ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

Spectrum of Cyber threats & Available Control Mechanisms

Vikram Mangla, Dr.S.N.Panda

Abstract - The Internet is undoubtedly the largest public data network enabling and facilitating both personal & business communications worldwide. Wireless networking has experienced a tremendous growth becoming an integral part of homes, offices & all type of businesses. It provides many advantages, but it is also coupled with many security threats and alters the organizations overall information security risk profile. Although implementation of technological solution is the usual respond to the wireless security threats and vulnerabilities, wireless security is primarily a management issue. Cyber crime is constantly evolving and the growing increase in the number of threats that use social engineering techniques is causing concern for several businesses. All it takes is for one user to click on a malicious link and a firm's network can be brought to a grinding halt. But the early days of cyber threats have gone now. Cyber threats have increased in large number. The volume of effect of these attacks has increased tremendously whereas the transaction time has decreased. The sources of attacks and exploitations are difficult to determine within time frames that enable victims to avoid damage, and any defensive measure is likely eventually to fail given the vulnerabilities of most cyber systems and the incapacities of users. In this paper we review different cyber threats and control mechanisms available and how these are affecting the network world.

Keywords: Cyber threats, Wireless Networking, Internet, WLAN, Security, Social Networking, Spam, Cyber criminals

I. INTRODUCTION TO CYBER THREATS

With advances in technology, everyday life is starting to depend on wireless network technology. Such technology is used to connect computers via routers and to connect hand-held devices with computers. With the proliferation of wireless technology comes a greater risk of security threats, making it critical for system administrators and average users to be informed about the types of threats and methods designed to neutralize them. The number of cyber threats has increased enormously over the last decade. The detection of these attacks is always the major concern for many governments and organizations all over the world. Many threats on wired as well as wireless networks are present. The computing systems and networks in the critical sectors like military, banking and finance, telecommunications, transportation, medical etc. are vulnerable to these growing cyber threats. Military & financial organizations are always on the top priorities of the attackers. Now-a-days politically motivated cyber threats are also increasing in number.

A cyber threat is a series of malicious computer activities that threaten and compromise the security & integrity of a computer/network system.

Some of the recent well-known cyber attacks include Nimda attack, SQL Slammer attack, July 2009 attacks, and Operation Aurora. The Operation Aurora cyber attacks were launched against major organizations like Google, Yahoo, Adobe Systems, Morgan Stanley, Dow Chemical Company, etc. in the second half of 2009. Recently in April 2011, a series of cyber attacks were launched against Sony's PlayStation Network which made the network go online for about 24 days [2]. In May 2011, cyber attacks were launched against Citibank and the account information of about 1% of its 21 million North American credit card customers was stolen. [2]

The most common cyber threats can be

a) Accidental Association
b) Malicious association
c) Ad-hoc Networks
d) Identity theft (MAC Spoofing)
e) Denial of Service attacks
f) Network Injection
g) Proliferation of Botnets
h) Pervasive devices & Social Networking
i) Mobile Threat Vectors
j) Web based attacks
k) Cryptographic attacks

1) Accidental Association – With more & more organizations deploying wireless network and allowing company personnel to access the internet or the wired backbone through wireless access points are increasingly getting exposed to the hacking attacks. In wireless network the data transfers in the same manner as in the wired network but it is more vulnerable to signal leak as proper mechanisms are not deployed for the same. Violation of security perimeter of corporate network can come from number of different methods & intends. One on these methods is "accidental association" [29]. When the user turns on the computer and it latches on to a wireless access point from the neighboring company's overlapping network, the user do not know or is unaware of this

connection. It is a security breach in the proprietary company's network. This type of association is just a case of mis-association where this association can be done accidently or deliberately [28]. This association becomes more problematic when the user computer is also connected to the wired network because it opens the gate for the hacker to access the data of an organization.

2) Malicious Association – When cracking laptop is used instead of company's access point (AP) to get access to network - a process is known as "Malicious associations". These types of laptops are known as "soft APs" and are created when a cyber criminal runs some software that makes his/her wireless network card look like an access point. Once the attacker has gained access, he/she can steal passwords and can launch attacks on the wired network [11]. Virtual private networks (VPNs) or network authentication mechanisms working at Layer 3 does not provide any protection as wireless networks operate at Layer 2. Wireless 802.1x authentications do help with some protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the attacker is just trying to take over the client at Layer 2 level [11]. These systems access security poor systems to enter into the network.

