THREATS POSED TO COMPUTING DEVICES ON NETWORKS AND THEIR POSSIBLE COUNTERMEASURES.

Abubakar Ibrahim

Computer Science Department
Umaru Ali shinkafi polytechnic, Sokoto
Email: abunbba@yahoo.com

ABSTRACT

Network security is a very sensitive issue that need to be given attention with the growing menace of cyber crime globally. This paper reviews the threat posed to computing devices on networks. Countermeasures as well as the technical, business, social and political consequences that stem from these threats are also highlighted. The future of network security was also highlighted. In these review different threats posed to the network that have negative impact has been identified and various defense mechanism were discussed. This paper found that businesses and government have been affected seriously by these network threats causing many business to lost millions pounds and reputation as well as preventing government to carry out its functions there by affecting that government politically. It has also heighted that many people social life has been negatively impacted as many people communicate through network. The future of network security is moving from biometric to an immune system that can act collectively to fight against any threats. Some recommendations for the way forward have been advanced.

INTRODUCTION

Over the past fifty decades Network has played a vital role in many aspects of our day to day activities. People and organizations such as business, health, and academic, transportation, political and military have benefitted immensely from network. Even with the benefit derived from the network, many people and their activities posing great threats to the network security and tend to undermine or completely damage this very important commodity. In the early days of network, network threat was not a real concern until by the year 2000 where many threats were posed to networks and made many organizations suffer a lot of damage, ranging from physical to business. With the current threat posed to network it has become imperative to protect this very important commodity since it has evolved to support almost all aspects of our daily life activities. The major threats posed to network are security threats.

According to Steward (2010, pp.111) network security should be a task of constant alertness because these network threats can be either within the organization from an unhappy employee or from outside hackers. As organization are trying to provide countermeasures and security control, also these criminals are trying to break these defence with their new tools they were developing to discover vulnerabilities and exploits to a network.

This report examines the threat posed to network and their countermeasure. The report will also discuss the technical, business, social and political consequences that emanate from the threat posed to network. Furthermore the report will also look at the future trends towards Network security.

LITERATURE REVIEW

Threats and attacks can occur on network and Computer system can be harmful to affect personal and organizational asset. Threat include any deliberate, malicious and unintended incidence to have negative effect to organizational asset and resources these asset can be software, hardware, database, file or the network at large (Newman, 2006). Furthermore Ikomi (2007) threat can become more complex because of difference in security architecture from verity of security suppliers with different type security design. More security vulnerabilities also rise from an online buying, selling and stretch corporate networks. In addition Gercek and Saleem (2005) Threats and security issues posed challenge to the large and small business, it's expected that in today's network setting is not all about connecting your computers on the network and internet, to avoid disappointment, time waste, profit lost and output. Vulnerabilities and solutions most also be of concern. Many threats occur on the internet due to its arrangement.

According Daya (2008).The possible attack spread across the network can be limited when the internet structural design is improve and better understanding of how possible an attack can occur on the internet has help many business organization to provide means to stay connected to the internet safely and protect themselves from possible threats by providing the necessary security measures.

Also, the growth in internet transactions has increased the number of internet crimes, due both to the ingenuity of internet criminals, but also to the lack of knowledge of internet users that participate in online transitions of how to

defend themselves. There is no secret that cyber-weapons are tools of the "modern war," so users of the internet should equip them self on how to deal with any attacks, preferably to prevent them but in case they happen, they should know how to mitigate them and to avoid future occurrence.
Cyber-crime can be seen as criminal activity using a computing devices on the network or internet to attack someone computer or network with a view to course damage financial or equipment, but it is also known as computer crime, technology crime, IT crime or digital crime.

Grabosky argues that internet crime is like an old wine in new bottles, suggesting that criminality has always been there, but now with the development of internet and performant computers it moved from offline area to online. (Grabosky, 2001)

From the various view it can be noted that security threat is a major problem pose to the network which can cause people, business both large and small to suffer financial and infrastructural damages as well as frustrations, time wastage and lack of Trust from customer and other business associate. Gercek and Saleem (2005) Network security is concern with the measure to protect the entire computers on the network and the network itself in the business environment from threats such as intrusion detection system, denial of service attacks, authenticity attack and eavesdropping. Meier *et al* (2006) define major terms that are concern with network threat and provide a clear picture of what they are.

