



Threat Will be zero - by cyber security

Mr.S. MOHAN¹, Dr.T. KALAIKUMARAN², Mrs V. RADHA³
 Department of Computer Science,
 V.S.B College of Engineering and Technical Campus,
 Coimbatore, Tamilnadu, India-642109

Abstract:

This paper discusses about zero-day threat, software attack etc..., also it is called zero trust security. Security told that in cryptography which one vital role of cyber security and this network security. Another one part of the cyber security. Which separately to do the networks in commonly either network or software and hardware security are given by the cyber society. Zero-day trust means does not then it's no threat. If refer to concept of zero trust security model. this model assumes no user or device is increasingly trust worthy and required strictly verification and authorised for every access request.it proactive approach to minimise potential damage from including zero-day exploits.

Key words: threat, plain text, cipher text, Grambling, protocol.

Introduction:

Network security is important because of keep sensitive data safe from cyber-attack on the ensure the network and usable and trustworthy successful network security. Strategy multiple security solution to protect and organisation from malware and cyber attack. Network composed to network interconnected devices such as computer, server, wireless network. Measuring of devices potential attack. Network security in world. Network security involved the use of a variety of software and hardware tools on the or software as a Services .security more important as a network grow more complex and rely more important and data to conduct business. Security method must evolve is threat action create new attack method on there increasing complex methods.

Important of network security

Prevent from cyber criminal from the gaining access to valuable data and sensitive information. when hacker get hold data they can take unity of problem that include data theft , stolen assets and reputable

1. Operation risk
2. financial rick for compressed potential identify information
3. Financial risk for comparison intellectual property
4. Regularity issues

How to work :

This is combination of hardware and software tools on awarded between the fact of network.

Network security software tool

- Access control
- Anti-virus
- Application security
- Cloud security
- Data loss process

- Email security
- Firewall
- Intrusion detection system
- Mobile data security
- Multi factor authentication
- Network system
- Sand box
- Security information and even management
- Virus prevent network
- Web security
- Zero trust network access.

Cryptography:

It is secure of communication technique only send reader receipt of the manage to read content is unknown as cryptography. The word Krypto's. Comes from Greek. Which means hidden days closely linked to encryption where is process of Grambling plain tax and cipher tax and then back again where it is receiver.

Encryption and decryption

Encryption the playing text known words but convert in to the cipher tax unknown unknown word. Cipher tax on the other hand. Encryption and decryption plain tax message must come pone of the cryptography when transmitting electronics data's symmetry or secret key approaches is most basic way. Encryption using secret key and encoder message and secret key are the delivery to receiver for decoding.

Example :

Plain text

CSE -

Cipher text

AUG-

C=A

S=U

E=G

Types of cryptography :

- Hashing
- Symmetric
- Asymmetric
- Key exchange algorithm.

Application of cryptography :

The form authentication means to cryptocurrency. cryptography some of the most application of cryptography listed .Computer password. Security when use login . Digital currency to protect transaction in prevent fraud digital currency like Bitcoin as also used cryptography.

Secure web browsing. Online browser security is provided by shoe cryptography where man in the middle assets.

- Public key screen socket layer .
- Transport layer security TCl protocol.
- Electronic signature

Digital equal and level written signature and are you sign document.

Authentication accessing bank book, login computer and screen ,network.

Crypto currency like Bitcoin and Ethereum to protect transaction.

End to end internal encryption.

Two way communication like video communication instant message and email .

Relations :

Cryptography is focus on encryption and ensuring only authorised user can access it . on the other hand cyber security is broader field that protect in the device network and data form malicious activities. Cryptography is way to protect information by timing in to secret code when you send message only same are which the right key can uncoded it's meaning. this helps keep your data. like password and credit card user safe from thieves.

Collaboration and sharing information.

Cyber security is shared responsibility joining force with the cyber groups expert or government organization can help stay ahead of global cyber threat. this involve sharing information about known vulnerability and attack with others which can help everyone defend against common threat.

Network security :

Protect themselves from variety of threats such as cyber attack data breaches and unauthorised access for digital world safe .as online network growth that tool is verify who were talking to keep our data private and ensuring message are not changed along with way.

Cyber threat and attack.:

A thread is a potential danger vulnerability that could be exploited by cyber-criminal on the other have and attack is to active exploitation of the threat to real world common.

like data breaches or system disturbance. Threat is realm information security is pressure of persistent hazard to information integrity. this import shape of harm computer viruses and security else.

An attack.:

Is actual act of exploding the information security systems weakness.

Active attack.:

Attempt to change the system resources or influence the operation.

Passive attack.:

Attempt understand or retrieve sustainable data from the system without influencing the system resources.

Role of cyber security:

Cyber-attack become increasingly common targeting business, Government and industrial alike according to the reports by cyber security. Cyber security involved safeguarding computer system networks data from theft danger unauthorised access it includes range of measure like firewalls antivirus software encryption technique. Define against cyber threat. The primary goal is to maintain integrity and availability of information while reading risk associated with different type of cyber-attack.

Conclusion:

Cyber security has become an important part of on daily lives it essential to understand how they benefit.

- 1.Network security
- 2.Application security
- 3.cloud security
- 4.information security
- 5 .end point security
- 6.mobile security
- 7.identity and access management
- 8.internet of things security
- 9.Data security
- 10.operational security.

The cyber security is umbrella term for network security and cryptography .which is the different part of the work. Its not related to the cyber security but is related to internal. cyber security broad field of this field .this nearly zero day and zero trust of the security. so as we assume that. Threat will be zero by cyber security.

References:

1. M. Arora A systematic literature review of machine learning estimation approaches in scrum projects. In Balas P., Bhoi V., and Chae and A., editors, *Mallick. Cognitive Informatics and Soft Computing. Advances in Intelligent Systems and Computing*, vol 1040. Singapore: Spring
2. F. Aydoan and A. Varol. Cyber Threats Targeting Android Mobile phones. in *Digital Forensic investigations and Security (ISDFS 2017), Tirgu Mures*, 2017. N. Varol, F. Aydoan, and A. Varol, "Cyber Threats Targeting Android Cellular phones," in *Computer Forensics Security (IDFS 2017), Tirgu Mures*, 2017.
3. J. Callas. The way forward for confidentiality. *Information Systems Protection*, 16 (1): 15–22, 2007.
4. K. Chahapara and S. Bhadwal. Secure cloud sharing using cryptog-raphy. In *Nirma Universitat International Conference on Engineers (NUICONE)*. Ahmedabad, 2013.
5. A. Diro, H. Reda, and N. Chilamkurti. zaman, n., nam, y., lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. in *IEEE Access*, 8 : 9045934, 2020.
6. N. Gupta, P. Gupta, D. Goyal, and M. Garg. *Computer science and technology advances*, vol. 10, no. 5. p, 770 (2017): 763–770,
7. O. O. Khalifa, M. R. Hussain, S. Khan, and M. S. Shebani "communication systems cryptography," by O. O. Khalifa, M. R. Hussain, S. Khan, and M. S. Shebani, in *Rf/ Microwave Conference*, 2004, 2004.
8. J. L. Harris "cryptographic protocols selective survey," *data communication*, vol. 85. p, 25(1986): 3–65, 1986.
9. B. Preneel. *Spriger Understanding Cryptographic techniques: A Text-book for Scholars and Trainees*, by B. Preneel, Springer, London, 2010.
10. V. S. Dhaka, S. V. Meena, G. Rani,, A survey of deep convolutional neural networks applied for prediction of plant leaf diseases. *Sensors*, 21: 14, 2021.

International Research Journal
IJNRD
 Research Through Innovation