ISSN No. 0976-5697

Volume 7, No. 1, January-February 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

The Review of Terms and Concepts used to Understand Cybercrime to Safeguard Ourselves from Cybercriminals

Dr.P.B.Pathak
Assistant Professor & Head, Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded
Maharashtra, India

Abstract: All the basic concepts from Computer Networks useful for understanding the mechanisms used by cybercriminals are essential. On must study broad categories of Networks, OSI Networking Model, TCP/IP Networking Model and the functions of all their layers. Study of Network Topologies, Network Hardware Hubs, Repeaters, Bridges, Switches, Routers, Network Software, Client Server Computing, Server and Client Software is of equal importance. Several Network Protocols (TCP / IP), Internet, Internet Evolution and the Internet Architecture and Wireless Networks all these topics are the foundation for the study of Security and Security Incidents. Under topics Security and Security it comes, Security of Computers, Incidents on Computer and Computer Networks like Intrusion and Attacks. This gives an idea about crimes in cyberspace and some substantial methods of commission of crime.

Keywords: Computer Network; Threat; Vulnerability; Security; Security Incidents; Cybercrime; Preventive measures; Cybercriminal

I. Introduction

Cyberspace is as important as real space. Cyberspace is vulnerable to borderless cyber attacks. Cybercrime is growing very fast all over the world. Cybercrime is a social and legal problem. To successfully fight it people in the IT & general population must work together. Application of tactics and techniques are needed to prevent Cybercrime. Developing formal and informal responses will maximize the chances of identifying and successfully prosecuting the Cybercriminals. Cybercrime can only be stopped / reduced by joint operation and sharing. The globalization has made Cybercrime cross border and global. Networked technologies provide opportunities for criminal activities. Various reasons for the rise in Cybercrimes can be given Global reach of the Internet, Lack of Security Management and awareness, Misconception about Firewalls and Antivirus, Increasing Complexity, Software without security, availability of attack scripts, ease of carrying out attacks, Anonymity by Computers and the Internet.

Threat can be defined as any potential occurrence, malicious or not, that can have an undesirable effect on the assets and resources associated with computer systems. Threats may be Confidentiality Threat, Integrity Threat, Denial of Service (DoS) Threat. Threats can be classified as Physical or Logical Threat, Accidental or Deliberate Threat, Active or Passive Threat.

Vulnerabilities are some characteristics of computer systems that make it possible for a threat to occur. Vulnerabilities are weakness discovered in operating systems, applications and devices by hackers, security professionals and organizations. Common Vulnerabilities include Misconfigurations and Human Error, Vulnerable Operating Systems, Unsecured and Unnecessary Network Services, Unprotected files, Databases, Applications, Physical Access, Eavesdropping, Sniffing, Weak Passwords etc.

II. Cybercrime Definitions And Types

Defining Cybercrime is not easy, the difficulty lies in what crimes should be considered as Cybercrimes. The terms Cybercrime, Computer Crime, Information Technology Crime, and High-tech Crime refer to crimes committed with, via, or by computer and other electronic media. In available literature there are number of different definitions of the term Cybercrime.

“Cybercrime is the use of computers and networks used to harass victims or set them up for violent attacks, even to coordinate and carry out terrorist activities that threaten us all. Altering, damaging, deleting, or otherwise using computer data to execute a scheme to defraud; deceiving, extorting, or wrongfully controlling or obtaining money, property, or data; using computer services without permission; disrupting computer services; assisting another in unlawfully accessing a computer; or introducing contaminants into a system or network, constitutes Cybercrime.”

“Cybercrime is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.” “Cybercrime is where the computer can be a tool for crime such as theft and fraud, a channel or a location of crime such as data destruction, and an object of crime such as the theft of computer chips.”

Cybercrimes can be classified as Violent Cybercrimes and Non Violent Cybercrimes. Cybercrimes against Individual, Property, Organization and Society. Cybercrimes where Computer or Network as Target, as Tool, for Incidental Purposes. Cybercrimes against the Confidentiality, Integrity and Availability of Computer Data and Systems. Computer Related, Content Related and Copyright Related Cybercrimes. Privacy Related, Content Related, Intellectual Property Related and Economic Cybercrime.[3,4]

Cyberterrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non combatant targets. Assault by Threat is threatening a person with fear for their lives through the use of a Computer Network such as email, videos, or phones. Cyberstalking is a form of electronic harassment. Online Sex Offences include Child

Pornography, Human Trafficking, Child Trafficking, Cyberprostitution. Cybertrespass is accessing a computer's or network's resources without authorization.

