Advancements in Cyber Attacks and Security

Yatin Kalra, Saket Upadhyay, Pushpinder Singh Patheja

***Abstract:** Succeeding the entrustment of the personal computer by Ed Roberts in 1975, the absolute first virus became known to exist in a trifling time span of six years. The adversary was called Elk Cloner. Not long before they established themselves as adverse. Forthwith, attacks become frequent by the clock at all levels possible. It is a direct indication to how important cyber security is considering the prolonging effect and enormous expansion caused by such events in recent years. Another major issue is the huge scale arrangement of gadgets with almost no security or a wide default security design susceptible to cyber-attack. Cyber security is swiftly transforming into an article of everyday usage. As attacks are becoming sophisticated, we expect gadgets like advanced mobile phones, PCs and significantly progressively computerized frameworks to be secure and the protection of the data to be fundamental.*

Our paper explores the variety of Cyber Attacks, their methodologies and core ideas with the motivations behind it, also the ways to circumvent the threats by putting lights on the ongoing and future technologies to tackle advanced threats.

***Keywords:** Malware, Phishing, Social Engineering, Cryptography, Trojan.*

I. INTRODUCTION

Cyber Attacks [1], [2], [4] can be defined as an attempt caused by a person or any team to gain the admin rights on other system without authorization, probably with malicious intent. It can range from setting a malware or spyware on any others computer or network system to attempting for destruction of the infrastructure of globe.

Cyber Security is a term that is a subset of term Information Security. It only works on protecting computer and network systems and their parts such as software, hardware and information – and digital setup from attack, unauthorized access. The Morris Worm, first virus invented in 1989, infected 6000 computers then to today, it has been consistently increasing day by day, There is no slowing down of it. As indicated by Robert Mueller, Former FBI Director – "There are just two kinds of organizations: Those that have been hacked, and those that is destined to be."

All websites, servers, accounts or setups, programs can be exploited with the help of cyber-attack [3].

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author

Yatin Kalra *, School of Computer Sciences and Engineering, Vellore Institute of Technology, Bhopal, India. Email: yatinkalra@yahoo.com

Saket Upadhyay, School of Computer Sciences and Engineering, Vellore Institute of Technology, Bhopal, India. Email: saketupadhya@gmail.com

Dr. Pushpinder Singh Patheja, School of Computer Sciences and Engineering, Vellore Institute of Technology, Bhopal, India. Email: pspatheja@gmail.com

II. MOTIVATIONS FOR CYBER CRIMES

1: To gain access to someone's personal information without prior consent.

2: To cause damage to any firm's / brand's reputation and income.

3: To harm someone Physically, Mentally or Economically (Example: One can alter the reports of Blood Group in any Hospitals which can lead to a mismatch of blood (when Doctor transfuses blood into the body) and it can lead to death.

No one either Hospital or Doctor is responsible for this death. This can be termed as Cyber Murder) [5].

III. RULES FOR CYBER SECURITY

In order to have a correct explanation regarding the Evolution of Cyber Attacks and Security, It is vitally important to draft some essential rules of cyber security. Acknowledgment of these sayings should evacuate a portion of the willful limitations that have maybe constrained the reasoning and the advancement of the cyber security network.

Rule 1: They are going to get in

The focal point of cyber security has for some time been on shielding malignant code and programmers from accessing frameworks. This center has prompted a methodology of growing defensive abilities at the edge of systems, especially passage associations with outer systems. Often there is arrange neutral ground (Demilitarized Zone) between an interior business system and the (public) Internet.

Rule 2: They are already in

While it is conceivable that the attackers have not got the control, it makes well to accept that hackers and their malware are already inside. System users who accept their system is as of now undermined are suspicious of everything that seems strange. The key component in all fruitful programmer trade-craft is the misuse of trust, so the best defenders don't believe whatever appears to be even somewhat impossible to miss.

Rule 3: Attacker stays

Defenders must not imply gratification. Just because past attacks were detected and turned back does not imply that it the ease time. To be sure, be synchronized with all the latest definitions of cyber-attack, installing all the necessary patches and tools. Constant surveillance is necessary, no matter how well-protected network seems to be.

Rule 4: It is going to get even worst It is safe to state that as innovation is inventive and effectiveness is expanded through mechanization and man-made reasoning strategies along these lines, as well, will enemies utilize similar advancements to build the productivity of attacks.

The present attackers regularly profoundly energetic and resourced and as long as it keeps on being beneficial, attackers will go to incredible length to create forefront innovation to break into systems.

IV. INFORMATION SECURITY COMPONENTS

To completely comprehend the significance of data security, it is important to audit the components of the information system. An Information System is considerably more than PC equipment. It is the whole arrangement of programming, equipment, information, individuals, and systems important to utilize data as an asset inside and outside the association. To shield the information and its related frameworks from threat, apparatuses, for example, approach, awareness, training, instruction, and innovation is vital.

Verifying the Components: When considering the security of Information System segments, it is critical to comprehend the idea of the PC as the subject of attack rather than the PC as the object of an attack. When a PC is the subject of an attack, it is utilized as a functioning instrument to lead the attack. At the point when a PC is the object of an attack, it is the entity being attacked.