- **Asset**: These are resource which includes information store in a database or on the files. Asset can also mean be all the hardware and software.
- **Threat**: Is any thin that can present potential occurrence of malicious or pose danger to recourses
- **Vulnerability**: Is an identify defect that expose system to attack
- **Attack (or exploit)**: The process of posing dander to an asset.
- **Countermeasure**: Is the security measure put in place to combat threat and correct risk

Threats Pose to Network and Countermeasures
Newman (2006) identifies variety of threats to a networking environment and ranks them as to the order of their effects on a networking environment these include Viruses, Worms, Trojan horse, denial of service, disclosure, Social engineering, phishing, brute force attack and eavesdropping. However, Daya (2008) and Meier *et a*l (2006) added that IP spoofing is also a threat to a network. Meier *et a*l (2006) went further to highlight another threat to network called Session Hijacking. Ting (2014) Distributed Denial of service (DDos), SQL injection and Cross site scripting are other threats to a network.

According to Daya, (2008) Different countermeasures were develop to combats threat posed to network which include cryptography, firewall, intrusion detection system, secure socket layer, anti malware software and scanners. Furthermore Kotkar *et al* (2013) said that countermeasures to computer network threat can secure computer and information store on its from attackers.

Viruses, Worms and Trojan horse Threats to Network and countermeasures

A virus is a computer program that can affect computer internal memory, disk and other program by replicating itself and move from one computer to another on a network. Virus accomplishes its task when triggered and executed by a specific event. The Computer virus causes harmful impact by destroying the computer's boot record, data and file allocation tables thereby causing serious problem to the computer and some of these viruses are very annoying by displaying unnecessary messages on the screen (Newman, 2006). In addition, Newman (2006) classify virus as follows: Boot sector, Macro, Multi part, polymorphic and stealth viruses.

None of the viruses mentioned above should be underrated because they can cause serious damage to your network.

Worms

Worms share some similarities with virus as they also replicate self. Unlike virus worms does not need to be triggered by any event, it can install self and course serious damage to a computer network by destroying data and other instructions. Email and internet are the delivery vehicles for worms which are very difficult to identify because they cannot be seen, you can only notice them when they begin to eat up your computer resources and slow down the operation of your computer system (Newman, 2006).

Trojan horse

A Trojan horse is different from virus and worms as it do not replicate self to infect other program. This kind of virus appear to be useful computer program obtained from a genuine owner but after you install them they become a delivery vehicle for destructive code. When Trojan horse is active it can be more problematic than virus and worms as it can delete file, damaging information, crash your system and also create unaware accesses for wicked users to remote control your system and at the same time can steal confidential information (Newman, 2006)

Countermeasures against Viruses, Worms and Trojan horse

if you run Microsoft Operating system make sure you have the latest version. Install Antivirus and it should be updated from time to time to deal with the latest viruses, worms and Trojan horse threats, and it should be able to scan e-mail and files as they are downloaded from the internet to prevent virus from entering your system. You also need to install firewalls and update your operating system. Using antivirus together with firewall both hardware and software will ensure better protection to your network (Newman, 2006).

Denial of service threats

Denial of service (DoD) attack makes system to become unavailable as the system consume all it resources and no more request can be responded to (Daya, 2008). In addition (Newman, 2006) Denial of service attack can occur by preventing lawful users from having access to the computer and network resources. These can occur as a result of sending unnecessary traffic to server on a network there by making the system unavailable to the legitimate user. This situation can be overall or brief blocked.

Below is a figure showing (DoD) where the attacker sends a ping request to all hosts and then all the hosts on the network will send traffic to the Victim.

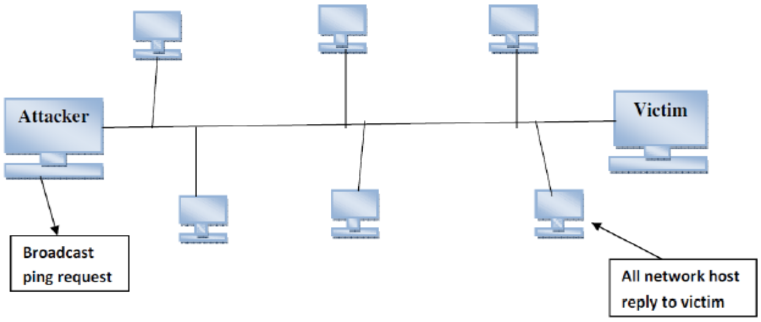


Figure:1 DoD threat (Kotkar *et al* 2013)

Countermeasures against Denial of service (DoS)
According to Karig and Lee (2001) DoS can occur at different level such as network device, Operating System, Applications and protocol level, each of which can be tackled at different ways.