Cybertheft There are many different forms of Cybertheft, or ways of using a Computer and Network to steal information, money, or other valuables. Cybertheft offenses include: Embezzlement, Unlawful Appropriation, Cyber Espionage: Economic / Corporate / Industrial, Infringement of Intellectual Property Right (Patents, Trademarks, Designs, Copyright, Plagiarism, Piracy), Identity theft, Acquiring Personal Information, DNS Cache Poisoning. Cyberfraud involves promoting falsehoods in order to obtain something of value or benefit.

Phishing the term Phishing originated in 1996 to refer to a practice of tricking users into giving up their America On-Line (AOL) accounts to be used to distribute pirated software and other misuse. Pharming is fraudster steals sensitive information. Pharming directs users to fake sites, via a bogus email or more commonly a virus or piece of Spyware, when they are trying to access legitimate websites. Cross Site Scripting represents the combination of Phishing and Pharming. The cyber criminal is able to exploit vulnerabilities in website design code to allow them to steal passwords and login codes.

Destructive Cybercrimes include those in which network services are disrupted or data is damaged or destroyed, rather than stolen or misused. These crimes include: Hacking / Cracking, Social Engineering, Malware or Malicious Code, Denial of Service attack, Distributed Denial of Service Attack. Other Cybercrimes incidentally use the Internet to accomplish criminal acts that have been around forever and include Internet Gambling, Internet Drug Sales, Cyberlaundering, and Cybercontraband.[5]

To understand networking it requires knowledge of how data, converted to electrical or light pulses, is sent across cabling or over the airwaves, as well as the processes used on the sending and receiving ends to prepare that data for sending and to translate received data back into a form usable by applications and, ultimately, computer users. The OSI and DoD models are layered to define specific tasks to be performed by protocols at different levels or steps in the network communication process. Different operating system platforms rely on different file-sharing protocols and authentication schemes, but most operating system vendors provide for interoperability with other operating systems because many of today's networks are heterogeneous. [1,20]

III. COMPUTER NETWORK BASICS AND TYPES

The earliest form of networking was called sneakernet because it involved physically transporting the data, software, or hardware being shared to the remote computer. It soon became obvious that there was a better way: connect the computers via cable so that data could be sent from one computer to another without anyone having to make the physical journey.

Digital signals are discrete state, whereas analog signals are not. Analog signals change state gradually, on a continuum, rather than going directly and instantaneously from one discrete state to another. Multiplexing refers to using a single link to send multiple streams, or channels, of information. Signals can be multiplexed in several different ways. In Frequency division multiplexing different streams of information can be sent on separate frequencies and is the typical method for multiplexing analog signals. In Time division multiplexing breaks each of the signals into small pieces called segments, and these are transmitted over the link one after the other. This method can be used for multiplexing digital signals. In Dense wavelength division multiplexing if the transmission medium is optical cable, light can be separated into different wavelengths, separate signals can be transmitted using separate wavelengths.

There are three different methods of signal travel are identified as Simplex transmissions unidirectional transmissions, Half-duplex transmissions signal transmission is bidirectional, but the signal can travel only one way at a time. In Full-duplex transmissions signals are transmitted both ways and can travel across the air or cable simultaneously. When a network adapter or other network device receives an incoming signal, it needs timing information in order to interpret the signals correctly. This is referred to as synchronizing the bits. In Asynchronous transmission method a start bit is included at the beginning of each message; this bit is used as a signal for the receiving device to synchronize its clock with that of the sending device. In Synchronous transmission method a timing mechanism built into the transmission synchronizes the clocks of the sending and receiving devices. Signals represent individual bits, and those bits are often grouped together in bytes for convenience, but computers send data across the network in larger units: packets, segments, datagram's, or frames.

When signals are transmitted on a network, there must be some mechanism for directing traffic that is, a way to ensure that when multiple computers are sending signals, all the data packets make it safely to their destinations. This is called the access control method. The popular access control methods are contention methods, token passing, and polling methods.

Networks can be categorized in many ways. Local Area Network is confined to one geographic area, Wide Area Network connects locations in widely dispersed areas, Metropolitan Area Network covers an area about the size of a typical city. Networks classification based on their architecture, standards and specifications for media type, physical and logical topology, access method, distance limitations, packet sizes, and headers and other criteria as Ethernet based, Token Ring based. A network protocol is a set of rules computers use to communicate. The U.S. Department of Defense (DoD) developed the original networking model on which TCP/IP is based. Later, the International Organization for Standardization (ISO) refined and expanded on this model, creating the Open System Interconnection (OSI) model.[7]

OSI model: The OSI model consists of seven layers. Physical layer interacts with the hardware to provide the actual stream of bits as signals at the electrical and mechanical levels. Data link layer is divided into two sub layers: media access control (MAC), and logical link control (LLC). Network layer handles routing and switching using logical addresses (IP addresses) by creating virtual circuits. Transport layer provides for transfer of data between hosts; handles acknowledgment, error checking, and recovery and flow control. Session layer establishes, manages, and terminates connections between applications at each end. Presentation layer deals with differences in the way data is represented translating from application to network format or vice versa. Application layer supports application and end-user processes; provides services for file transfer, e-mail, and other network software services.