Security and Access Balancing: When thinking about data security, understand that it is impossible to get flawless security. Security isn't an outright; it is a procedure, not an objective. Security ought to be considered harmony among insurance and availability. To accomplish balance the degree of security must permit sensible access, yet ensure against dangers. Where data is excluded from revelation, it infers that safety efforts will apply in full. Information security in the present venture is a "well informed sense of confirmation that the data dangers and controls are in balance."

In 2002, Donn Parker proposed an elective model for the classic CIA triad that he called the six components of information. The components are confidentiality, integrity, authenticity, availability, utility and possession

Confidentiality: Confidentiality is the camouflage of information or assets. Confidentiality implies making sure that data is just observed by individuals who have the right to see it. Keeping data secret from unauthorized access is likely the most widely recognized perspective of information security

Integrity: Integrity alludes to the reliability of information or resources, and it is normally stated as far as preventing improper or unapproved change.

Availability: Availability alludes to the capacity to utilize the information or asset wanted. Accessibility implies having access to your data when you need it. In other words, it implies ensuring no individual or occasion is capable to block genuine or auspicious access to data.

Table 1: Different kinds of Security Attributes with Attack methods and Technology used/can be used for Security Purposes [6]

Security Attributes	Attack Methods	Technology for Security
Confidentiality	Password Attacks Unauthorized Access Tail Gaiting	Deterrent Methods Password Policy Guarding
Integrity	Viruses, Worm and Code Injection	Antivirus Scanner Code Monitoring
Availability	DOS DDOS BOTS	DOS Mitigation Network Analyzers

V. TYPES OF CYBER ATTACKS

5.1 Hardware Attacks

5.1.1Introduction to Hardware Attack

Computer Hardware can be defined as physical, corporeal components, such as Motherboard, Cabinet, Keyboard, Mouse, Data Storage Systems, Graphics and Sound Card, Central Processing Unit, Monitor. On the other hand, Software is a set of instructions that can be run with the help of Hardware. Firmware is intermediate between Hardware and Software. Only Software can direct Hardware to execute any command.

Hardware Vulnerabilities can be defined as weakness that can be exploited in a computer system that is used by the attacker to attack hardware through remote or physical access to system.

Any undesirable code can be executed on Computer System due to Hardware Vulnerabilities [7].

5.1.2: Hardware Vulnerabilities

5.1.2.1: PCs with conventional BIOS System

The PC which is based on the Older BIOS System (before October 2012) cannot run the Secure Boot System. It was a feature of UEFI, added in Windows 8 and now appeared in earlier versions as well as Windows Server.

It helps in preventing the control of malware at the time of the boot process.

5.1.2.2 Computers without pre-boot authentication (PBA) or a Trusted Platform Module (TPM)

PBA makes sure the prevention of loading in the operating system with the unavailability of USER AUTHENTICATION such as USERNAME & PASSWORD. PBA actually kicks in play after BIOS starts and before Operating System boots. This feature has been in place over several years and has been replaced by Microsoft BitLocker using TPM.

5.1.2.3 Device Drivers without self-encryption feature

It has become very vital that Device Drivers Writers and Architects must involve Threat Modelling as an integral part of Drivers. Security must be a fundamental design for any Driver. One can assume that if one is using a Driver in the computer, somewhere, sometime or someone has will try to use that Drivers to compromise the Security of Computer Systems [8].

5.1.2.4. Vulnerabilities with Instruction Set

Christopher Domas [9] in his paper talks about the presence of a backdoor in the VIA C3 processor. The paper likewise talks about the system of its revelation. The shrouded center likewise alluded to as profoundly implanted center is actuated by a model-specific register (MSR) which adds new guidance set to the existing x86 guidance set. This instruction set can be utilized to execute code legitimately on the shrouded center bypassing the security highlights ofthe framework to pick up root access. MSR allows to run code at kernel level or at ring 0 [38].

5.1.3 Security Solutions for Hardware Attacks

- Identifying the possible vulnerable points which can be helpful for an Attacker
- Analysis type of Attack that can be embedded to that points
- Ensuring that the driver is fully ready to be safe against that Identified attacks by pen testing it.

5.2 Software Attacks

5.2.1 Introduction to Software Attacks

Computer Software can be defined as a collection of Data, Programs and Instructions that tell the Operating System and Hardware how to perform the desired task. This is on the other hand of the System Hardware, by which the computer actually built-in and performs different tasks. PC equipment and programming require one another and neither can be practically utilized without anyone else [10].

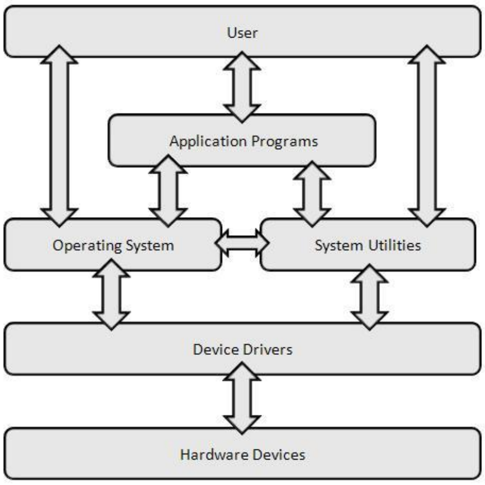

Fig 1: Enhanced Interaction Layered System [11]

Nowadays, Computer Users frequently download different software for various purposes such as social media, music, etc [37]. They don’t care about the malignity of the software; they are just concerned about their own purpose/motive. Because of these reasons, the number of infected Computers/Systems is increasing every moment.

