A Review of Cyber Security Threats in Internet of Things

[1]Jeeva Jose, [2]Vijo Mathew

[1]Associate Professor, [2]General Manager
[1]Department of Computer Applications,
[1]BPC College, Piravom, Kerala, India

Abstract: Internet of Things is the integration of cyber systems and physical systems. All the security attacks expected in the cyber system will affect the Internet of Things also. Cyber security or digital security in the Internet of Things at various levels are ensured by cryptography. Cryptology involves cryptography and cryptanalysis. Cipher is the component that makes cryptography and cryptanalysis operational. Crypto system functions to ensure security and privacy of communication. These systems itself have the possibilities of various cyber-attacks. Various types of identified crypto system attacks in Internet of Things are reviewed in this paper.

Index Terms: Cryptology, Cipher, Security, Cryptosystem, Internet of Things, Cyber-attacks

I. INTRODUCTION

Security has become a major area for reliable operation of information system. Security in information system is the defense of digital information and information technology assets against internal or external, malicious and accidental threats. This defense includes detection, prevention and correction to threats through the use of security policies, software tools and information technology services. Information system is an indispensable component of Internet of Things (IoT) and a detailed review of security related to IoT will support the development of reliable and secure systems of future. IoT is the interconnection of devices which can be uniquely addressed and identified with an Internet Protocol (IP) address. With the IoT, devices can be connected to the Internet, sense, gather, receive and send data and communicate with each other and applications through IP technologies, platforms and connectivity solutions. IoT security [1] is the act of securing IoT devices and the networks they are connected to. All hardware, software and connectivity need to be secure for IoT to work effectively. Without proper security in IoT [2] [3], any connected object can be hacked. Once hackers gain control, they can take the device's functionality and steal the user's digital data. IoT privacy is the special consideration required to protect the information of individuals from exposure in the IoT environment, in which almost any physical or logical entity or device can be given a unique identifier and the ability to communicate autonomously over the Internet or similar network. IoT security [4] refers to protection against the unauthorized access to the device, network, server, cloud, actuator etc.

II. CRYPTOLOGY

Cryptology is the science concerned with data communication and storage in secure as well as in secret form. Cryptology can be divided into two branches cryptography [5] and cryptanalysis as shown in Fig. 1.

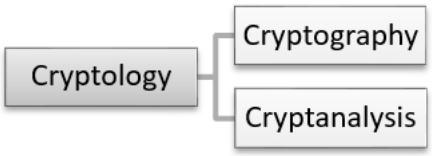

Fig. 1 Classification of Cryptology

A. Cryptography

Cryptography [6] is the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption.

B. Cryptanalysis

The process of conversion of cipher text to plain text this is known as decryption. Cryptanalysis [7] is the decryption and analysis of codes, ciphers or encrypted text. In cryptology, a cipher [8] is an algorithm for performing encryption or decryption with a series of well-defined steps that can be followed as a procedure. It is also known as encipherment. Encipher or encode is the process of converting information into cipher or code. Ciphers are also known as encryption algorithms which are systems for encrypting and decrypting data. A cipher converts the original plaintext into cipher text using a key.

III. CRYPTOSYSTEM

A cryptosystem [9] is a pair of algorithms that take a key and convert plaintext to cipher text and back. Cryptosystems use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices such as smartphones, and applications. A cipher suite uses one algorithm for encryption, another algorithm for message authentication, and another for key exchange. This process, embedded in protocols and written in software that runs on operating systems and networked computer systems, involves public and private key generation for data encryption or decryption, digital signing and verification for message authentication, and key exchange. The cryptosystem is also called cipher system. The various components of a basic cryptosystem are plain text, encryption algorithm [10], cipher text [11], decryption algorithm [12], encryption key [13] and decryption key as shown in Fig. 2.

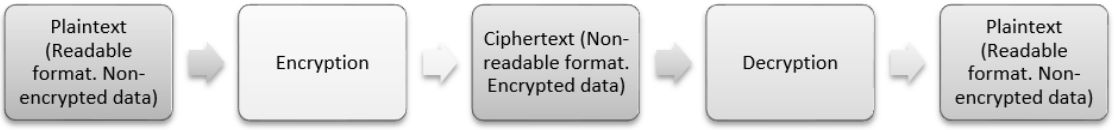

Fig. 2 Cryptosystem Process

Plaintext is what we want to protect which is the input to an encryption algorithm. It is the data to be protected during transmission. Encryption algorithm is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text. Cipher text is the unreadable output of an encryption algorithm. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel. This is also called cryptogram. Decryption algorithm is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it. Encryption key is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text. Decryption key is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext. For a given cryptosystem, a collection of all possible decryption keys is called a key space. An interceptor (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the cipher text and may know the decryption algorithm.

IV. CRYPTOSYSTEM ATTACKS

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the cipher text. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain. Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised. Based on the methodology used, attacks on cryptosystems are categorized as in Fig. 3.

