DIFFERENTIATING IEEE 802.11i RESOURCE AND SECURITY REQUIREMENT FOR MOBILE AND NON-MOBILE DEVICES

PARISA NARAEI

A project submitted in fulfillment of the

requirements for the award of the degree of

Master of computer science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

This thesis is dedicated to all the people who never stopped believing in me and have always been my ‘footprints in the sand’.

My mother, thank you for touching my heart and showing me the light when I turn to you.

My father, thank you for your endless support and encouragement and thanks for being my father.

The best brother ever- Pouyan, thank you for being a terrific friend and a strong shoulder to rely on.

And lastly thanks to **my Grandmother**, for her encouragement and positive energy.

ACKNOWLEDGEMENT

First and foremost, I would like to express my heartfelt gratitude to my supervisor **Associate Professor Dr.Mazleena Salleh** for her bright and intelligent recommendations during my project.

Besides, I would like to thank my Co-supervisor **Dr. Majid Bakhtiari** for his consultancies and supportiveness. Also, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with good environment and facilities such as computer laboratory to complete this thesis with software which I needed during the process.

ABSTRACT

AES-CCMP128 incorporates two sophisticated cryptographic techniques that are counter mode and CBC-MAC, and adapts them to Ethernet frames. This is to provide a robust security protocol between the mobile clients and furthermore the mobility characteristic of mobile devices makes it difficult for an eavesdropper to spot data patterns. However adding security functionality to mobile devices can reduce the Wi-Fi time connection rate due to the limited resources of mobile devices. Therefore, the lack of balance between the security level, resource usage and network speed required in mobile devices is eminent. The aim of this study is to speed up the Wi-Fi connection in mobile devices and also to optimize the resource usage by reducing two rounds of AES-CCMP resulting in 20% increase in network connection speed and optimization in the resource usage of mobile devices. Round 8 and Round 9 of AES-CCMP are the suggested results named “Short Time” (ST) and “Long Time” (LT) usage of mobile devices for less than two hours and more than two hours respectively. On the other hand, non-mobile devices do not have the same restrictions instead higher CPU, memory, battery charge and hardware. But on the other hand, the stationary characteristic makes non-mobile device an easy target to attack. Therefore, the security level they require is higher in comparison to that of mobile devices but the resource usage is yet to be optimized. Consequently, the possibility of AES-256 in 9 rounds has been investigated in this study for non-mobile devices considering Moore’s law and as such, 10% optimization has been achieved in the resource usage. The proposed scenarios of ST and LT are implemented by using C# language and the results are gained from execution time, memory usage, avalanche effect and crypt analysis for non-mobile and mobile devices.

ABSTRAK

AES-CCMP128 menggabungkan dua teknik kriptografi yang canggih ,mod kaunter dan CBC-MAC, dan disesuaikan dengan bingkai Ethernet untuk menyediakan protokol keselamatan yang mantap antara pelanggan mudah alih dan pusat akses tetapi mengurangkan kadar sambungan Wi-Fi. Selain itu, sumber peranti mudah alih yang terhad serta ciri-ciri mobiliti peranti mudah alih, menyukarkan pengintip mengesan coraknya. Oleh itu, kekurangan imbangan di antara tahap keselamatan, penggunaan sumber dan kelajuan rangkaian yang diperlukan dalam peranti mudah alih adalah sangat tinggi. Tujuan kajian ini adalah untuk mempercepatkan sambungan Wi-Fi dalam peranti mudah alih dan juga untuk mengoptimumkan penggunaan sumber dengan mengurangkan dua pusingan AES-CCMP menghasilkan 20% peningkatan kelajuan sambungan rangkaian dan pengoptimuman dalam penggunaan sumber peranti mudah alih . Pusingan 8 dan Pusingan 9 AES-CCMP adalah keputusan yang disyorkan dan dinamakan “Short Time” (ST) dan “Long Time” (LT) untuk penggunaan peranti mudah alih iaitu masing-masing adalah kurang daripada dua jam dan lebih daripada dua jam. Manakala, ciri-ciri statik menjadikan peranti bukan mudah alih sasaran yang mudah untuk diserang. Oleh itu, tahap keselamatan yang diperlukan adalah lebih tinggi berbanding dengan alat-alat mudah alih namun penggunaan sumbernya masih belum optimum. Oleh yang demikian, kemungkinan AES-256 dalam pusingan 9 telah diselidiki dalam kajian ini untuk peranti bukan mudah alih dengan mempertimbangkan undang-undang “Moore” dan oleh itu, 10% pengoptimuman telah dicapai dalam penggunaan sumber. Senario cadangan ST dan LT dilaksanakan dengan menggunakan bahasa C # dan keputusan yang diperolehi adalah masa pelaksanaan, penggunaan memori, kesan “Avalanche” dan analisis kripto untuk peranti bukan mudah alih dan mudah alih.