- Patches and upgrade can be use to solved problem with software or bugs also router can be use to verify packet to hinder IP spoofing.
- Modifying protocol configuration can prevent attack.
- The use of intrusion detection system can dictate malicious activities based on its manners.
- System scanning software can be installed to scan the system for malware on the system that has been violated.
- Protocol with latest security features can be use to authenticate the legitimacy of users before using protocol that is vulnerable to DoS attack.

The figure below shows DoS attack at different levels and their countermeasures.

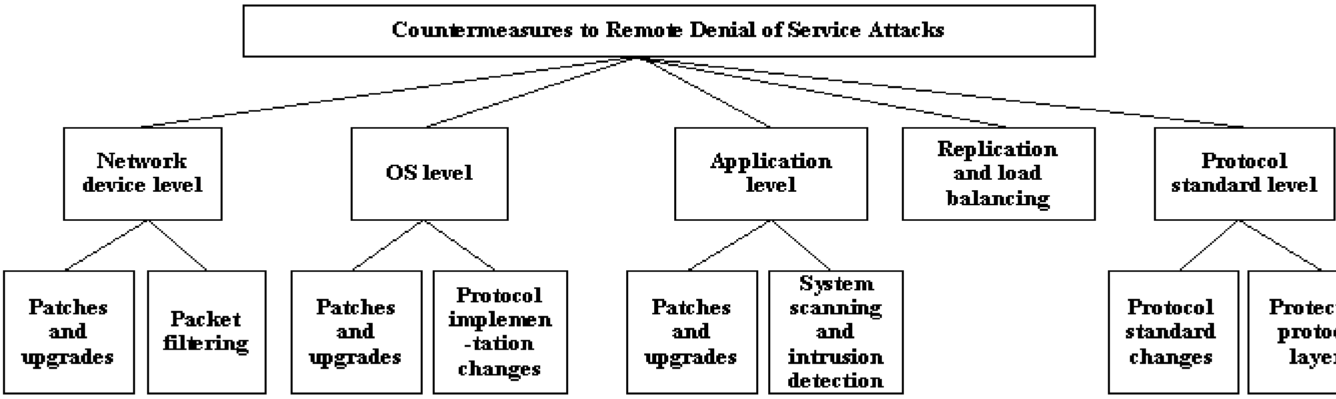

Countermeasures to Remote Denial of Service Attacks
Network device level
OS level
Application level
Replication and load balancing
Protocol standard level
Patches and upgrades
Packet filtering
Patches and upgrades
Protocol implemen -tation changes
Patches and upgrades
System scanning and intrusion detection
Protocol standard changes
Protec proto laye

Figure:2
Source: Karig, D. and Lee, R. (2001)

Disclosure threats

Disclosure some time called leak is a deliberate distribution of information kept on a network resources or in transit by authorised users to unauthorised persons without permission. The information can be personal or governmental and terrorists engage in this act to obtain important government information without trace and used it for future attacks and the technique used here is called sabotage or espionage (Newman, 2006).

Countermeasures against disclosure attack

Checking the user role before accessing any sensitive data which ensures that only authorize person can perform operations on the data. Access control list can be used to discover the access right on windows resources as well as encrypting important data maintained in database and configuration record (Meier *et al*, 2006).

Social engineering threats

Social engineering involves obtaining confidential network security information through nontechnical means such as stealing employee or technical personnel login detail that can be used to have access to the secure location. The people engage in this act are very smart and intelligent and always target new employee to enhance their success (Newman, 2006).

Countermeasures against social engineering

According to Newman (2006) Employee and users without skills and experience contribute much to the social engineering threats and to counter social engineering the following must be adhered to:

- Employee should have the basic training on the security of the environment such as knowing how to identify e-mail, dump trash to avoid dumpster and how to authenticate remote access.
- User or customer ID should be produced before any outside or inside technical support procedure is accepted. This verifies the legitimacy of the support person.
- Routers and firewalls should be used to check any outgoing and incoming packet
- Security strategy should be developed

Phishing threats

Phishers persuade users and obtain their personal information, such as bank detail or online baking information and other valuable data (Daya, 2008). Furthermore, Newman (2006) added that phishing is an activity carried out by the scammers to send fake e-mail to thousands of internet users and lure them into disclosing their personal and financial information to the attacker that can be used to commit crime. Most phishers target people using ebay, paypal, and online payment services.

