International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 4860~4865
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp4860-4865

Ensuring telecommunication network security through cryptology: a case of 4G and 5G LTE cellular network providers

Adnan Manasreh[1], Ahmed A. M. Sharadqh[2], Jawdat S. Alkasassbeh[3], Aws Al-Qaisi[4]
[1]Department of Electrical and Computer Engineering, Applied Science Private University, Jordan
[2]Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Jordan
[3]Department of Mechanical Engineering and Electronic Information, China University of Geosciences, China
[4]Department of Communication Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Jordan

Article Info

Article history:

Received Feb 28, 2019
Revised Jun 11, 2019
Accepted Jun 27, 2019

Keywords:

KERBEROS
PGP
SSH
SSL

ABSTRACT

This paper aims to present the details regarding telecommunication network security through cryptology protocols. The data was based on scientific data collection and the quantitative method was adopted. The questionnaire was developed and the primary respondents were approached who were working in 4 telecommunication networking companies namely Huawei, Ericsson, SK Telecom and Telefonica. The sample size of the research was 60 participants and the statistical analysis was used to analyze research. The finding shows that cryptology protocol such as SSH, SSL, Kerberos PGP and SET are implemented within the companies in order to secure network.

Corresponding Author:

Aws Al-Qaisi,
Department of Communication Engineering,
Faculty of Engineering Technology,
Al-Balqa Applied University,
P. O. Box 15008, Marka 11134, Jordan.
Email: aws.alqaisi@bau.edu.jo

1. INTRODUCTION

The telecommunications network security includes the transmission methods, transport formats, structures and security means which provides integrity confidentiality, authentication and availability for the transmission over the public and private communication media and network [1-3]. The information security domain is highly concerned with the data protection for voice and video communication. With the passage of time and advancement in technology the telecommunication network is taking multiple initiates in order to improve their network security. The improvement in security networks boosts the flexibility and it improves the efficiency. It further saves the time and cost and provides efficient business solutions.

Despite growing need for telecommunication security, many companies have not adopted efficient infrastructure which results in risk and failure. The security services aim to add security to the system so that various types of security attacks can be encounter [4]. The cryptography plays a significant role in the network security and in order to understand the inherited vulnerabilities in the telecommunication network security the development of cryptographic mechanism helps in combating against the security weakness. The cryptography is widely applied in the telecommunication network and it creates direct effects on the transparency to users [5, 6]. The cryptology is a Greek word and it means ‘hidden secret”. This practice is applied for the purpose of securing the communication in the presence of the third parties

which are referred to as adversaries. The cryptography is about construction and analysis about the protocols which prevent the public or third party from reading the private messages [7]. The reason to use cryptography in a telecommunication network is that the network system is vulnerable towards various risk and threat due to data confidentiality, data authentication, data integrity and non-repudiation [8].

The modern cryptography is intersected in the electrical engraining, mathematics, physics and communication services and it has brought the security towards chip-based payments, digital curries, electronic commerce and military communication [9-11]. The cryptography refers to encryption and it ensures the conversion of information. The modern cryptology is based on computer science practices and mathematical facts [12, 13]. The algorithms are developed around the computational hardness assumptions which are hard to break by an adversary. The Figure 1 illustrates the encryption algorithm.

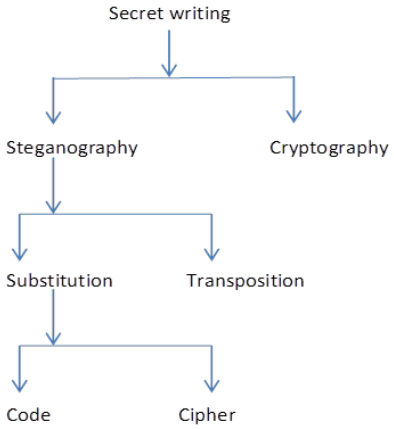

Figure 1. Encryption algorithm

There are two major requirements for the cryptography [14-16]:

a. The first is that it must be computationally infeasible towards deriving the plaintext from ciphertext within the knowledge of decryption key
b. Another requirement is that it must be computationally infeasible to derive cypher text from plain text within the knowledge towards encrypting key

Hence, these two conditions must be satisfied even which the decryption and encryption algorithms are known. In addition, the symmetric cryptography is referred as the cryptographic system where the same or the similar key is applied for the purpose of decryption or encryption [17, 18]. In the symmetric cryptosystem, the communication entities share the secret key which is similar in nature [19]. The asymmetric is the public key which is used in the cryptography system that includes the pair of keys. It includes private and public key where the public key is distributed but the private key remains secret by the entity. Hence, there are two various types of asymmetric key pairs which include decryption and encryption of data while the rest technologies only generate and validate the digital signature.

