I J C T A, 9(3), 2016, pp. 1765-1773

Threat and Mitigation Awareness Based Upon a Model Network Scenario with BYOD Aspects

Lewis Meehan* and Carlene Campbell, Kapilan Radhakrishnan**

Abstract: This paper consists of research into BYOD networks and what security issues they represent to a company looking to implement such architecture. Following this will be the model scenario section, where a virtual model network was discussed to include security countermeasures that will not only help with BYOD security but with general network security as a whole, while also looking at a suitable security policy that could be applied alongside any countermeasures.

Keywords: BYOD; Security; Wireless; Security Policy.

1. INTRODUCTION

A bring your own device (BYOD) [1] network is a key security concern in any organisation. This is due to the lack of control a network administrator has over the devices connecting to the network or what software the user can use, whether connecting wirelessly or through conventional Ethernet. A number of security techniques can help mitigate the multitude of risks that emanate from BYOD networks. As well as actively mitigating risks, security policies can also be implemented to help to proactively lower risks from both internal and external sources.

2. SECURITY ASPECTS IN A "BRING YOUR OWN DEVICE"

When companies allow external devices to access their data and network, a range of security [2] issues are immediately apparent to any administrator. Devices that can access the company information need to be protected in all aspects, one of the most basic being physical security. Personal mobile phones and tablets are more susceptible to being stolen by thieves, rather than company desktops and servers. Once these devices are stolen, they can still maintain access to the company network and sensitive data displaying an extreme security breach to the network. The amount of user devices stolen each year is enormous, Bill Morrow of Quarri Technologies found that,

> *"64% of enterprise respondents reported that users" devices containing sensitive or proprietary data had been lost or stolen, but few had specific solutions in place to protect those devices.'*[3].

One of the only ways this can be combated is by employing configuration profiles for the BYOD network that allow devices to be remotely wiped or locked in the event of theft or losing the device. However, because of the freedom that a BYOD network allows this might not always be possible with the vast array of devices available to employees. Software might not always be available for this application

* BSc (Hons) Computer Networks School of Applied Computing, University of Wales Trinity Saint David Swansea, United Kingdom, *Email: meehanlj@live.co.uk*

** School of Applied Computing, University of Wales Trinity Saint David, Swansea, United Kingdom, *Email: Carlene.campbell@uwtsd.ac.uk, kapilan.radhakrishnan@uwtsd.ac.uk*

and could be dependent on the individual operating system or the specific device hardware, possibly making it an inadequate solution for commercial operation.

Devices are even vulnerable when they are being used legitimately. The network administrator does not have control over the end users antivirus or firewall settings, meaning devices that may be connecting to the network might have already infected with viruses along with harmful Trojans or worms while connected to other, unsecured networks and could distribute them into the corporate network. There is no way to avoid virus infection from other networks, but by implementing security policies that connecting devices must adhere to, you can deny connection to the network based on certain criteria, for example ensuring that all devices connecting are running up-to-date antivirus definitions and have run scans recently. However, yet again the problem lies with a lack of device control. Not all devices can adhere to the same security policy, as some (such as phones) might not have anti- virus available for download. Secondly, getting a device to virus scan every time it connects to the network is impractical due to the amount of time a virus scan can take to scan the whole device. Contrary to this, if the device is not scanned every time it initiates a connection it may have connected to another network and obtained a virus or harmful program. Whichever route is taken there still needs to be firewalls in place to protect the network from the BYOD addition as user devices will never be as secure as static, administratively controlled workstations.

Something not immediately thought of when introducing a typical BYOD wireless network is if the network resources can handle it, not only the possible extra users but also all the devices that they may connect. An excellent point made by Steve Mansfield-Devine, highlighted that employees do not just need a single connection to the BYOD, but need multiple. End users can be found to carry up to five devices that need to connect to the network at a single time, putting serious strain on network services [4]. Core IP services and other network resources can fall victim to resource exhaustion if the BYOD upgrade is not designed with this in mind. Everything from firewall inspection rates to wireless access point coverage needs to handle the greater number of connections.