3) Ad-hoc Networks – Ad hoc network is a decentralized type of Wireless network [30]. This type of network does not rely on the pre-existing infrastructure such as routers in the wired network or access points in managed (infrastructure) wireless network. Instead each node in the network participates in forwarding data for other nodes, and the determination of which nodes forward data is made dynamically based on the network connectivity. Ad hoc networks use flooding along with classic routing in forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. The earliest wireless ad hoc network was the "packet radio" networks (PRNETs) in 1970s, sponsored by DARPA after the ALOHAnet project [31].

Sample Example of Ad hoc Network in Infrastructure Mode

Ad hoc networks can pose a security threat [31] [32]. These networks usually have very little protection, encryption methods can be used to provide some security to these networks. The security hole is not in the Ad hoc network itself but the bridge it provides into other networks, usually in the corporate environment and the unfortunate default setting of Windows Operating System unless it is explicitly disabled. Thus the user does not know that the unsecured ad hoc network is present on their system. We need to consider malicious attacks not only from outside but also from within the network from compromised nodes. Thus following are the ways by which the security can be breached [33] –

I) **Vulnerability of Channels** – In wireless networks, without accessing the physical network components, messages can be eavesdropped and fake messages can be injected into the network.
II) **Vulnerability of nodes** – Network nodes can easily be captured and can fall under the control of the attacker as these nodes are not physically protected.
III) **Absence of Infrastructure** – These networks are supposed to work without any fixed infrastructure. This makes the classical security solutions based on the certification authorities and on-line servers inapplicable.
IV) **Dynamically changing Topology** – The security of topology in these networks requires the additional challenge as it is changing according to the need of the user. The topology is an ever changing topology. Due to which it requires the sophisticated routing protocols.

These networks should have the distributed architecture with no central entities as it increases vulnerability. Security mechanism need to be dynamic and not static and it should be scalable. The different attacks on Ad hoc network are as follows –

i. **Location Disclosure** – Targets the privacy requirements of the ad hoc network. An attacker is able to discover the location of the node, or even the structure of the network.
ii. **Black Hole** – In this, a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to the destination [34].
iii. **Replay** – An attacker that performs a replay attack injects into the network routing traffic that has been previously captured.
iv. **Wormhole** – This is strongest of all the attacks on these networks. It involves the cooperation between two malicious nodes that participate in the network [35]. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to this attack is packet leashes.
v. **Blackmail** – This attack is relevant against the routing protocols that use the mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [36]. An attacker may

fabricate such reporting messages and try to isolate legitimate nodes from the network.

vi. **Denial of Service** – These attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [37]. Instances of these attacks include routing table overflow and the sleep deprivation torture.

vii. **Routing table Poisoning** – All routing protocols maintain routing tables which hold information regarding the routes of the network. In poising attacks, the malicious nodes generate and send fabricated signal traffic, or modify legitimate messages from other nodes, in order to create false entries in the routing tables of the participating nodes [37].

viii. **Breaking the neighbor relationship** – An intelligent filter is placed by an intruder on the communication link between two information Systems could modify the information in the routing updates or even intercept traffic belonging to any data session.

ix. **Passive Listening & traffic analysis –** The intruder could passively gather exposed routing information. Such an attack can not affect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected.

4) Identity theft (MAC Spoofing) – Every network interface controller (NIC) has a unique MAC (Media Access Control) address [12].