TCP/IP Model: The TCP/IP Networking Model consists of only four layers, compared with the OSI model's seven layers. The Application/Process Layer is the top layer of the TCP/IP model encompasses all three OSI upper layers: application, presentation, and session. The Host-to-Host (Transport) Layer is sometimes labeled the transport layer, even on four-layer TCP/IP diagrams, and it maps to the transport layer on the OSI model. The Internetworking Layer corresponds closely to the

OSI network layer. The Network Interface Layer maps to OSI's data link and physical layers.

Network Topologies: The term network topology refers to the way in which the nodes of a work are linked together. It determines the data paths that may be used between any pair of nodes in the network. In Star Topology all computers attach to a central point. A star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. In Ring Topology Computers connected in a closed loop. All messages travel through a ring in the same direction either clockwise or anticlockwise. Bus Topology use a common backbone to connect all devices. Bus networks work best with a limited number of devices. Tree Topology is also known as the 'Hierarchical topology', the tree topology is a combination of bus and star topologies. Mesh Topology involve the concept of routes. A mesh network in which every device connects to every other is called a full mesh. Partial mesh networks also exist in which some devices connect only indirectly to others.

Network Hardware: The network interface card (NIC) is the hardware device most essential to establishing communication between computers. The network media are the cable or wireless technologies on which the signal is sent. Cable types include thin and thick coaxial cable, twisted-pair cable, or fiber optic cable, which sends pulses of light through thin strands of glass or plastic for fast, reliable communication but is expensive and difficult to work with. Wireless media include radio waves, laser, infrared, and microwave.

Hubs and Repeaters: Hubs and Repeaters are connection devices. Repeaters connect two network segments and boost the signal so the distance of the cabling can be extended past the normal limits at which attenuation, or weakening, interferes with the reliable transmission of the data. Hubs are generally used with Ethernet twisted-pair cable, and most modern hubs are repeaters with multiple ports; they also strengthen the signal before passing it back to the computers attached to it. Passive hubs serve as connection points only; they do not boost the signal. Active hubs serve as both a connection point and a signal booster. Intelligent or Smart hubs are active hubs that include a microprocessor chip with diagnostic capabilities so that you can monitor the transmission on individual ports. Switching hubs operate at the data link rather than the physical layer and are more commonly called simply a switch. Bridges operate at the data link layer of the OSI model. Switches work at the data link layer, and they are installed in place of the active hubs that have been more typically used to connect computers on a UTP-cabled network. Routers routers are multiport connectivity devices.

Network Software: The term Network Operating System (NOS) is used in three different ways , sometimes used to refer to any computer operating system that has built-in networking components, sometimes used to refer to the components of the operating system that make networking possible, sometimes used to refer to the server operating system software. [9]

Client/Server Computing: The term client/server computing has different meanings, depending on the context in which it is used. This is a system in which database files are stored on a server, but a client query results in the entire file being transferred to the client machine, where the sorting takes place. Authentication Server-Based Networks controls access to the network, storing a security accounts database that holds users' networkwide account information. The authentication server is a centralized point of security and network resource management and must run special server software. Peer-to-Peer Networks Networks without an authentication server are called workgroups or peer-to-peer networks. Server Software is a operating systems capable of providing network authentication services. There are also many server applications that can be installed only on a system running a server operating system. Client Software are in which case client machines don't necessarily have to run an operating system made by the vendor of the network's server software.