A prevalent mitigation perspective, outlined in the IT Professional Journal highlights a possible change of path for BYOD networks,

> *"Of course, not all organizations let their employees use personal devices for company data, precisely because of these security and control issues. For example, close to a third of the respondents in the Aruba survey said their organizations have banned employees from connecting their personal devices to the company network."*[5].

This method of BYOD implementation eliminates the security risks of user owned devices entering the corporate network. In this particular instance, the BYOD traffic can have access to external networks while being kept separate to the sensitive business data. Separation can occur logically on the same physical architecture, or for a more secure option the networks can be physically separated and use completely different network equipment. However, separating the BYOD network either physically or logically could be seen to defeat the primary advantages of implementing BYOD. This point can be proven by looking at data from Niharika et al. who, found that the second most prevalent advantage of BYOD networks is the increased productivity [6].

3. RESEARCH MODEL SCENARIO

The scenario is based upon a basic network for a small to medium business that has a mission critical network that includes a BYOD aspect. The original model network (shown in fig. 1) was not designed with any security measures. No security within a corporate network is especially concerning due to the number of malicious or unintentional attacks that can occur. Not only did the original network not have any dedicated security devices but also no security implemented within any architecture on the network. The aim of this

model scenario is to upgrade the network to a reasonable standpoint so that it can resist basic attacks and have a base on which it can expand its security.

3.1. Assumptions

When designing the updated model network assumptions were made about particular aspects of their business and future aspirations, as not all information would be known. These assumptions are stated below:

- Networking is a key area that the company wishes to expand to keep up with the increasing business demands. Therefore, they are willing to spend money to upgrade equipment and introduce redundancy in all aspects of their architecture.

3.2. Attack Mitigation techniques

3.2.1. Network design security

When designing or upgrading a network for enhanced security, network resilience and reliability is also a crucial aspect. This brings to mind redundancy [7] or backups that allow the network to perform under failure, either from a malicious security based attack or from a non-malicious network issue. Firstly, to achieve optimum performance from the network, the original collapse core design needed to be changed to a fully hierarchal structure, with clear-cut core, distribution and access layers. With this expansion (fig. 2), the network design changes into a more typical hierarchical topology and a network design such as this allows for greater traffic management as well as increased redundancy.

The network design now includes redundant links and devices within both the access and distribution layers of the network. These give network traffic an alternate route to the destination if a link or network device becomes unavailable. Redundancy within the distribution and access layers prevents a single point of failure, allowing the network to keep intra- network communications operational in the event of hardware failure. In order to manage these redundant links, the per- VLAN spanning tree protocol (PVSTP) was introduced concurrently so that links may be dynamically brought up or down to keep an active link to the core layer, without introducing switching loops. By manually setting the PVSTP priority on the core layer three switches, PVSTP always keeps a single path available to the network gateway, therefore allowing internet access even after re-convergence.

Pulling away from the aspect of redundancy and looking more at one of the more vulnerable sides of the network, the BYOD wireless changes, brought about WPA2 [8] passwords for devices to connect. This gives a first line of defence against filtering unwanted users connecting to the network and only authorised employees can connect devices once they know the passcode. Along with this, the access point (AP) does not broadcast the service set identifier (SSID). For devices to connect to this hidden SSID they must first know the exact SSID spelling, as well as the password for connecting. A setup like this provides basic security for the wireless and is a key method for deterring attack methods like war driving [9].

A major advantage of modelling networks can also be one of the biggest disadvantages. Physical security cannot be represented within any modelling software but it is an integral part of network design when considering security. Although it cannot be represented, devices must be kept accessible by only authorised personnel, in a controlled environment to keep temperatures, humidity and power at the correct levels. Key card doors and locked network racks should be standard practice in any corporate network environment.