5.2.2 Software Vulnerabilities

Vulnerabilities are the loopholes by which attackers get into the systems. It involves Bugs in software. They are basically error made during coding and building the software [12].

5.2.2.1) Backdoor

A Backdoor is a way to get to a PC framework or encoded information that sidesteps the framework's standard security instruments. An engineer may make indirect access so an application or working framework can be gotten to for investigating or different purposes [13].

5.2.3 Software Attacks

5.2.3.1 Malware

It is a kind of system application (Software) that is intentionally designed to make damage to the targeted server, computer network and victim. It does damage after its implantation in some way to the target’s computer [14].

5.2.3.1.1 Virus

A Computer Virus is intentionally designed to spread from one system host to another having ability to replicate the same. In other words, it is a type of malicious code or program to alter the permissions assigned by user to get unauthorized access to server or client’s information and data. It can spread through any forms such as text messages, internet files, social media links and any downloaded media [15].

5.2.3.1.1.1) Symptoms of having VIRUS

a) Frequent Pop up of Windows
b) Unusually slow computer performance
c) Unknown program starts at the time of start-up

5.2.3.1.1.2) Way to safeguard computer from Virus

a) Use trusted antivirus software
b) Scan Email Attachments always
c) Avoid using/clicking any random advertisements

5.2.3.1.2 Ransom wares

It is a type of Malware Attack which threatens to use the victim’s data or block access to it, and allowing it in cost of desired ransom [16].

5.2.3.1.3 Trojan Horse

Trojan is a sort of malware that gives unapproved access to touchy communications of the clients, for example, buy exchanges, premium rate calls, and so on out of sight of the unfortunate casualty's gadget. Along these lines, the objective of this sort of malevolent applications is transmitting under the front of genuine applications or documents. For instance, in view of the most recent report discharged by Tencent security scientists, they have revealed another financial Trojan which is named "Swearing".

5.2.4 Security Solution for Software Attacks

- Signature Based Techniques

This is a sort of malware investigation systems which works dependent on distinguishing explicit examples of known malware, which is called signature. As it were, mark based procedures produce an interesting mark for a known malware, which can apply to distinguish the malware by looking at a recently recognized signature with the database of marks that have been recently constructed.

- Heuristics Analysis Techniques

Heuristic investigation is a technique signed by numerous PC antivirus programs intended to identify beforehand obscure PC virus, just as new variations of virus as of now in "nature". Heuristic investigation is a specialist-based examination that decides the helplessness of a framework towards specific danger/chance utilizing different choice guidelines or gauging techniques. Multicriteria investigation (MCA) is one of the methods for gauging. This technique varies from factual examination, which puts together itself with respect to the accessible information/measurements.

- Machine Learning Techniques

This kind of malware detection techniques utilizes machine-learning algorithms on the benign malware samples to generate the learning patterns, which can exploit for detecting both unpredicted (or new malware) and known malware [17].

5.3 Network Attacks

5.3.1 Introduction to Network

Network can be outlined as the collection of computers, servers, mainframes, network enabled devices, peripherals or any other devices which is connected to one another with the permission of sharing data. Desktop Computers, Laptops, Consoles, Firewalls, Bridges, Repeaters, Switches, Hubs, Modems, Routers, Webcams, Smartphones are some more used example of Network Devices [18].

A first-rated example of network is INTERNET, which connects about billions of people all around the globe [19].

5.3.2 Network Attacks

There is a list of numerous network cyber-attacks such as Social Engineering, Phishing, Spear Phishing, Whaling, tailgating, DoS, DDoS, Man in the middle, Buffer Overflow, ARP Poisoning, Evil Twin and many more [20]. Some of them are discussed here:

5.3.2.1) Phishing

In this attack, the target is contacted by electronic mails, messages, telephones or any other direct or in-direct mode of communication, the attacker acts like a substantial institution to attract people in giving confidential information, for example, bank details, id's and passwords. Then the information is used in accessing the important account and can lead to financial, and other kind of loss.

5.3.2.1.1 Common Features of Phishing

5.3.2.1.1.1) Sense of Urgency

A most loved strategy among cybercriminals is to request your demonstration quick on the grounds that the super arrangements are just temporarily. Some of them will even disclose to you that you have just a couple of minutes to react. At the point when you run over these sorts of messages, it's ideal to simply overlook them.

5.3.2.1.1.2) Hyperlinks

A connection may not be all it seems, by all accounts, to be. Drifting over a connection demonstrates to you the real URL where you will be coordinated after tapping on it. It could be totally extraordinary or it could be a well-known site with an incorrect spelling.

Example, www.bankofarnerica.com - the 'm' is really a 'r' and a 'n', so look cautiously.