Countermeasures against Phishing

Stay away from reading and supplying your personal information to an unexpected e-mail demand, which can be an attempt of phishing and even if you expect the e-mail verify from the customer care of the company to assure that the e-mail is authentic before given out your personal information (Newman, 2006).

Brute force attack threats

In brute force attack combination of passwords are used on computer to break password and secured information that has been protected by hashing and encryption (Meier, J.D. et al, 2006).

Countermeasures against Brute force attack

Woods (2009) said that there are many methods used to protect against brute force attack which include account lock, tar pitting, fake logging, Captcha and abandon password.

- Account Lock: this involves locking account in the database after certain number of attempts by the user
- Tarpitting: this can also be use to slow down attack by limiting the number of login attempt in a minute to prevent attacker try several attempt within minute
- Fake login: can also be use to direct the attacker to a fake page when login failed the will make the attacker tool to stop working as it successfully login to the fake page.

- CAPTCHA: this make automated login difficult as the attacker has to presume the username, password and captcha and it is very difficult to automatically break the captcha image generated by system for every login.
- Abandon password can also be used to combat brute force attack; these include security token, smart card, card space and credential exchange.

Eavesdropping threats

Involves listening of conversation on a network by attaching software or hardware on transmission medium such as satellite, wireless, and mobile users to capture data packet on transit from genuine users and then analyze the packet with the software and present the attacker with sensitive data such as password and username especially when the network send data in plaintext (Newman, 2006). The figure 1 below explained how an eavesdropper use a rogue wireless access point to launch an attack to his victim, the first thing he does is to set a fake wireless network once the victim is connect to the network and open application the attacker will provide him with fake credential through the HTTP and then the attacker can capture packet in plain text between the victim and other system (Hill, 2013).

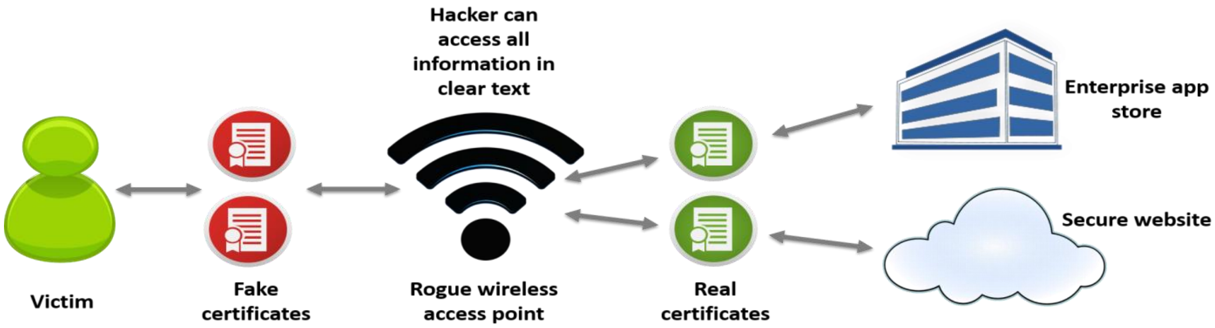

Hacker can access all information in clear text
Enterprise app store
Secure website
Victim
Fake certificates
Rogue wireless access point
Real certificates

Figure:3 1

Source: Hill (2013)