Destination address (DA) (48 bits)	Source address (SA) (48 bits)	Type/Length (16 bits)	Data (...)	Frame Checksum (FCS) (32 bits)

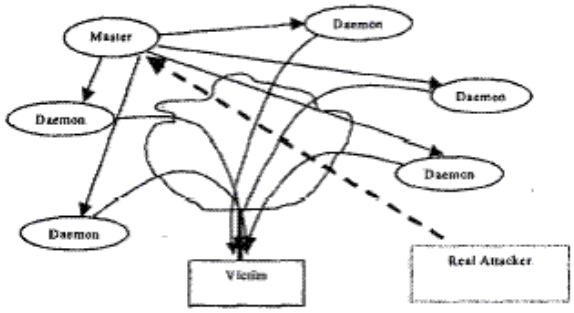
Type interpretation:

DA	Destination MAC Address	(6 bytes)
SA	Source MAC Address	(6 bytes)
Type	Protocol Type	(2 bytes)
Data	Protocol Data	(46 - 1500 bytes)
FCS	Frame Checksum	(4 bytes)

Source - http://netcert.tripod.com/ccna/internetworking/eframes.html

The Ethernet numbers include a 48- bit MAC address assigned to each Ethernet interface, and 16-bit value used in the Type field of the Ethernet frame [38]. MAC spoofing is computer identity theft, for good or for bad reasons, and it is relatively easy. The MAC address is burnt into the NIC at the time of manufacturing and it is unique. Hackers use MAC spoofing to impersonate a legitimate network user. MAC address is used as an authentication factor in granting the device access to the network. The hacker will change his device's MAC address to that of a user and thus gain access to the network. If the hacker is using the MAC address of a top executive with access privileges to sensitive material, a great deal of damage can be done [39]. Hackers use brute force attack, in which software tries a string of random numbers until the desired one. Then this address is used by the hackers to gain access of the user computer. Another method can be to monitor traffic using some pre-defined software and try to find out the desired MAC address.

5) Denial of Service attack – A Denial of Service (DoS) attack is the prime example of an attacker's ultimate malicious intent in their desire to bring normal network functioning and network resources access requests to a grinding halt. A DDoS attack [6] involves breaking into hundreds or thousands of machines over the Internet. The function of a denial of service attack is fundamentally to flood its target machine with so much traffic that it prevents it from being accessible to any other requests or providing services. The target machine is kept so busy responding to the traffic it is receiving from its attacker that it has insufficient resources to respond to legitimate traffic on the network. A distributed denial of service attack adds a many-to-one dimension to these forms of attacks. This form of denial of service generally involves a machine containing a master program and several machines which have been enslaved as zombie machines [17].



Denial of Service Attacks
Source - http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group2/

Basic Denial of Service attack Techniques –

a) Storage consumption attacks – In these types of attacks all storage space of local hard disk is consumed causing the machine to slow down. Tactics adopted for this is to flood very large size emails with huge attachments, mainly in the form of huge BMP or JPEG images of high resolution.

b) Connection Resources Consumption attacks – By sending very large number of erroneous requests for connection, attacker consumes all of available resources thereby resulting in the target being unable to initiate new request for connection.

c) Buffer Overflow attacks – This attack occurs when a process receives much more data than expected and no program to control such excessive data. This situation can give an unexpected result but can be useful for an attacker. "Ping of Death" is an example of these types of attacks.

d) **Ping of Death attacks –** This attack is also called as "Large Packet Ping Attack" and easy to initiate. All an attacker needs to do to initiate a "ping of death" attack is to use the ubiquitous network utility PING (Internet Control Message Protocol (ICMP) Packet Internet Groper) to

"ping" the target with an illegally modified and very large IP datagram. This will result in overfilling of the target system's buffers causing the target to reboot or hang.

e) **Long file or username attack –** This is another basic buffer overflow attack where the attacker sends the packets to the target machine, with file names more than 256 characters long.

f) **SYN attacks –** This attack occurs when the attacker exploits the use of buffer space during the Transmission Control Protocol (TCP) session initialization three way handshakes.

g) **Smurf attacks –** In this a combination of IP Address Spoofing and ICMP flooding are used to saturate a target network with traffic to such an extent that all normal traffic is effectively "drowned out" thereby causing a Denial of Service (DoS) attack. Smurf attacks consist of three separate elements; the source site, the bounce site and the target site.

6) Network Injection Attacks – This problem allows for attackers to sneak program instructions into places where the developer expected only benign data. By sneaking in program instructions, the attacker can instruct the program to perform actions of the attacker's choosing. To perform an injection attack, the attacker attempts to place data that is interpreted as instructions in common inputs. A successful attack requires three elements [18] –

a. Identifying the technology that the web application is running.
b. Identifying all possible user inputs.
c. Finding the user input that is susceptible to the attack.