The last and main addition to the network for its design is the Cisco 5505 Adaptive Security Appliance (ASA) firewall. A standalone firewall device is much better at handling the traffic and can have more security features than a conventional software firewall. The placement of the ASA allows it to sit in- line with network traffic and inspect all traffic originating from and destined for external networks. The ASA treats the external networks as unsecure and only permits traffic based upon a zone firewall structure as

well as a context-based access control (CBAC) firewall for TCP established connections. Apart from the basic configuration settings, which include passwords and usernames, an access control list (ACL) [10] has been configured to allow the gateway router to access the authentication, authorisation and accounting (AAA) server without inspection, both of which are discussed in more detail later in this document. Finally, the global inspection policy has been changed to allow ICMP echo reply packets to enter the network from the outside interface. By adding this to the global inspection policy on the ASA, it allows device pings destined for external networks to re-enter the network and show up as a reply on the local device.

3.2.2. Virtual Security

When adding security within a network we are looking to manage, control and protect the traffic traversing the network. We can do this, not only physically but also virtually. Virtual local area networks (VLANs) can split a large network into multiple segments in order to manage and secure them. The model design has various departments as well as a BYOD network, VLANs are implemented accordingly. As the VLANs separate the traffic into logically separate networks, each one needs its own IP addressing scheme in order to communicate using layer three information in the correct manner. Variable length subnet mask (VLSM) subletting is introduced to provide an efficient addressing scheme for each VLAN. In this particular case, the /27 address is used for each department and the /25 is used for the whole BYOD network, by using a bigger block or subnet means there is scope or capacity for increase when a larger number of devices are connecting. This help to mitigate resource exhaustion as highlighted in the BYOD research by Steve Mansfield-Devine [4].

Using VLANs is an effective way of logical separation in both layer two and three connections. However, this means that if a device should make a connection to a device on another VLAN, then it would be unable to do so. Inter-VLAN routing would solves this problem by routing packets in between their respective VLANs in the core of the network. After implementation, the various departments are able to communicate through the core layer three switch, employing a router-on-a-stick method to do so. At a glance, this seems like a nonsensical idea, but it gives control, for traffic management and is explained later in this paper.

3.2.3. Configuration security

The first line of defence when it comes to configuring network hardware is hardening. Device hardening can consist of multiple techniques but only the following were included in this network.

Autosecure is a Cisco proprietary command set that is available on specific routers and switches. Within the modelling software, only the gateway router and the core layer three switch have the capability to use the Autosecure feature and after running through the interactive menus, the router and switch both employ security countermeasures pre-set by Cisco. The feature makes an extensive list of changes depending on the user input and the model of device, aiming to create a basic configuration for a network administrator to add more specific security measure to the configuration in the future.

Although included within the Autosecure feature, passwords were configured on devices before performing any commands. Administrators can use a local username and password if external authentication fails or if the device does not support external authentication, as in the case of the access and distribution switches. The local logins in the higher-level network devices automatically block attempts if they exceed a threshold of three incorrect tries within 30 seconds. This mitigates brute force password attacks and improves general password security. To accompany the local login credentials, password encryption is also enabled on all devices. Even if an attacker can force a configuration dump from the device, the passwords will be in the encrypted format and be unreadable. This can also stop possible internal attacks as nobody else can see the plain text password if looking at an administrators screen or configuration file.

An aspect in which security should be disabled or strictly controlled is remote access. Control should be enforced by two main factors; authentication via a one-time password or by public/private keys with strong passphrases. In-band management for the network devices can be completely disabled in order to protect against password attacks and remote reconfiguration. An option to keep security while enabling in-band management is to use SSH [9] instead of telnet. SSH encrypts all management traffic so that packets cannot be seen if they are intercepted while traversing the network.