Countermeasures to Eavesdropping

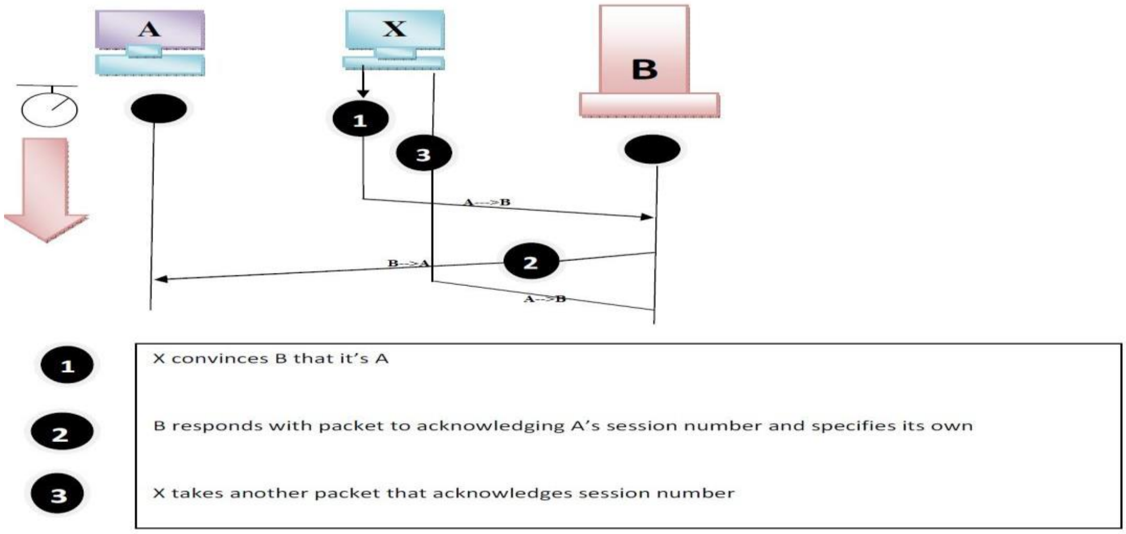
Meier *et al* (2006) said that the used of methods of authentication that do not allow transmission of password on the network and the used of encrypted communication (SSL) link will protect your password and data packet on transmission.

This will render the password or data packet captured by eavesdropper useless because it has been encrypted.

IP spoofing threats

Is the used of stolen or false IP address to gain access to a host as a lawful user of the host and once access is granted the attacker can change some settings and abuse the system (Meier *et al*, 2006). According to Kotkar *et al* (2013) the attacker capture a packet on transmission change the source IP with his own IP and pretend as the legitimate sender while having access to the computer he is not authorize.

Figure: 2 below describe IP spoofing.



1 X convinces B that it's A

2 B responds with packet to acknowledging A's session number and specifies its own

3 X takes another packet that acknowledges session number

Figure:4 2

Source: Kotkar *et al* (2013)

Countermeasures to IP Spoofing

Authentication and encryption are techniques that can be used to combat IP spoofing. IPv6 eliminate IP spoofing threats because it has a better authentication method for filtering package going in and out of the router. This can help to protect against IP spoofing (Kotkar *et al*, 2013)

Session hijacking threat

Session hijacking involves misleading a network device server or client machine into accepting an attacker host as the genuine host which will then give power to the attacker to control the network as it pretend to be genuine host (Meier *et al*, 2006). Furthermore, Kotkar *et al* (2013) added that it also involve obtaining session ID of the genuine user.

Below is a diagram showing the attacker using the session ID of his Victim.

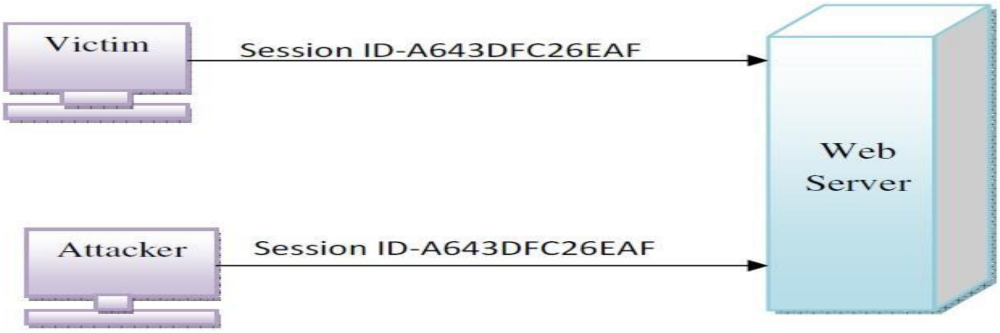


Figure: 5 session hijacking (Kotkar *et al.*, 2013)

Countermeasures to Session Hijacking

According to Meier *et al.*, (2006) the used of authentication cookies over HTTP link and using secure socket layer (SSL) to create communication channel can prevent session hijacking. The Session ending can also be used to enforce the next coming user to be verified before having access to the system. When you are not using SSL to allocate minimal amount of time to session cookie it will limit the time of the attack on the system. Furthermore Kotkar, A. et al (2013) said that changing logging ID after every session and encryption can also be considered.

Distributed Denial of service (DDoS) threats

Ting, (2014) Said that DDoS is an network threat where the attacker sends a command to small number of hosts called handler zombies, which then send to the larger number of hosts called agent zombies which in turn send fake request to target and causing the target to run out of memory or run slowly.