5.3.2.2) Social Engineering

It is an art of handling the people so they/their social media accounts provide up confidential information. The type of information attacker seeks may vary in different cases, but they usually trick you into giving them your passwords or bank data, or access your PC to covertly introduce malevolent programming that will offer access to your passwords.

It is usually easier method to exploit your natural impulse to trust rather than to discover ways to hack your computer.

5.3.2.3) Evil Twin

An evil twin is a deceitful Wi-Fi passage that has all the earmarks of being genuine yet is set up to spy on remote communications. The underhanded twin is the remote LAN likeness the phishing trick.

This sort of attack might be utilized to take the passwords of clueless clients, either by observing their associations or by phishing, which includes setting up a deceitful site and drawing individuals there.

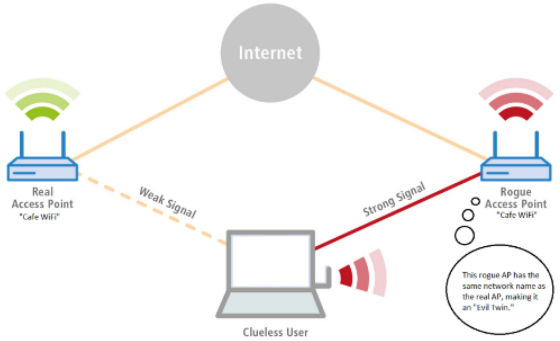

Fig 2: Evil Twin – A Network Based Attack [21]

5.3.2.4) E-Mail Bombing

Email Bombing is described by abusers over and over sending an indistinguishable email message to a specific location. Email spamming is a variation of bombing. It alludes to sending email uncountable clients. Email spamming can be aggravated if beneficiaries answer to the email, making all the first addressees get the answer. It might likewise happen guiltlessly, because of making an impression on mailing records and not understanding that the rundown detonates to a huge number of clients, or because of a mistakenly arrangement automated assistant message. Email bombarding/spamming might be joined with email caricaturing making it increasingly hard to figure out who from whom the email is originating.

On the off chance that your email framework looks moderate or email doesn't seem, by all accounts, to be sent or got, the explanation might be that your mailer is attempting to process an enormous number of messages. At the point when a lot of email are coordinated to or through a solitary site, the site may endure a refusal of administration through loss of system availability, framework accidents, or disappointment of a help due to over-burdening system associations, utilizing all accessible framework assets and filling the plate because of various postings and coming about syslog passages.

5.3.2.5) Denial-of-Service Attack

In security, a denial-of-service attack (DoS attack) is a digital attack wherein the culprit tries to make a machine or system asset inaccessible to its proposed clients by briefly or inconclusively upsetting administrations of a host associated with the Internet. Refusal of administration is regularly cultivated by flooding the focused-on machine or

Asset with unnecessary demands trying to over-burden frameworks and avoid a few or every single genuine solicitation from being satisfied [22].

5.3.2.6) Distributed Denial-of-Service Attack

A distributed denial-of-service (DDoS) is an enormous scale DoS attack where the culprit utilizes more than one extraordinary IP address, regularly from a large number of hosts contaminated with malware. A dispersed refusal of administration attack ordinarily includes more than around 3–5 hubs on various systems; less hubs may qualify as a DoS attack however isn't a DDoS attack.

Since the approaching traffic flooding the unfortunate casualty begins from various sources, it might be difficult to stop the attack essentially by utilizing entrance sifting. It likewise makes it hard to recognize authentic client traffic from attack traffic when spread over different purposes of starting point. As another option or increase of a DDoS, attacks may include the producing of IP sender addresses (IP address caricaturing) further confounding recognizing and vanquishing the attack.

The size of DDoS attacks has kept on ascending over ongoing years, by 2016 surpassing a terabit for each second. Some basic instances of DDoS attacks are Fraggle, smurf, and SYN flooding.

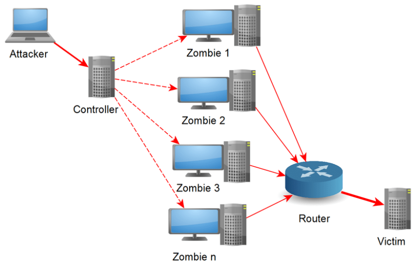

Fig 3: Distributed Denial-of-Service – A Network Based Attack [23]

5.3.3 Security Solutions for Network Based Attacks

With the rapid growth of Internet, the security component of internet has become a vital concern throughout the globe. On the other hand, various tools to penetrate the network security are now widely available in the market. The benefits of Internet Security tools include the security for encryption, authentication, and block or filter packets, etc.

5.3.3.1 Cryptographic Techniques

It can be defined as an art of making data inaccessible to any unknown user with the help of ciphers. It is a transcendent instrument for security designing today since one can see that the PC business has comprehensively utilized cryptography as a principal standard in confirmed programming headway. The essential methodology of cryptography is to encode or scramble a data message called 'plain substance' with a cryptography computation, which achieves a yield message called 'figure content or cryptogram'. At the recipient side, to change figure content into a clear design, a cryptographic key must be used for unravelling. A cryptographic key is produced using a progression of digits. If a comparable key is used for both encryption and unscrambling, it is called symmetric key. Another kind of key is an uneven key, which basically suggests the encryption key differences from the unscrambling key. Right now, solid cryptography is an extensively incredible security innovation. The solid cryptography calculation depends on the unwavering quality of numerical computations. The computation of the cryptographic key is muddled to the point that it couldn't be broken inside a brief span. Anybody, who needs to break it, should take quite a while to accomplish his objective. For whatever length of time that individuals depend on scientific intricacy, solid cryptography is as yet the most proficient instrument to defend PC security. The prompt or noteworthy contentions against this thought have not yet approached [24].