AAA [12] is a framework for server based security and auditing for network devices. A combination AAA and dynamic host configuration protocol (DHCP) [13] server connected to the core layer three switch houses the username and password database that allows authorised devices to challenge user login attempts against them, using the encrypted TACACS+ protocol. The higher-level devices that have the

TACACS + ability access the server and allow administrators to use a central username and password to login. On a successful login, the server communicates the level of access the user is allowed on the device, as well as the device communicating back auditing information. The server holds the auditing information so administrators can see successful and unsuccessful login attempts and by using the auditing information, they can track malicious attempts and act accordingly.

Improving security further down the network hierarchy, focuses on access layer switches. The access switches in which employees might have access to should have all their unused ports disabled to prevent extra devices accessing the network. As well as this, active ports have been configured with port security that dynamically links to the connected devices mac address on switch start up and shuts down the interface if the countermeasure is violated.

From a management perspective, devices still need to provide lawful statements to authorised and unauthorised network administration connections, in order to back up their acceptable use policy and lawfully allow them to pursue unauthorised access attempts. On the devices a message of the day (MOTD) banner has been configured, to display an administrator defined message to all global connections.

As discussed earlier, inter-VLAN [14] routing appears to defeat the objective of VLANs, however when combined with ACLs they provide greater control over the network traffic. ACLs have been deployed

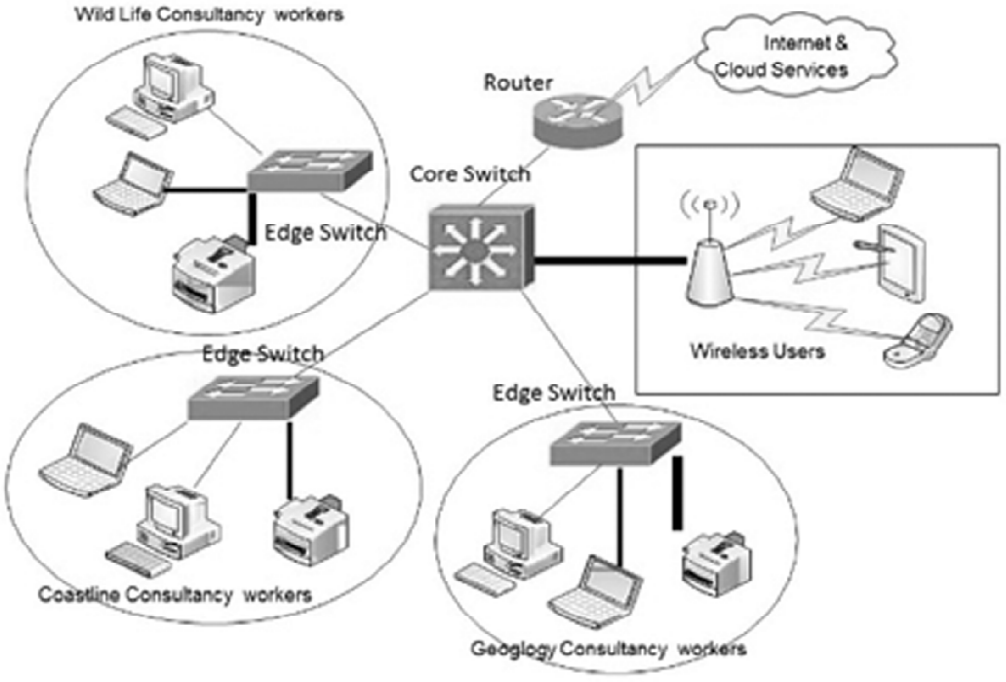

Figure 1: Original Network Model

upon both the gateway router and core layer three switch. The ACLs configured upon the gateway provide some basic protection against un-routable IP addresses from entering the outside interface, protecting from certain types of routing attacks. The layer three switch uses ACLs also, in this case to block all BYOD VLAN traffic from accessing any other network apart from the internet. This totally segments the BYOD network from the rest of the business devices and provides a major increase in security. As well as this, the BYOD network is only allowed to access the server for DHCP addressing purposes, as all other connections are refused. This limits the uncontrolled wireless to only the resources and access it requires, in order to increase general network security. Network access layer, as it does not allow the specified BPDU ports to perform STP.