*Network File Systems and File Sharing Protocols:*Network file systems and file sharing protocols allow users to access and update files on remote computers as though they were on the local computer. Server Message Block Protocol is used to allow client applications to access and write to remote files and request services from server applications on remote systems. Common Internet File System is a protocol proposed as an Internet standard for allowing access to remote files across the Internet. CIFS run on top of the TCP/IP protocol stack. NetWare Core Protocol is actually a set of protocols that provide file and printer access, among other services, between clients and remote servers on NetWare networks. Network File System is a client/server application developed by Sun Microsystems that runs on TCP/IP to allow remote file access. Network Protocols in order for any network communication to take place between computers, the computers must be running a common network protocol. Protocols are simply sets of rules that define the communication process. Networking protocols generally work together in protocol stacks or suites. A stack is two or more protocols working at different layers of the OSI or TCP/IP model. TCP/IP on the Internet is a familiar, networking component to most modern network administrators and information technology professionals. [10,15]

Routing: Computers on an internetwork send packets to one another in one of two ways Directly if the source and destination computers are on the same subnet. Indirectly if the source and destination computers are on different subnets by forwarding the packets to a router. IP routing involves discovering a pathway from the sending computer to the destination computer whose address is designated in the IP header. IP routing refers to forwarding of packets from a source computer to a destination computer by going through routers that support IP routing. Every computer has a table of network numbers, known as a routing table.

A gateway address is listed there for each network number, and the gateway is used to reach that network. The gateway doesn't have to connect directly to the destination network; it is just the starting point. Each gateway, or router, that the message must go through is called a hop. At each router, the destination IP address on the packet is compared to the routing table, and the best route is used to decide the endpoint of the next hop. Typically, a router is connected to two or more networks or subnets. The router, a dedicated device or a computer acting as a router, is said to have an interface to each network to which it is connected. Routing comes in two basic flavors. Static Routing the routing table must be constructed manually; an administrator must enter the IP addresses defining the routes to remote networks one by one. Dynamic Routing the table is configured using dynamic routing and maintained automatically because the dynamic router can communicate with and learn from other routers on the network.

The Transport Layer Protocols are the TCP and the UDP. These two protocols provide two different types of connection services. In the Connection Oriented Services TCP first establishes a virtual connection between the sending and receiving computers. In Connectionless Services a connectionless transport protocol like UDP doesn't provide the service of dividing a message into packets and reassembling it at the other end, as the connection oriented TCP does. Since UDP doesn't sequence the packets that the data arrives in, an application program that uses UDP has to be able to make sure that the entire message has arrived and is in the right order.[18,19]

IV. The Internet Evolution and Architecture

The Internet began as a modest network called the ARPANET, first deployed in 1969 with just four routers known as Interface Message Processors (IMP), interconnecting a small number of host computers and terminals. Funded by the ARPA within the U. S. Department of Defense, the ARPANET project was intended to facilitate the sharing of computing resources among researchers at various institutions across the country. In the early 1970s, ARPA began to explore two alternative applications of packet switching technology based on the use of synchronous satellites (SATNET) and ground-based packet radio (PRNET).

A key architectural construct was the introduction of gateways called routers between the networks to handle the disparities such as different data rates, packet sizes, error conditions, and interface specifications. The gateways would also check the destination Internet addresses of each packet to determine the gateway to which it should be forwarded. The TCP/IP protocol suite was developed and refined over a period of four more years and, in 1980, it was adopted as a standard by the U.S. Department of Defense. On January 1, 1983 the ARPANET converted to TCP/IP as its standard host protocol. Gateways were used to pass packets to and from host computers on local area networks. Refinement and extension of these protocols and many others associated with them continues to this day by way of the Internet Engineering Task.

Wireless Networks: A Wireless Network is a network of Computers and Computer peripherals that are connected to each other without wires. This enables ease of communication, especially for mobile computing platforms. Further, there are a number of other advantages to a wireless network that make them increasingly common in both the workplace and at home. A Wireless Router is a device that performs the functions of a router but also includes the functions of a wireless access point. Wireless Clients can be mobile devices such as laptops, personal digital assistants, IP phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface. The IEEE 802.11 standards specify two Wireless Operating Modes. Infrastructure Mode is used to connect computers with wireless network adapters, also known as wireless clients, to an existing wired network with the help from wireless router or access point. Ad Hoc Mode is used to connect wireless clients directly together, without the need for a wireless router or access point.

Security is the key to preventing or detecting Computer and Computer Network related criminal activity. Cybercrime is possible because Computers and Networks are not properly secured. There are many reasons for security problems. Lack of knowledge of Security and Security issues, Lack of time for Security Mechanisms, Psychological denial that it can’t happen to me. None of these reasons is good enough to justify the potential loss due to Cybercrime, and those fact costs lots after the network and its data have been compromised.[5,6,23]

V. Security and Security Incidents

Wherever Computer Security and in particular Network Security is based on three pillars Confidentiality means keeping information secret from all except the intended readers. Integrity means to protect information from being altered by unauthorized entities. Availability means to protect the information from becoming unavailable either by accident or sabotage. Identification and Authentication is the verification of a claimed identity. Nonrepudiation is the process of ensuring that the author of a document cannot later claim not to be the author. Access Control encloses any mechanism of granting access to data or performing an action, and the access control mechanism grants and revokes privileges based on predefined rules, and finally Accountability means to track and record events occurring in a system and all these are important aspects of information security. [21]

Security can be defined variously. Security is the prevention of or protection against access to information by unauthorized recipients, or intentional but unauthorized destruction or alteration of that information. System Security is about much more than just keeping out malicious users and preventing attacks. It is also about maintaining and providing access to resources for authorized users, and it is about maintaining the integrity of the data and the infrastructure.