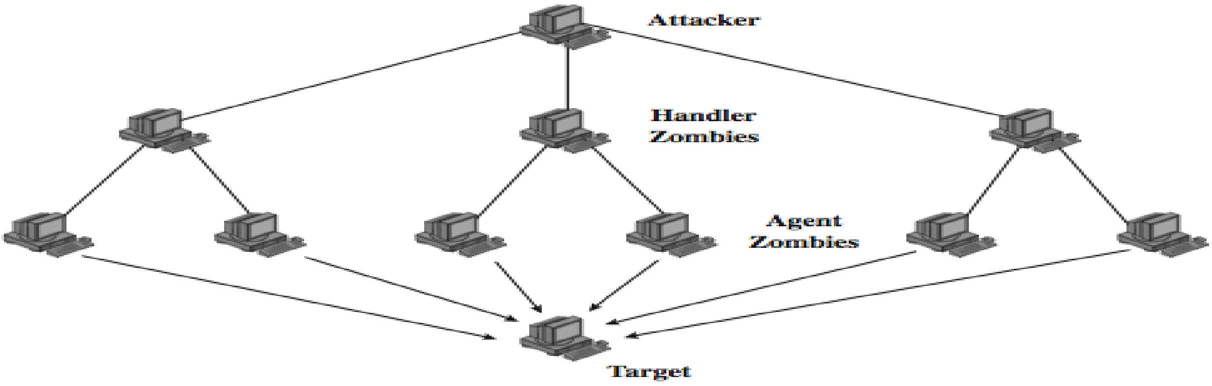


Figure 6: DDoS threats (Ting, 2014)

Countermeasures to DDoS

Ting (2014) heighted that avoiding your system from getting compromise will stop your system from involving in DDoS attacks.

SQL injection

According to Ting (2014) SQL injection attack requires only the SQL queries to hack a system without any tools needed and this kind of attack occurs on internet pages that have database at the backend through the text box of the web pages such as login and search boxes.

Countermeasures to SQL injection threats

According Meier *et al* (2006) Carrying out complete input confirmation before accepting any request and making sure that input request are not recognize as executable statement will counter SQL injection threats.

Cross side scripting (XSS) threats

this is an attack that can be carried out on a web page application by inserting a code script on a web page accessed by other users and the most common method of inserting this code is through the uniform resource locator (URL) Ting (2014). Below is scenario explaining XSS attack.

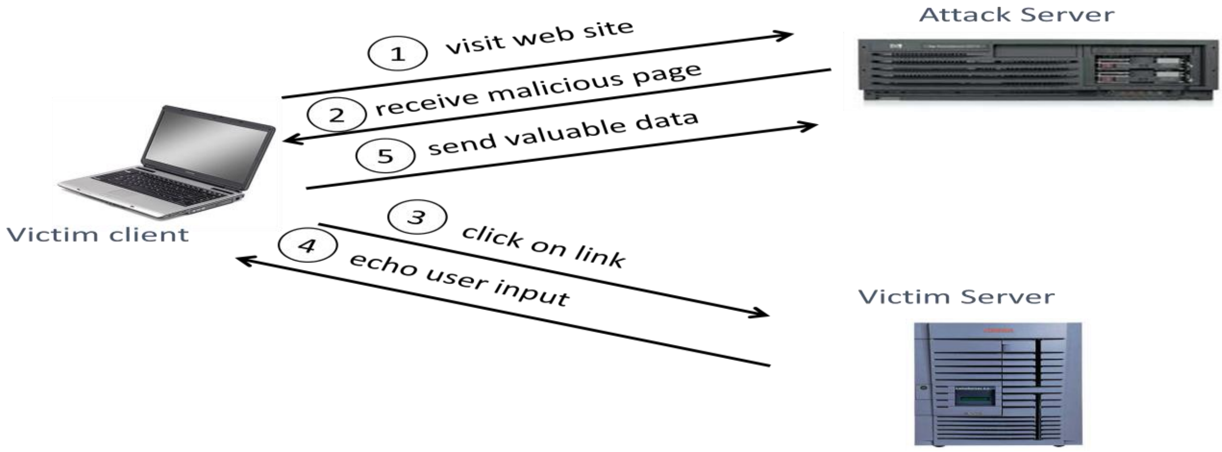


Figure 7: XSS threats (Ting, 2014)

Countermeasures to XSS

Conducting general input validation ensures the legitimacy of the input and the use of HTML Encode and URL Encode to encode any output request by the user can reduce the risk of XSS (Meier *et al,* 2006). Furthermore, Ting (2014) stated that to counter XSS attack script in browsers should be stop.