TABLE OF CONTENTS

2 LITERATURE REVIEW

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
AS	-	Authentication Server
CBC	-	Cipher Block Chaining
CIA	-	Confidentiality, Integrity, and Availability
CTR	-	Counter
DES	-	Data Encryption Standard
DLS	-	Direct Link Setup
GTK	-	Group Temporal Key
IEEE	-	Institute of Electrical and Electronic Engineers
ISM	-	Industrial, Scientific, and Medical
IV	-	Initial Vector
KCK	-	Key Conformation Key
KEK	-	Key Encryption Key
LAN	-	Local Area Network
LLC	-	Logical Link Control
LT	-	Long Time
MAC	-	Message Authentication Code
MIMO	-	Multiple Input, Multiple Output
MIC	-	Message Integrity Code
MAC	-	Media Access Control
MPDU	-	MAC Protocol Data Unit
NIST	-	National Institute of Standards and Technology
PMK	-	Pairwise Master Key
PHY	-	Physical
PTK	-	Pairwise Transient Key
PN	-	Packet Number

QoS	-	Quality of Service
RF	-	Radio Frequency
RADIU	-	Remote Access Dial-In User Service
ST	-	Short Time
RSNA	-	Robust Security Network Association
TK	-	Temporal Key
TKIP	-	Temporal Key Integrity Protocol
TMTO	-	Time Memory Trade Off
WEP	-	Wired Equivalent Privacy
WPA	-	Wi-Fi Protected Access
WPA2	-	Wi-Fi Protected Access II

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, wireless technology can be found everywhere. Different users are using wireless technology and a wide range of wireless devices exists like PCs, Laptops, Tablets and Fablets. Wireless transmissions, use the microwave specter. The available frequencies are situated around the 2.4 GHz ISM band for a bandwidth of about 83 MHz and around the 5 GHz U-NII band, for a bandwidth of about 300 MHz divided into two parts. The accurate frequency allocations are set by laws in different countries; the same laws also adjust the maximum selected transmission power and location. Although this technology is being generally used, different devices have different capabilities in the usage. Since wireless networks have more vulnerabilities than other types of computer networks, preparing security in Wireless Local Area Network is more essential (Kumar *et. al*, 2008). The security mechanism chosen for different devices may differ. A satisfactory security technique in wireless network is a balance between data security and network performanc

This chapter discusses the problem background of IEEE 802.11 standards and determines security model of 802.11 named 802.11i. Besides, it explains the aim of this research and defines objectives and the scope of this study.

1.2 Problem Background

Nowadays, the kind of devices being used for Wi-Fi connection is different from previous decade. People used to connect with their PCs and laptops; but nowadays they use mobile devices rather than main computers. The new mobile devices need security for the data transmission on the internet, so the necessity of secure algorithms and protocols for encryption and decryption of the data becomes more and more apparent. For this purpose, new devices had to follow the existing security protocols which were designed and implemented on main computers for Wi-Fi connections (Rahman and Pathon, 2011)

IEEE 802.11 standard defines an interface between a wireless client and an access point or between two or more wireless clients. IEEE 802.11i is a revision to the original IEEE 802.11. The draft standard was sanctioned by the IEEE on 24th of June 2004. This standard specifies security mechanisms for wireless networks. For confidentiality 802.11i uses new model of encryption. The modern cryptography is based on the Advanced Encryption Standard (AES) algorithm, which was selected by NIST and adopted by the United States government as a national standard and replacement for the previous standard based on the Data Encryption Standard (DES) algorithm. Strong encryption and authentication are added as the primary components of 802.11i to complete the 802.11i standard (VRAP and LLNL, 2007).