The aim of this research is to examine ways by which the telecommunication network security can be enhanced within the 4G and 5G LTE network. Based on this the objective are:

a. To explore the concept of cryptography in telecommunication network security
b. To explore the information about cryptographically based protocols used by telecommunication network for security purpose
c. To determine the Impact of cryptographically on security in 4G and 5G LTE networks

2. RESEARCH METHOD

The paper presents the empirical information on telecommunication network security through cryptography in 4G and 5G LTE networks. The paper focused on primary and secondary sources. The primary sources of the paper are the employees working in IT departments of various telecommunication companies such as Huawei, Ericsson, SK Telecom and Telefonica. Huawei is Chinese Telecommunication Company and it provides products and services in more than 10 countries. Ericsson is a Swedish multinational telecommunication and networking company and it provides broad internet services and mobile broadband services. SK Telecom is a South Korean company that provides wireless telecommunication services in the local market. Lastly, Telefonica is a Spanish multinational firm which provides

telecommunication services within the American and European market. The case study approach was selected for the paper and 4 cases were used. The research was based on a deductive approach and the hypothesis was developed to gather specific and fact-based data. The quantitative research method allowed quantifying the use of cryptology by these firs and its impact on the telecommunication network security.

According to Table 1, the questionnaire was selected as the data collection instrument and the primary responses were selected who were working in the 4 companies. The total sample size of the study was 60 and from each company 20 respondents were approached. The employee working in Information technology department, the research and development department and customer service department were selected. Besides this, the secondary sources were also gathered in order to gather a comprehensive perspective about cryptography. The secondary sources were gathered by exploring the various journals relevant to the security in the telecommunication sector and the concept of cryptography. The cross-sectional data was gathered within limited time and from a limited population. The data were pooled into SPSS for the statistical testing and the one-sample t-test and Pearson correlation test was performed to identify the impact of SSH, SSL, Kerberos PGP and SET protocol on providing telecommunication network security within 4G and 5G LTE network.

Table 1. The questionnaire

Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
SSH					
My company uses Secure shell to secure the remote login	□	□	□	□	□
My company use strong authentication with encryption	□	□	□	□	□
SSL					
My company use secure socket layers to establish encrypted links	□	□	□	□	□
The use of SSL ensures that the information transmit between the bower and server remains encrypted	□	□	□	□	□
Kerberos					
My company provides strong authentication through using Kerberos protocol	□	□	□	□	□
The company uses secret-key for the cryptography	□	□	□	□	□
PGP					
My company ensures cryptographic privacy as the web of trust	□	□	□	□	□
By use of PGP the information is secured throughout signing, encryption and decryption	□	□	□	□	□
SET					
My company offers security and integrity by using SET	□	□	□	□	□
The SET ensures restriction towards sharing any information with third party	□	□	□	□	□
Network Security					
Due to application of cryptography protocol the network system is secured	□	□	□	□	□
The company ensures preventive measures to reduce security threat and provide safety	□	□	□	□	□

3. RESULTS AND ANALYSIS

The Table 2 are the cryptography based protocols used by telecommunication network in order to enhance their security. The Table 3 and Table 4 summarizes the one and t-test sample performed on the above protocols.

Table 2. The protocols

SSH	Secure Shell
SSL	Secure socket Layer
Kerberos	Network Protocol
PGP	Pretty good Privacy
SET	Secure Electronic Protocol
Network Security	Network Security protocol

Table 3. One-sample test

	N	Mean	Std. Deviation	Std. Mean
SSH	60	3.675	0.66908	0.08638
SSL	60	4.125	0.6485	0.08372
Kerberos	60	3.8	0.92608	0.11956
PGP	60	3.6583	0.54843	0.0708
SET	60	3.875	0.75703	0.09773
Network Security	60	3.6167	0.9037	0.11667

Table 4. T-sample test

	t	df	Sig. (2-tailed)	Mean	upper	lower
SSH	42.546	59	0	3.675	3.5022	3.8478
SSL	49.271	59	0	4.125	3.9575	4.2925
KERBEROS	31.784	59	0	3.8	3.5608	4.0392
PGP	51.67	59	0	3.6583	3.5167	3.8
SET	39.649	59	0	3.875	3.6794	4.0706
Network Security	31	59	0	3.6167	3.3832	3.8501

SSH – It is used as the encrypted tunnel for the purpose of data exchange. It is used as the transport layer for the non-secure protocols. The SSH provides the security services by ensuing cryptographic mechanism. The variable was proved with the sig value of 0.000 and the mean difference was 3.67500. Besides this, the t value was 42.546 and the number of respondents was 60 and the standard error was .668908.