Some of the techniques are:

5.3.3.1.1 DES

Data encryption standard (DES) has been discovered defenseless against extremely ground-breaking attacks and in this manner, the notoriety of DES has been found somewhat on decay.

DES is a square figure, and encodes information in squares of size of 64 piece each, implies 64 bits of plain content goes as the contribution to DES, which produces 64 bits of figure content. A similar calculation and key are utilized for encryption and unscrambling, with minor contrasts. The key length is 56 bits

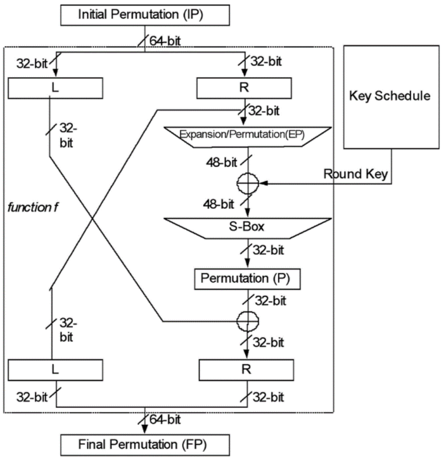

Fig 4: Block Diagram - Data encryption standard (DES) [25]

5.3.3.1.2 Base64

In software engineering, Base64 is a gathering of double to-content encoding plans that speak to paired information in an ASCII string group by making an interpretation of it into a radix-64 portrayal. The term Base64 starts from a particular MIME content exchange encoding. Each Base64 digit speaks to precisely 6 bits of information. Three 8-piece bytes (i.e., a sum of 24 bits) can accordingly be spoken to by four 6-piece Base64 digits.

Regular to all binary to text encoding plans, Base64 is intended to convey information put away in parallel organizations crosswise over channels that just dependably bolster content substance. Base64 is especially common on the World Wide Web where its uses incorporate the capacity to insert picture documents or other double resources inside literary resources, for example, HTML and CSS records.

5.3.3.2 Anti-Malware Software and Scanners

Virus, worms and Trojan ponies are on the whole instances of malevolent programming, or Malware for short. Unique alleged against Malware instruments are utilized to identify them and fix a contaminated framework. This sort of hardware goes about as an interior barrier system. The most widely recognized kind of hostile to Malware programming is infection scanners. These apparatuses regularly comprise of two diverse however related parts: a scanner (or verifier) and a disinfector.

5.3.3.3 Firewall

Firewall is a guard between your PC/Network and the web, and one of the significant hindrances to anticipate the spread of digital dangers, for example, virus and malware. Ensure that you set up your firewall gadgets appropriately or they may not be completely powerful. Peruse progressively about firewalls in server security.

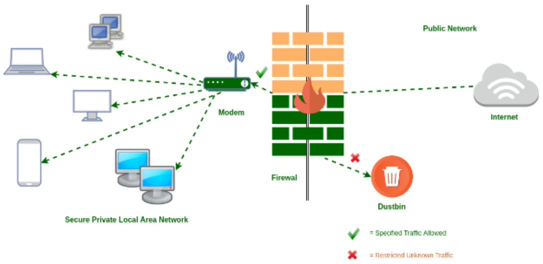
Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

Fig 4: Firewall [26]

5.3.3.3.1 Types of Firewall

5.3.3.3.1.1 Packet Filter

Packet Filter Firewall works in network layer of OSI Model. It applies a lot of on every packet and dependent on the result, chooses to either advance or dispose of the packet.

5.3.3.3.1.2 Stateful Inspection Firewall

It is otherwise called 'Dynamic Packet Filters'. It monitors the condition of dynamic associations and utilizations this data to choose which parcels to permit through it, i.e., it adjusts to the present trade of data, dissimilar to the typical bundle channels/stateless packet channels, which have hardcoded directing guidelines.

5.3.3.3.1.3 Circuit Level Gateways

Circuit Level Gateways works on session layer of OSI Model. It is the propelled variety of Application Gateway. It goes about as a virtual association between the remote host and the inward clients by making another association among itself and the remote host. It furthermore changes the source IP address in the pack and puts its own special area at the spot of source IP address of the package from end customers. Thusly, the IP address of within customers are hidden and confirmed from the outside world.

5.3.3.3.1.4 Application Layer Firewall

An Application Level Firewall is where one application-level (i.e., not bit) process is utilized to advance every session that an inner client makes to a system asset on people in general system.

Application Level Firewall's are viewed as the most secure kind of Firewall's, yet they bring about a noteworthy exhibition punishment. The punishment emerges in light of the fact that another procedure must be begun each time a client begins another session - for example by following a URL to another World-Wide Web webpage.