SQL injection attack is the best example of these types of attacks. Most web applications today use SQL database to store persistent data for the application. The SQL queries used for these databases are vulnerable to these attacks as most of these are open source systems. An attacker can modify these queries very easily by modifying the string values in such a manner that this value passed is always true [19]. In this way an attacker enters into the database of an organization and can sneak or modify the data. After entering into the database the values can easily be modified by an attacker.

7) Proliferation of Botnets – A botnet is a collection of compromised computer in the network. [8]. **"**Compared with viruses and spam, botnets are growing at the faster rate "– Wenke Lee, Associate Professor at GTISC. In 2008 & 2009 botnets were the major cyber threats all along the organizations & were more destructive. While remaining on the machine it performs more malicious functions. Sometimes firewalls are not able to detect these bots as these are the normal traffic is regulated using the accepted ports. These bots are engaged in number of malicious activities such as –

a) Data Theft (Credit card numbers, Social security numbers etc)
b) Denial of Service attacks
c) Spam delivery
d) DNS server spoofing

According to a report compiled by Panda Labs, in 2Q 2008, 10 million bot computers were used to distribute spam and malware across the Internet each day [18]. Most botnet sites can be traced back to China. The targeted attacks are increasing day by day. In August 2010, Symantec reported that 95% of all spam is from botnet [40]. At its peak, the Mariposa botnet included more than one million members, including compromises in half of the Fortune 1000. Another alarming trend in the botnet space is the resurgence of previous attacks, which occurred recently with the large, spamming botnet, Kraken. The Kraken botnet, which at one point comprised about 650,000 members including 10 percent of the Fortune 500, [15] reemerged about a year after its takedown, bootstrapped by another botnet that acted as a malicious installation service. New threats such as identity laundering and reputation hijacking have appeared in the recent times.

8) Pervasive devices & Social Networking - Smartphones are the new computers. Mobile phones are becoming less expensive and more powerful day by day. The features & utilities provided by these phones are becoming more users friendly and more attractive. According to the survey over 4.5 billion users use a cell phone daily and this number is going to double or triple within the next 5 years [14]. As the mobile phones are becoming smart day by day the applications are also becoming more social & attractive. The privacy issue with these social networking sites is an issue. Security professionals are more concern about the security of these sites & the data available on these sites. Many of the accounts on these social networking sites are legal but illegal accounts also exist on these sites. Cyber criminals are becoming more active by "friending" or "following" the users which leads to malicious sites [15].

One key example of a social networking attack is the Koobface (Facebook inverted) worm that spread through social networking sites last year, attempting to steal users' personal information, redirect them to malicious sites and recruit their systems for use in botnets, among other insidious actions [15]. Another security issues pertaining to phones is that they offer so many different gateways of attacks, as the computer do. Attackers can take advantage of smartphone users through e-mail, Internet applications or through text messaging. Call fraud is also increasing day by day where the attackers are making fake calls to the users asking for their bank account details etc. Spoofing method is used in such process where it seems the legitimate original call. According to Robert Smith, CTO & co-founder of M.A.D partners – "Mobile phone stores are the greatest malware delivery system ever developed by man". Social Networking sites are more vulnerable. The more information you put, more vulnerable you become. Even you use more security settings; still the things can become vulnerable. Predators, hackers, business competitors, and

foreign state actors troll social networking sites looking for information or people to target for exploitation. In a three month period in 2010, Symantec said 65 percent of the malicious links it found on networking sites used shortened URLs. About 75 percent of such links were clicked 11 or more times, according to the report [41] [42]. Symantec also saw a rise in mobile device malware last year. There were 215 incidences, compared to 165 in 2009. But the security company acknowledges that compared to traditional computer threats, mobile threats are still relatively uncommon.