SSL – The SSL protocols are used as the encrypted tunnel in order to create the channel for exchange of arbitrary data which is the transport mechanism for the non-secure protocols [2]. The SSL provides the security services which aims to protect against the reply of attacks. The variable was proved with the sig value of 0.000 and the mean difference was 4.12500. Besides this, the t value was 42.271 and the numbers of respondents were 60 and the standard error was .08372.

KERBEROS – The Kerberos is the complex protocols which are applied in the open system in order to ensure multiple authentications for the server and the client [20]. It is based on unique comparison towards similar authentication protocols which is used in the symmetric key [21]. The variable was proved with the sig value of 0.000 and the mean difference was 3.80000. Besides this, the t value was 31.784 and the number of respondents was 60 and the standard error was .92608.

PGP – The PGP is applied for the encryption on context by using an asymmetric encryption key. It ensures data integrity, confidentially and use for the security mechanism [22, 23]. The variable was proved with the sig value of 0.000 and the mean difference was 3.65833. Besides this, the t value was 51.670 and the numbers of respondents were 60 and the standard error was .54843.

SET – The SET protocol is developed in order to protect the credit card transaction on the internet. It suppliers the security services and used the mechanism of cryptographically [17, 24]. The variable was proved with the sig value of 0.000 and the mean difference was 3.87500. Besides this, the t value was 39.649 and the numbers of respondents were 60 and the standard error was .75703.

The correlation model proves the strong relationship among variables that shown in Table 5. Based on the Table 5, it is concluded in Table 6.

Table 5. Correlations

		SSH	SSL	KERBEROS	PGP	SET	Network Security
SSH	Pearson Correlation	1	.476**	.420**	0.039	.370**	.470**
	Sig. (2-tailed)	0	0	0.001	0.769	0.004	0
	N	60	60	60	60	60	60
SSL	Pearson Correlation	.476**	1	.762**	0.229	.421**	.719**
	Sig. (2-tailed)	0	0	0	0.078	0.001	0
	N	60	60	60	60	60	60
KERBEROS	Pearson Correlation	.420**	.762**	1	.339**	.749**	.904**
	Sig. (2-tailed)	0.001	0	0	0.008	0	0
	N	60	60	60	60	60	60
PGP	Pearson Correlation	0.039	0.229	.339**	1	0.1	.338**
	Sig. (2-tailed)	0.769	0.078	0.008		0.449	0.008
	N	60	60	60	60	60	60
SET	Pearson Correlation	.370**	.421**	.749**	0.1	1	.678**
	Sig. (2-tailed)	0.004	0.001	0	0.449	0	0
	N	60	60	60	60	60	60
Network Security	Pearson Correlation	.470**	.719**	.904**	.338**	.678**	1
	Sig. (2-tailed)	0	0	0	0.008	0	0
	N	60	60	60	60	60	60

Table 6. Summary

Protocol	Sig value	Pearson Value	Conclusion
SSH	0	0.476	Strong relationship
SSL	0	0.42	Strong relationship
KERBEROS	0	0.039	Moderate relationship
PGP	0	0.769	Strong relationship
SET	0	0.37	Strong relationship
Network Security	0	-470	Strong relationship

4. CONCLUSION

The analysis presents in the paper summaries that for telecommunication network it is essential to ensure security in order to avoid the attacks. The telecommunication network security ensures confidentiality that makes the data secured by ensuring that the access data can access it. Besides this, the integrity allows assessing that the data cannot be changed or malice. It is opposite to the alteration and the availability ensure that the data is accessible whenever needed and without any destruction. Therefore, in the telecommunication sector the network security helps in securing the information system, and it results in the prevention and detection of data. The findings reveal that the cryptography protocols such as SSH, SSL, Kerberos PGP and SET provide telecommunication network security within 4G and 5G LTE network of Huawei, Ericsson, SK Telecom and Telefonica.

REFERENCES

[1] L. Merrien, *et al*., "System and method for securely using multiple subscriber profiles with a security component and a mobile telecommunications device," *Patent No.: US 9,647,984 B*, 2017.

[2] A. Rashid, *et al*., "Scoping the cyber security body of knowledge," *IEEE Security & Privacy*, vol. 16, pp. 96-102, 2018.

[3] G. Parekh, *et al*., "Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes," *IEEE Transactions on Education*, vol. 61, pp. 11-20, 2017.

[4] N. Ferguson, *et al*., "Cryptography Engineering: Design Principles and Practical Applications," New York : John Wiley and Son, 2010.

[5] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security & Privacy*, vol. 16, pp. 38-41, 2018.

[6] A. John, *et al*., "Oversimplifying quantum factoring," *Nature*, vol. 499, pp. 163-165, 2013.

[7] R. T. Peltier, "Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management," CRC Press, 2013.

