THREATS POSED TO COMPUTING DEVICES ON NETWORKS AND POSSIBLE COUNTERMEASURES.

Abubakar Ibrahim And Rilwanu Yusuf Gigane, Shehu Sidi Abubakar
Umaru Ali Shinkafi Polytechnic, Sokoto
abunbba@yahoo.com

ABSTRACT

The network has been playing a vital role in many aspects of lives such as security, health academics, etc it, therefore, requires attention due to the growing menace of cybercrime globally. This paper studied the threats posed to computing devices on network; Countermeasures as well as the technical consequences that stem from the threats. The work reviewed previous researches discussed different threats posed to networks and identified various defense mechanisms. The study found that businesses and governments have been affected seriously by network threats, causing loses and reputation. its also observed that no single countermeasure can absolutely solve the problems of network security. in addition,the network security is moving from biometric to an immune system that can act collectively in fighing any attack. Lastly, the research made some recommendations for the way forward.

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, academic, and military have benefitted immensely from the computer **network.** In spite of the benefit derived from the computer network, many people pose serious threats to network security and tend to undermine or completely damage the very important commodity. The growing dependence of computer networks in our private lives as well as in business and industry leads to the exposure to various threats (Joram *et al*.,2018) Due to the creation of new devices and skills, network attack is constantly in the increase and causing huge damage to a number of people and organization. Bendovshi (2015) in addition network security threats have for long time a concern to corporations and individual. Recently a number of high profile network attacks are real cause of financial and business damage as well as cause effect to the personnel relationship (Joram *et al*.,2018). In the early days, network threats was not a real concern until recently. Computer networks has became a momentous assets in any digitalize organization and protecting them from threats is becoming imperative (Sarala, 2016)

According to Steward (2010, pp.111) network security should be a task of constant alertness because the networks threats can be either within the organization from an unhappy employee or from outside hackers. As organizations are trying to provide countermeasures and security control, also these criminals are trying to break the defense with the new tools to discover vulnerabilities and exploit the network. The research tends to identify major security threats to the computer network and suggest how best the network can be secured, if the above is achieved there will be enabling environment for businesses to survive various attacks.

LITERATURE REVIEW

Threats and attacks can occur on network and Computer system which can be harmful to the personal and organizational asset. Threats can be deliberate, malicious and unintended incidence to have a negative effect on organizational resources like software, hardware, and databases (Newman, 2006). Ikomi (2007) is of the view that threat can become more complex because of difference in security architecture from variety of security suppliers with different types of security design. More security vulnerabilities also arise from an online transaction. Gercek and Saleem (2005) added that 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, waste of time, profit loss and output. Vulnerabilities and solutions most also are of concern. Many threats occur on the internet due to its arrangement.

According Daya (2008) revealed that the possible attack spread across the network can be limited when the internet structural design is improved and a better understanding of how possible an attack can occur on the internet has helped organizations to provide means to stay connected to the internet safely.

The explosive growths of the Internet facilitate cyber-crime which leads to a number of threats such as loss of private data and wearing down consumer trust in an online transactions (Upadhyaya, 2016). Acording to Jamal (2014) Cyber-crime are procedures adopted with intend to detour defence mechanisims of computing device on the network. In addition, Chloe (2017) said that in mainly through the Internet to attack someone's computer or network with a view to course financial loss.

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

From the various views, the security threat is major problems 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 another business associate.

Gercek and Saleem (2005) found that Network security is concerned 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 a*l (2006) defined major terms that are a concern with network threat and provided a clear picture of what they are.

- **Asset**: These are resources which include information stored in a database or on the files as well as hardware and software.
- **Threat**: Is anything that can present potential occurrence of malicious attacks or cause damage to resources
- **Vulnerability**: Is an identity defect that exposes the system to attack
- **Attack (or exploit)**: The process of posing danger to an asset.

Countermeasure: Is the security measure put in place to combat threat and corre

THREATS POSE TO NETWORK AND COUNTERMEASURES

Newman (2006) identifies a 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 IP spoofing threat. Meier *et a*l (2006) went further to highlight another threat to a network called Session Hijacking. Ting (2014) identified Distributed Denial of service (DDoS), SQL injection and Cross-site scripting as additional.

According to Daya, (2008) Different countermeasures were developed to combat the threat posed to network which includes cryptography, firewall, intrusion detection system, secure socket layer, anti-malware software, and scammers. Furthermore, Kotkar *et al* (2013) claimed that countermeasures to computer network threat can secure computer and information from attackers.