An information security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Incidents include activities such as Unauthorized access to a system or its data, Unwanted disruption or denial of service, Unauthorized use of a system for the processing or storage of data, Unauthorized changes to system hardware, firmware, or software. There exit several ways of categorizing the incidents. Incident Classification must possess some criteria’s like it should be Accepted, Mutually Exclusive, Comprehensible, Complete/Exhaustive, Unambiguous, Repeatable, Terms Well Defined, and Useful. When an attack takes place, there is a possibility it uses several vectors as a path to a full blown cyber attack. An attack vector is defined as a path by which an attacker can gain access to a host. This definition includes vulnerabilities, to launch a successful attack it may require several vulnerabilities like Misconfigurations, Kernel Flaws, Buffer Overflow, Insufficient Input Validation, Symbolic Links, File Descriptor, Race Condition, Incorrect File/Directory Permission, and Social Engineering. Various attacks target a variety of hosts, leaving the defender unknowingly susceptible to the next attack. These targets are Operating System (Kernel, User, Driver), Network, Local Computer, User and Application. Broadly the incidents are categorized as intrusion and attacks.

Intrusion and Attacks: There are many ways for attackers to obtain illicit access to computer systems. This kind of access is often called Intrusion, and the first thing an intruder does is usually trying to obtain special/administrative privileges i.e. a root access on that system. In general, there are three main ways to intrude into a system. Physical Intrusion happens when an intruder has a physical access to the target machine. In System Intrusion intruder exploit unpatched security vulnerabilities in order to escalate their privileges to administrative level. In Remote Intrusion an attacker tries to get into the system remotely through the network. They initially do not have any privileges to the system, but one way or another.

A Computer Network Attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Cyberattacks usually require that the targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, that the malicious code can exploit. Broadly CAN come in two forms. Active Attacks attempt to cause harm typically through system faults or brute force, and attempt to overload the victim’s computer to the point that it either slows to an unusable crawl, hangs, or completely crashes. Passive

Attacks are in the nature of eavesdropping on, or monitoring of transmissions where the goal of the attacker is to obtain the information that is being transmitted i.e. interception. These attacks can be used by a trespasser to degrade the anonymity of the clients through Predecessor Attack, Denial of Service Attack, Sybil Attack, Local Eavesdropping, and Attack on Critical Information Infrastructure Protection. [25]

Threat and Vulnerability: Threats to Cybersecurity include Misconfigurations of Computer Systems, Poor User and Administrator Education, Poor Software Design, Network and System Design Issues, Substandard Operational Procedures, Use of Insecure Protocols, Weak Passwords, and finally, Lack of Awareness & Indifference. Threat may be from some categories like Networking threat, Hardware and virtualization threats, Weak devices threat, Complexity threat, Data Manipulation threat, Attack infrastructure threat, Human factors threat and Insufficient security requirements threat.

Threat can be defined as “A threat is the potential for one or more unwanted consequences caused by a circumstance, capability, action, or event that could be harmful to a system or person. Threats can be caused naturally, accidentally or intentionally. In essence, a threat is a ubiquitous phenomenon.” One other definition may be “A threat is the presence of dangerous or adverse circumstances or events with the potential to impact operations, assets, or individuals via disclosure, modification, destruction, or disruption of service.” The motivations for an attack gives some insight about which areas of the network are vulnerable and what actions an intruder will most likely take. Some of the common motivations for attacks are Greed, Prank, Notoriety, Revenge, and Ignorance.

Types of Threats: Threat classification may be based on some factors like Impact describes how many users are affected and what damage level is to be expected, Likelihood captures the expected probability that a threat in question is actually carried out, Obliviousness captures the lack of awareness of the public and the research community for a threat, Research and Development (R&D) Needs captures the extent to which new R&D efforts are needed to mitigate a threat.

