Vulnerabilities in Public Key Cryptography

Mohamed Abdulla[1], Muhammad Ehsan Rana[2,*]

[1,2] Asia Pacific University of Technology & Innovation, 57000, Bukit Jalil, Kuala Lumpur, Malaysia
[*]Corresponding author. Email: muhd_ehsanrana@apu.edu.my

ABSTRACT

Cryptography plays a vital role in securing data for IT infrastructure by enabling an adequate level of security to the business. The increased significance of security in the IT infrastructure has raised the demand for public key cryptography. Public key cryptography eliminates the primary concern in private key cryptography, i.e. exchanging the key between the sender and the receiver by having a pair of keys. Public key cryptography enables the exchange of the key even in an unsecured network. After the introduction of public key cryptography, this type of cryptography is the best solution in securing the transmitted data between the sender and the receiver. However, there are vulnerabilities in this type of cryptography that both the sender and the receiver need to know. This research is focused on determining the vulnerabilities of public key cryptography. It also emphasizes how security specialists can overcome these vulnerabilities in public key cryptography.

Keywords: *Cryptography, Asymmetric Cryptography, Public Key Cryptography, Vulnerabilities, IT Infrastructure Security.*

1. INTRODUCTION

Cryptography involves Mathematics and Computer Science concepts to encode data into a specific format, where the decoding will be only possible using the same key used in the encoding process. Public key cryptography (asymmetric cryptography) is the most widely used type of cryptography to secure data in most fields. On the other hand, symmetric cryptography is mostly used in the military field [24-31].

In the past decades, symmetric cryptography was the primary technology to encrypt the data, but it lacks in exchanging the secret private key securely. To overcome the drawbacks of the symmetric cryptography, researchers invented public key cryptography [1].

Public key cryptography, usually known as asymmetric cryptography, involves paired keys, i.e. public key and a private key. In order to encrypt the data, a public key is used with the encryption algorithm, and for decrypting the data, the private key (corresponding to the public key) is used with the encryption algorithm. Data decryption will only be possible by using the corresponding private key, of the public key used in the encryption process with the same algorithm. There is no fear to distribute a public key even in the unsecured network connection. However, the private key should be kept in secret [2].

The strength of cryptography primarily depends on the length of the key and the encryption algorithm [32-35]. However, in order to secure the encrypted data, all the vulnerabilities to the encrypted data need to be identified.

2. BRIEF HISTORY AND BACKGROUND

Cryptography theory was stared in the early 1970s, but the concept of the public key cryptography came out during the time of 1976 after the publication of Whitfield Diffie and Martin Hellman’s paper "New Directions in Cryptography" [3] [4]. The public key concept became popular after the advent of the RSA algorithm that came out during 1978 through a renowned publication "A Method for Obtaining Digital Signatures and Public Key Cryptosystems".

RSA algorithm was presented by a group of a security researchers, Ronald Rivest, Adi Shamir, and Leonard Adleman. The term RSA was derived from the names of the three developers of this algorithm. Till now, RSA is most widely used as a public key cryptographic algorithm. After that, ElGamal and Elliptic Curve Cryptography came out with more security features compared to RSA. However, modern cryptography essentially began during the Second World War [5].

3. PUBLIC KEY CRYPTOGRAPHY ARCHITECTURE

Public key cryptography architecture depends on the following key steps as depicted in Figure 1.

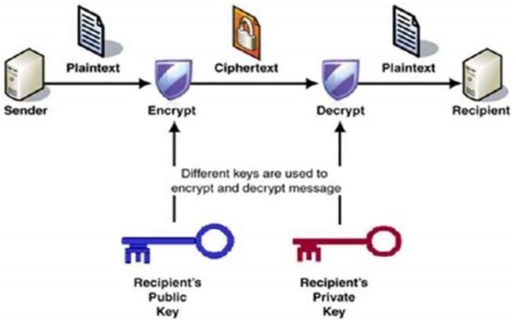

Figure 1 Process of encryption and decryption [6].

- The receiver will create the public key and private key to use in the encryption process.
- The private key will be created form the public key, and both keys will be mathematically related, but they will not be identical.
- The receiver will send his public key to the sender for data encryption process.
- The plain text will be converted to ciphertext using the public key of the receiver and encryption algorithm.
- The ciphertext will be transmitted to the receiver.
- Finally, the receiver will decrypt the ciphertext using his private key and the algorithm used in the encryption process.