9) Mobile Threat Vectors - The mobile era is underway & year 2013 will find people more dependent on these devices to control their personal, professional & public lives. This over reliance on the device is encouraging attackers, as the people are putting their important & sensitive data on the risk. Privacy has become the major concern for these smartphone as the numbers of threats are emerging on Android & iOS. Theft & physical attacks are also increasing on these smartphones as the people are using more and more expensive mobile phones and tablets [16]. User initiated installation of malicious software is strongly addressed by the new mobile phone platforms. Today, even less expensive mobile phones are coming with Web browser, which can be exploited and leads to the vulnerability of the attacks. Major mobile applications run on browser, so more and more attacks launched against the mobile devices are Web based. Interestingly, security on mobile phones is not as strong as the desktop devices. Mobile devices generally do not receive frequent patches or updates as the computer does. The OS of mobile remains the same as it was installed at the time of manufacturing which gives attacker the advantage. Emerging threats to mobile devices will expand and develop more rapidly. In the current scenario data theft is major attack on the mobile devices. Threats targeting Android and iOS are on the rise. "The Zeus-in-the-Mobile (ZitMo) and several other examples of Android malware are acting more like traditional bots by communicating with a command-and-control (C2) architecture," says Ollmann, Vice President of research for Damballa [14]. The ZitMo attack targeted Android users in an attempt to defeat banking two-factor authentication, steal credentials, and ultimately money, from users' bank accounts. The Spitmo ("SpyEye in the Mobile") Trojan for Android appeared in September 2011 and also attacks dual authentication. It is a part of another large family of PC banking Trojans [43]. Comprised of blended techniques, this Trojan-based attack involves phishing, social engineering, intercepting SMS messages and sending authentication credentials to a remote server. Mobile devices will become major targets of the attacks in the near future.

10) Web Based Attacks – These attacks are related to Web applications. Before starting how these attacks work lets first discuss what the Web applications are. The web applications started with the static applications created using HTML. These were used to present the pictures or some static information generally in the form of email. But these web applications soon converted to the dynamic web pages or information as the need and requirement of the user changed. As a result web applications evolved to provide user conveniences such as searching, posting & uploading. Many web application development languages and frameworks emerged into the market like CGI, ASP.Net, J2EE, AJAX, Ruby on Rails etc [10]. As more and more application development started in web based software, security became the major concern for these applications.

Web based attacks are considered by security experts to be the greatest and oftentimes the least understood of all risks related to confidentiality, availability, and integrity [10]. In these attacks network or the host is the target of attack. Web based attacks focus on an application itself and operates on Layer 7(Application Layer) [44]. It is assumed that nearly 70% of these attacks are on Layer 7. Application vulnerabilities could provide the means for malicious end users to breach a system's protection mechanisms typically to take advantage or gain access to private information or system resources. Information gathered can include social security numbers, dates of birth, and maiden names, which are all often used in identity theft. The basic categories of application attacks are as follows [10] –

a) **Spoofing –** Act of mimicking another user or process to perform a task or retrieve information that is usually not allowed.

b) **Repudiation -** In order to tie specific actions of a single user, applications must have reasonable repudiation controls such as web access, authentication, and database transaction logs. Without collaborating logs, the online web application users could easily claim that they did not transfer equities from one acct to an external acct of another.

c) **Information Disclosure –** Large organizations maintain the personal information of their customer base. Information disclosure is the biggest threat where the attackers are capable of retrieving this private information of the user of the web site. This cause the confidence of the customer in that organization which leads to loss in sales, stock price and marketability.

d) **Denial of Service –** These attacks are likely the most well known of all application attacks, often generated by malicious users. Famous examples include attacks upon SCO a couple of years ago by individuals upset about lawsuits aimed at LINUX.

e) **Elevation of privileges –** Authorization control is the most basic requisite of any web application. Escalation of privileges requires a malicious user to either already possess or gain through unlawful methods authorization privileges of a regular user. Once this malicious user enters into the system it will spoof the information from the victim system.

Who is at the risk – All organizations which maintain the web applications and data are at the risk of such kind of attacks. These organizations are at risk of these attacks. The

level of attack can be different for each organization. There can be different factors which are important for determining these threat levels.

