Wireless Networks Speed Depending on the Encryption using Windows 8.1 x64 Operating System

Tamás Krausz

Faculty of Informatics
University of Debrecen
krausz.tamas@inf.unideb.hu,

János Sztrik

Faculty of Informatics
University of Debrecen
sztrik.janos@inf.unideb.hu

***Abstract* - We can use variety of encryption standards to encrypt data traffic to ensure the safety of wireless networks. The question is to what extent the security of the network affects network performance. For answering this question, experiments were performed without data encryption, and the use of various encryption standards.**

Keywords: wireless networks, security, encryption, WEP, WPA/TKIP, WPA2/AES

I. INTRODUCTION

Wireless networks are increasingly exposed to the risk of unauthorized access. The reason for this is that the information runs instead of cable into the air. So it is enough to be in radio signal propagation range, and eavesdropping is easy (password and file contents can be stolen). You can use other internet subscriptions, and perform various illegal activities.

Avoiding illegal access to our network, we can encrypt the data flow. We can read about various wireless security tools in books [6], [7]. Wireless network security was examined in [2], [3], [5]. Paper [1] discovers the effects of the IEEE802.11i security specification on the performance of wireless networks. In [4], the throughput performance of IPv4 and IPv6 using UDP for wireless LAN networks with 802.11n and with and without security for two client-server networks were compared.

The question arises as to the security of wireless networks influences the speed of data transfer, that is, the network performance. To answer this question, we performed experiments without data encryption, and the use of various encryption standards. We changed the number and type of clients and measured the ftp service speed in the context of encryption in Windows 7 operating system. The results were published in papers [8] and [9].

Additional experiments examined the effects of cryptography in Windows 8.1 x64 operating system, and the relationship between the distance from the router and the speed of file transfer. This paper contains the results of these experiments.

II. THE EFFECT OF ENCRYPTION USING SMB FILE SHARING

Using Windows 8.1 file sharing and different encryption standards, writing and reading speeds were measured between two laptops.

In this experiment we copied files between the two laptops using a TP-Link wireless router wr2543ND. Both machines were running Window 8.1 x64 operating system.

laptop 1: dell studio 1557 (Dell 1520 wireless N card, Core i720Qm, 8GB RAM
laptop 2: dell inspiron core i5 3337U 8GB RAM
router: TP-link wr2543ND (Atheros AR7242 @400MHz CPU 64MB RAM)

The following encryption standards were used in the experiments:

1. WEP (Wired Equivalent Privacy) is a security algorithm for IEEE 802.11 wireless networks. Obsolete, it is not safe in today's circumstances. Each 802.11 packet is encrypted separately with an RC4 cipher stream generated by a 64-bit RC4 key.

2. WPA/TKIP (Wi-Fi Protected Access, Wi-Fi Protected Access), which is similar to the WEP uses RC4 coder 128-bit key and 48-bit initialization vector, but this has been introduced in accessing the TKIP (Temporal Key Integrity Protocol, temporary secure key protocol), which continuously rotates keys used in the link.

3. WPA2/AES (Advanced Encryption Standard) uses a new coder instead of the old RC4.

TABLE I.

Speed of Upload (MB/sec)	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	ave-rage
Without encryption	6,39	6,45	6,36	6,37	6,41	6,4
Wep	1,28	1,32	1,3	1,29	1,29	1,3
Wpa/tkip	1,27	1,27	1,3	1,28	1,29	1,28
Wpa2/aes	6,22	6,28	6,17	6,23	6,2	6,22

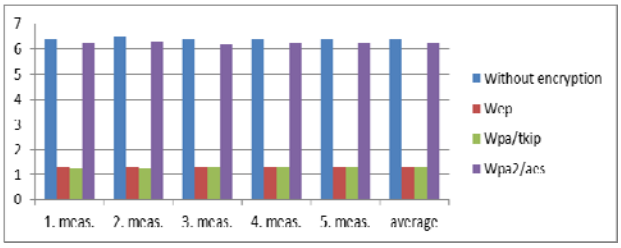

Fig.1 Speed of Upload (MB/sec)

TABLE II.