4. VULNERABILITIES

In this section, researchers have identified and discussed the key vulnerabilities in public key cryptography.

4.1. Design of Cryptography

In order to have a secure system, all the elements in the system need to be secured including encryption, digital signature algorithm, one-way hash function and encryption key. If there is a weakness present in any element of the encryption process, the security of the data will be compromised [7].

4.2. Randomness in Key Generation

The key to the security of the cryptography is the randomness of the prime numbers used in the key generation process. The used prime numbers should have sufficient randomness in order to make it unpredictable to find. If the number is generated in low computing hardware and weak software (algorithm), there is a high probability that the generated random number will be weak to be used in the key creation process. It is challenging to design a perfect system to generate random numbers. A random number generator system may significantly work excellent for one purpose while it is not appropriate for other purposes [8]. The existence of the backdoor is brought about by a fundamental lack of true randomness. As a result, there is a significant weakness in the security of the algorithm used in the encryption process [9].

4.3. Man-in-the-Middle Attack

The originality of the data for the receiver cannot be guaranteed, as there is a possibility that an attacker can intercept and decrypt data from incoming communication and re-encrypt the data before the receiver receives it. Here the attacker will appear to the sender as a receiver, and for the receiver, the attacker will act as a sender in the communication channel. The attacker will provide his public key to the sender pretending that he is the person that the sender is communicating, enabling sensitive and essential data getting visible to an unauthorized person. If the sender does not ensure that the receivers public key belongs to the right person from an authentic source or protocol, man-in-the-middle attack is possible in public key cryptography [10]. The process is illustrated in Figure 2.

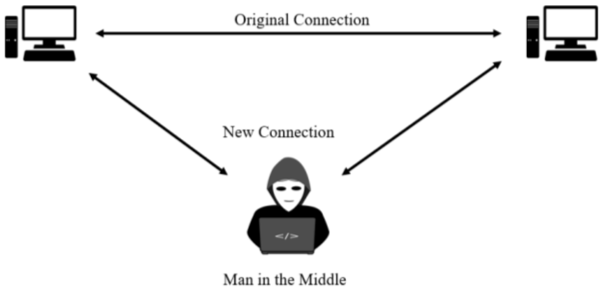

Figure 2 Man-in-the-Middle Attack.

4.4. Time Spent on the Process ("Timing Attack")

Some tools can determine the length of the key according to the time incurred in the encryption/decryption process. If such type of malware is injected to the private key holder's system, it will be easy to find the time that the receiver spends on decrypting the data; finally, it can be used to predict the private key. This type of attack was hit during 1995, enabling to determine RSA private key by measuring the time frame that the cryptographic process took. Hackers already have been successful in this type of attack in smart cards, security tokens and other electronic equipment [11].

4.5. Leave Plain Text after Encryption

In order to secure data in the encryption process, an application takes a backup of the data to some location in the disk. After the encryption process is over, the application accidentally may leave the backup data on the disk. In this case, the strength of encryption will not benefit the user as the backed-up data is available to the attackers [12].

4.6. Length of the Key

The overall strength of the key depends on the number of bits in the key. According to [13], in the past decade, researchers have successfully found a way to factorise the keys from 512-bit keys to 1024-bit keys. However, the drawback of using a lengthy key like 2014-bit is that it will require enormous computation power for the encryption and decryption process and will be a massive challenge in exchanging data between the sender and the receiver.

4.7. Memory Leak

In the computer systems, information stored in a RAM remains until the system is shut down or restored. The possibility of the generated private key to be alive in the RAM is high. This lures the attacker who has good knowledge in accessing the data in the RAM. In this case, the attacker might succeed in obtaining the private key left by the user after the key generation. Once the attacker gets the private key of the user (receiver of the data), he/she will easily be able to decrypt the data and misuse it for any malicious purpose [14].

4.8. Lifetime of the Key

There will be a high risk when the user uses the same key pair in many different encryption processes. If the same key is used for a more extended period, it will be easy for the attacker to crack the key. Moreover, the key must be destroyed, once it has been expired. When the attacker gets the user's private key, the user will lose all the data at once if one key is used to encrypt all the data [15] [16].