The encryption methods of three generation of 802.11i are described as follows:

Wired Equivalent Privacy (WEP): Uses the RC4 stream cipher for providing confidentiality, and the ICV (CRC-32) for integrity. WEP has the following weaknesses

(Habibi, *et al*., 2009) Some of the weaknesses of WEP include not being able to stop packet forgery and replay attacks. Besides, attackers can easily record and replay packets. WEP uses RC4 inappropriately. Keys are not strong, and attacker can do brute-force attack in less than an hour. This protocol reuses initialization vectors. Some attack techniques are able to decrypt data without key and it allows an intruder to invisibly modify a plaintext without having the key for encryption. Besides, Key management is weak and upgrading is not perfect. There are some problems which exist both in the RC4 algorithm and WEP message authentication which can be easily forged.

Wi-Fi Protected Access (WPA): Regarding to the issues in the WEP method, the WPA has been developed in order to solve them, without making any changes in hardware. This standard similar to WEP identifies two modes including personal and enterprise modes. In addition the WPA has the following weaknesses (Habibi, *et. al*, 2009):

i. Brute-force attack
ii. Dictionary attack

In the context of security, a brute force attack is a particular strategy used to break one's crafted password. This is the most widely used method of cracking. Dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying different possibilities, such as words in a dictionary. WEP Uses the RC4 for confidentiality, and the Temporal Key Integrity Protocol (TKIP) / Message Integrity Code (MIC) for providing integrity.

Wi-Fi Protected Access II (WPA2): WPA2 has been developed after two generations of 802.11i which are WEP and WPA; they used RC4-CRC and RC4-TKIP/MIC in order. WPA2 is known as the best security protocol in wireless networks. WPA2 exchanged RC4 with AES and substituted Michael by message authentication code. Like WPA, WPA2 supports two security modes. The first mode is personal and the second mode is enterprise (Habibi, *et. al*, 2009).

i. A pre-shared secret is used in home personal. Clients and access points are manually configured to use the similar secret of up to 64 ASCII characters or 256-bits.

ii. In enterprise mode providing security is built on 802.1X, EAP authentication framework such as RADIUS, which is one of several EAP modes like EAP-TLS, and it delivers a much stronger authentication mechanism, and secure key distribution.

WPA2 Offers confidentiality by using AES in Counter (CTR) mode, and offer authentication and integrity by using Cipher Block Chaining-Message Authentication Code (CBC-MAC).

Internet connection speed and broadband connectivity have reached to 17.5 Mbps in the world but such a net speed is not achieved in wireless networks yet; since the strong security protocol of AES-CCMP (WPA2) slows down the wireless speed. Despite the popularity of mobile devices, their performance and energy bottlenecks remain hidden due to a lack of visibility into the resource-constrained mobile execution environment with potentially complex interaction with the Wi-Fi connection (Feng *et. al,* 2011). AES-CCMP is working tardily in mobile devices with resource limitation, and preparing ideal encryption in AES-CCMP leads to speed reduction and this is the issue that should be considered.

1.3 Problem Statement

IEEE 802.11i encryption technique provides strong security mechanism in computer systems but it is not optimized in the usage of resources. Besides, in mobile devices which are power and resource-constrained, the wireless connection speed decreases. The level of security provided in AES-CCMP is not needed in mobile devices since the mobility characteristic of mobile devices restricts an attacker’s required time to hack the victim device and the session would be terminated whenever the location of mobile device changes. Thus, there is a lack of balance between security level and resource usage that should be investigated.

