Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P.14037-14043 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

A Review On Study Of Cyber Security And Cryptography

Dr. Mohammad Nasiruddin [1], Alfiya Farheen[2] , Ruhina Quazi[3]

[1] Associate Professor,Department of Electronics & Telecommunication Engineering,
Anjuman College of Engineering and Technology, Nagpur
[2] MTech Computer Science & Engineering,Dayanand Sagar University, Bengaluru.
[3] Assistant Professor,Department of Electronics & Telecommunication Engineering,
Anjuman College of Engineering and Technology, Nagpur

.**How to cite this article:** Mohammad Nasiruddin, Alfiya Farheen, Ruhina Quazi (2024) A Review On Study Of Cyber Security And Cryptography. *Library Progress International,* 44(3), 14037-14043.

ABSTRACT

Ethical hacking helps to fix different types of vulnerabilities and also it has different fundamentals to teach social media users that prevents from unauthorized access and frauds. Cyber-crimes are increasing day by day from ordinary messages, professionally written fraud mails to whaling an organizations data. Crimes that take place on the network by unauthorized user is far beyond than we think if it's a professional hacker, so basically, in this case we need more strong algorithms and techniques for encryption& decryption because exchange of some confidential payloads needs more security and chances of threats may increase or decrease, depending on the platform too. In this study of ethical hacking, we'll be looking into different frauds and types of methodology that can be taken against it moreover, there exist different encryption techniques and algorithms that helps to prevent unauthorized hacking and safe exchanges of payload.

Key Words: Information technology ,Cyber-attacks Cyber security Emerging trends Key management.

INTRODUCTION

Cyber crimes are the problems that everyone come across to and that leads them to learn ethical hacking.

It is ethical until an organization is using it for their own system check and searching its weak points, testings and investigations. Unethical or unauthorized interruption takes place when data of particular person or an organization is stolen in a wrong way and used for an illegal work. Unethical hacking not only profits the hacker but also leads the victim into a big problem and loss, loosing all their personal details, confidential information and it can also result in leak of payloads that should not be shared.

Ethical hacking not only aware us about the threats and frauds but also provide measures that should be taken against it. It allows many organizations to check their security systems and set-up higher standards for their confidential payloads. Moreover, in business ethical hacking plays a vital role for that particular organization to test and setup higher standards, if possible, as many clients would be setting up bonds and trust relations with it!

Network security mechanisms

Security services are related with the security mechanism. First simply listing the mechanism that are included in network security are: Encipherment, data integrity, digital signature, authentication exchange, traffic padding, Routing Control, Notarization and Access channel.

Encipherment is used to provide confidentiality by hiding or covering the data. Basically, two techniques are used here that is -cryptography and another is -Steganography.

Data integrity consist of appending the data with the check value that is created from the data itself. We consider check value as the code that should be same while sending and receiving the data because any minor change in the check value represents alteration of the payload.

Digital signature it is used for electronically signing and verifying the signatures. Private and public key is generated and public key is shared by the sender to the receiver for verification.

Authentication exchange here the sender and receiver handshakes and ensures that the secret information should be taken place among them, it is done with the help of TCP/IP handshaking before sharing the secret information. Traffic padding malicious actor also attempts to do traffic analysis so bogus data is added to the data traffic.

Routing control to prevent eavesdropping of a particular route, router between sender and receiver are continuously changed.

Notarization a trusted third party used for communication between the sender and receiver, it also keeps record of communication to prevent later denial.

Access control it assures access rights of the authorized user, it can be achieved by applying passwords, firewall or just by adding PIN to the data.

II. LITERATURE REVIEW

Cyber-attacks fall into a broader context than what is traditionally called information operations. Information operations integrated use of the main capabilities of electronic warfare ,psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities and to penetration, stop, destroy or hijack human decisions and It is one of the decision-making processes of national institutions . Fig. 1 describes the anatomy of a cyber-attack. From the USNM Strategy for cyberspace operations, computer network operation is composed of the attack, defense, and utilization enabling The latter is different from network attacks and network defense, because this type of operation focuses more on collection and analyzing information than interrupting networks, and may itself be the prelude to an attack These operations can be carried out of disseminating information and propaganda purposes