One way of threat classification may be as attacks against the infrastructure of the Internet, Denial of service attacks, attacks against the confidentiality or integrity, both on wired and wireless links. Unauthorized Access is, when an unauthorized entity gains access to an asset and has the possibility to tamper with that asset. Some common methods used to identify potential targets are: A reachability check, Port scanning, Tapping into the Physical Wire, Remote Dial-In Access, Wireless Access, and Social Engineering. Impersonation is the ability to present credentials as if you are something or someone you are not. Impersonation can take several forms: Impersonation of Individuals, Impersonation of Devices and Stealing a Private key or recording an authorization sequence to replay at a later time. Denial of Service is an interruption of service either because the system is destroyed or because it is temporarily unavailable. Common Denial of Service Attacks are TCP SYN attack, Ping of Death, Land.c Attack, Teardrop.c Attack, Smurf Attack, Fraggle Attack. Distributed Denial of Service is a variant of a DoS attack. This is the DDoS attack, where multiple machines are used to launch a DoS attack.

Human Error Threat: A long list can be given of Human Error Threat. Equipment Loss, Miscommunication, Implementation Error, Malfunction Threats, Software Malfunction, Hardware Malfunction, Process Malfunction, Power Disruption, Malicious Threats, Physical break in, Eavesdropping, Malicious Authorized User, Equipment Theft, Social Engineering, Malware that requires user interaction, Malicious Scan, Malicious Unauthorized User, Self Replicating Malware, Process Violation, Environmental Threats, Lightning, Damaging Wind, Temperature or Humidity Extremes, Electronic Emanation/Electromagnetic Pulse, Hazardous Materials, Fire, Flood and Power Surge. [24]

Vulnerability in a system is a potential weak point in the system that can be accidentally or intentionally exploited to harm the system. The global presence, explosive growth and open access of the Internet and modern communications technology have dramatically increased the vulnerability. A successful cyber attack requires finding only vulnerability, whereas a successful cyber defense requires finding all possible vulnerabilities.

Vulnerability can be defined variously as “Vulnerability is a flaw or weakness in a system’s design, its implementation, or operation and management that could be exploited to violate the system and, consequently, cause a threat. Vulnerabilities may have different dimensions: technical, functional or behavioral.” and “A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth that could be exploited by a threat to gain unauthorized access information or disrupt critical processing i.e. a weakness in a system allowing unauthorized action.”[2,11,17]

VI. SAFEGUARDS FROM CYBERCRIME

There should be common agreed upon Cyberlaws all over the globe. The second is to ensure that Network Security and General Security awareness as effective as possible. This can be achieved by applying Strong Authentication Techniques, by keeping Forensic Readiness and by providing strong system & Network Security.

The basic concepts involved in computer and network security includes the importance of multilayered security and the components that make up a multilayered security plan. The physical security is the first line of defense. The Hardware Security and the Software Security. An effective security does not rely on one technology or solution but instead takes a multilayered approach.

The Crime Triangle with three criteria. The criteria’s are Motive: An intruder must have a reason to want to breach the security of the network, Means: An intruder must have the ability, Opportunity: An intruder must have the chance to enter the network because of flaws in the security plan, holes in a software program that open an avenue of access, or physical proximity to network components.

One of the most important, and at the same time most overlooked, aspects of a comprehensive network security plan is physical access control. Ensuring physical access control includes Securing the Servers, Securing the Workstations, Securing the Network Devices, Securing the Cables, Security Considerations for Wireless Networks, Security Considerations for Portable Computers, Printed Data Security, Removable Storage Security.

Cryptography: Cryptography is a way of concealing information by rendering it unreadable to anyone not in possession of the right key. The key is a binary number, which is used in conjunction with an encryption algorithm to transform plaintext into ciphertext and vice versa. Cryptographic techniques include Encryption involves applying a procedure called an algorithm to plain text to turn it into something that will appear to be gibberish to anyone who doesn’t have the key to decrypt it and Steganography is a means of hiding the existence of the data, not just its contents. This is usually done by concealing it within other, innocuous data. Cryptographic techniques such as encryption are the basis of digital certificates, digital signatures, and the PKI. All of these technologies are important components of an enterprise level security. There are many different ways to scramble text or hide its meaning in such a way that only authorized persons are able to read it. Some common cipher/code types are: Substitution Cipher, Transposition Cipher and Obscure Languages Code.

Encryption is a form of cryptography that scrambles plain text into unintelligible cipher text. Encryption is the foundation of such security measures as digital signatures, digital certificates, and the PKI that uses these technologies to make computer transactions more secure. Encryption methods are usually categorized depending on the number of keys that are used, Symmetric encryption is also called secret key encryption, and it uses just one key, called a shared secret, for both encrypting and decrypting, Asymmetric Encryption is to address the problem of key exchange, another type of encryption was developed. Asymmetric encryption is also called public key encryption, but it actually relies on a key pair. Two mathematically related keys, one called the public key and another called the private key, are generated to be used together.