4. FUTURE RECOMMENDATIONS

Not all security solutions could be deployed within the models. If repeating the model upgrade a second time it would be wise to make a few security additions. For this instance, the current gateway provides a single point of failure within the network and could be mitigated with the use of multiple internet service providers (ISPs), alongside another gateway device. This could have been coupled with the hot standby routing protocol available on the layer three switch to provide complete redundancy to the internet.

A feature that is not available within the devices used in the model is the bridge protocol data unit (BPDU) guard. This will help prevent spanning tree protocol (STP) attacks at the network access layer, as it does not allow the specified BPDU ports to perform STP. AAA could also be expanded to include BYOD

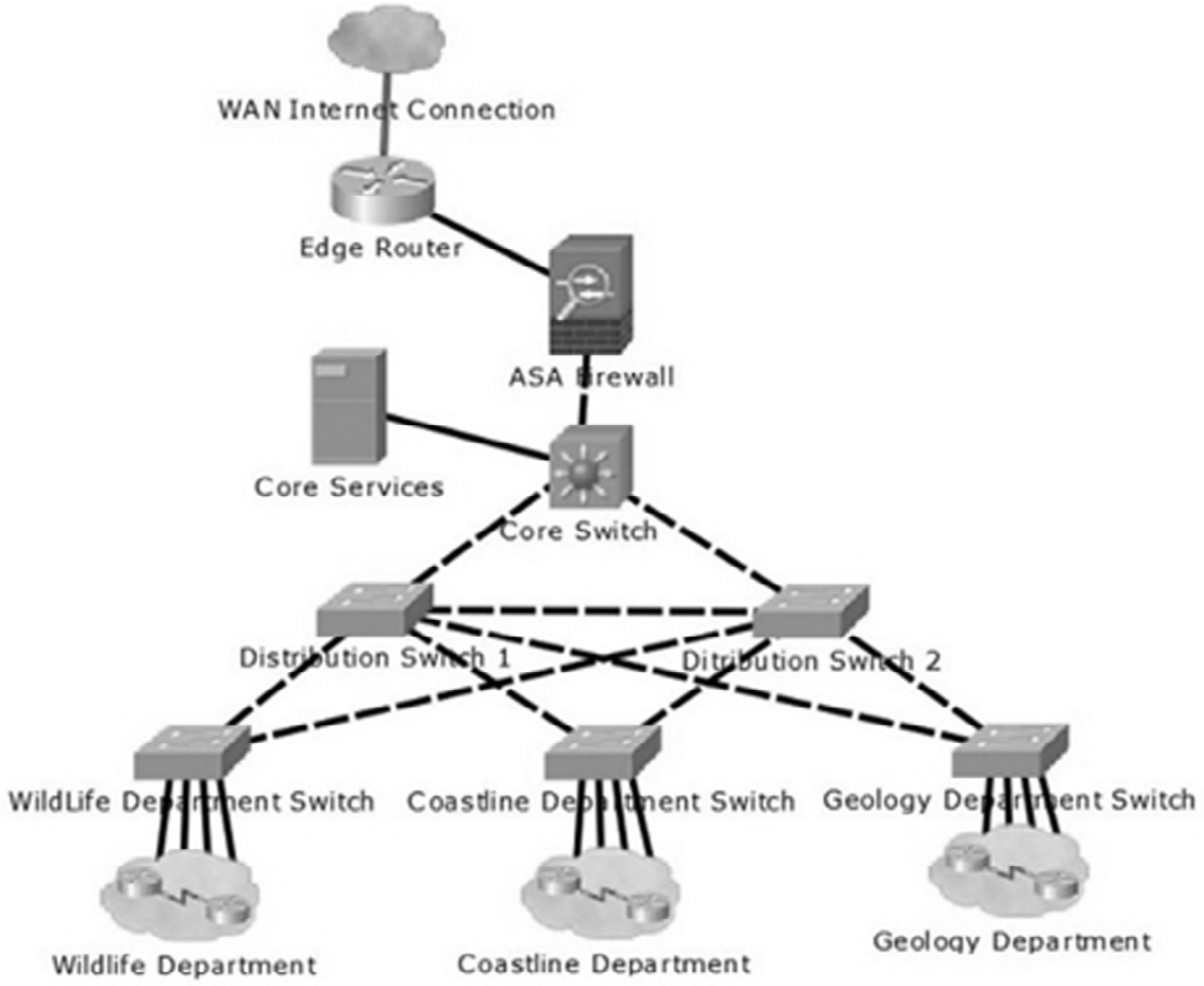

Figure 2: Upgraded Network Model

login credentials [15]. This could provide another layer of security for the BYOD network; however, it would require administrative overhead to teach users how to connect using this framework. Finally, an apparent issue is shown in the model, the single connection point to the server creating a single point of failure. However, if the server or its link were to fail then all devices would still communicate using their leased DHCP address for 24 hours and AAA framework would resort to the local account logins. If this were to be changed, a backup server or redundant link could be introduced, although is not necessary.

5. SECURITY PLOCIES

In order for employees to understand what they can and cannot do regarding to computer security, there needs to be a set of rules that they can abide by. These rules are generally published in the form of an acceptable use policy (AUP) of some kind, to which all employees have access and are encouraged to read. This creates a framework for the company upon which they can base disciplinary procedures and technology best practises for employees. Outlined below is a only a small example of a general security AUP for the modelled company network as AUPs can often span a vast number of pages and cover details in depth.

5.1. Security Acceptable Use Policy

5.1.1. Overview and Scope

This proposed security acceptable use policy (AUP) is to mitigate security issues, regardless of intention or accidental. It provides a framework to which all employees of the proposed company network are advised to adhere to and is in effect throughout all affiliated aspects associated with the company. Breach of this AUP leaves the employee/employee's that are involved with said breach, vulnerable to disciplinary action after investigation.