Denial of service threats

Denial of service (DoD) is the easiest attack on wireless network (Al-Sakib, (2016). Hence, the DoD attack makes the victims information unavailable as the system consume all its resources and no more request can be granted (Varga *el. al*, 2017) . Al-Sakib (2016) clearly stated that the aim of the DoD attack is to simply hinder communication between legitimate users on a wireless network through creating a rowdy atmosphere. 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.

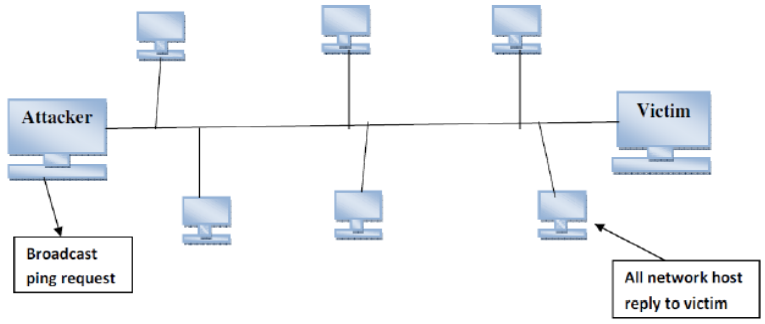

Figure:1 DoD threat (Kotkar *et al* 2013)

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 in different ways.

- Patches and upgrade can be used to solve the problem with software or bugs also router can be used to verify packet to hinder IP spoofing.
- Modifying protocol configuration can prevent the attack.
- The use of intrusion detection system can detect 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 used to authenticate the legitimacy of users before using a protocol that is vulnerable to DoS attack.

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

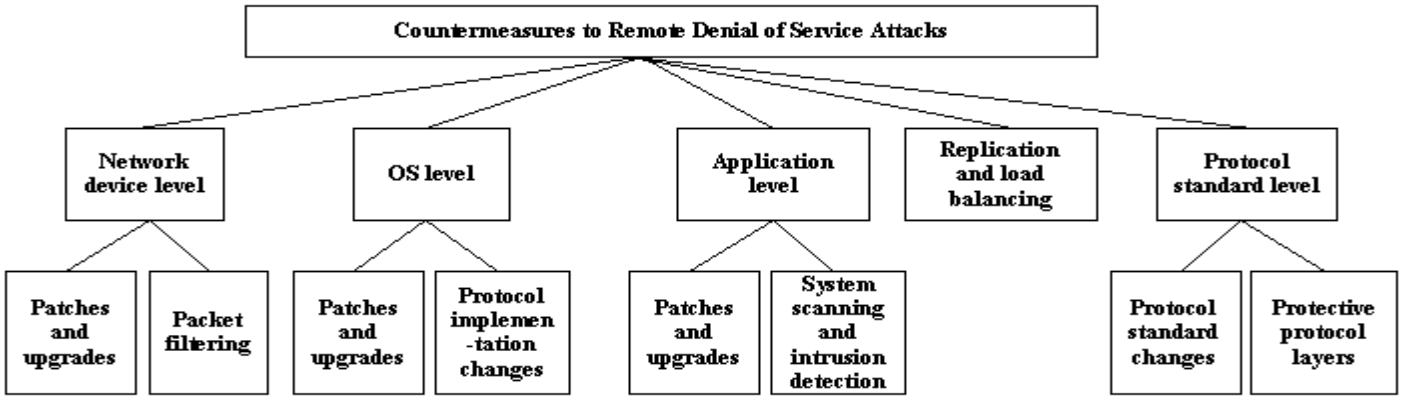

Figure:2
Source: Karig, D. and Lee, R. (2001)

Brute force attack threats

In brute force attack combination of passwords are used on a computer to break password and access information that has been protected by hashing and encryption (Meier, J.D. et al, 2006). It is also acerted that the brute force attack is an act in which the attacker made several guesses of victim's password, encrypted file among others until exact key is found and gain access to the ionformation (Bendovschi, 2017).

Countermeasures against Brute force attack

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

- Account Lock: this involves locking account in the database after a certain number of attempts by the user
- Tarpitting: this can also be used to slow down the attack by limiting the number of login attempts in a minute to prevent an attacker from several attempts within a minute
- Fake login: can also be used to direct the attacker to a fake page, when login failed the attacker's tool stopped working as it successfully log in to the fake page.
- CAPTCHA: this makes 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 the system for every login.
- Abandon password can also be used to combat brute force attack; these include a 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 sends data in plaintext (Newman, 2006). In addition, Varga *el. al*, (2017) rightly said that the eavesdropping an attack unless the eavesdropper alter the captured message and send it to ethier parties. The figure 1 below explained how an eavesdropper uses 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 connected 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 another system (Hill, 2013).