Literally thousands of different cryptographic algorithms have been developed over the years. Cryptographic algorithms can be classified as: Encryption algorithms, Signature algorithms, Hashing algorithms. Encryption is used for a number of different purposes in organizations that deal in sensitive data of any type. There are different ways encryption technologies can be used to protect that information. Data on Disk, Data across the Network.

Steganography from the Greek word for covered writing refers to a method of hiding data not just concealing its contents as encryption does, but concealing its very existence. Content in files. The process of detecting Steganography data is called steganalysis. The use of cryptography naturally led to the science of cryptanalysis, the process of decrypting encrypted messages. Cryptanalysts throughout history have used a number of different methods to break encryption algorithms, including Known plain-text analysis, Differential cryptanalysis, Ciphertext-only analysis, Timing/differential power analysis, Key interception.

Cryptographic techniques concern themselves with the basic purposes: Authentication, Confidentiality, Integrity and Nonrepudiation Many different methods can be used to authenticate a user's identity. In general, the user is asked to provide something that is associated with his or her user account that could not easily be provided by someone else. The requested credential is generally one or more of the Password, Smart Card, Biometric, Logon, and Remote Access. The protocols used for authenticating identity depend on the authentication type. Some common protocols used for authentication include: Kerberos, NTLM, Password Authentication Protocol, Challenge Handshake Authentication Protocol, Remote Authentication Dial-In User Service, AppleTalk Remote Access Protocol, Secure Shell.[12]

Confidentiality refers to any method that keeps the contents of the data secret. Usually this means encrypting it to prevent unauthorized persons from understanding what the data says even if they intercept it. In a high-security environment, where network communications necessarily involve information that should not be shared with the world, it is important to use strong encryption to protect the confidentiality of sensitive data. Data integrity, in the context of cryptography, means that there is a way to verify that the data was not changed after it left the sender, that the data that was sent is exactly the same as the data that is received at the final destination. Nonrepudiation is a means of ensuring that whoever sends a message cannot later claim that he or she didn't send it. Nonrepudiation just goes a step further than authentication.[22]

Hardware security solutions can come in the form of network devices: Firewalls, Routers and Switches. In general, these devices are dedicated computers themselves, running proprietary software. Hardware based firewalls are often referred to as firewall appliances. Other hardware based components of your network security plan may include devices that provide extra security for authentication, such as: Smart Card Readers, Fingerprint Scanners, Retinal and Iris scanners, Voice Analysis Devices. These devices can be used in environments that require a high level of security for secure and reliable network authentication.

Software security solutions cover a much broader range than do hardware-based solutions. These solutions include the security features built into the network operating system as well as additional security software made by the operating system vendors or third-party vendors. A number of mechanisms exist, for protecting the information assets in a system. Some of these can be used alone, to directly protect some of the three properties. Most need to be combined with one or more others to offer complete protection. The most commonly used mechanisms are Electronic Signing is an application of cryptography that makes it possible for an entity to sign an amount of digital data so that anyone can verify that the data has been signed by the signer and that the data has not been changed in any way since it was signed. Certification can be implemented using electronic signing. A certificate is a piece of information, signed by a publicly recognized authority. Auditing is an important activity for maintaining availability by continuously measuring the system load. Redundancy is an important tool for maintaining system availability. Thousands of cryptographic products are available for different purposes: disk/file encryption, e-mail encryption, Steganography.

A new standard of XML aware digital signatures, recommended by W3C, provides authentication, data integrity, and support for non-repudiation. The main purpose of PKI is to provide the safe system for distributing Digital Certificates. Digital Certificates are digital documents that identify someone or something and they contain their Public Key. Digital Certificates can be issued by many different PKI's in the world today. There are three different types of Certificates Individual Certificates, Non-Individual Certificates, Device Certificates.

*Public Key Infrastructure (PKI):*Almost all sectors of economy need some tool or formula that would provide trusted and private secure transmission of electronic data between any two parties. PKI offers a solution of overcoming these problems. PKI is a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each entity involved in an online transaction. PKI allows the secure exchange of encrypted electronic data between parties over the internet. So, it can be used for email communication, web browsing, online banking, or lodging tax returns. PKI is the name given to the combination of hardware, software, and people policies with aim to manage digital certificates [13,14]

Firewalls: A firewall is simply a programme or hardware device that filters all of the information coming through the Internet connection into your private network or computer system. A firewall is an essential piece of the security jigsaw. A firewall goes a bit further than just standing in for the local computers and hiding them from view on the global network, as a proxy server does. Firewalls are specifically designed to control inbound and outbound access, preventing unauthorized data from entering the network and restricting how and what type of data can be sent out. Firewall comes in two options.