This AUP is applicable to all information technology related interaction, be it internet, intranet or extranet related systems, wireless access or hardware devices, including any third party or temporary systems being used. It covers all use of information, data, network resources, employee conduct and third party conduct, regarding the applicable systems.

The policy is active to protect both the employee and the company regarding electronic equipment and data. It applies to every employee, contractor, guest and temporary employee

5.1.2. Policy Statements

- All data associated with, held in or traversing the network, remains the property of company. This data must comply also with the Data Protection Act 1998 [16] and is the employee's duty to ensure this happens upon their interaction with said data.
- Employees have a duty to report any suspicious digital activity to management and expected to use good judgment when doing so.
- When interacting with computer systems regarding work at the company, employees must exercise a high level of security regarding sensitive information, company data and any logon credentials they have access to. Employees must also only ever use their own credentials that are assigned to them. Use of other logons is considered a serious security breach.
- Personal devices connecting to the BYOD network must be password protected and locked when not in use. Loss or theft of the device must be report to management immediately.
- Devices connecting to the BYOD network must have approved up-to-date security software installed and running. Any attempt to knowingly transmit malicious or unauthorised files across the network is breach of this policy.

- Accessing external data such as webpages or email is allowed but extreme caution on the employees part is expected. Harmful files can be unwillingly downloaded from unknown websites or emails and can occur without the knowledge of the user. For this reason, opening emails from unknown senders or websites that are not commonly accessed are prohibited.
- Employees must always use the information technology systems with security on their mind, as network security is the job of every employee. No employee must participate in malicious activity regardless of intent and must not participate in fraudulent or illegal activities.
- Using network management tools is strictly forbidden unless authorised and any attempt to scan or access network devices will result in disciplinary action.

5.1.3. Compliance

Employee's compliance to this policy will be checked by the means of auditing, business reports and feedback. Any exceptions to the policy must be confirmed with the policy director and logged accordingly. Failure to comply could result in relevant disciplinary action being taken against employees.

