Emerging Trends in Cyber Crime and Cyber Security

S.K.Kharkate

Lecturer, Department of Computer Engineering M.B.Manalwar,Lecturer,Department of Electonics and Telecommunication Government Polytechnic Gadchiroli, Maharahtra, India

Abstract: *With growing reach of internet, today various organizations are using internet for storing, processing, transmitting their sensitive information and data. Destruction, theft, denial of such information leads to huge financial losses to organizations. In today's world cyber security is not only important for organizations but also for ordinary people who uses internet. This paper describes various types of cyber attacks and recent instances of these attacks. It also describes emerging technologies in the field of cyber security. This paper addresses the need of strengthening and securing the space.*

Keywords *: cyber security, cyber attacks, cyber crime, malware, blockchain, context aware security, vdn*

I. Introduction

Today internet is spreading rapidly, it has become integral part of our life. For mailing, entertainment, shopping, chatting, education etc. we use internet through computers and smartphones. Various organizations like business, universities, governments, military, financial institutions, research centers, health institutes store and process very large amount of confidential information. This data is often communicated over computer networks. When the world is moving towards digitization, study of cyber crime and cyber security has become today's need. Cybercrime, or computer oriented crime, is crime that involves a computer and a network. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)". Cyber security or computer security or IT security is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

Cyber Attacks :-

Malware attack :-

Malware is any software intentionally designed to cause damage to a computer, server or computer network.[1] [1],Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.[2][2]it can be viruses, worms, Trojan horse, spyware, adware, scareware.
Ex:-Kovter, Emotet, ZeuS/Zbot ,CoinMiner, Mirai, Redyms
Ransomewareattacks :-

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.[1][2][3][4][3][4]
Ex:-WannaCry, NotPetya, Locky, Nemucod, Jaff, jigsaw.

Derive-by Download:-

Derive by Downloads means downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically or Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.[1][5]

Out-of date Unpatched Software:-

Unpatched and unauthorized software leaves a backdoor for hackers which can put business in serious security risks. Over the last decade software vulnerabilities have increased drastically. Most of the security breach

Occurs exploiting unpatched operating system, network equipment, Internet-related software, Including add-ins, browser helper objects etc.
Phishing attacks:-

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.[1][2][6][7] The word is a neologism created as a homophone of *fishing* due to the similarity of using a baitin an attempt to catch a victim. Phishing is typically carried out by email spoofing[4][8] or instant messaging.
Ex:- Phishing attack on Qatar (2017),IRS W2 Tax Season Spear-Phishing Scam

Denial of Service(DOS):-
In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended usersby temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1][9]
Ex:- Buffer Overflow

Man in the middle attack:-
In cryptography and computer security, a **man-in-the-middle attack** (**MITM**) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of man-in-the-middle attacks is active eavesdropping.

Eavesdropping is secretly or stealthily listening to the private conversation or communications of others without their consent.
Ex:- Digital Certificates for the 'things'

Malvertising attacks:-
Malvertising is the use of online advertising to spread malware.[1][10] It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
Ex;- Browser based cryptocurrency miners, Malicious Ads target adult-themed sites, WordPress Vulnerability Leads to Malvertising, Malvertising distributes ransomware. Equifax stained by malicious redirects

Rogue Software:-
Rogue security software is a form of malicious software and Internet fraud that misleads users into believing there is a virus on their computer, and manipulates them into paying money for a fake malware removal tool (that actually introduces malware to the computer).

SQL Injection:-
SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[1][11] SQL injection must exploit a security vulnerability in an application's software, SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.
Cross-site Scripting:-

Cross-site scripting (**XSS**) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy

Recent Technologies in Cyber Security:-
Context-aware security:-
Context-aware security (or adaptive security) empowers organizations to base real-time security decisions on the total risk associated with multiple pieces of security information.[12]
Contrary to the ring-of-keys approach, context-aware security is like a wellinformed, completely ethical guard accompanying each user and unlocking the door only when appropriate. As an additional measure of security,

the guard may ask the user for a second form of ID if he does not recognize the user or if knows that the user rarely enters by that door.

The security analytics engine

One context-aware model implements a security analytics engine (SAE) that returns a risk score based on multiple factors

1. Browser used
2. Location pattern
3. Specific location
4. Time
5. Blacklist
6. Whitelist

Virtual Dispersive Networking:-

Dispersive's "virtual dispersive networking" is a unique approach to cybersecurity that takes a page out of now-traditional military radio spread-spectrum security approaches, where radios rotate frequencies randomly or split up communications traffic into multiple streams, so that only the receiving radio can reassemble them properly. With Dispersive, however, the Internet (or any network) is now the underlying communications platform.

Dispersive Technologies can not only split up a single message into several different simultaneous parts, but it can encrypt each component message separately and even route them over different protocols following independent paths. "We put routing on servers, computers, even mobile phones," explains Twitchell. No longer must organizations rely upon firewalls to ensure message security, as now any device anywhere on the Internet can serve as a "deflect," Dispersive's term for one of these impromptu routing devices.