11) **Cryptographic attacks –** When important and sensitive information travels outside the trusted system, it should be encrypted. Even if we use the encryption, threats to confidentiality still exists. Two such threats are cryptographic attacks, or try to break the encryption code and the loss of private key in a public key cryptography. Cryptographic attacks are designed to subvert the security of cryptographic algorithms and they are used to attempt to decrypt data without prior access to a key [45]. Unencrypted data is called plaintext where as encrypted data is called cipher text. In these attacks this cipher text is tried to be broken by the attacker and tries to fetch the confidential data of the organization. There are six cryptographic attack methods [27] , which are –
    a. Plaintext Based attacks
        i. Known Plaintext
        ii. Chosen Plaintext
        iii. Adaptive Chosen Plaintext
    b. Ciphertext Based attacks
        i. Ciphertext only
        ii. Chosen Ciphertext
        iii. Adaptive Chosen Ciphertext

II.RELATED WORK - CONTROL MECHANISMS

If these attacks are not controlled the affect of these can be devastating. Many methodologies are there to control these attacks but no method is fool proof to control each & every type of attacks. Sometimes it depends on the threats and the organization that what safety mechanisms can be applied to control the particular threat. The different mechanisms to control different threats are –

a) The Wormhole attack in ad hoc network can be controlled by developing some strong and robust mechanism which can be applied for these attacks. The main objective of this approach can be [46] –

    a. To prevent eavesdropping
    b. To avoid packet modification
    c. Provide authentication & confidentiality.
    d. Reduce packet load
    e. Minimize computation.

    To achieve the above detection of malicious nodes and secure transmission is very important. The route on which the data is going to be transmitted is to be made secure. The Wormhole attack problem can be rectified by cryptographic approach i.e by implementing RSA algorithm.

b) Now-a-days one question arise in our mind is – "Is our Web application Secure". Basically this is the most difficult question to answer as the attackers can find one way or another to attack the web site of an organization [13]. Till now many control mechanisms have been developed for SQLIA, XSS & BOF. The details of these are –

a. **Defense Mechanism for SQL Injection Attack** – SQL Injection attack (SQLIA) is a method through which the attacker enters into the database of an organization quite easily. Through this method the attacker has the direct access to the databases. The different methods to control such attacks are Variable Normalization, Tokenization, Regular expression, SANIA etc. In the proposed method to detect SQL injection attacks by using the Query tokenization is the QueryParser method. When an attacker wants to perform the attack he uses space, single quotes or double dashes in his input. This method tokenizes original query and a query with injection, separately. After tokens are formed each query forms an array where every token becomes an element of the array. After this the length of the both array is compared. If the length of both the arrays is equal then there is no injection, otherwise there is an injection.

b. **Syntatic and Semantic Analysis for Automated Testing against SQL Injection –** This generates the attack request based on a syntactical analysis of the SQL queries generated by the web applications. This method is designed to be used by the web designer during the development & debugging phases. After capturing HTTP requests and SQL queries, it checks for any SQL injection vulnerabilities using the following three steps: An attacker can embed maliciously crafted strings that cause SQL injection attacks. To identify the vulnerable spots, a web application developer sends innocent HTTP requests to the web application. Second, it generates attack requests that attempt to exploit the vulnerable spots where SQL injection attacks may occur and By sending the attack requests generated from the second step, it checks if SQL injection vulnerabilities lie in a web application.

c. **Defense Mechanism for Cross Site Scripting (XSS) –** XSS attacks are easy to implement but very difficult to detect & prevent. Due to the breaches of web browser security, XSS enables the attackers to inject client-side script into the Web pages viewed by other users. Cross site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities as documented by Symantec in 2007 [47]. Cross site scripting is generally of two types – persistent & non-persistent. Non-persistent is most common of the two. This show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts to parse and display a page of results for and to that user,

without properly sanitizing the request. Persistent or stored XSS vulnerability is more devastating variant of the cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping [48]. The defense mechanisms for XSS can be –

i. Contextual output encoding/escaping
ii. Safely validating untrusted HTML input
iii. Cookie Security
iv. Disabling String

c) MAC spoofing protection – MAC address is a hardware address of NIC which is burnt into it at the time of manufacturing. MAC spoofing is computer identity theft, some good or bad reasons, and it is relatively easy. It refers to the changing the MAC addresses on the NIC. To prevent MAC address spoofing, one needs the knowledge of the two schemes involved in preventing MAC spoofing attacks. One scheme is to detect the spoofing while other is to harden the system & the access points. The quick way to detect suspected MAC address, run RARP (Reverse Address Resolution Protocol) against it. There are advantages of MAC spoofing in penetration testing.