1.4 Purpose of the Study

Nowadays, the number of wireless devices is growing significantly, but they all used to be computer systems. Wireless technology was not accessible in mobile and portable devices until recently. The purpose of this research is to determine the issues of the performance of current encryption methods in AES-CCMP in different types of devices and handle it so that an optimized resource usage would be achieved with the required security. Finally, two scenarios for 802.11i for two different groups of devices will be created and evaluated with current encryption method for AES-CCMP in order to compare their performance.

1.5 Objectives of the Study

To achieve the intention of the study, the following objectives are specified:

i. To implement the components of AES-CCMP and to analyze its function.

ii. To create two scenarios which have short time and longtime usage for AES-CCMP, for portable systems which have resource limitation like mobile devices.

iii. To test and validate the possibility of optimizing resource usage in non-mobile devices.

1.6 Significance of the Study

The number of mobile and portable devices like tablets and fables with limited resources and the security mechanism of AES-CCMP being run on these devices is increasing. Such mechanism makes them slow in terms of wireless connections; therefore, offering an optimized technique for solving the mentioned issue will make the mobile devices faster in Wi-Fi connection. It is able to prepare a strong security and optimized resource usage for main computer users and to prepare the required security and higher speed for mobile device users. Mobile device users will consider the required security, high speed data transfer and the power limitation consequently.

1.7 Scope of the Study

This research focuses on the secure model of 802.11 standards named AES-CCMP in two groups of devices. Based on the resource and power limitation the two groups are divided into mobiles and non-mobiles. This study offers an improved performance of mobile devices in terms of wireless connection using IEEE 802.11i standard. In this study, C# language is applied for implementation in a network environment.

1.8 Organization of the Study

This study is divided into six chapters. Chapter one briefly describes the overview of the project and understanding of the project problem background. It also includes the project scope, purpose of this research and objectives. Chapter two discusses 802.11i standard, encryption components in 802.11i, AES-CCMP framework and the issue of AES-CCMP in mobile devices. The methodology of this research is explained in detail in Chapter three. Chapter four contains explanations of design and implementation of this study for mobile devices. Chapter five explains explanations of design and implementation of this study for non-mobile devices. Finally, Chapter six reviews and summarizes the whole project findings and suggests some recommendations.

1.9 Summary

WLAN has a good future with 802.11 as a perfect standard to adopt in LAN environments. Also, 802.11 offers reliability and strong security (Daemen and Rijmen, 1998). This chapter illustrates the 802.11i standard. Then this chapter defines statement of the issues in performance of AESCCMP encryption protocols in mobile devices. In addition, it explains the purpose of this research as well as the scope of the study and defines objectives.

REFERENCES

Ahmed Khan, M., Cheema, A. R., & Hasan, A , (2008). *Improved Nonce Construction Scheme for AES CCMP to Evade Initial Counter Prediction*. Paper presented at the Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Phuket.

Habibi-lashkari, a., Seyed-danesh, m. m., & Samadi ,(2009). *A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)*. Paper presented at the 2nd IEEE International Conference. Computer Science and Information Technology (ICCSIT) Beijing.

Ho Yung, J., Joon Hyoung, S., Jung Hee, S., In Cheol, H., & Jun Rim, C, (2004). *Compatible Design of CCMP and OCB AES Cipher Using Seperated Encryptor and Decryptor for IEEE 802.11i.* Paper presented at the Circuits and Systems (ISCAS).

IEEE-Computer-Society, (2004). *IEEE Standard for Information technology-Telecommunications and information-exchange between systems-Local and Metropolitan Area Networks* - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6 : Medium Access Control (MAC) Security, Enhancements (pp. 0_1 - 175).

Razvi Doomun, M., & Sunjiv Soyjaudah, K. M, (2008). Resource Saving AES-CCMP Design with Hybrid Counter Mode Block Chaining – MAC. *IJCSNS International Journal of Computer Science and Network Security, 8,* 1 -13.

