate access by a wireless client (typically a laptop or pc) to a wireless router, typically a Cisco Aironet base station.[5]

RADIUS is a widely deployed protocol for network access authentication, authorization and accounting (AAA). [6]

This paper presents an analysis of the data transfer performance achieved by laptops and PDA's when using 64 and 128 bit keys with WEP and when transmitting clear text using an infrastructure WLAN.

2 Experimental Section

2.1 Equipment Used

Two laptops and a PDA were used as clients. A third laptop was used as server. A brief description of the equipment can be found in table 1.

The access point that was used was a Microsoft Broadband Networking Wireless Base Station Model MN-500, which is Wi-Fi certified.

2.2 Performance measurement

In order to obtain performance measurements of common uses of a WLAN, a simple web-based script was written in PHP, running on an Apache 2.0.48 web server with PHP Engine 4.0.1. Measurements were stored using mySQL 4.0.13.

The PHP script sends a random stream of bytes, ranging from 100 to 5000 kilobytes. Three fields are stored in the database, the client's IP address, the amount of data transferred and the time that the transfer took.

The resulting web page is reloaded 5 seconds after the transfer is finished and a new stream of different size is sent to the client.

2.3 Test scenarios

Several tests were performed, in order to test different situations and compare them.

The first variable is the length of the key, three different scenarios were tested in this case, with no key (no WEP encryption), 64 bit, and 128 bit keys.

The second variable is distance, 3 different distances were tested. In every case, all the devices were at the same distance.

a) Five feet away from the Access Point. No interferences.
b) Twelve feet away from the Access Point. No interferences.
c) Forty feet away from the Access Point. On the second floor, home environment (Computers and PDA were on the first floor).

For each scenario, 1200 samples were gathered, 400 for every mobile device.

Using the gathered data, simple statistical analysis was calculated, specifically, the mean value of the samples and the standard deviation.

3 Results and Discussion

3.1 Performance with no WEP encryption

	5ft	12ft	40ft
HP Laptop	170.21	148.9	122.83
IBM Laptop	169.26	145.8	120.46
iPAQ PDA	168.6	148.39	119.14

Table 2: Average results in KB/S with no WEP encryption.

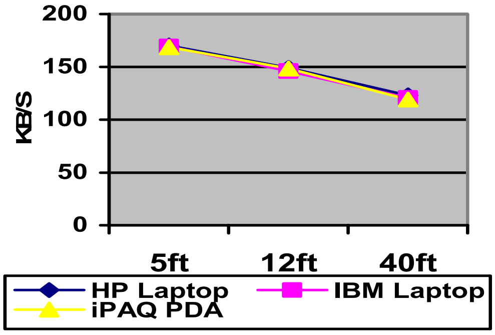

Figure 1: Data transfer performance no WEP encryption

When using no WEP encryption, the performance loss is similar on both laptops and the PDA as shown in Table 2 and Figure 1.

3.2 Performance with 64 bit key WEP encryption

	5ft	12ft	40ft
HP Laptop	162.19	147.32	112.14
IBM Laptop	158.22	149.41	115.11
iPAQ PDA	154.63	141.32	104.78

Table 3: Average results in KB/S with WEP and a 64 bit key.

Test results with a 64 bit key show that the PDA's performance was more noticeable than both laptops. This can be observed in Table 3 and Figure 2.

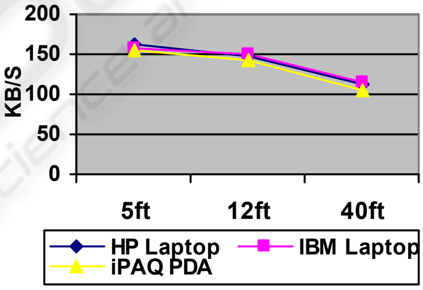

Figure 2: Data transfer performance 64 bit key WEP encryption

3.3 Performance with 128 bit key WEP encryption

	5ft	12ft	40ft
HP Laptop	147.24	140.33	118.75
IBM Laptop	150.81	145.28	117.63
iPAQ PDA	140.29	134.5	90.69

Table 3: Average results in KB/S with WEP and a 128 bit key.

