Traditional and New Security Challenges - A Suggestive Review on Safe Computing

Hyma Birudaraju[#1],V.Poorna Chander [#2] , N.Sukanya [#3]

Assistant professor [#1], Assistant professor [#2] , Assistant professor [#3]

Department of MCA
Guru Nanak Institutions Technical Campus,
A.P , India
[1]hymaomkaram@gmail.com
[2]poorimcaonline@gmail.com

Abstract— Network security has become an important aspect of day today life and for businesses. Breaching network security is often much easier than breaking physical and local security. Network security has become more vital to general users, organizations and also for military applications. With the arrival of the internet, security has became a major concern and the history of security substantiate an enhanced understanding and improvement in security technologies in a progressive way. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks but it does have issues to resolve. Combined use of IPv6 and security tools, such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property in the near future. The network security field may have to evolve more rapidly to deal with the threats and induced viruses and users must be equipped to combat at user level. This paper explores classical and new security threats and its vulnerabilities. The paper focuses on how to deal, plan and to incorporate counter measures. This would induce safety from impending threats and advise a choice of method to combat threats from attackers.

Keywords : security, Online , E-commerce, SME, trusted.

I.**INTRODUCTION**

A. *Traditional Security Issues*

In the 21st century the world has entered into a series of security challenges that go beyond the traditional dimensions of security. This security outline consists the architecture of the internet, when modified can reduce the possible attacks. Knowing the attack methods may permit the suitable security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms.

Non-traditional security issues move away from inter-state conflicts and geo-political concerns. They concentrate on non-military security concerns and comprise both states and non-state. non-traditional security issues that are mainly significant to human security. The so-called new security outline is often associated with the rhythm of globalization. Policy makers and practitioners have had to deal with matters such as human smuggling, cross-border crime and drug trafficking for so much of time. These issues have now been incorporated in a new security outline. Hence, rather than creating these new forms of insecurity, the forces of globalization have extended and accelerated their significance. In other words, the effects of globalization have considerably enlarged their spread and impact[4].

B *Current Security Issues*

In the current scenario the most important issue to be resolved is the security to ensure success of electronic commerce [1]. In the business, the usage of internet brought a revolutionary change in terms of low cost and wide availability of the access online. The following steps with the help of the online transactions can do the purchase of goods. For example, first, the merchant makes an offer for specific goods or services. Next, according to the offer, the customer may put forward the request online and then the customer proceeds to make a payment and finally the merchant delivers the goods or services to the customer. Here the payment can be through online banking, post office, and cash on delivery and so on. Many organizations are using the opportunities offered by e-commerce, and many more are expected to follow. Very good applications include online shopping, online banking , distance education and online games as shown in figure 1. Even though the E-commerce is well advanced still many businesses and customers are careful about participating in ecommerce as security concerns are often cited. This loss of trust on exchange online is being fuelled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse.

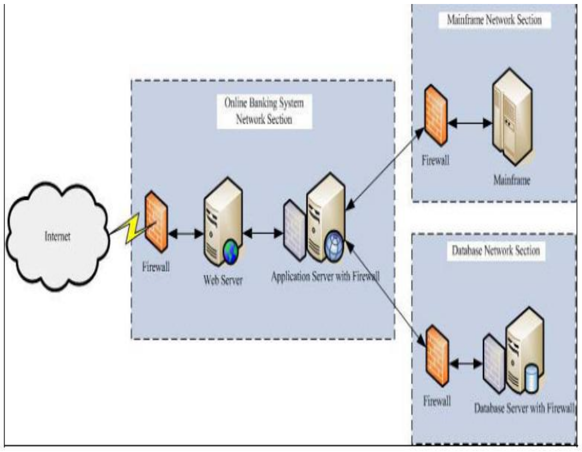
Mainframe Network Section
Online Banking System Network Section
Firewall
Mainframe
Internet
Firewall
Web Server
Application Server with Firewall
Database Network Section
Firewall
Database Server with Firewall

Fig. 1. General of online banking system

To provide security for online transactions we need to implement communication security. Communication security is the measure that controls and deny unauthorized person to derive information from telecommunication and ensure the authenticity of such telecommunication.

Communication security includes crypto security, transmission security, emission security, traffic-flow security and physical security of communication security equipment.