Speed of Download (MB/sec)	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	ave-rage
Without encryption	5,79	5,72	5,73	5,75	5,77	5,75
Wep	1,35	1,35	1,34	1,29	1,34	1,33
Wpa/tkip	1,28	1,29	1,32	1,29	1,3	1,3
Wpa2/aes	5,63	5,6	5,68	5,62	5,63	5,63

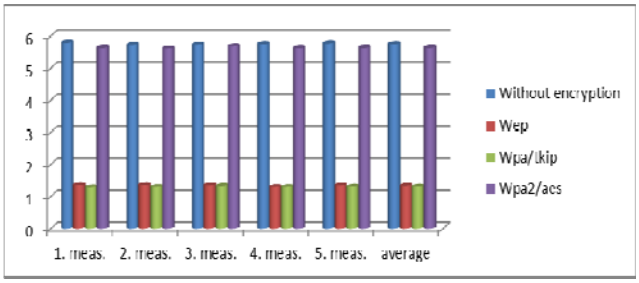

Fig.2 Speed of Download (MB/sec)

A. *Conclusion*

There is no significant difference between reading and writing WPA2/AES encryption and no encryption using Windows 8.1 file sharing.

The 802.11n does not allow WEP and WPA/TKIP encryption, so the router will switch back to 802.11 g mode, so despite the weaker encryption is much slower speeds are obtained. The WEP is no longer secure and only marginally faster than the WPA/TKIP encryption.

III. File transfer speed in case of FTP server

We studied upload and download speed depending on encryption using two machines with Windows 8.1 x64 operating system. We used Cerberus FTP x64 server and Total Commander x64 client.

The router was close to the computers in the first experiment and far in the second experiment.

WPA2/AES standard and no encryption were used in these experiments.

A. *First experiment: The router is physically close to the computers*

In the first experiment a file was copied between the two computers using the TP-link wr2543ND wireless router (Atheros AR7242@400MHz CPU 64MB RAM).

The two computers used Window8.1 x64 operating system.

laptop 1: dell studio 1557 (Dell 1520 wireless N card, Core i720Qm, 8GB RAM)

desktop 1: TP-Link TL-W722N usb wireless network card, Intel core duo E6500 processor, 8GB RAM.

During the experiments ca. 99 MB (99074904) transfer file was used.

The following speeds were measured:

TABLE III

Close Download	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	ave-rage
wpa2/aes (MB/sec)	2,09	2,11	1,9	2,28	2,11	2,09
without encryption (MB/sec)	2,27	2,11	2,3	2,48	2,45	2,31

Close Upload	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
wpa2/aes (MB/sec)	5,33	4,75	5,21	5,52	5,34	5,21
without encryption (MB/sec)	5,81	6,09	5,67	5,74	5,83	5,83

B. *Second experiment: The router physically far from the computers*

In the second experiment the computers were two floors away from the router.

In the second experiment a file was copied between the two computers using the TP-link wr2543ND wireless router (Atheros AR7242@400MHz CPU 64MB RAM)

The two computers used Window8.1 x64 operating system.

laptop 1: dell studio 1557 (Dell 1520 wireless N card, Core i720Qm, 8GB RAM)

desktop 1: TP-Link TL-W722N usb wireless network card, Intel core duo E6500 processor 8GB RAM

During the experiments ca. 99 MB (99074904) transfer file was used.

The speeds measured are presented in TABLE IV and TABLE V.

TABLE IV

Far Download	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	ave-rage
wpa2/aes (MB/sec)	1,44	1,48	1,51	1,3	1,32	1,41
without encryption (MB/sec)	1,66	1,57	1,63	1,5	1,63	1,6

TABLE V

Far Upload	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	ave-rage
wpa2/aes (MB/sec)	1,93	2,13	2,17	2,21	1,94	2,07
without encryption (MB/sec)	2,43	2,59	2,63	2,39	2,56	2,52

C. *Conclusions*

Using Windows 8.1 operating system and decreasing the router distance from the computers, the file transfer speed increases significantly.

The WEP security is poor and 802.11n switches back to 802.11g, and therefore we have not measured the WEP transfer speed.