A firewall can be designed to permit all packets to pass through unless they are expressly denied and a firewall can be designed to deny all packets unless they are expressly permitted. Firewall products support the filtering of messages to either allow data to pass through or prevent it from doing so, according to specified criteria. The best firewalls support layered filtering. Packet filtering does most of its work at the network layer of the OSI networking model or the internetwork layer of the DoD model, dealing with IP packets. Circuit filters operate at a higher layer of the OSI model, the transport layer or the host-to-host layer in the DoD model. An application filter operates at the top layer of the networking model, the appropriately named application layer. Application filters can use the packet header information but are also able to allow or reject packets on the basis of the data contents and the user information.

Many firewalls also incorporate an intrusion detection system that can actually recognize that an attack of a specific type is being attempted and can perform a predefined action when such an intrusion is identified, such as: Send an e-mail message to the administrator, Send a network message to the administrator, Page the administrator, Write an event entry to the event log, Run a previously specified program or script, Stop the firewall service.[8,9,16]

VII. CONCLUSION

The Review of terms and concepts used to understand Cybercrime starts with the introduction to term Cybercrime and all similar terms implying the same meaning. The study of Cybercrime and all the Components of Cybercrime, Cybercriminals, the loss due to Cybercrime, Preventive Measure, and how far the current measures are effective all these things are very significant. Cybercrime can be variously defined. There are various possibilities of categorizing Cybercrime.

VIII. REFERENCES

[1] Bluefire Security Technologies. (2003) “Mobile insecurity: A practical guide to threats and vulnerabilities.” http://www.bluefiresecurity.com

[2] Shaffter G. “Good and Bad Passwords How-To: Password Cracking Goals, Techniques and Relative Merits and Cracking Times of Different Techniques.” http://geodsoft.com

[3] Clark R (2004) “Message Transmission Security” http://www.anu.edu.au

[4] Kunene G. (2004) “XML Standards Provide Web Services Security.” http://www.devx.com

[5] Baker W. H. & Wallace L. (2007) “Is information security under control?” IEEE Security & Privacy.

[6] McAfee. (2007) “McAfee for small and medium business.” http://www.mcafee.com

[7] James L. (2005) “Phishing Exposed “ Rockland MA Syngress Publishing.

[8] The Presidents Identity Theft Task Force (2007) “Combating Identity Theft: A Strategic Plan.” http://www.idtheft.gov

[9] Sumit Kasera and Nishit Narang (2005) “3G Mobile Networks. Architecture, Protocols and Procedure.” Tata MCGraw-Hill Publishing Company, limited edition

[10] Davis, Mark (2005). “Network Security and Encryption.” Dublin Institute of Technology: http://www.electronics.dit.ie

[11] Tutanescu, Ion, and Sofron, Emil (2005) “Anatomy and Types of Attacks against Computer Networks.” Department of Electronics and Computers, University of Pitesti, ROMANIA http://conference.iasi.roedu.net

[12] Khalid A. (2004) “Cyber crime: Business and the law on different pages.” The Star. http://www.niser.org.my

[13] Bhatia J. S., Sehgal R. (2008) "Multi layer cyber attack detection through honeynet", Proceedings of New Technologies, Mobility and Security Conference and Workshops.

[14] Ryu J. , Na J. (2008) "Security requirement for cyber attack traceback" Fourth International Conference on Networked Computing and Advanced Information Management.

[15] Karygiannis T, Owens L. (2004) “Wireless network security 802.11, Bluetooth and handheld devices.” http://csrc.nist.gov

[16] Elliott G. , Phillips N.(2004) “Mobile Commerce And Wireless Computing Systems” Pearson Addison Wesley

[17] Silver Lake Editors (2006) “Scams & Swindles” Silver Lake Publishing, Aberdeen WA.

[18] Mirkovic J., Reiher P. (2004) “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM CCR

[19] “Intrusion Detection Message Exchange Format.” (2008) http://www.ietf.org

[20] Chauhan (2003) “Protecting port 80: Techniques for Eliminating Web Application Vulnerabilities.” A Teros White Paper.

[21] Germain J. (2005) “Internal Threats Still Major Network Concern.” http://www.macnewsworld.com

[22] Barua-Dayal “Cybercrimes Notorious Aspects Of The Hmans And The Net”

[23] Maria Kjaerland “Approaches For Analysing Cyber Incidents”

[24] E.C.Viano, J.Magallanes , L.Bridel “Transnational Organized Cybercrime Myth, Power And Profit”

[25] Maria (2004) “Analyzing Cyber Incidents”