1.*Cryptosecurity*: The piece of communications security that results from the specification of technically sound cryptosystems and their proper use. This includes covering message confidentiality and authenticity.

2.*Emission security:* It is the resultant of the protection from all measures taken to reject unauthorized user access. This includes protection from interception and analysis of compromising emanations from crypto-equipment, automated information system and any telecommunications systems.

3.*Physicalsecurity*: It is the component of communications security that results from all physical measures necessary to preserve apparatus, material, and documents from access thereto or observation thereof by unauthorized persons.

4.*Transmissionsecurity*: It is a element of communications security that outcome from the application of actions designed to guard transmissions from interception and utilization. Network security controls and practices are older, but network traffic is not nagging past traditional controls, especially with the recent explosion of new mobile wireless and other IP-enabled devices

C. *Rise in need for security*

Most of the enterprise employees are looking to access corporate networks through Wi-Fi hotspots, both internally and externally with the rise of mobile enterprise applications and related trends such as the utilization of IT. The data leakage of these Wi-Fi hotspots depends mainly on an organization's strategy for network security. If organizations continue to trust on network security as a key control in the protection of their data, Wi-Fi is a potential possibility for data leakage, according to Matthew Lord, chief information security officer at IT-enabled business services firm Steria UK and he also said, “An attacker by trying a combination of user IDs and passwords until they gain access by just sitting in an organization’s car park and try to force their way into the network”.

If enterprises want to use Wi-Fi hotspots securely, they must follow two data leakage prevention strategies. It has to set up as an internet hotspot with no access to internal systems and use a well-built form of authentication such as client-side certificate authentication. In internal Wi-Fi hotspots there are separate corporate and guest networks. The corporate network has tight controls, including device authentication. However, corporate users could be attracted to switch to the guest network in which there are fewer or no controls, and that is where leakage could occur. The set up of guest network requires temporary credentials to enable connections for better practice. As SMEs do not commonly use VPNs they are typically at highest risk of data leakage through public Wi-Fi hotspots.

II. PUBLIC WI-FI HOTSPOT DANGERS

Public Wi-Fi hotspots, such as those provided by coffee shops hotels are usually unencrypted, in which all the data packets are opened and any wireless sniffer or rogue wireless access point can get all the traffic information . Hence, the data leakage prevention depends on how the mobile device is accessing the network and configured. Best thing for public hotspots can be moved to WPA2 to encrypt each session and for businesses to allow access to internal networks only through a virtual private network (VPN) client. This means a traffic sniffer would see a stream of encrypted data packets. This also put off traffic redirection and man-in-the middle attacks associated with web access over https.

Small and medium enterprises (SMEs) are typically at highest risk of data leakage through public Wi-Fi hotspots because they do not commonly use VPNs. SMEs open connections on the firewall to the mail server or a remote desktop protocol (RDP) server, and possibly don't really check the consistency. SMEs are a real problem prone and need to be educated and can be exhibited how much it is easy to penetrate the security wall.

If we have ad-hoc networking turned on, a malicious user may gain access to your system and steal your data or do pretty much anything else. Ad-hoc networking creates a direct computer-to-computer network that bypasses typical wireless infrastructure like a wireless router or access point. Turn off ad-hoc networking in Windows XP by going to your Wireless Network Connection's properties and make sure you have "Access point (infrastructure only)" as the one option selected for type of networks to access. Kenyon College has visual instructions for turning off ad-hoc wireless for Windows XP, Windows 7, Vista, and Mac operating systems.

A. *Security of 3G and 4G-based hotspots*

According to William Beer, rogue Wi-Fi hotspots are the major goal, although kits exist for setting up rogue base stations capable of intercepting 3G traffic. Wi-Fi is easier to target because of all the built-in safeguards in 3G, which require expertise that is more specific and advanced hardware to intercept, representing a lower return on investment. It is Best practice to use voice-over-IP (VoIP) instead, and run a peer-to-peer call manager software to encrypt the traffic, for mobile devices that support 3G, high- and Wi-Fi according to Jirasek. This facilitates all traffic to be encrypted over an entrusted network.

Another potential possibility of data leakage is the growing number of IP-enabled devices within the enterprise, including printers, CCTV cameras, point-of-sale systems, building access, and other control systems.