d) Control Mechanisms for Social Networking Attacks – As new employee entering into the organization, social networking is no more a luxury it has become a necessity now. But organizations are not implementing all security measures for these social networking sites, which is leading to the attack on the organizational & personal data of an employee. You certainly need to implement and enforce an acceptable usage policy covering the use of social networking sites. As you say, it will help prevent data leaks and reduce the chances of a social networking-based attack from succeeding. Staff should get adequate training to implement policy related to social networking. It's an enterprise social networking security best practice to permit access only to social networking sites that have obvious business benefits and only to users with a business need to access them. When deciding which sites employees are allowed to access, you should take into account the sites' terms and conditions, as well as what they can do with user information and content. Web monitoring tools, such as Websense Inc.'s Web Security Gateway, or BlueCoat Systems Inc.'s ProxyAV line, can detect holes in your acceptable usage policy [49].

e) Defense Mechanisms for Cryptographic attacks – Defense mechanisms to control cryptographic attacks were by the classical ciphers where each character was replaced by another (plaintext ciphers), or transposition (shuffling the character) [26]. These are very easy to break but are no longer used now-a-days. These classical ciphers are least used or no more used. Another method to control these attacks are Stream Ciphers in which a random bit stream is generated, and then the XORing of this is done bit by bit by plaintext. This is also called a Vernan Cipher. This depends on both the sender and receiver having synchronised streams of both ciphertext, and the keys - packet loss would send the streams out of synch. A very large amount of work has been done on random stream generation; it's more difficult than it first appears.

f) Countermeasures for Mobile threats – First & foremost protection against these type of attack is security at the level of Operating System of the smartphone. Along with the basic operations like scheduling & process management, OS should also have the protocols to deal with the external applications & data without any risk. The central idea found in the mobile operating system is the idea of sandbox. As the smartphones are designed to deal with multiple mobile applications from many sources, the mechanisms should provide safe handling of this data. If any malicious data tries to enter into the device then vulnerable area should be kept as small as possible. iOS limits its API applications to its App Store whereas Android based phones are limited to Linux. Along with the OS security is security software which is installed in the smartphone [50]. Antivirus & firewalls can be deployed on the device to verify that it is not infected with the known malware or viruses. After this an smartphone are also checked for Network exchange to check whether they are capable of handling the network or not and also check the vulnerabilities in the network environment.

III.CONCLUSION

Wireless networking has become the integral part of an organization as this make an organization to work more efficiently & effectively but these have also open the doors for the attackers as these type of networks are more vulnerable and less secure. In today's scenario new devices are emerging daily with the capability of network communication. The cyber threats are increasing day by day and also at an alarming rate. These threats are effecting by capturing the important data from the organizations databases. If proper measures are taken by the organizations then these attacks can be minimized, if not avoided. The available control mechanisms if properly implemented can somehow control the effect of these cyber threats.

REFERENCES

1. Bocjj P. and McFarlane, L. (2002). "Online harassment: Towards a definition of cyber stalking." Prison Service Journal, number 139, pp. 31-38.
2. Sandeep Gutta (2008). "A New Distributed Framework for Cyber attack – Detection & Classification".