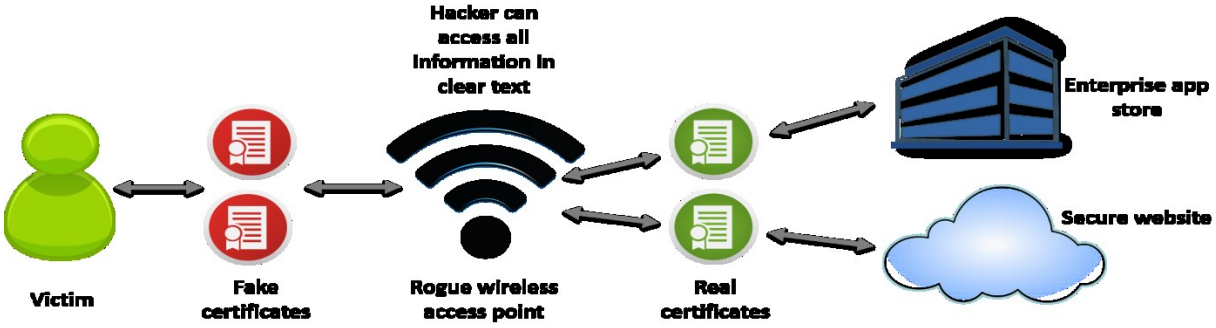

Figure:3 1

Source: Hill (2013)

Countermeasures to Eavesdropping

Meier *et al* (2006) said that the use of authentication method that does not allow transmission of password on the network and the use of encrypted communication (SSL) link will protect the password and data packet on the transmission which rendered the password or data packet been captured by eavesdropper useless. In addition, the physical protection the line of transmission could help to reduce the vulnerability (Al-Sakib, 2016).

IP spoofing threats

Is the use 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 unauthorized computer.

Figure: 2 below describe IP spoofing.

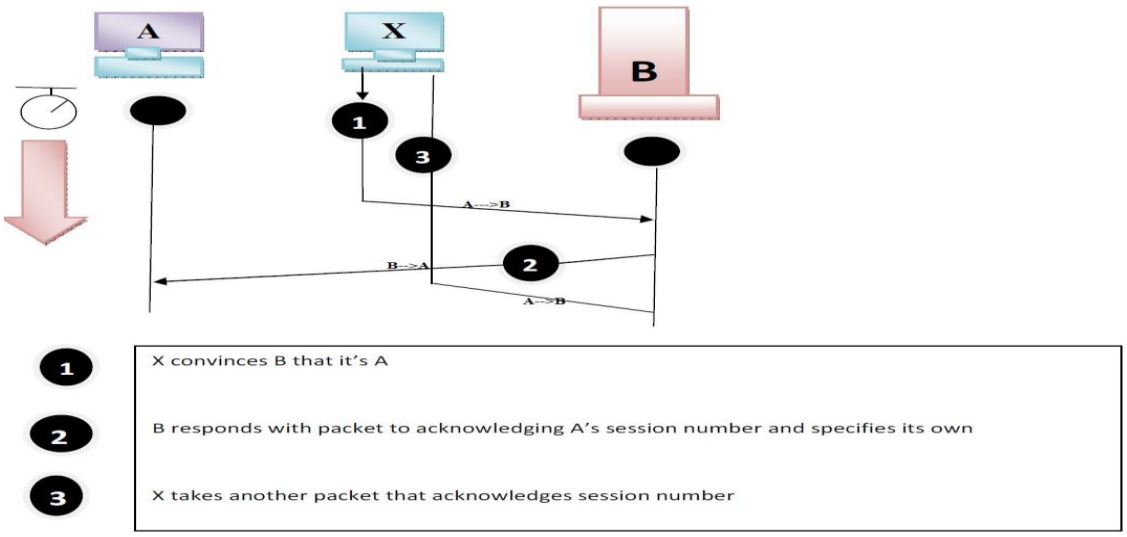

Figure:4 2

Source: Kotkar *et al* (2013)

Countermeasures to IP Spoofing

Authentication and encryption are techniques that can be used to combat IP spoofing. IPv6 eliminates 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)

Distributed Denial of service (DDoS) threats

Ting, (2014) Said that DDoS is a network threat where the attacker sends a command to a 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. The DDOS is also said to be an attack that alter/endanger the victim's information by sending several commands to flood the server, until it becomes unusable (Bendovschi, 2017).