VOCAL, (2003). *CCMP AES Counter CBC-MAC Protocol Advanced Encryption Standard*. VOCAL, from VOCAL Technologies

Qian F., Wang Z., Gerber A., Mao Z., Sen S. and Spatscheck O., (2011) *Profiling resource usage for mobile applications: a cross-layer approach*, In *Proceedings of* *the 9th international conference on Mobile systems, applications, and services* (pp. 321-334). ACM.

R. Karri AND P. Mishra ,(2003) “*Analysis of energy consumed by secure session negotiation protocols in wireless networks*”, International Workshop on Power and Timing modeling, Optimization and Simulation, Torino, Italy, Sep

Daemen J, Rijmen V ,(2002) *The design of Rijndael: AES—The advanced encryption standard*. Springer,

Gilbert H, Minier M, (2005) *A collision attack on 7 rounds of Rijdael*. In: The third AES candidate conference, pp 230–241

Saberi I., Shojaie B., Salleh M.and Niknafskermani M, (2011).*Enhanced AES-CCMP key structure in IEEE 802.11 i.*In Computer Science and Network Technology (ICCSNT), International Conference on (Vol. 1, pp. 625-629).IEEE

Saberi I., Shojaie B., Salleh M., Niknafskermani M., and Rostami M. J, (2012) *Preventing TMTO Attack in AES-CCMP in IEEE 802.11 i. Computer Networks*, 181-190

Saberi I., Shojaie B., Salleh M., Niknafskermani M., and Alavi S. M, (2012) *mproving confidentiality of AES-CCMP in IEEE 802.11 i.* In Computer Science and Software Engineering (JCSSE), International Joint Conference on (pp. 82-86). IEEE.

Abdul, S., Arshad, A., & Nassar, I, (2007). *An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless Standard*. Paper presented at the 31st Annual International Computer Software and Applications Conference(COMPSAC), Beijing.

VRAP, & LLNL , (2007) Securing WLANs using 802.11i Draft *Recommended Practices Guide Securing WLANs using 802.11i* (pp. 1 - 17). United States: Control Systems Security Program (CSSP).

Demirci H, Taskin I, Coban M, Baysal A , (2009) *Improved meet-in-the-middle attacks on AES*. In: Roy B, Sendrier N (eds) INDOCRYPT . Lecture notes in computer science, vol 5922, Springer, Heidelberg, pp 144–156

Bahrak B, Aref MR , (2008) *Impossible differential attack on seven-round AES-128.* IET Inform Security 2:28–32

Zhang W, Wu W, Feng D, (2007) *New results on impossible differential cryptanalysis of reduced AES*. In: Nam K-H, Rhee G (eds) ICISC 2007, Lecture notes in computer science,vol 4817, Springer, Heidelberg, pp 239–250

Kumar D, Aseri TC, Patel RB, (2008) *Multi-hop communication routing (MCR) protocol for heterogeneous wireless sensor networks*. Int J Inform Technol Commun Converg 1(2):130–145

Rahman MZ, Pathan A , (2011) *A case study: establishing redundant access networks in the telecommunication sector of a developing country*. Int J Inform Technol Commun Converg 1(1):108–126

Daemen, J., Rijmen, V, (1998) *AES proposal: Rijndael*

Siau, E.-P.L. and K., (2003) *Advances in Mobile Commerce Technologies*, United States of America by Idea Group Publishing.

Biryukov, A., Khovratovich, D., Nikolic, I (2010). *Distinguisher and Related-Key Attack on the Full AES-256.* 231–249

Mala, H., Dakhilalian, M., Rijmen, V., Modarres-Hashemi, M, *(*2010). *Improved Impossible Differential Cryptanalysis of 7-Round AES-128*. In Gong, G., Gupta, K.C., eds.: In docrypt. Volume 6498 of Lecture Notes in Computer Science., Springer 282–291

Gilbert, H., Minier, M. *A* ,(2000). *Collision Attack on 7 Rounds of Rijndael.* Candidate Conference. 230–241