5.3.3.4 Intrusion Detection and Prevention System

One can utilize intrusion detectors to screen framework and abnormal organize the movement. On the off chance that a discovery framework presumes a potential security rupture, it can produce a caution, for example, an email alert, in light of the kind of action it has recognized [27].

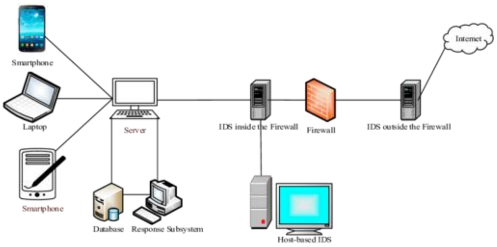

Fig 5: Intrusion Detection System [28]

5.3.3.5 Update System and Software

Updates contain vital security upgrades that help protect against known bugs and vulnerabilities. Make sure that you keep your software and devices up-to-date to avoid falling prey to criminals.

VI. VI. RECENT CYBER ATTACKS AND LEARNINGS

6.1) Cyber Attacks

6.1.1) The WannaCry ransom ware attack was a May 2017 overall cyber-attack by the WannaCry ransom ware crypto worm, which focused PCs running the Microsoft Windows working framework by encrypting information and requesting buy-off instalments in the Bitcoin cryptographic money.

It proliferated through Eternal Blue, an endeavor found by the United States National Security Agency (NSA) for more seasoned Windows frameworks. Eternal Blue was taken and spilled by a gathering called The Shadow Brokers a couple of months before the attack. While Microsoft had discharged fixes already to close the adventure, quite a bit of WannaCry's spread was from associations that had not applied these, or were utilizing more seasoned Windows frameworks that were past their finish of-life. WannaCry likewise exploited introducing indirect accesses onto tainted frameworks.

6.1.2) Red October was a cyber-espionage malware program found in October 2012 and revealed in January 2013 by Russian firm Kaspersky Lab. The malware was apparently working worldwide for as long as five years preceding disclosure, transmitting data running from strategic insider facts to individual data, including from cell phones. The essential vectors used to introduce the malware were messages containing connected reports that misused vulnerabilities in Microsoft Word and Excel. Afterward, a site page was discovered that abused a known weakness in the Java program module. Red October was named a progressed cyber-espionage crusade planned to target conciliatory, administrative and logical research associations around the world.

6.1.3) On September 7, 2017, Equifax reported some upsetting data for purchasers – a cyber-security disappointment had prompted programmers accessing the data of around 143 million individuals. As far as size, this rupture is positively huge, in spite of the fact that it's not the biggest break ever. That questionable respect goes to Yahoo's rupture a year ago. Be that as it may, as far as seriousness, the Equifax digital attack is difficult to beat [29].

6.2) Learnings

6.2.1) The threats weren't necessarily new

Attacks like WannaCry happened with Sony in 2014 and Blaster in 2003 (Ward, 2017). Firewalls and ordinary fixing can avoid the attacks, and the particular fix for the WannaCry defencelessness was discharged just about two months in front of the attack. At the point when word got out that this shortcoming existed and that it was anything but difficult to abuse, those that didn't demonstration rapidly to fix their vulnerabilities experienced the attacks.

6.2.2) Many organizations were still susceptible

As per Hackett (2017), the NotPetya digital attacks focused on organizations that neglected to fix their frameworks against the Microsoft defencelessness (SMB-1). In the event that you haven't as of now, ensure you apply Microsoft fix MS17-010 and square associations with Microsoft Windows' port 445 (Howard, 2017).

6.2.3) Payment to ransom doesn't guarantee return of files

The email administration (Posteo) immediately obstructed the email utilized for receipt of Bitcoin, cutting off any connection for further correspondence. Further, paying to ransom will motivate attackers to attack more frequently.

6.2.4) Back up your data

Even after applying patches, no firewall or hostile to infection programming is totally impeccable, so it's ideal to store significant information in another area outside of the system (Weavers, as referred to by Satran, 2017) [30].

VII. FUTURE OF CYBER SECURITY

7.1 Cyber security in Internet of Things

IoT or internet of things are becoming an integral part of human lives and soon it will be fully integrated into the system. Internet of Things gives power of internet and networking to basic items around us such as dishwasher, AC, Dustbin, Mailbox etc. but with the power of networking comes the vulnerabilities of the same. In case IoT devices

they have to be small and modular, hence in the process we need to strip down processing power to make it 'just enough' to do the job which, if we see as portability and modulation is great but with the lens of cyber security is a large step back.

As decreasing storage and processing power we also lose power to computer stronger encryption protocols and generate long cryptographic keys to encrypt the data transmitted through the network. This also results in stripping down many protocols so that it will not use a lot of resources available, at last removing some of the essential parts of it needed to ensure high security.

Some of the common attack surface available for IoT devices are Firmware, Passwords, Sniffing, and Session Jacking etc.

7.2 Artificial Intelligence and Machine Learning in Cyber Security

Cyber security is a vast field and it grows in its complexity we need to enhance our methods to detect attacks and malware and there comes the implementation of AI and ML. The ML models are trained on the data collected by scanner, IPS, IDS and research over time and then used to predict upcoming traffic or fie to check if the pattern matches or not [31].