4.9. Storage Security

Private key of the user needs to be stored in a particular key management device. If the key is stored with the same location as of the data, the data will be insecure [17]. In most cases, private key should be stored using offline storage, and it should only be online when it is required. In addition to that, if the key need to be moved to some other system, it should be transferred with sufficient protection [18]. If the key is manually managed on a paper or spreadsheet, there is a high vulnerability that a hacker may find the key.

4.10. Growth of Quantum Computers

Within the current technologies, it is practically impossible to determine a private key from a public key which has more than 1024-bits. However, the Growth of Quantum Computers will result in a significant disaster to current technologies in public key cryptography [19]. Quantum computers will have very high-speed calculation power compared to traditional computers, enabling to determine the private key using a public key, within much less time [20]. While at present these types of computers are not available the prediction is that these machines will arrive within a decade.

4.11. Certificate Authority Issues

Currently, there is no central authority to issue the certificate in the public key infrastructure, so the possibility of issuing a fake certificate is one of the main vulnerabilities [21]. Certificate authorities exist in many countries, but the trustworthiness of these authorities are not clear at all [22]. If they wish to provide a certificate on behalf of any computer or user, it is possible. For political and other reasons, these types of activities have already done by some certificate authorities.

4.12. Ransomware

In the year 2000, a first ransomware attack was hit in Russia, and then it started to grow with new technologies. During the time 2016, it became a global problem for the whole IT industry. According to a survey conducted by [23], more than 56% of organizations have suffered ransomware attack during the past 12 months. Considering the growth of ransomware, researchers are trying to find a more convenient way to provide encryption to the data.

5. CONCLUSION

Public key cryptography has provided the highest level of security for the sensitive data to transmit between the sender and the receiver. The public key cryptography has evolved immensely over a period of time. New techniques and new algorithms are developing almost every year, but the strength and usefulness of this cryptography technique are not faded. With the rapid change in technology, the end user devices are frequently, leading to increase in the number of vulnerabilities. These vulnerabilities can be handled by using new techniques and new solutions. These new techniques will increase the sophisticated level of the algorithm and the keys and will result in better security for users.

REFERENCES

[1] P. Wei and Y. Zheng, "On the Construction of Public Key Encryption with Sender Recovery," International Journal of Foundations of Computer Science, vol. 26, no. 1, pp. 1-31, 2015.

[2] S. Nagaraj, Dr.G.S.V.P.Raju and V.Srinadth, "Data Encryption and Authentication Using Public Key Approach," Bhubaneswar, 2015.

[3] I. A. Jasmin, D. Roshidi and A. Mazida, "Analysis Review on Public Key Cryptography Algorithms," Indonesian Journal of Electrical Engineering and Computer Science, vol. 12, no. 2, pp. 447-454, 2018.

[4] E. Bresson, O. Chevassut, O. Pereira and D. Pointcheval, "Two Formal Views of Authenticated Group Die-Hellman Key Exchange," ACM CCS 01, 2001.

[5] J. Stapleton, "A Concise History of Public Key Infrastructure," Vienna, 2012.

[6] Tutorialspoint.com, "Public Key Encryption," Tutorialspoint, 2019. [Online]. Available: https://www.tutorialspoint.com/cryptography/public_key_encryption.htm. [Accessed 18 April 2019].

[7] S. K. Gil , "Asymmetric Public Key Cryptography by Using Logic-based Optical Processing," Journal of the Optical Society of Korea, vol. 20, no. 1, pp. 55-63, 2016.

[8] D. Lazar, "Why does cryptographic software fail?: a case study and open problems," Beijing, 2014.

[9] L. Kocarev, M. Sterjev, A. Fekete and G. Vattay, "Public-key encryption with chaos," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 14, no. 4, pp. 1078-1082, 2004.

[10] Ayushi, "A Symmetric Key Cryptographic Algorithm," International Journal of Computer Application, vol. 1, no. 15, pp. 1-4, 2010.

[11] J. Darshana, F. Jayani, H. Ranil and R. Roshan, "Remote Cache Timing Attack on Advanced Encryption Standard and countermeasures," in 2010 Fifth International Conference on Information and Automation for Sustainability, Colombo, 2010.

[12] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," Maryland, 1990.

[13] E. S. Alashwali, "Cryptographic Vulnerabilities in Real-Life Web Servers," Jeddah, 2013.