If we use ftp server with Windows 8.1 x64, the slowing down of transfer speed on modern computers caused by encryption is significantly less. In most of the cases if security matters you have to use WPA2/AES encryption. If speed is more important than safety (such as anonymous FTP service or video playing), you can disable the encryption and speed of 10-15 per cent gain can be obtained using Windows 8.1 x64 with modern computers.

IV. Wireless speed without router using SMB filesharing

Windows 8.1 file sharing WPA2 encryption standard were used between two laptops directly connected without wireless router. I have found no way in the Windows 8.1 operating system to make wireless router without encryption.

In this experiment we copied files between the two laptops using a the second laptop as wireless router Both machines were running Window 8.1 x64 operating system. The laptops were close to each other.

laptop 1: Toshiba satellite Atheros 956x wireless N card, Core i4700MQ, 8GB RAM

laptop 2: Dell Inspiron core i5 3337U 8GB RAM

For the test we used 210MB length file. The following were measured.

TABLE VI

Close without router	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	ave-rage
writing (MB/sec)	6,07	6,15	5,89	6,30	6,01	6,08
reading (MB/sec)	6,19	6,04	6,18	6,37	6,35	6,23

A. *Conclusion*

The file transfer speed is a little bit faster without wireless home router end maybe the encryption slowing is less. In real life wireless networks are used with clients and wireless router.

V. Summary

In wireless networks where devices on the network are compatible and security matters, always should be used WPA2/AES encryption. The weaker encryptions switch back the more modern devices, on the older devices do not give a significantly better rate, but their security is worse. If speed is more important than safety (eg, media playback with wireless, public downloading), you can disable the encryption speed of 10-15 percent gain can be obtained.

After these results we can raise the question what is more responsible for slowing down the transmission speed, the encryption or the full bandwidth of the device.

ACKNOWLEDGEMENT

The publication was supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.

REFERENCES

[1] Gin, R. Hunt: Performance Analysis of Evolving wireless IEEE 802.11 Security Architectures, The International Conference on Mobile Technology, Applications and Systems , ACM, Ilan, Taiwan, 2008.

[2] P. Georgopoulos, B. McCarthy, C. Edwards: Providing Secure and Accountable Privacy to Roaming 802.11 Mobile, ACM, MPM'12, Bern, 2012.

[3] Bruce Potter: Wireless Hotspots: Petri Dish of Wireless Security, Communication of the ACM, 2006, vol.49, no.6, pp. 51-56.

[4] Samad S. Kolahi, Zhang Qu, Burjiz K. Soorty, and N. Chand: The Performance of IPv4 and IPv6 using UDP on IEEE 802.11n WLANs with WPA2 Security, ACM, 2009.

[5] T. Chenoweth, R. Minch, S. Tabor: Wireless Insecurity: Examing User Behavior on Public Networks, Communication of the ACM,2010, vol.53, pp.134-138.

[6] Vivek Ramachandran: BackTrack 5 Wireless Penetration Testing , PACKT Publishing, 2011

[7] Willie Pritchett, David De Smet: BackTrack 5 Cookbooks, Networking & Telephony, Open Source , PACKT Publishing, 2012

[8] T. Krausz, J. Sztrik: Performance Evaluation of Wireless Networks Speed Depending on the Encryption, Annales Mathematicae et Informaticae, 42 (2013) pp. 45–55, Eger, http://ami.ektf.hu

[9] T. Krausz, M. Princz, Gy. Bujdosó:Vezeték nélküli hálózatok sebessége a titkosítás függvényében, [Wireless Networks Speed Depending on the Encryption] SzámOkt 2013 XXIII. Nemzetközi Számítástechnika és Oktatás Konferencia Kiadványa. Nagyszeben, Erdélyi Magyar Műszaki és Tudományos Társaság, ISSN 1842 4546., pp.247–252.

[10] Y. Atsuya, S. B. Ayed, F. Teraoka: Network Access Authentication Infrastructure Using EAP-TTLS on Diameter EAP Application, ACM, AINTEC'11, Bangkok, Thailand, 2011