One of the implementation of ML in Cyber security is malware detection were set of malware are collected in controlled environments and then all the features are extracted from the malware to distinguish different types and classes of the same and then fed into the neutral network, then the machine is left to learn the pattern based on the information given in the forms of vectors most of the time.

The similar vectors are passes to the models when testing for new malware and if the pattern is matched with any one of the classes then the target is declared as malware with the most votes for the specific classification received if any.

Feature engineering plays an important role in using AI or ML in any field and the same is the case with cyber security.

7.3 Genetically Detection of Malware

Malware is any software intending to disturb PC activity. It is additionally used to accumulate touchy data or access private PC frameworks. This is broadly observed as one of the significant dangers to PC frameworks these days. Generally, antagonistic to malware programming relies upon an imprint identification framework which continues refreshing from the Internet malware database and along these lines observing known malware.

As of late, a few AI strategies have been utilized for malware location, making noteworthy progress. In Artificial Intelligence, Genetic programming (GP) is a system of developing projects, beginning from a populace of unfit (generally arbitrary) programs, fit for a specific assignment by applying activities comparable to normal hereditary procedures to the number of inhabitants in programs.

It has been used to solve issues in network security.

In Cyber Attacks and Security, Malware is one of the chanciest threats over the decades. Malware Attack is one of the principle dangers in the course of recent decades. As indicated by a report discharged by an enemy of antivirus, Malware can impede the activity of PC frameworks, take delicate data or even control client's PCs. Malware attacks cause significant financial misfortune consistently. In 2006, noxious virtual products lost $ 13.3 Billion internationally [36]. In this manner, protection against malware is vital for both PC clients and endeavors. Normally, hostile to malware programming projects are regularly founded on a mark definition framework. In this, a piece series of pernicious code is put away and used to determine if the file is contaminated by coordinating measurement. Rieck et al. [32] proposed a structure for programmed examination of malware conduct utilizing AI. Countless malware tests were gathered and their practices were observed utilizing a sandbox situation. Grouping technique was utilized to recognize the classes (especially, novel) of malware with comparable conduct. Doling out obscure malware to these found classes was finished by classification. The outcomes demonstrated that this methodology was equipped for preparing the conduct of numerous malware doubles on regular routine. Tian et al. [33] extricated API call arrangements from executable while executing in a virtual situation through a computerized instrument. Mentioned API call successions are utilized as highlight vector for AI techniques accessible in the WEKA library. They utilized a dataset of 1368 malware and 456 kind-hearted files to show their work. Their outcomes demonstrated that the calculations in Weka can separate malware files from clean files with a precision of about 95% [34], [35].

VIII. RESULT

Cyber Security is perplexing in the term of rising technology. In such a situation, security measures applied for small well-characterized frameworks can't work productively. The absence of legitimate information, comprehension software and security engineering prompts vulnerabilities in security frameworks. Also, Different security measures must be consolidated to be successful against various kinds of cyber-attacks and the security of framework must be continually checked.

In this paper we aim to go through the current strategies and project achievable future strategy platform to build further research environment, improving overall defensive stance from security perspective

IX. CONCLUSION

A threat to mankind altogether being a massacre that cyber dreads are, they keep prolonging to become hideous worldwide till the day critical data and information is mobile over the internet. In the following research prospectus we ought to consider the pros and cons of security solutions for various types of Cyber Attacks and their Security Methods. Extensively tracing from the early attacks and strategies to the current use of Artificial Intelligence, Machine Learning and Genetic approach in the field. One might wonder that the level of sophistication we are developing under the stream Cyber Security will one day outreach every possible level of security hindrance but, for a matter of the fact that development is swifter in the shady side of the branch. In the near future, new security innovation will be available to improve the effectiveness of business and correspondences.