Fig. 3 Types of Cryptosystem Attacks

Cipher Text Only Attack

In cipher text only attacks (COA) [14] method, the attacker has access to a set of cipher text(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of cipher text. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against cipher text-only attacks.

Known Plain Text Attack

In Known Plaintext Attack (KPA) [15] method, the attacker knows the plaintext for some parts of the cipher text. The task is to decrypt the rest of the cipher text using this information. This may be done by determining the key or via some other method. The best example of this attack is linear cryptanalysis against block ciphers.

Chosen Plain Text Attack

In Chosen Plaintext Attack (CPA) [16] method, the attacker has the text of his choice encrypted. So he has the cipher text-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks. The chosen cipher text attacks are as below.

Dictionary Attack

Dictionary attack [17] has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of cipher texts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the cipher text, he refers the dictionary to find the corresponding plaintext.

Brute Force Attack

In Brute Force Attack (BFA) [18] method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is 2^8 = 256. The attacker knows the cipher text and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long. Botnets are commonly used to carry out distributed denial of service (DDoS) attacks against target servers and various types of brute force attacks.

Password Spraying Attack

Password spraying attack [19] is also known as brute force attack. Here the attacker takes an approach that's basically the opposite of the simple technique of brute force attack. A password spraying attack involves an attacker using a targeted list of common secrets (passwords) while guessing a large list of potential usernames. Basically, they "spray" the pre-determined list of passwords while rotating through their massive list of usernames to see what sticks.

Birthday Attack

Birthday attack [20] is a variant of brute-force technique. It exploits the mathematics behind the birthday problem in probability theory. The probability that a person does not have the same birthday as another person is 364 divided by 365. There are 365 days in a year and 364 days are not a person's birthday. This means that any two people have 99.726027 percent chance of not matching birthdays or 0.28% of matching birthdays. Utilizing this theory, password can be assumed with high probability and can launch the cyber-attack.

Credential Stuffing Attack

As the name implies, a credential stuffing attack [21] involves a cybercriminal repeatedly "stuffing" known credentials into various websites' login form fields. This process involves testing known credentials (ie., those that have been stolen or otherwise compromised) on multiple websites. The attacker will eventually get one or more of the target websites where someone has an account that uses those credentials.

Man In The Middle Attack

The targets of Man In The Middle Attack (MITM) [22] attack are mostly public key cryptosystems where key exchange is involved before communication takes place. User wants to communicate to web application, hence requests public key of B. An attacker intercepts this request and sends his public key instead. Thus, whatever user sends to web application, the attacker is able to read. In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to web application. The attacker sends his public key as user's public key so that web application takes it as if it is taking it from user.

Side Channel Attack

Side Channel Attack (SCA) [23] is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem. The different types of side channel attacks and their counter measures are provided in Table 1.

Table 1 Side Channel Attacks

Side Channel Attack Types		Explanation	Counter Measures
Timing Attack [24]		Analyze the time taken by the device in different computations	Constant time techniques, Injection noise, Determinism, Partitioning time & hardware, Auditing
Electromagnetic Attack [25]		Analyze electromagnetic field of the device to obtain secret information	Circuit redesign, Electromagnetic shielding, Creating secure zone
Fault Analysis Attack [26]		Analyze faulty outputs to get confidential information	Restart the process again on getting faulty output
Power Analysis Attack [27]	Simple Power Analysis	Analyze the power traces on the inputs given	Hiding, Masking
	Differential Power Analysis	Involves statistical analysis of large number of power traces	Hiding, Blinding, Masking, Noise insertion, Temporal de synchronization and algorithmic measures

Timing Attack

They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is be possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.

Electromagnetic Attack

Electromagnetic attacks are side-channel attacks which operates by sensing electromagnetic radiation emitted from a device and analyzing that signal. An example of this is analyzing the electromagnetic radiations from an ATM or POS machine while the customer key-in the PIN. The measures to counter these types of attack is to design the hardware to keep the electromagnetic radiations within the enclosure of the equipment.

Fault Analysis Attack

Fault analysis attack is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults to unexpected environmental conditions of cryptographic implementations, to reveal their internal states. In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information. A fault attack is an attack on a physical electronic device (e.g., smartcard, HSM, USB token) which consists in stressing the device by an external mean (e.g., voltage, light) in order to generates errors in such a way that these errors lead to a security failure of the system (key recovery, ePurse balance increase etc.). This is also known as Differential Fault Analysis attack (DFA).

Power Analysis Attack

These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations. Power analysis attacks allow the extraction of secret information from smart cards. Smart cards are used in many applications including banking, mobile communications, pay TV, and electronic signatures. In all these applications, the security of the smart cards is of crucial importance.

V. CONCLUSION

Cryptology that is formed by combination of cryptography and cryptoanalysis is explained in this paper. Cryptology, its importance and relationship with the security of IoT are reviewed in this paper. Various cryptosystem types and the attacks are also studied in this paper. The cryptosystem process is analyzed and various crypto system attacks related to IoT are identified. These are organized in a structured manner and presented with suggested counter measures for development.