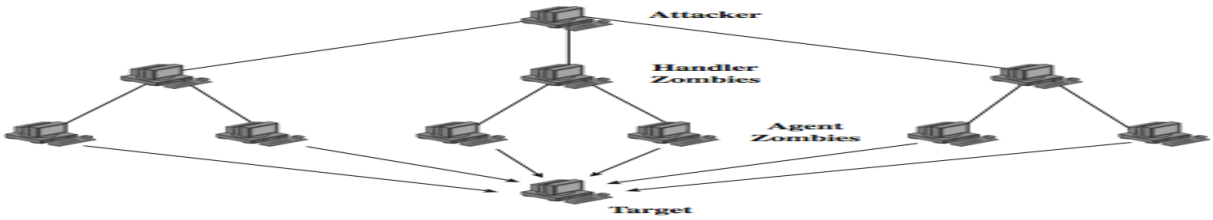

Figure 6: DDoS threats (Ting, 2014)

Countermeasures to DDoS

Ting (2014) highlighted that avoiding the system from getting compromise stopped the system from involving in DDoS attacks.

SQL injection

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 a database at the backend through the text box of the web pages such as login and search boxes (Ting, 2014).

Countermeasures to SQL injection threats

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

Cross site scripting (XSS) threats

The 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.

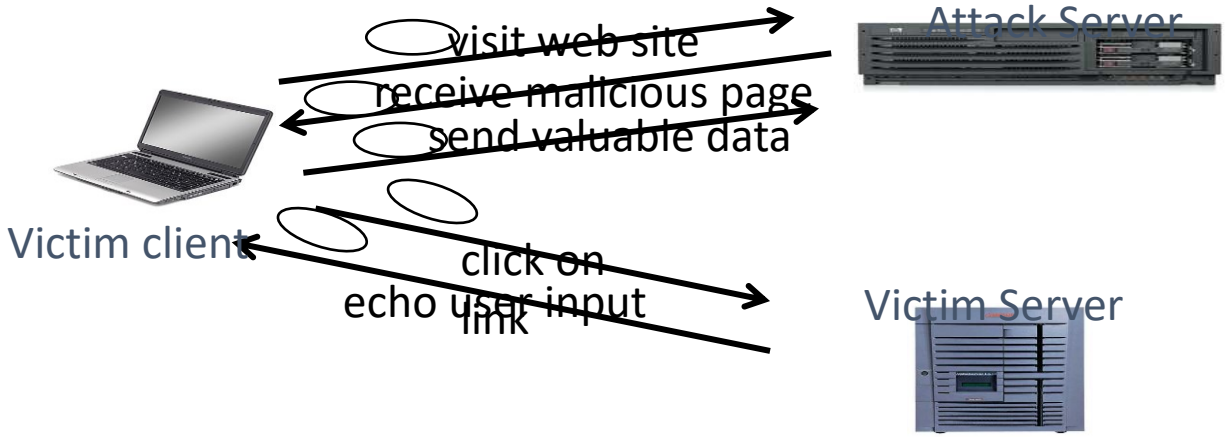

Figure 7: XSS threats (Ting, 2014)

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 stopped.

FINDING

From the finding of this work, it could be noted that there is no single effective countermeasures that could be put in place to combat the various network security threat, because these threats could come from various vulnerabilities and in different forms so is difficult to use one or two countermeasures to reduce the menace of the security threats.

The study found out that the use of intrusion detection system, account lock, tar pitting, fake logging, Captcha, antivirus and antimalware are among the best way to counter a number of network security threats but cannot solve all. Threats like social engineering, phishing, XSS and SQL injection cannot be prevented easily with these countermeasures.

The biometric identification 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. One of the best ways to counter network security threats is to train your staff on network security threats especially those that cannot be combated using nontechnical means like social engineering and phishing.

The review observed that the best way to counter network security problems is to be proactive by integrating the security measure into the structure of network design so as to prepare the system from any forms of security threat that might eventually occur as opposed to the depending on the application programs and security hardware to handle and control access to the network.