The fact that most devices can operate on an IP network, coupled with the fact that most corporations need to save money today. Inevitably means that there is an increasing use of the corporate network as a communications backbone for more than just file and print servers. In light of this fact and the need to block as many opportunities for data leakage as possible, organizations need to treat their internal networks as unreceptive and apply the right level of security on all networked devices.

"A good example would be to encrypt CCTV footage between the camera and the recorder or apply a hardened factory control server with a firewall on the network, rather than an unprotected workstation running system control software," said Steria's Lord. Again, the best practice is to separate different types of devices and apply different security controls accordingly. Another suggestion is not to put IP devices on the same domain or network as your computers.

B**.** *Network access requires careful management*

Although monitoring traffic is desired but when you make a cost/benefit analysis, it may seem excessive to do so. We need to make a judgment call based on the threat analysis whether it is worth putting these controls into some segments as mentioned by Jirasek. It would be very bad practice to have it all on the same network, but this is what small companies are doing. SMEs do not really have money to segregate the network.

Having anomaly detection protection which baselines the network traffic and looks at the patterns and identifies the anomalies. From a pure network traffic point of view it is best, but for the determined attacker you need to be prepared on the host. Therefore, we should tightly secure those users who are not having admin rights by some sort of protection against RAM-scraping malware, good anti-virus and anti-malware, the data classified and potentially segregated with access over some kind of Citrix session. Ideally, if the user has access to secrets inside the organization they should use a different PC for browsing the internet," said Jirasek. Complexity is the major challenge for large enterprises. Security vulnerabilities typically arise because of misconfigurations. It is not an issue of data sneaking past network controls, but of misconfiguration of those controls and a reluctance to fix known misconfigurations for fear of blocking business access to the network.

For large corporate and government networks, there needs to be a complementary proactive capability to build a picture of overall risk by identifying all network access. This enables organizations to reduce risk by blocking unnecessary access paths before there is a security incident. "Most organizations are amazed when we show them how many paths there are to their network that could be used for un authorized access," said Brazil.

FireMon, has said that, focus on rival configuration management systems by combining traditional operational capabilities with continuous risk monitoring and visibility, which includes the ability to identify and prioritize risk mediation tasks and model the knock-on effects of any network configuration changes. Many organizations are still relatively weak when it comes to continuous monitoring According to PwC's Beer, "I am always surprised to see how log data is not being used to pinpoint potential attacks”.

III SUGGESTED SOLUTIONS FOR SECURITY ISSUES.

A. *Educating users about security risks.*

Enterprises need to make sure that employees are conscious of the risks of using mobile devices to access corporate networks and data. There are a whole range of mobile device management suppliers, but enterprises need to do more around people and awareness because of the problem is often the user, who becomes the weakest link.

Even though most of the organizations have proper technologies, policies and awareness programs in place for desktop and laptop computers, it is often missing when it comes to smart phones and other mobile devices. The level of consciousness of the potential risks of IP-enabled devices is also comparatively low. As the number of these vulnerabilities is only going to increase. We need to raise the profile of unmanaged IP-enabled devices. E-commerce sites need to modify their security architecture to meet the demands of consumer ensuring consumer’s data privacy and that company resources are not used to attack other Internet sites. A business can surely continue to exist the hype generated if their network is used to attack another site. However, it certainly would not exist if that customer credit, purchase, or personal data is stolen or copied without their knowledge or permission by that site.

For example, an Internet music store CD Universe has broken by a hacker, and when the store refused to meet his demands then he published 3,00,000 customer credit card numbers which lead to most of the credit card users who are affected subsequently requested credit card companies to issue replacement cards. The ecommerce industry suffered a major setback in its effort to dispel consumer fears about security when it was revealed that CD Universe's site was open to hackers for a few hours before the attack was discovered [3]. It suffered another blow when the security investigation revealed that the security hole was well known and that a vendor patch was available to close the hole. The hacker could have easily mounted a data integrity attack on CD Universe's customer database instead of demanding a payment. The company was spared only by the impulse of the hacker [6].

