International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

Estimation of Major Online Security Attacks and Solutions during Recent Years

Dr. C. P. Agrawal[1], Zeenat Hasan[2]
[1]Professor Computer Science & Application Department, MCNUJC, Bhopal, M.P., India
[2]Research Scholar Computer Science & Application Department, MCNUJC, Bhopal, M.P., India

Abstract**—** *Online transaction security has become more important to computer users, organizations, and the Businesses. With the expansion of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Many businesses secure themselves from the internet by means of firewalls and encryption mechanism. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. Knowing the attack methods, allows for the appropriate security to emerge. In this paper a survey is done upon various attacks over last five years in different countries.*

Keywords*- Denial of service, encryption**, intrusion detection systems, secure socket layer .*

I. BACKGROUND

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Online Transaction security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

II. COMMON INTERNET ATTACKS

All Common internet attack methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. They can also interfere with the system's intended function, such as viruses, worms and trojans. The other form of attack is when the system's resources are consumed uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name.

A. Eavesdropping

All Common internet attack methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. They can also interfere with the system's intended function, such as viruses, worms and trojans. The other form of attack is when the system's resources are consumed uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream [1]. Since eavesdropping activities do not affect the normal operation of network transmission, both the sender and the recipient can hardly notice that the data has been stolen, intercepted or defaced .

B. Viruses

Viruses are self- replication programs that use files to infect and propagate. Once a file is opened, the virus will activate within the system. A computer virus is software that affixes itself to another program like a spreadsheet or word document. While active, the virus attempts to reproduce and attach itself to other programs. This can tie up resources such as disk space and memory, causing problems on any home computer. An email virus is the latest type of computer virus that is transported through email messages and usually replicates by automatically distributing itself out to all contacts on the victims email address book.

C. Worms

A worm is similar to a virus because they both are self replicating, but the worm does not require a file to allow it to propagate [1]. There are two main types of worms, mass mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers. Network aware worms are a major problem for the Internet. A network aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

D. Trojans

A Trojan horse is a coded program which masks the existence of a virus or malware by making its appearance look normal while containing malicious utilities transparent to the

Dr. C. P. Agrawal and Zeenat Hasan, "Estimation of major online security attacks and solutions during recent years," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 13-17, 2016.

user; utilities that execute unnoticed in the background until it is too late.

E. *Phishing*

Phishing is a scam where fraudsters 'fish' for your personal details by using hoax emails claiming to be from financial institutions. This method continues to be favoured by online thieves. Hoax emails claiming to be from banks are often generated overseas, and are sent in bulk asking recipient to provide sensitive information such as their username, password, Customer Registration Number or Debit Cards / Credit Cards numbers and PINs by providing a link leading to a fake website, enabling thieves to gather the details for later fraudulent use.

F. IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IPspoofed packets cannot be eliminated.

G. Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [2]. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

III. Technologies for Online Transaction Security

If Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks.

1) Encryption

Using encryption methods one can prevent hacker listening onto the data because without the right key it will just be garbage to him. Different encryption method such as using HTTPS or SHTTP during the transmission of data between the client and user, will prevent Man in the middle attack (MIM), this will also prevent any sniffing of data and thus any eavesdropping. Using VPN will encrypt all the data going through the network, it will also improve the privacy of the user. Encryption also has downsides as all the encrypted mail and web pages are allowed through firewall they can also contain malware in them. Encrypting data takes processing power from the CPU. This in turn reduces the speed at which data can be send, the stronger the encryption the more time it takes [3].

2) Firewall

It is the most widely sold and available network security tool available in the market. This is the wall which stands between the local network and the internet and filters the traffic ad prevents most of the Network attacks. There are three different types of firewalls depending on filtering at the IP level, Packet Level or at the TCP or application level [4]. Firewalls help preventing unauthorized network traffic through an unsecured network to a private network. They can notify the user when an un-trusted Application is requested access to the internet. They also create a log of all the connections made to the system. These logs can be very harmful in case of any hacking attempts. Firewalls only work if they are correctly configured, if somebody makes a mistake while configuring the firewall, it may allow unauthorized to enter or leave the system. It takes certain knowledge and experience to correctly configure a firewall. If the firewall goes down one cannot connect to the network as in a case of DOS attacks. Firewall also reduces the speed of network performance as it examines both incoming and outgoing traffic. Firewall does not manage any internal traffic where most of the attacks come from. Many companies are under false assumptions, that by just using a firewall they are safe, but the truth is they are not, firewall can be easily be circumvented. The best thing while configuring firewall is to deny anything that is not allowed.

3) Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

4) Anti Malware Software and Scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called AntiMalware tools are used to detect them and cure an infected system.

5) Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity. It uses both asymmetric and symmetric keys encryption transfer data in a secure mode over a network. When SSL is used in a browser it establishes a secure connection between the browser and the server. It's like an encrypted tunnel in which the data can flow securely. Anyone listening on the network cannot decipher the data flowing in the tunnel. It provides integrity using hashing algorithms and confidentiality using encryption. The session begins with an asymmetric encryption. The server then sends the client its public key. After the asymmetric connection both the sides switches to a symmetric connection. Asymmetric algorithms are slow and use much more CPU power than symmetric ones. Even while symmetric encryption, CPU load is high, servers can only handle a fraction of connections as compared to servers with no encryption [5].

Dr. C. P. Agrawal and Zeenat Hasan, "Estimation of major online security attacks and solutions during recent years," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 13-17, 2016.

6) Secure HTTP (SHTTP)

It's an alternative to HTTPS, it has the same working as HTTPS and is designed to secure web pages and their messages. There are differences between SHTTP and SSL protocol such as SSl is a connection oriented protocol and it works it transport level by providing a secure tunnel for transmission whereas SHTTP works on application level and each message is encrypted separately, but secure tunnel is created. SSL can be used for secure TCP/IP protocols like FTP but SHTTP works only on HTTP. Its use is fairly limited as compared to HTTPS.

Secure Electronic Transaction (SET) is a specification designed to utilize technology for authenticating the parties involved in payment card purchases on any type of online network, including the Internet. SET was developed by Visa and MasterCard, with participation from leading technology companies, including Microsoft, IBM, RSA, Terisa Systems, and VeriSign. By using sophisticated cryptographic techniques, SET will make cyberspace a safer place for conducting business and is expected to boost consumer confidence in electronic commerce. SET focuses on maintaining confidentiality of information, ensuring message integrity, and authenticating the parties involved in a transaction. The significance of SET, over existing Internet security protocols, is found in the use of digital certificates. Digital certificates will be used to authenticate all the parties involved in a transaction. SET will provide those in the virtual world with the same level of trust and confidence a consumer has today when making a purchase at any of the 13 million Visa-acceptance locations in the physical world. Payments are the important factor of any transaction and Internet hardware/software vendors has put their efforts in concentrating the factor in secured way. Confidentiality of information is ensured by the use of message encryption; payment information integrity is ensured by the use of digital signatures; cardholder account authentication is ensured by the use of digital signatures and cardholder credentials, merchant authentication is ensured by the use of digital signatures and merchant credentials; and interoperability is ensured by the use of specific protocols and message formats.

7) Virtual Private Network (VPN)

VPN, is a way to transport traffic on an unsecured network. It uses a combination of encrypting, authentication and tunneling. There are many different types of methods of VPN but of these 5 are easily recognized. The most known and used protocols are as follows:

· Point-to-Point Tunneling Protocol (PPTP)
· Layer 2 Tunneling Protocol (L2TP)
· Internet Protocol Security (IPsec)

VPN allows a user to secure it privacy as it's very hard to correctly detect the location of the user as the network data may be routed through multiple locations spread across the world before finally reaching its destination. It also can be used to bypass firewall and blocks of websites [5].

8) E-Mail Security

As both the sender and receiver of the email one must be concerned about the sensitivity of the information in the mail, it being viewed by unauthorized users, being modified in the middle or in the storage. Email can be easily counterfeit therefore one must always authenticate its source. E-mail can also be used as a delivery mechanism for viruses. Cryptography as in many other fields plays a crucial role in email security. Emails are very unsecure. As they pass through many mail servers during transits they can be easily intercepted and modified. While using common Email there is no process to authenticate the sender and many users would not give a thought to authenticate the email received. There are many standards one can choose in order to secure his emails some of these are: PGP, PEM, Secure multipurpose Internet mail extension (MIME), Message Security Protocol (MSP).