CONCLUSION

Network security threat is a buzz-phrase, nowadays. This review addressed the most common network threats and countermeasures as well as the technical consequences that stem from the menace of network threats. Many private organizations both small and large, governments and individuals have suffered a lot of network security challenges. So today's network setting should involve more than just having internet connectivity but also security of the organizational infrastructures should also be considered to avoid huge financial losses, equipment damage and to safeguard the information stored on the networks.

RECOMMENDATIONS

In bringing the way out to the lingering computer network threats the study put forward the following recommendations:

- ✓ The use of a combination of network security measure since one solution alone may not be helpful to a particular risk.
- ✓ Educating the end-users through regular awareness training on possible (new) threats and ways of fighting them.
- ✓ The periodic update of software and network operating system.
- ✓ The use of Routing Activity Theory (RAT) which prevent crime practices by increasing the risk of attackers being caught and reducing the rewards of offending.
- ✓ Finally, the protection of the computer network from attacks is achievable through YOU by doing the right thing at the right time.

REFERENCES

Al-Sakib. K. P. (2016). Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. francis group, Boca Raton Florida: CRC Press, retrieved from https://books.google.com.ng/books?hl=en&lr=&id=ZtBnZoijaDcC&oi=fnd&pg=PP1&ots=cMX8Epx1e9&sig=DlnFqykvFreny6otII-8w4pjeIE&redir_esc=y#v=onepage&q&f=false

Andreea, B. (2015. April) Cyber-Attacks – Trends, Patterns and Security Countermeasures. Paper presented at 7th *international conference on financial criminology* 13-14 April, 2015,Wadham College, Oxford, United Kingdom, Retrieved from https://www.sciencedirect.com/science/article/pii/S2212567115010771

Chloe, B. (2017) Why is cyber crime increasing? Retrieved from https://www.itgovernance.co.uk/blog/why-is-cyber-crime-increasing

Daya, B. (2008). Network Security: History, Importance, and Future. *University of Florida Department of Electrical and Computer Engineering,* retrieved from 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*, ***14***(3), 18-28. Retrieved from http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=220a3f41-80c7-459d-a7dc-2172e30313d0%40sessionmgr114&hid=122

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. *Scmagazine*, Retrieved from http://www.scmagazine.com/eavesdropping-on-enterprise-apps/article/316361

Jamal, R. (2014) A survey of Cyber Attack Detection Strategies. *International Journal of Security and Its Applications, 8(1), 247-256*. Doi:10.14257/ijsia.2014.8.1.23

Kotkar, A., Nalawade, A., Gawas, S., & Patwardhan, A. (2013). Network Attacks and Their Countermeasures. *International Journal of Innovative Research in Computer and Communication Engineering, 1*(1), 85-89 Retrieved from 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*. Retrieved from http://msdn.microsoft.com/en-us/library/ff648641.aspx

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,* Retrieved from http://doi.acm.org/10.1145/1231047.1231064

Sarala, R., & Zayaraz, G. V. (2016). *Optimal Selection of Security Countermeasures for Effective Information Security*. Proceedings of the International Conference on Soft Computing

Systems, Advances in Intelligent Systems and Computing 398, DOI 10.1007/978-81-322-2674-1_33

Sharwan, K. J., Shyam, P. J., William, M. H., & Madhav, S. (2018). COMPUTER IMPOSED COUNTERMEASURES DRIVEN BY MALWARE LINEAGE. Retrieved from https://patentimages.storage.googleapis.com/32/7f/5b/e334c889f45549/US9892261.pdf

Stewart, M. (2010*). Network Security, Firewalls, and VPNs*. Jones & Bartlett Learning. Retrieved from http://proquestcombo.safaribooksonline.com/9780763791308

Ting, J. (2014). *Internet and communication technologies*. Lecture 16: Hacking. Retrieved from http://wolf.wlv.ac.uk/>

Ting, J. (2014). *Internet and communication technologies*. Lecture 15: Hacking and web security. Retrieved from http://wolf.wlv.ac.uk/>

Upadyaya, R. (2016) Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. Doi: 10.1109/CCAA.2016.7813706

Varga. P., Sandor P. G. S., & Csaba H. (2017). *Security threats and issues in automation IoT.* IEEE 13th International Workshop on Factory Communication Systems (WFCS), retrieved from https://ieeexplore.ieee.org/abstract/document/7991968

Woods, D. (2009). Brute Force Attack Countermeasures. Retrieved from http://www.haveyougotwoods.ca/2009/07/28/brute-force-attack-countermeasuers