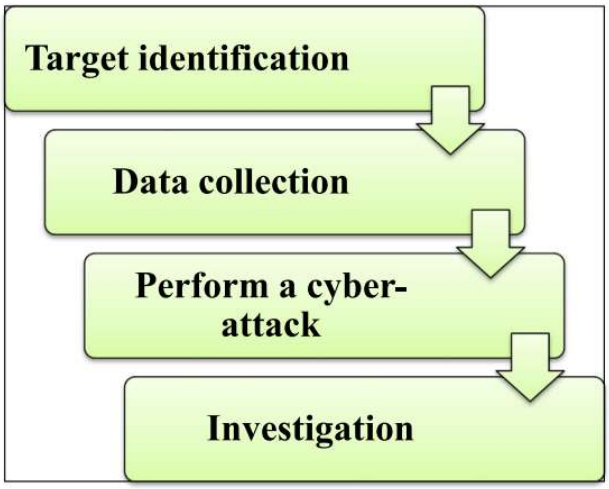

Fig.1. Anatomy of acyber-attack.

. Cyber-attacks exist within a wider framework than what is conventionally referred to as information operations. These operations involve a coordinated approach that combines key aspects of electronic warfare, psychological tactics, computer network strategies, military deception, and security measures, alongside special support capabilities. The aim is to infiltrate, disrupt, dismantle, or manipulate human decision-making processes, which are crucial to the decision-making functions of national organizations **(Hart et al., 2020). Figure 1**

illustrates the components involved in a cyber-attack. According to the USNM Strategy for cyberspace operations, computer network operations encompass attack, defense, and enabling utilization (Ma et al., 2021).

The latter differs from network attacks and defenses, as this type of operation prioritizes the collection and analysis of information rather than disrupting networks, and may in fact serve as a precursor to an attack (Alghamdie, 2021). These operations can also be employed for the purposes of information dissemination and propaganda (Thomson, 2015). Operations enabling computer network exploitation may aim to steal critical data from computers. In this regard, tools like Trap Sniffers and Doors are useful for cyber espionage (Liu et al., 2021). Trap Doors allow an external user to access software at any moment without the knowledge of the computer's owner. Sniffers are utilized to capture usernames and passwords (Karbasi and Farhadi, 2021). Table 1 outlines the fundamental definitions and concepts related to cyberspace. The repercussions of cyber warfare may include (Khan et al., 2020; Furnell and Shah, 2020; Mehrpooya et al., 2021):

Encryption serves as a robust method for safeguarding sensitive and private information against threats posed by outsiders and criminals while also obscuring unauthorized activities from law enforcement. As computing power increases and security methods evolve, cryptographic algorithms require ongoing enhancement to maintain their effectiveness and prevent vulnerabilities (Zou et al., 2020). It is essential to recognize that a general distinction exists between cyber-crime, cyber-warfare, and cyber-attacks. Figure 2 and Table 2 illustrate the differences between these concepts, clarifying their unique characteristics

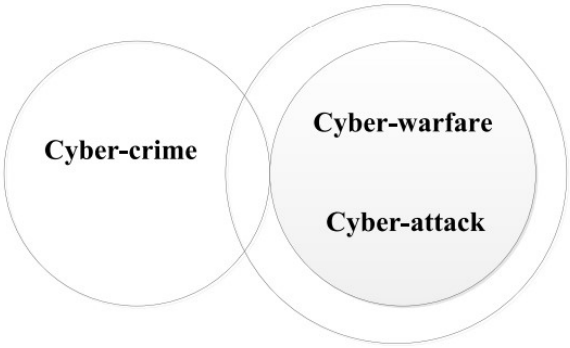

Fig. 2. Distinction between cyber-crime, cyber-warfare, and cyber-attack.

Table 2

Distinction between cyber-crime, cyber-attacks, and cyber-warfare (Zhang, 2017; Dash et al., 2021)

Type of cyber action	Nature and characteristics
Cyber-crime .	Cyber actions taken only by non-governmental attackers.
Cyber-crime	The cyber action is carried out by a computer system and is merely in violation of criminal law.
Cyber-attack and cyber-warfare	The purpose of a cyber-attack is to destroy and disrupt the operation of a computer network.
cyber-warfare	The effects of a cyber-attack are the same as an armed attack or the cyber act took place in the context of an attack.