The Consequences of Networks Threat to Business, Social and Political

In this section the consequences of network threat to business, social and political is discussed.

Business Consequences from threat posed to network

Attack to networks causes a lot of damage to business which includes low business output, spending more time on customer care, system repairs and disruption of business. 4 out 10 companies suffered network threats that compromise their customers' data and this significantly impacted on the prospect of the company. Also 55% and 46% have their customers' data given away and suffer financial damages respectively. However, 6% of the companies in US have suffered financial damages worth 500,000 to 10 Million dollars while 8% of UK companies have suffered between 500,000 to 4 million pound (Paganini, 2013). In addition more than 1.8 million people have been affected by business lost to hacking in UK the lost is more than 2.7 billion pound a year (Curtis, 2012, in Ting 2014). British Broadcasting Corporation (BBC) (2010) in Ting (2014) reported that student attack paypal and cost them to lost 3.5 million pound.

GFI (no Date) said that many small and medium business have lost thousands of dollars as a result of data leakage, down time, and loss of reputation which made the companies to loss both existing and prospecting customers that drastically affect the company proceeds and prospect in general and some time it may lead some companies to face the law.

Social Consequences from threat posed to network
Attack on the network in this modern life will affect most part of the society as most of the present societies relied on technology and internet for providing basic services such as safety, security, effective deliverance of services. Today internet has become the driving force for communication within the society as well as providing means of conducting voting electronically and other process (CACI International Inc (CACI), 2010).

From the above it can be noted that attacking network can also affect many societies since many of them used internet to communicate through the social network, such as facebook, twitter, whatapp and linkin.

Political Consequences from threat posed to network
According to US Government Accountability Office (GAO), (2013) Threat to system that support federal operation has put sensitive data at risk, which in turn impacted on the governmental and military operations, these threats can lead to misused of government, private, and personal information GAO added that there is significant increase of 782% in attack to the government network. Furthermore Globalpost (2013) reported that cyber attack by the US on china has gear up political tension among the two countries. International Inc (CACI), (2010) reported that in 2007 Estonian government has suffered greatest cyber threat where its network infrastructures were attacked causing the government incapable of carrying some of its obligations as well as preventing some of its populace from conducting financial transition from the internet.

When looking at the CACI report and GAO critically this can cause serious political problem among these countries.

Future Trend of Network Security

The biometric technology that is currently used is not quite effective as it is not vigorously pursued because it has only slight differences with the older method of network security. The future of internet (network) security is possibly to build a system with immune against attack and it should be able to act as an immune system that can fight back against its enemies (Baya, 2008).

> According to Rendell, (2012) "In the very near future, security will be defined entirely in terms of "*who* should have access to *what*", with "who" and "what" woven into the fabric of the network as opposed to relying on applications to handle identity, as we do today. Simple really, but it is only now that the technologies and standards are coming to market to deliver this vision."

CONCLUSION

Network security threat is a buzzword nowadays many authors has agree with that this review addressed the most common network threats and their countermeasures as well as the technical, business, social and political consequences that stem from the menace of network threats. Many private organization both small and large, government and individual have suffered a lots of network security threats. So today's network setting should involve more than just having internet connectivity but also security of the organization infrastructures should also be considered to avoid millions of dollar lost and provide security to the information stored on our networks. The used of Antivirus, firewall, e-mail scanning software, Intrusion detection system, encryption, authentication and educating the staff of the organization are very critical for overall network security. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

RECOMMENDATIONS

- Network and computer security should be the first priority of any government and business that relay on the internet to carry out it functions.
- The security infrastructures put in place in any given organization should be well monitored to ensure that they are up-to-date.
- Government should set out security standard and monitor compliance to all organizations
- Government and business organizations should budget more funds to universities and security research institutions in other to come up with latest network security tools.