REFERENCES

1. M. A. Iqbal, O. G. Olaleye and M. A. Bayoumi, "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches", Global Journal of Computer Science and Technology: ENetwork, Web & Security, vol. 16, 2016.
2. M.U. Farooq, M. Waseem, A. Khairi and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT) ", International Journal of Computer Applications, vol. 111, 2015, pp. 1-6.
3. F. Ali, M. S. Khan and Hassan Akhtar, "Security Review in Internet of Things", Internet of Things and Cloud Computing, vol. 7, 1019, pp.80-87.
4. I. Ali, S. Sabir and Z. Ullah, Internet of Things Security, Device Authentication and Access Control: A Review International Journal of Computer Science and Information Security (IJCSIS), vol. 14, 2016, pp. 456-465.
5. M. H. Rajyaguru, "CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, vol. 2, 2012, pp. 329-332.
6. S. Boonkrong, "Introduction to to Cryptography. In: Authentication and Access Control.", Apress, Berkeley, CA, 2021,
7. V. Nachef, J. Patarin and E. Volte, "Introduction to Cryptanalysis and Generic Attacks", Springer, Cham, 2017, pp. 57-64.
8. S. K. Pasupuleti and D. Varma, "Lightweight ciphertext-policy attribute-based encryption scheme for data privacy and security in cloud-assisted IoT", Advances in Ubiquitous Sensing Applications for Healthcare, 2020, pp. 97-114.
9. Q. Kester, "A Hybrid Cryptosystem Based on VigenèreCipher and Columnar Transposition Cipher", International Journal of Advanced Technology & Engineering Research, vol.3, 2013, pp. 141-147.
10. N. A. Sharma and M. Farik, "A Performance Test on Symmetric Encryption Algorithms - RC2 Vs Rijndael", International Journal of Scientific & Technology Research", vol. 6, 2017, pp. 292-294.
11. A.P. Madushani and P.G.R.S. Ranasinghe, "A symmetric and a transposition cipher using the Euler's totient function", Ceylon Journal of Science, vol. 48, 2019, pp. 327-330.
12. N. S. Noor, D. A. Hammood, A. A. Naji and Javaan Chahl, "A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication", Computers, vol. 11, 2022, pp.1-16.
13. T. Virtue and J. Rainey, "Privacy and Security in Healthcare", HCISPP Study Guide, 2015, pp. 61-89.
14. M. Naor and M. Yung, "Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks" In Proceedings of the twenty-second annual ACM symposium on Theory of computing, 1990, pp. 427-437.
15. E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys", Journal of Cryptology", vol. 7, 1994, pp. 229-246.
16. I. N. Sarbini, L. F. Koo, T. J. Wong, F. H. Naning and P. H. Yiu, "An Analysis for Chosen Plaintext Attack In Elliptic Curve Cryptosystem Based On Second Order Lucas Sequence", International Journal of Scientific & Technology Research, vol. 8, 2019, pp. 1193-1196.
17. E. Conrad, S. Misenar and J. Feldman, "Domain 5: Identity and Access Management (Controlling Access and Managing Identity)", CISSP Study Guide, Third Ed. 2016, pp. 293-327.
18. K. T. Dave, "Brute-force Attack "Seeking but Distressing", International Journal of Innovations in Engineering and Technology (IJIET), vol. 2, 2013, pp. 75-78.
19. F. Chen, D. Luo, T. Xiang, P. Chen, J. Fan and H. Truong, "IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-Oriented Applications", ACM Computing Surveys, vol. 1, 2021, pp. 1-35
20. M. R. K. Soltanian and Iraj S. Amiri, "Theoretical and Experimental Methods for Defending Against DDoS Attacks", Elsevier, 2016.
21. M. F. K. Sial, "Security Issues in Internet of Things: A Comprehensive Review", American Scientific Research Journal for Engineering, Technology, and Sciences, vol. 53, pp 207-214.
22. J.McGowan, J. S.Bardin and J. McDonald, "SAN Security", Computer and Information Security Handbook (Third Edition), Morgan Kaufmann, 2013, pp. 165-187.
23. D. Schepers, A. Ranganathan and M. Vanhoef, "Practical Side-Channel Attacks against WPA-TKIP", In Proceedings of AsiaCCS '19, 2019, pp. 415-426.
24. Q. Ge, Y. Yarom, D. Cock and G. Heiser, "A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware", Journal of Cryptographic Engineering, vol.8, 2019, pp.1-27.
25. M. Randolph and W. Dieh, "Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman", Cryptography, vol. 4, 2020, pp. 1-33
26. E.Jeevalatha and.S.S. Murugan, "Evolution of AES, Blowfish and Two fish Encryption Algorithm", International Journal of Scientific & Engineering Research, vol. 9, 2018, pp. 115-118
27. H. Houssain, M. Badra, T. F. Al-Somani, "Power Analysis Attacks on ECC: A Major Security Threat", International Journal of Advanced Computer Science and Applications, vol. 3, 2012, pp. 90-96.