[8] Y. Choi, *et al*., "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors (Basel)*, vol. 14, pp. 10081-10106, 2014.

[9] K. M. Abdullah, *et al*., "New Security Protocol using Hybrid Cryptography Algorithm for WSN," *1st International Conference on Computer Applications & Information Security, IEEE ICCAIS 2018.* pp. 1-6, 2018.

[10] T. Bin, *et al*., "A security framework for wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 17, pp. 118-122, 2010.

[11] R. Rizk, *et al*., "Two-phase hybrid cryptography algorithm for wireless sensor networks," *Journal of Electrical Systems and Information Technology*, vol. 2, pp. 296-313, 2015.

[12] X. Guo-bo and G. Long, "Elliptic-Curve-Based Security Processor for RFID," *IEEE Transactions on Computers*, vol. 11, pp. 1514-1527, 2008.

[13] A. Satoh, *et al*., "A Scalable Dual-Field Elliptic Curve Cryptographic Processor," *IEEE Transactions on Computers*, vol. 52, pp. 449-460, 2003.

[14] S. Nagpal, *et al*., "Collaboration of Cryptography and Steganography for Enhanced Security: A Review," *International Journal of Engineering Science Invention*, vol. 7, pp. 2319-6726, 2018.

[15] M. E. Saleh, *et al*., "Data Security Using Cryptography and Steganography Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, pp. 390-397, 2016.

[16] K. R. Babu, *et al*., "A Survey on Cryptography and Steganography Methods for Information Security," *International Journal of Computer Applications*, vol. 12, pp. 13-17, 2010.

[17] Patil A. and Goudar R., "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices," *International Journal of Scientific & Technology Research IJSTR*, vol. 2, pp. 61-65, 2013.

[18] S. A. Vanstone, "Next generation security for wireless: elliptic curve cryptography," *Computers & Security*, vol. 22, pp. 412-415, 2003.

[19] M. Agrawal, *et al*., "A Comparative Survey on Symmetric Key Encryption Techniques," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 4, pp.877-882, 2012.

[20] B. C. Neuman, *et al*., "Kerberos: an authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, pp. 33-38, 1994.

[21] S. M. Bellovin, *et al*., "Limitations of the kerberos authenication system," *Computer Communication Review*, vol. 20, pp. 119-132, 1990.

[22] K. Shafinah, *et al*., "File Security based on Pretty Good Privacy (PGP) Concept," *Computer and Information Science*, vol. 4, pp. 10-28, 2011.
[23] J. D. Haney, "The use of cryptography to create data file security: with the Rijndael cipher block," *Journal of Computing Sciences in College*, vol. 21, pp. 30-39, 2006.
[24] S. Lu, *et al*., "Model checking the secure electronic transaction (SET) protocol," *Proceedings of the Seventh International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, MASCOTS '99, 1999.

BIOGRAPHIES OF AUTHORS

Adnan Manasreh was born in 1969. He received his B.S, M.S, from Leningrad Polytechnic University, Russia in 1995, 1997 and Ph.D, from Saint Petersburg State Electrotechnical University, Russia in 2001. Currently he is working as an Assistant Professor at the Department of Electrical Engineering, Applied Science Privet University, Amman, Jordan. His current research interests include CMOS technologies and nano devices technologies.

Dr. Ahmed A. M. Sharadqh received his PhD Degree in Computer, computing system and networks from National Technical of Ukraine "Kyiv Polytechnic Institute Ukraine in 2007. Since 2009, Dr. Ahmed sharadqh has been an Associate professor in the Computer Engineering Department, Faculty of Engineering Technology, at Al-Balqa Applied University. His research interests include Performance of network, Quality services, security network, image processing, digital systems design, operating system, and Microprocessors.

Jawdat S. Alkasassbeh was born in April, 1983 in Jordan. He received his B.Sc. in Communications Engineering, Department of Electrical Engineering, Faculty of Engineering, Mu'tah University, Jordan in 2006. He had a master degree in Communication Engineering from the University of Jordan in 2011. Currently, a Ph.D. student at China University of Geosciences (Wuhan). His research interests include digital wireless communication systems, MIMO Radar and Evolutionary Algorithms

Dr Aws Al-Qaisi is an associated professor in the Communication Engineering Department, Faculty of Engineering and Technology, Al-Balqa' Applied University, Jordan. Al-Qaisi was received his PhD and MSc in communication and signal processing from Newcastle university in 2006 and 2010 respectively. Dr. Aws research interest includes Digital signal processing, seismic signal processing, Wireless communication, Digital communication and wireless sensor network. He served as reviewer in many international journals where he has published more than 16 scientific papers in the field of communication and signal processing.