REFERENCES

Consolidated Analysis Canters, Inc (CACI) (2010) *Cyber* Threats to National Security. *cover at Symposium One: Countering Challenges to the Global Supply Chain,*[online]. [Accessed 4th june 2014] Available at: <http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf>

Daya, B. (2008) Network Security: History, Importance, and Future *University of Florida Department of Electrical and Computer Engineering* [online]. [Access 08 Feb 2014]. Available at: <http://www.alphawireless.co.za/wp-content/uploads/2013/01/Network-Security-article.pdf>

Gercek, G, & Saleem, N.(2005) Securing Small Business Computer Networks: An Examination of Primary Security Threats and Their Solutions. *Information Systems Security* [online], **14**(3), pp. 18-28 . [Accessed 28th May 2014] Available at:
http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=220a3f41-80c7-459d-a7dc-2172e30313d0%40sessionmgr114&hid=122

GFI (no date)Security threats: a guide for small and medium businesses. *White paper* [online]. [Access May 28th 2014]. Available at: <http://www.gfi.com/whitepapers/security_threats_SMBs.pdf>

Globalpost (2014) 16 disturbing things Snowden has taught us (so far) [online]. [Accessed 4th June 2014] Available at: <http://www.globalpost.com/dispatch/news/politics/130703/edward-snowden-leaks>

Government Accountability Office (2013) *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* [online]. [Access June 1st 2014]. Available at:<http://www.gao.gov/assets/660/652169.pdf>

Grabosky, P. N. (2001). Virtual criminality: old wine in new bottles? Social and Legal Studies, 10(2), 243-250.

Hill, G. (2013) *Eavesdropping on enterprise apps* [online]. [Access 28 June 2014]. Available at: <http://www.scmagazine.com/eavesdropping-on-enterprise-apps/article/316361/>

Kotkar, A., Nalawade, A., Gawas, S., Patwardhan, A. (2013) Network Attacks and Their Countermeasures. *International Journal of Innovative Research in Computer and Communication Engineering* [online]. **1**(1), pp.**85**-89 [Accessed 6th June 2014] Available at:
http://ijircce.com/upload/2013/march/14_Network%20Attacks.pdf

Meier, J.D., Mackman A., Dunner, M., Vasireddy, S., Escamilla, R. & Murukan, A. (2006) *Threats and Countermeasures* [online]. [Accessed 4th June 2014] Available at:< http://msdn.microsoft.com/en-us/library/ff648641.aspx>

Mohamed, A. (2007) A clearer picture of security threats. *Computer Weekly*. [online].pp. 30-35[Accessed 29th May 2014] Available at: <http://web.b.ebscohost.com/ehost/detail?sid=d54fb03b-aebf-46f7-a8130e1428f6f7cb%40sessionmgr110&vid=5&hid=117&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=cph&AN=27890863>

Paganini, P. (2013) *Webroot – Impact of Web-borne threats on businesses*.[online]. [Access 8th June 2014]. Available at: <http://securityaffairs.co/wordpress/13336/security/webroot-impact-of-web-borne-threats-on-businesses.html>

Rendell, J. (2012) *Comment: The Future of Network Security* [online]. [Accessed 8th June 2014] Available at:<http://www.infosecurity-magazine.com/view/24735/comment-the-future-of-network-security/>

Robert C. Newman. (2006) Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities:*3rd annual conference on Information security curriculum development* [online] New York, USA. [Access 08 Feb 2014]. Available at: <http://doi.acm.org/10.1145/1231047.1231064>

Stewart, M. (2010*) Network Security, Firewalls, and VPNs* [online]. Jones & Bartlett Learning [Accessed 8th June 2014] Available at:< http://proquestcombo.safaribooksonline.com/9780763791308>

Ting, J. (2014) *Internet and communication technologies*. Lecture 16: Hacking [online]. [Accessed 13th June 2014] Available at: <http://wolf.wlv.ac.uk/>

Ting, J. (2014) *Internet and communication technologies*. Lecture 15: Hacking and web security [online]. [Accessed 13th June 2014] Available at: <http://wolf.wlv.ac.uk/>

Woods, D.(2009) Brute Force Attack Countermeasuers [online]. [Accessed 6th June 2014] Available at: <http://www.haveyougotwoods.ca/2009/07/28/brute-force-attack-countermeasuers>

APPENDIX 1

The table below gives acronyms of the abbreviated words used in this report.

The lists of Acronyms used.

S/NO	ACRONYM	DEFINITIONS
1	IT	Information Technology
2.	OLTP	Online Transaction Processing
3.	OLAP	Online Analytical Processing
4	DSS	Decision Support System

Sources: from the largest database acronyms checker and abbreviation on the web, available at: http://www.acronyma.com

Reference to this paper should be made as follows: Abubakar Ibrahim, (2019) Threats posed to computing Devices on Networks and their Possible Countermeasures. *J. of Education and Leadership Development Vol. 11, No. 3, Pp. 61-84*

.