TABLE I. Security attacks and suitable protection technologies.

Security issues	Attacks	Security Technologies
Authorization, Access Control	Denial of Service	SET,FireWall
Confidentiality	Eavesdropping,Phishing Dos,IP Spoofing	IDS, Firewall,Encryption,SSL
Non-repudiation	Man in Middle Attack	SET(Digital signature)
Integrity	Virus Worms Trojan Eavesdropping	IDS,Anti-Malware,Software

IV. Enhancing Online Transaction Security

One should remember following key point to perform secure transaction:

1. If the network is not properly secured- avoid online banking, shopping, entering credit card details, etc Check your online account frequently and make sure all listed transactions are valid
2. Never ever click on a suspicious link- Be extremely wary of e-mails asking for confidential information they could be phishing e-mails from fraudsters. Do not click on link given in a spam e-mail.
3. Always delete spam e-mails immediately and empty the trash box to prevent clicking on the same link accidentally.
4. Beware of lotteries- beware of lotteries that charge a fee prior to delivery of your prize. Do not respond to lottery messages or call on the numbers provided in the text messages.
5. Check if the website is secure- While using a credit card for making payments online, check it if website is secure as the CVV will also be required for online transactions, is printed on the reverse of credit card. Do not provide photocopies of both sides of the credit card to anyone. It can be misused by the fraudsters for online purchases.
6. Notify your bank/credit card issuer - if you do not receive the monthly credit card statement on time, if a credit card is misplaced or lost, immediately inform to your bank/ credit card issuer.
7. Do not share bank credentials in public or over phone.

V. Estimation of Major Online Security Attacks

1. As per "BBC news" Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers

Dr. C. P. Agrawal and Zeenat Hasan, "Estimation of major online security attacks and solutions during recent years," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 13-17, 2016.

increasingly conducted their financial affairs on the internet. The rise is due to increased use of computer malware and con-artists tricking consumers out of personal details. Overall losses on UK cards from fraud totaled £479m in 2014, up 6% on 2013, according to Financial Fraud Action. The figures also showed that losses caused by criminals using UK cards fraudulently abroad, where they can circumvent some security features, were up sharply. Losses increased to £150.3m in 2014, up 23% from the previous year [6].

2. According to "Business Standard" the increase in banking on mobile phones and the internet, financial frauds in the system have also seen an uptick, says a survey on financial frauds in the financial sector by Assocham and PwC. The report said that financial frauds led to approximately $20 billion (Rs 1.26 lakh crore) in direct losses annually. The report states that currently, 74 per cent of the population has mobile phones and this has led to a steady rise in banking on the go. According to Reserve Bank of India data, the volume of mobile banking transactions has risen from around Rs 1,819 crore in 2011–12 to approximately Rs 1,01,851 crore in 2014-15. Whether it's financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions [7].
3. As per "Business Insider India" report - consulting arm of Mahindra Group, suggests that the number of cyber crimes in the country is expected to double and cross the 3-lakh mark in 2015. As per the study, the cyber crimes are growing at a rate of 107% year on year while registering over 12,000 cases every month. According to the report, the number of cases of cyber crimes was 13,301 cases in the year 2011, which was followed by 22,060 such cases in 2012 and 71,780 cases in 2013. By May 2014 alone, the cyber cells in India had registered a whopping increase in cyber crime cases and registered 62,189 cases. The increasing use of mobile, smart phones, tablets for online banking and financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age groups, stated the report. The economic growth of any nation and its security whether internal or external and competiveness depends on how well is its Misuse of the ATM-cum-debit card had been a common problem for all. Often debit card users report fraudulent transactions have been made through their ATM cards even when the cards were in their possession [8].
4. Assocham-Mahindra SSG study has released a report stating the number of cyber crimes in India may double to 3 lakhs in 2015. India now being the favorite and easy to target for cybercriminals, mostly hackers, other malicious users could pose serious economic and national security challenges. India has been prone for all the identity theft, spamming, phishing and other types of fraud, as there is an upturn usage of Smart phones and tablets for online banking and other financial transactions in recent times. The Study also revealed that ―the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE‖ are the countries from where most of the cyber space attacks have been originated, which is a major concern. India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014. As per the study, Andhra Pradesh, Karnataka and Maharashtra are in top three positions in 2014 when it comes to the number of cyber crimes cases registered under the new IT Act in India. It further added, these three states together contribute more than 70 percent to India`s revenue from IT and IT related industries [9].
5. A report from PTI New Delhi shows that the increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. Rising at an alarming rate, the number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges. India has emerged as a favorite among cybercriminals, mostly hackers and other malicious users who use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud. As per the study's findings, total number of cyber crimes registered during 2013 and 2014 is 71,780 and 1, 49,254 respectively. The origin of these crimes is widely based abroad in countries like China, Pakistan, Bangladesh and Algeria, among others. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. Maximum number of offenders belong to the 18-30 age group, added the report. The study revealed that the attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE. It further stated that mobile frauds are an area of concern for companies as 35-40 per cent of financial transactions are done via mobile devices and this number is expected to grow to 55-60 per cent by 2015.Rising Internet penetration and online banking have made India a favorite among cybercriminals, who target online financial transactions using malicious software (malware). India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014, the study said. Andhra Pradesh, Karnataka and Maharashtra have seen the highest number of cyber crimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries [10].
6. According to a Lok Sabha reply on May 4, 2016, more than 8,000 websites were hacked in the first three months of 2016, and as many as 13,851 spamming violations were reported. Cyber security crimes, such as phishing, scanning, introducing malicious code, website intrusion and denial of service, rose 76 percent over the last five years, from 28, 127 in 2011 to 49,455 in 2015 [11].