[14] G. Le, L. Jingqiang, L. Bo, J. Jiwu and W. Jing, "Protecting Private Keys against Memory Disclosure Attacks using HardwareTransactional Memory," in 2015 IEEE Symposium on Security and Privacy, San Jose, California, 2015.

[15] A. Chris, "Exploring the Lifecycle of a Cryptographic Key," www.cryptomathic.com, 19 March 2018. [Online]. Available: https://www.cryptomathic.com/news-events/blog/exploring-the-lifecycle-of-a-cryptographic-key-. [Accessed 11 June 2019].

[16] R. A. Liliya, K. A. Evgeny, B. O. Igor and V. S. Stanislav, "Increasing the Lifetime of Symmetric Keys for the GCM Mode by Internal Re-keying," IACR Cryptology ePrint Archive 2017, 2017.

[17] G. Vairaprakash, S. Kannan and T. Maria Mahajan, "Cryptographic Tree and Its Key Management for Securing Outsourced Data in the Cloud," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 5, pp. 255-259, 2017.

[18] S. Rob, "Cryptographic Key Management - the Risks and Mitigation," www.cryptomathic.com, 21 May 2018. [Online]. Available: https://www.cryptomathic.com/news-events/blog/cryptographic-key-management-the-risks-and-mitigations. [Accessed 11 June 2019].

[19] J. B. William and W. Alan, "Will quantum computers be the end of public key encryption?," Journal of Cyber Security Technology, 2016.

[20] M. Vasileios, V. Kamer, D. Z. Mateusz and J. Audun, "The Impact of Quantum Computing on PresentCryptography," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, pp. 1-10, 2018.

[21] M. A. Specter, "The Economics of Cryptographic Trust: Understanding Certificate Authorities," Massachusetts Institute of Technology, 2010.

[22] E. Carl and S. Bruce, "Ten risks of PKI: What you're not being told about Public Key Infrastructure," Computer Security Journal , 2000.

[23] Sentinelone, "SentinelOne: Global Ransomware Study 2018," Sentinelone, California, 2018.

[24] Prabu, S., Lakshmanan, M. and Mohammed, V.N., 2019. A multimodal authentication for biometric recognition system using intelligent hybrid fusion techniques. Journal of medical systems, 43(8), pp.1-9.

[25] Prabu, S., Velan, B., Jayasudha, F.V., Visu, P. and Janarthanan, K., 2020. Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study.

International Journal of Pervasive Computing and Communications.

[26] Parameshachari, B.D., Panduranga, H.T. and liberata Ullo, S., 2020, September. Analysis and computation of encryption technique to enhance security of medical images. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012028). IOP Publishing.

[27] Parameshachari, B.D. and Panduranga, H.T., 2021. Secure Transfer of Images Using Pixel-Level and Bit-Level Permutation Based on Knight Tour Path Scan Pattern and Henon Map. In Cognitive Informatics and Soft Computing (pp. 271-283). Springer, Singapore.

[28] Kowsalya, T., Babu, R.G., Parameshachari, B.D., Nayyar, A. and Mehmood, R.M., 2021. Low Area PRESENT Cryptography in FPGA Using TRNG-PRNG Key Generation. CMC-COMPUTERS MATERIALS & CONTINUA, 68(2), pp.1447-1465.

[29] Shahriar, M.R., Al Sunny, S.N., Liu, X., Leu, M.C., Hu, L. and Nguyen, N.T., 2018, June. MTComm based virtualization and integration of physical machine operations with digital-twins in cyber-physical manufacturing cloud. In 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 46-51). IEEE.

[30] Seyhan, K., Nguyen, T.N., Akleylek, S., Cengiz, K. and Islam, S.H., 2021. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. Journal of Information Security and Applications, 58, p.102788.

[31] Nguyen, T., Liu, B.H., Nguyen, N., Dumba, B. and Chou, J.T., 2021. Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks. IEEE Transactions on Power Delivery.

[32] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, "Secure Artificial Intelligence of Things for Implicit Group Recommendations", IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.

[33] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, F. A. Khan, "Securing Critical Infrastructures: Deep Learning-based Threat Detection in the IIoT", IEEE Communications Magazine, 2021.

[34] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin and G. Srivastava, "An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things," IEEE Journal of Biomedical and Health Informatics, 2021, doi: 10.1109/JBHI.2021.3075995.

[35] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things", ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.