It is clear that the PDA decreased its performance more than laptops. This can be seen in Table 3 and figure 4.

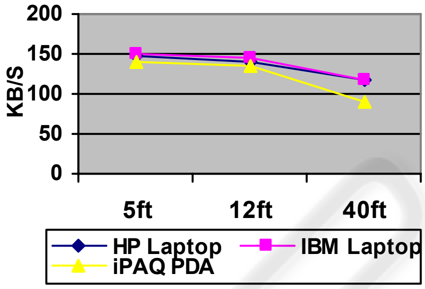

Figure 3: Data transfer performance 128 bit key WEP encryption

3.4 Results Analysis

	No WEP	64 bit	128 bit
HP Laptop	147.31	140.55	135.44
IBM Laptop	145.17	140.91	137.90
iPAQ PDA	145.37	133.57	121.82

Table 4: Overall Performance in KB/S

It is clearly visible that the PDA's performance (See Table 4) was considerably reduced by WEP encryption. It is clear that the reduced computing power of the PDA resulted in a bigger impact on performance.

As mentioned above, WEP uses symmetric keys, because of that, we expected better performance results on the PDA, but it affected it visibly. We would now expect that using EAP-TLS or other similar technique the performance loss to be greater.

TKIP changes the ciphering key very often, and requires much more resources. Based on this, we can extrapolate the results and consider that when using TKIP, the performance loss will be much bigger.

Both laptops had similar behavior, and they were not visibly affected by WEP encryption.

We can see an overall comparison of performance in figure 4.

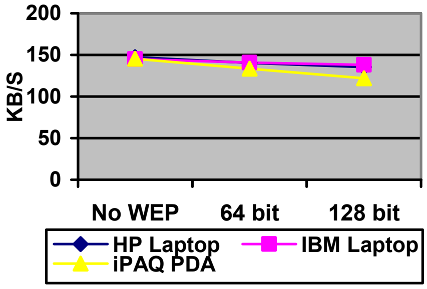

Figure 4: Overall performance comparison

4 Future Works

We will repeat these tests with ciphering techniques specified by WPA and evaluate their performance in order to search alternatives for mobile devices if there is a considerable loss of performance.

5 Conclusions

Approximately, the PDA lowered its performance to 83.80% compared to the 91.94% observed in Client 1 and 94.99 % of Client 2, when looking their performance based on no WEP encryption and 128 bit encryption.

From the standard deviations observed, the PDA had the lowest levels overall, this can be because laptops usually run other processes on the background that might impact some measurements.

Security is vital to wireless communications, there has been a big amount of effort and research to provide reliable ciphering techniques. Progress has been achieved in this field; however there are new scenarios where wireless communications were not very popular a few years ago.
Mobile devices have limited resources and processing power, this is why, ciphering techniques used in these devices, have to meet their constraints and yet meet security levels.

It will be vital to take these constraints when designing new security schemes, and when these schemes are deployed to new operating systems for mobile devices, they must allow limited devices to work properly, without degrading QoS and providing secure, reliable data transfers.

WPA security protocols are expected to consume more resources than old protocols such as WEP, so special protocols for limited devices should be developed, so their performance is not affected.

References

[1] Nichols, Randall and Lekkas, Panos. Wireless Security: Models, Threats, and Solutions. McGraw Hill. Edition 1, 2002. ISBN: 0071380388

[2] Nikita Borisov, Ian Goldberg, David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11 http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[3] Shon Harris, Latest trends in wireless security http://a907.g.akamai.net/7/907/3644/v0001/ntschool1.download.akamai.com/3644/_vl/Articles/WIRELESS-SECURITY-SHONa.pdf

[4] Arunesh Mishra and William A. Arbaugh, An Initial Security Analysis of the IEEE 802.1X Standard, University of Maryland. http://www.cs.umd.edu/~waa/1x.pdf

[5] Cameron MacNally, Cisco LEAP protocol description http://www.missl.cs.umd.edu/wireless/ethereal/leap.txt

[6] Bernard Aboba. Wireless LAN Security Site. http://www.drizzle.com/~aboba/IEEE/