VI. CONCLUSION

The survey shows that cyber crime remains a serious concern. Cybercrime affects millions every year, yet consumers still do not take action to protect. The constant

Dr. C. P. Agrawal and Zeenat Hasan, "Estimation of major online security attacks and solutions during recent years," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 13-17, 2016.

increase in cybercrime and its impact, it is important for organizations to identify the crown jewels that need to be protected. Enterprises need to carry out cyber risk assessment in depth to ensure that the right assets are adequately protected to limit impact of attacks. The online transaction security field may have to evolve more rapidly to deal with the threats further in the future. The internet is the medium for huge information and medium of communication around the world, it is necessary to take certain precautions while operating it. It is very important to educate every one and make them aware of cyber crimes and punishments –penalties for safe surfing and browsing, make them aware how to use and handle mobile and online banking, how to secure personal information, how to use various applications, what precautions has to be taken while doing online banking transactions. It is necessary to strong enforcement of cyber crimes rules and regulations.

REFERENCES

[1] O. Adeyinka, "Internet attack methods and internet security technology," *Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)*, pp. 77-82, 2008.

[2] G. A. Marin, "Network security basics," *Security & Privacy, IEEE*, vol. 3, issue 6, pp. 68-72, 2005.

[3] S. Alabady, "Design and implementation of a network security model for cooperative network," *International Arab Journal of e-Technology*, vol. 1, issue 2, pp. 26-36, 2009.

[4] B. Daya, Network security: History, importance, and future," University of Florida Department of Electrical and Computer Engineering, 2013. [Online].Available: 2013.http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[5] J. Tyson, How Virtual private networks work. [online]. Available: http://www.howstuffworks.com/vpn.htm

[6] Kevin Peachey (27 March 2015) [Online]. Available: http://www.bbc.com/news/business-32083781.

[7] B. S. Reporter, "Cyber frauds on rise with increase in digital banking," Assocham -PwC, Business Standard, July 10, 2015.

[8] P. Das, "Cyber crimes to surge in India likely to touch 3 lakh," Business Insider, 2015.

[9] Karthik, "Cyber crime to Double in India by 2015: A Report," world post, January 5, 2015.

[10] PTI New Delhi, "Cyber crimes in India likely to double Published," indianexpress, 2015.

[11] Indiatodaynews,[online].Available http://indiatoday.intoday.in/technology/story/as-net-use-spreads-cyber-crimes-up-19-times-over-10-years/1/683449.html