Dispersive's innovation doesn't stop with simply splitting up the messages. The data also "roll" dynamically to optimum paths – both randomizing the paths the messages take while simultaneously taking into account congestion or other network issues. The end result: "They're making an attacker work a lot harder," according to Rosenberg. "The bad guy would have to figure out the paths, the hops, and what order" to put the messages in – a daunting task. There are also many opportunities for Dispersive's technology in the cloud computing world. Not only can the cloud easily host the deflects at the core of their approach, but cloud environments can leverage Dispersive to establish secure interactions between clouds or between on-premise data centers and clouds. These hybrid cloud scenarios often depend upon VPNs, which tend to be flaky and slow. With Dispersive Technologies, VPNs become a thing of the past – improving the security, performance, and manageability of hybrid clouds as well as virtual private clouds.

Furthermore, Dispersive's spread spectrum technology also serves to bypass traditional network bottlenecks and allow organizations to combine multiple network routes for blisteringly fast data transfer speeds. The result is an approach to solving Big Data's data gravity problem: moving large data sets over the Internet can be agonizingly slow. With Dispersive, the fact that moving large data sets can now be both fast as well as secure is an added bonus. Dispersive Technologies blocks Man-in-the-Middle (MiM) attacks, a common arrow in the hacker's quiver.

Active Cyber Defence:-

active cyber defense (**ACD**) means acting in anticipation to oppose an attack involving computers and networks. Proactive cyber defense will most often require additional cybersecurityfrom internet service providers. [13]

Some of the reasons for a proactive defense strategy are about cost and choice. Making choices after an attack are difficult and costly. Proactive defense is key to mitigating operational risk.

Active Cyber defence techniques include - Rescue missions to recover assets, White-hat ransomware, Coordinated sanctions, indictments, and trade remedies, Botnet takedowns, Intelligence gathering in deep web/dark web, Beacons (information), Beacons (notification), Hunting, Denial and deception, Tarpits, sandboxes, and honeypots, Information sharing

Block Chain Technology :-

blockchain,[1][2][3][14][15] originally **block chain**,[4][5] is a growing list of records, called *blocks*, which are linked using cryptography.[1][6] Blockchains which are readable by the public are widely used by cryptocurrencies. Each block contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data (generally represented as a merkle tree root hash). By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".[8] For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.[1][23] This allows the participants to verify and audit transactions inexpensively.[24] A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests.[25] The result is a robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. Blockchains have been described as a value-exchange protocol.[13] This blockchain-based exchange of value can be completed quicker, safer and cheaper than with traditional systems.[26][16] A blockchain can assign title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Hardware Authentication :-

A hardware authenticator is a type of device that is used to verify the identity of an individual on a particular system. It is implemented in multifactor or two-factor authentication processes, whereby a user must have a valid hardware authenticator to be granted access to a system or network. A hardware authenticator is also known as an authentication token. A hardware authenticator consists of any hardware device that acts a security token or identity verifier, including a USB stick, smart card or embedded circuit within an external device. In a typical scenario, an individual plugs a hardware authenticator into a system which first validates the hardware authenticator and then requests another identity or password.[17]

SAML and the Cloud :-

his technology encompasses encryption with SAML and intrusion detection technologies to regain control of corporate traffic. This way the information in the cloud is corralled. The alert system signals the organization of issues like unexpected logins, suspicious activities, etc.[18]

II. Conclusion

In this paper we have described various types of cyber attacks and recent cybercrimes world wide. We have also described emerging technologies in the field of cyber security. We also mentioned how frequency of cyber crimesis increasing day by day. Through this paper we stressed the importance of securing and strengthening of digital information and infrastructure.

Future Work :-

In future we are looking to address security issues in emerging technologies like cloud computing, Internet of Things, deep learning, Artificial intelligence. We are working to study recent trends in cyber crimes to provide efficient solutions to detect and prevent them and secure cyber space.

References

[1]. "Defining Malware: FAQ". technet.microsoft.com. Retrieved 10 September 2009.

[2]. "An Undirected Attack Against Critical Infrastructure" (PDF). United States Computer Emergency Readiness Team(Us-cert.gov). Retrieved 28 September 2014.

[3]. Young, A.; M. Yung (1996). *Cryptovirology: extortion-based security threats and countermeasures*. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.

[4]. Jack Schofield (28 July 2016). "How can I remove a ransomware infection?". *The Guardian*. Retrieved 28 July 2016.

[5]. "Exploit on Amnesty pages tricks AV software". *The H online*. Heinz Heise. 20 April 2011. Retrieved 8 January 2011.

[6]. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark &Stavroulakis, Peter. *Handbook of Information and Communication Security*. Springer. ISBN 978-3-642-04117-4.

[7]. Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.

[8]. "Landing another blow against email phishing (Google Online Security Blog)". Retrieved June 21, 2012.

[9]. "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.

[10]. William Salusky (2007-12-06). "Malvertising". SANS ISC. Retrieved 2010-08-05.

[11]. Microsoft. "SQL Injection". Archived from the original on August 2, 2013. Retrieved August 4,2013

[12]. https://www.oneidentity.com/context-aware-security/

[13]. https://www.heritage.org/sites/default/files/2017-05/BG3188.pdf

[14]. "Blockchains: The great chain of being sure about things". *The Economist*.

[15]. Morris, David Z. (15 May 2016). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". *Fortune*. Archived from the original on 21 May 2016. Retrieved 23 May 2016.

[16]. Tucci, Michele (29 November 2015). "Can blockchain help the cards and payments industry?". *Tech in Asia*. Archived from the original on 19 November 2016. Retrieved 16 November 2016.

[17]. https://www.techopedia.com/definition/23920/hardware-authenticator

[18]. https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field