Jim Seymour stated in a recent article on a problem entails a horrendous cost if the e-commerce site is always up and available. He claims e-commerce will not be crippled by the DDOS attacks. E-commerce as an overall business factor will not be crippled but individual e-commerce sites will be affected. Software developers need to plan software that is engineered for safety and security. It is still possible to add ease-of-use features but they should be initially turned off. Automated security updates are another characteristic that could be used to help in limiting the scope of these attacks. Microsoft released a patch that disabled some of the features of its Outlook/Exchange tool. This was most done to combat negative publicity of the company. Proper training programs for the system administrators are the easiest and most effective way to prevent major security compromises. The Audit group needs to evaluate the security methods to ensure their compliance with company policy and general Internet security standards.

B. *Do Not Allow Automatic Connections to Non-Preferred Networks*

When you are in the wireless network connection, disable the property of automatically connection to non-preferred networks. If the setting is enabled the problem is that your computer or mobile device may automatically (without even notifying you) connect to *any* available network, including rogue or bogus Wi-Fi networks designed only to attract unsuspecting data victims.

C**.** *Use of VPN*

VPN makes a secure tunnel over a public network, and therefore is a enormous way to stay safe when using a Wi-Fi hotspot. Use the VPN connection to access corporate resources, as well as create a secure browsing session when your company supplies you with VPN access.

1. Remote access solutions such as LogMeIn can also create a secure tunnel to a second computer at home, from which you can access files.
2. You can also use a free personal VPN service like Hotspot Shield, designed specifically to protect you when using an unsecured network.

D. *Beware of Physical Threats*

The hazard of using a public Wi-Fi hotspot is not restricted to fake networks, data intercepted, or someone hacking your computer. A security breach could be as simple as someone behind you seeing what sites you visit and what you type for example "shoulder surfing." Very busy public locations like airports or urban coffee shops also increase the risk of your laptop being stolen.

IV.CONCLUSION

The E-commerce industry is slowly dealing with security issues on their internal networks. There is guiding principles for securing systems and networks available for the ecommerce systems. In order to achieve this, the consumers need to be knowledgeable on security issues but it is still proven to be a critical element of the E-commerce security architecture. Trojan horse programs launched against client systems pose the greatest threat to E-commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in online transactions. These programs can be installed on a remote computer by means of email attachments. In order to train general people for security awareness on internet, orientation programs will become more critical. The traditional authentication mechanism is based on identity to provide security or access control methods. This paper has focused on traditional and new trends of mechanisms to safeguard the network traffic, which s would assist the readers to accrue knowledge to choose the best security option for his online tasks.

REFERENCES

[1]. Peng Xinying. Research on e-bunsiness security. *Gansu Science and technology*, 2009, **25(**2): 43-45.
[2]. Peter Keen. Ensuring E-Trust. ComputerWorld, 3/13/00 issue.
[3]. www.usatoday.com/life/cyber/tech/cth186.htm
[4]. “Lucrative mail theft on the rise”, RoanokeTimes reprint of LA Times article, 6/1/00.
[5] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,PP. 137-139.
[6] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005 .

Authors Biographies:

#1. Hyma Birudaraju working as an Assistant Professor in MCA Department for Guru Nanak Institutions Technical Campus, Hyderabad, She had 4 years of teaching Experience. She completed M. Tech(SE) through JNTUH, Kukatpally and MCA through Osmania University, Hyderabad. Her area of interest include Computer Programming languages, ,Advanced Data Structures, WebTechnologies, ,Mobile Application Development, Linux Programming and Computer Organization.

#2. V. Poorna Chander working as an Assistant Professor in MCA Department for Guru Nanak Institutions Technical Campus, Hyderabad, He had 6 years of teaching Experience. He completed M. Tech(CSE) through JNTUH, Kukatpally and MCA through Kakatiya University, Warangal. He has published six papers to his credit. His area of interest include Web Technologies, Network and Information Security, Data Mining and Software analysis and Design Engineering.

#3. N.Sukanya working as Assistant Professor in MCA Department for Guru Nanak Institutions Technical Campus, Hyderabad, She had 5 years of teaching Experience. She completed M. Tech Jand B.Tech from JNTUH University, Hyderabad. Her area of interest include Network Security,Advanced Data Structures, WebTechnologies, ,Mobile Application Development, Linux Programming, and Computer Organization.