Cyber-attack and cyber-warfare	The attack must have political or security purposes

The current characteristics of cyberspace indicate that there is no technological capacity to reliably attribute activities to specific individuals, groups, or organizations. The primary threats within cyberspace include: external threats, internal threats, threats within supply chains of products and services, and risks arising from the inadequate operational abilities of local forces (Al-Ghamdi, 2021). Foreign intelligence agencies exploit cyber tools for their intelligence and espionage operations. Numerous incidents globally have reported the misuse and destruction of national information infrastructures, which include computer systems, internet networks, and the processors and controllers integrated into critical industries. Additionally, there are groups that target cyber systems for financial gain, and the frequency of these attacks is on the rise (Beechey et al., 2021). Furthermore, some hackers breach networks to voice their opinions, leveraging minimal expertise and skills by downloading necessary software and protocols online for use against various sites.

Another group, known as Hacktivists, conducts attacks on widely-used websites or email services for political reasons. These actions typically increase the load on email servers, while infiltrating websites allows them to broadcast their political messages (Solomon, 2017). Moreover, internal discontented individuals within organizations pose a significant threat, as they often do not require advanced knowledge of cyberattacks; their familiarity with the target systems often grants them unrestricted access to compromise systems or misappropriate sensitive information.

Terrorists represent an additional source of risk, aiming to incapacitate, damage, or maliciously exploit critical infrastructure with the intent to threaten national security, inflict significant financial damage, erode the economy, and diminish public trust (Saxena and Gayathri, 2021). Fig. 3 illustrates the various sources of cyber threats.

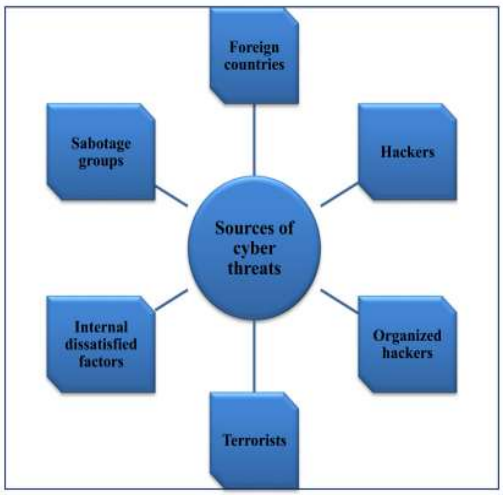

Fig. 3. Sources of cyber threats

III. METHODS OF ENCRYPTION

The message that is in original readable format is known as “plain text” and when it is converted to unreadable format then that coded message is called as “cipher text” and the process is called as encryption or encipherment, converting the cipher text to the plain text is called as decryption or deciphering [4].

Classic techniques in symmetric cipher:

3.1 Substitution techniques

Caesar cipher: it is the simplest substitution cipher by Julius Caesar. Here we normally replace each letter of the alphabet with the alphabet letter that is standing three places further to it. We can understand it with details below,
Plain text**:**

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

Cipher text: wrapped using plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n
d	e	f	g	h	i	j	k	l	m	n	o	p	q

o	p	q	r	s	t	u	v	w	x	y	z
r	s	t	u	v	w	x	y	z	a	b	c

C: cipher text whereas, p: plain text
k: the range between 1 to 25
E: encipherment or encryption
C ⇨ E(k, p)= (p+ k) mod 26
D: decipherment or decryption
D ⇨ D(k, C)= (C- k) mod 26
Plain text: Meet me tomorrow
Cipher text: phhw ph wrpruurz

Monoalphabetic cipher: here relative frequency of letter is determined and compared to a standard frequency distribution in English, P has the highest as 13.33 and R as lowest 0.00 however C, K, L N too comes in same frequency as R do. Such an approach is known mono alphabetic substitution in cipher because in this, our single cipher alphabet is used to make per simple message, as we have used it in a tool for example is mentioned below[5]:

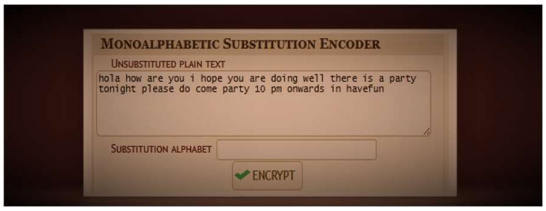

Fig -4: Encoding plain text

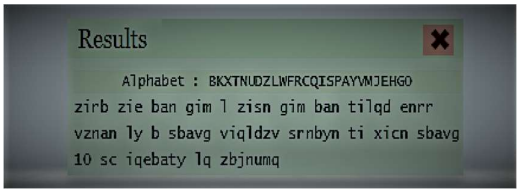

Fig -5: Result of encryption

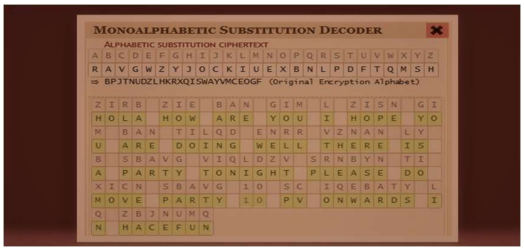

Fig -6: Decoded

Playfair cipher: it is based on 5x5 matrix, using the keywords. Originally, it somewhat looks like this,

A	**B**	**C**	**D**	**E**
F	**G**	**H**	**I/J**	**K**
L	**M**	**N**	**O**	**P**
Q	**R**	**S**	**T**	**U**
V	**W**	**X**	**Y**	**Z**

Now, when we use and plaintext it starts occupying space in this matrix from letter A, words should not be repeated repeating words are filled once in the matrix and filler is used instead like in BALLON, we use BA LX LO ON.
Plain text : meet me tomorrow

IV.CONCLUSION

Cyberspace and its associated technologies have become one of the most powerful forces in the third millennium. Its distinct characteristics—such as low entry barriers, anonymity, vulnerability, and asymmetry—have contributed to a diffusion of power. While traditionally, power was concentrated among governments, other entities like private corporations, terrorist organizations, criminal groups, and individuals have emerged as influential actors. Despite this shift, governments still maintain a pivotal role within this evolving landscape. Notably, this trend does not necessarily weaken national security.

The implications of this shift can be viewed through several key perspectives. First, the concept of security has broadened. National security is no longer limited to military concerns or the distinction between internal and external borders. Today, the decline in citizens' quality of life is seen as a critical national security threat. Second, cyber threats have transcended geographical boundaries. Unlike traditional military threats confined to specific regions, cyber threats can emerge from anywhere, making them more difficult to detect and counter. Third, the vulnerabilities linked to cyber threats are vast and diverse. These irregular, multifaceted threats, which often target sensitive networks and infrastructure, have the potential to cause significant harm.

REFERENCES

[1] .. Hart, S., et al., 2020. Riskio: A serious game for cyber security awareness and education. Comput. Secur. 95, 101827

[2] . Ma, L., et al., 2021. Security control for two-time-scale cyber physical systems with multiple transmission channels under DoS attacks: The input-to-state stability.

[3] Alghamdie, M.I., 2021. A novel study of preventing the cyber security threats. Mater. Today: Proc

[4] .. Karbasi, A., Farhadi, A., 2021. A cyber–physical system for building automation and control based on a distributed MPC with an efficient method for communication

[5] Khan, S.K., et al., 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions

[6] Furnell, S., Shah, J.N., 2020. Home working and cyber security – an outbreak of unpreparedness?

[7] Mehrpooya, M., et al., 2021. Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device.

[8] Alibasic, A., et al., 2016. Cybersecurity for smart cities: A brief review. In: Nternational Workshop on Data Analytics for Renewable Energy Integration.

[9] ji, Z., et al., 2021. Harmonizing safety and security risk analysis and prevention in cyber–physical systems. Process Saf. Environ. Prot. 148, 1279–1291. Judge

[10] Sun, C.-C., Hahn, A., Liu, C.-C., 2018. Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56

[11] Zou, T., et al., 2020. Smart grids cyber–physical security: Parameter correction model against unbalanced false data injection attacks. Electr. Power Syst. Res. 187, 106490

[12] . Saxena, R., Gayathri, E., 2021. Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. Mater. Today: Proc..

[13] Varga, S., Brynielsson, J., Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. Comput. Secur. 105, 102239

[14] Zhao, J., et al., 2020. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Comput. Secur. 95, 101867. Z