3. Gregory C. Wilshusen, Director (2012). "Cyber Security – Threats impacting the Nation", United States Government Accountability Office (GAO).
4. Shailendra Singh & Sanjay Silakari. (2009). "A survey of Cyber attack Detection System", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.
5. Hemraj Saini, Yerra Shankar Rao, T.C.Panda (2012). "Cyber Crimes & their Impact – A Review", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209.
6. D. Kaminsky, et. al., "Hack Proofing Your Network", Syngress, 2nd Edition, Mar. 2002. ISBN: 1928994709.
7. Natarajan Meghanathan, "A Tutorial on Network Security: Attacks and Controls".
8. Babu Lokesh, "Covert Botnet Implementation and Defense against Covert, Botnets", Utah State University, 5-1-2009.
9. Ashutosh Singh, "Social Networking for Botnet Command & Control".
10. Justin Crist (2007), "Web Based Attacks", SANS Institute InfoSec Reading Room.
11. Jie Gao (2007). Wireless LAN Security.
12. Edgar D Cardenas, 23 August 2003, "MAC Spoofing – An Introduction", Global Information Assurance Certification Paper.
13. D.R. Ingle and Dr. B. B. Meshram, "Attacks on Web Based Software and Modelling Defense Mechanisms", International Journal of UbiComp (IJU), Vol. 3. No. 3, July 2012.
14. Emerging Cyber threats Report 2012, Georgia Tech Cyber security Summit 2011.
15. Emerging Cyber threats Report 2011, Georgia Tech Cyber security Summit 2010.
16. Emerging Cyber threats Report 2009, Georgia Tech Cyber security Summit 2008.
17. Alexander Murphy, Audrey Pender, Louise Reilly *and* Siobhan Connel, "Denial of Service & Countermeasures"
18. http://www.darkreading.com/document.asp?doc_id=161524.
19. http://greendark-team.blogspot.in/2011/04/how-injection-attacks-work.html.
20. http://www.symantec.com/threatreport/.
21. http://www.csoonline.com/article/713033/mobile-apps-are-new-cyber-crime-attack-vector.
22. http://www.spslandforces.net/story.asp?id=165.
23. http://money.cnn.com/2007/09/17/technology/symantec_internetthreats/index.htm.
24. http://www.cloudmark.com/en/whitepapers/taxonomy-of-current-and-potential-mobile-threats.
25. http://www.ukessays.co.uk/essays/communications/ad-hoc-network-security.php.
26. http://www.pling.org.uk/cs/cry.html.
27. https://sites.google.com/a/pccare.vn/it/security-pages/cryptographic-attacks-and-countermeasures.
28. http://www.infosecurity-magazine.com/view/7410/comment-top-reasons-why-corporate-wifi-clients-connect-to-unauthorized-networks-
29. Parveen Dalal, Wireless Security: Some Measures, September 21, 2006.
30. C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002.
31. http://en.wikipedia.org/wiki/Wireless_ad_hoc_network
32. http://www.lsec.be/index.php/wiki/wireless_security/
33. Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks" Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93-B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.
34. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.
35. Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003. To appear.
36. Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005.
37. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. MobiCom, 2004.
38. http://www.ethermanage.com/ethernet/descript-troubleshoot.html
39. Jenny Coupe, "The Wireless LAN and Sarbanes – Oxley Compliance", An Airmegnet Technical Paper, 2005.
40. http://www.symantec.com/about/news/release/article.jsp?prid=20100824_01
41. John Wagley, "Social Media attacks on the Rise", 04-11-2011.
42. http://forum.worldstart.com/archive/index.php/t-153712.html
43. http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android
44. http://www.applicure.com/downloads/documentsV4.20/Web_Application_Security_101.pdf
45. http://www.giac.org/cissp-papers/57.pdf
46. Nisha S Raote, "Defending Warmhole attack in Wireless Ad hoc Network," IJCSES,Vol 2, No. 3, 2011.
47. Symantec Internet Security Threat Report Trends for July–December 07, Volume XIII, Published April 2008.
48. http://en.wikipedia.org/wiki/Cross-site_scripting.
49. http://searchsecurity.techtarget.com/answer/Social-networking-best-practices-for-preventing-social-network-malware.

50. http://mobile-security-software-review.toptenreviews.com/bitdefender-mobile-security-protect-your-smartphone.html.

Vikram Mangla, Associate Professor, Chitkara University, Punjab. I am having 14 years of teaching experience, out of which 7 years in current organization. He is a member of Computer Society of India. His interested area is Database management System & Computer Networks. Currently pursuing Ph.D from Punjab Technical University, Jallandhar. Email id – vikram.mangla@chitkara.edu.in

Dr. S.N. Panda, Professor & Principal, RIMT-IMCT, Mandi Gobindgarh, Punjab. Dr. Panda is having experience of nearly 20 years of teaching. He is having more than 45 research papers to his credit. Email id – panda.india@gmail.com.