REFERENCES

1. Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. IECON Proceedings (Industrial Electronics Conference). https://doi.org/10.1109/IECON.2011.6120048
2. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. The Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2017.1476
3. Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance. https://doi.org/10.17645/pag.v6i2.1569
4. Konakalla, A., & Veeranki, B. (2013). Evolution of Security Attacks and Security Technology. *IJCSMC*.
5. Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*. https://doi.org/10.19101/ijacr.2016.623006
6. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*. https://doi.org/10.1016/j.cose.2013.04.004
7. Cage, G. W. (1986). Computer hardware. Dermatologic Clinics. https://doi.org/10.5005/jp/books/10167_2
8. Sagstetter, F., Lukasiewycz, M., Steinhors, S., Wolf, M., Bouard, A., Harris, W. R., … Chakraborty, S. (2013). Security challenges in automotive hardware/software architecture design. Proceedings -Design, Automation and Test in Europe, DATE. https://doi.org/10.7873/date.2013.102
9. Domas C. Hardware backdoors in x86 CPUs. 2018. https://www.blackhat.com/us-18/briefings/schedule/index.html#god-mode-unlocked—hardware-backdoors-in-x-cpus-10194
10. Wang, J. A., Wang, H., Guo, M., & Xia, M. (2009). Security metrics for software systems. Proceedings of the 47th Annual Southeast Regional Conference, ACM-SE 47. https://doi.org/10.1145/1566445.1566509
11. www.cs.sru.edu/~mullins/cpsc100book/module05_SoftwareAndAdmin/module05-02_softwareAndAdmin.html
12. Krsul, I. V. (2014). Software Vulnerability Analysis. Uma Ética Para Quantos? https://doi.org/10.1007/s13398-014-0173-7.2
13. Singh Kunwar, R. (2018). MALWARE ANALYSIS OF BACKDOOR CREATOR : FATRAT. International Journal of Cyber-Security and Digital Forensics. https://doi.org/10.17781/p002362
14. Zeidanloo, H. R., Tabatabaei, F., & Amoli, P. V. (2015). All About Malwares (Malicious Codes). Security and Management.
15. Furnell, S., & Ward, J. (2013). Malware. In Information Security and Ethics. https://doi.org/10.4018/978-1-59904-937-3.ch271
16. Savage, K., Coogan, P., & Lau, H. (2015). The Evolution of Ransomware. Research-Technology Management. https://doi.org/10.5437/08956308X5405012
17. Stallings, W. (2005). Cryptography and Network Security: Principles and Practices. In Cryptography and Network Security. https://doi.org/10.1007/11935070
18. Patheja, P. S., & Waoo, A. A. (2011). Challenges for Mobile Wireless Devices for Next Generation in Pervasive Computing. Soft Computing.
19. Lin, M., Chen, Q., & Yan, S. (2014). Network in network. 2nd International Conference on Learning Representations, ICLR 2014 - Conference Track Proceedings.
20. Marty, R., & Rexroad, B. (2017). Network security. In Building the Network of the Future: Getting Smarter, Faster, and More Flexible with a Software Centric Approach. https://doi.org/10.1201/9781315208787
21. www.thecybersecurityman.com/2018/08/11/pentest-edition-creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-1-setup/
22. Needham, R. M. (1993). Denial of service. 1st ACM Conference on Computer and Communications Security. https://doi.org/10.1016/b978-1-59749-549-3.00001-8 www.researchgate.net/figure/Elements-that-constitute-a-distributed-denial-of-service-attack_fig1_319901682
23. Encryption. (2002). In Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. https://doi.org/10.1201/
24. www.researchgate.net/figure/Block-diagram-of-DES-algorithm_fig1_220850878 geeksforgeeks.org/types-of-firewall-and-possible-attacks
25. Vaseer, G., Patheja, P. S., & Ghai, G. (2017). Intrusion Detection a Challenge: SNORT the savior. International Journal of Computer Trends and Technology. https://doi.org/10.14445/22312803/ijctt-v45p101
26. www.researchgate.net/figure/Intrusion-detection-system-architecture-37_fig2_315662151
27. www.en.wikipedia.org/wiki/List_of_cyberattacks
28. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and Security. https://doi.org/10.1016/j.cose.2013.04.004
29. I. H. Witten and E. Frank. Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, 2005.
30. K. Rieck, P. Trinius, C. Willems, and T. Holz. Automatic analysis of malware behavior using machine learning. Journal of Computer Security, 19(4):639668, 2011.
31. R. Islam, R. Tian, L. M. Batten, and S. Versteeg. Classification of malware based on integrated static and dynamic features. J. Network and Computer Applications, 36(2):646–656, 2013
32. F. I. L. C., E. A., and N. A.S. Analysis of machine learning techniques used in behavior-based malware detection. In 2010 Second International Conference on Advances in Computing, Control and Telecommunication Technologies (ACT), pages 201-203. IEEE, 2010
33. Landage, J., & Wankhade, M. (2013). Malware and Malware Detection Techniques: A Survey. International Journal of Engineering Research & Technology.
34. Le, T. A., Chu, T. H., Nguyen, Q. U., & Nguyen, X. H. (2015). Malware detection using genetic programming. Proceedings of the 2014 7th IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2014. https://doi.org/10.1109/CISDA.2014.7035623
35. Taleby, M., Li, Q., Rabbani, M., & Raza, A. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. International Journal of Advanced Computer Science and Applications. https://doi.org/10.14569/ijacsa.2017.081005
36. Lokhande, V. G., & Vidyarthi, D. (2019). A study of hardware architecture based attacks to bypass operating system security. Security and Privacy. https://doi.org/10.1002/spy2.81

AUTHORS PROFILE

Yatin Kalra, is currently pursuing Bachelor of Technology in Computer Science and Engineering from Vellore Institute of Technology, Bhopal. His research area interest includes OS Hardening, security analysis in cybersecurity.
Email: yatinkalra@yahoo.com

Saket Upadhyay, is currently pursuing Bachelor of Technology in Cyber Security and Digital Forensics from VIT Bhopal. His research area interest includes malware analysis, reverse engineering and machine learning in cybersecurity.
Email: saketupadhya@gmail.com

Dr. Pushpinder Singh Patheja, is currently working in Vellore Institute of Technology as an Associate Professor – Senior, School of Computing Science and Engineering (SCSE), Bhopal, India. His experience is more than 28 years in the field of teaching and research. He has published more than 50 National and International papers. He is a member of various research organisations and has a specialization in computer network, adhoc network and network security. Email: pspatheja@gmail.com