6. CONCLUSION

Introducing BYOD on a network is a risk factor for any company. However, by implementing various security procedures along with a high quality security policy it is possible to lower the level of risk. Complete segmentation from the company network is the best option for BYOD security, although less drastic options are available.

The models outline various security measures and an example policy that can accompany them to provide a layered approach to increasing security in any network, including onewith a BYOD aspect. In this scenario, virtual segmentation of the BYOD is present, similar to the segmentation mentioned in the research [5]. It is also imperative that companies have a security policy to outline security measures and acceptable use to the employees, as not all threats are malicious or necessarily from an external source.

References

[1] A. Sedigh, C. Campbell, and K. Radhakrishnan, "BYOT Network Solutions for Enterprise Environment," *2014 UKSim-AMSS 16th International Conference on Computer Modelling and Simulation*, pp. 489-493, 2014.

[2] A. Sedigh, K. Radhakrishnan, C. E. Campbell, and D. Singh, "Trust Evaluation of the Current Security Measures Against Key Network Attacks," vol. 2, no. 4.

[3] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989. [1] B. Morrow, "BYOD security challenges: control and protect your most sensitive data," Network Security, vol. 2012, no. 12, pp. 5-8, Dec. 2012.

[4] S. Mansfield-Devine, "Interview: BYOD and the enterprise network," Computer Fraud & Security, vol. 2012, no. 4, pp. 14-17, Apr. 2012.

[5] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, no. 5, pp. 53-55, Sep. 2012.

[6] N. Singh and M. Phil, "B.Y.O.D. Genie Is Out Of the Bottle – 'Devil Or Angel,'" Business Management & Social Sciences Research, vol. 1, no. 3, pp. 1-12, 2012.

[7] M. A. AlZain, B. Soh, and E. Pardede, "A New approach using redundancy technique to improve security in cloud computing," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 230-235, Jun. 2012.

[8] D. Tepsic and M. Veinovic, "Comparative analysis of UDP throughput on IPv4 and IPv6 operating systems in IEEE 802.11n wireless networks protected with WPA2 security protocol," in 2012 20th Telecommunications Forum (TELFOR), 2012, vol. 7, pp. 111-114.

[9] H. Said, M. Guimaraes, N. Al Mutawa, and I. Al Awadhi, "Forensics and War-Driving on Unsecured Wireless Network," in 6th International Conference on Internet Technology and Secured Transactions, 2011, no. December, pp. 1-24.

[10] S. Maity, P. Bera, and S. K. Ghosh, "Policy Based ACL Configuration Synthesis in Enterprise Networks: A Formal Approach," 2012 International Symposium on Electronic System Design (ISED), pp. 314-318, Dec. 2012.

[11] O. Gasser, R. Holz, and G. Carle, "A deeper understanding of SSH: Results from Internet-wide scans," 2014 IEEE Network Operations and Management Symposium (NOMS), pp. 1-9, May 2014.

[12] M. Y. Lee, "Diameter-based AAA architecture to support small AAA client," 2010 International Conference on Information and Communication Technology Convergence (ICTC), pp. 497-498, Nov. 2010.

[13] J. Wang & T. Lee (2002). Enhanced intranet management in a DHCP- enabled environment. *Proceedings 26th Annual International Computer Software and Applications*, 893-898. doi:10.1109/CMPSAC.2002.1045119

[14] R. O. Verma and S. S. Shriramwar, "Effective VTP Model for Enterprise VLAN Security," 2013 International Conference on Communication Systems and Network Technologies, pp. 426-430, Apr. 2013.

[15] M. Baentsch, P. Buhler, L. Garces-Erice, T. Gschwind, F. Horing, M. Kuyper, A. Schade, P. Scotton, and P. Urbanetz, "IBM Secure Enterprise Desktop," IBM Journal of Research and Development, vol. 58, no. 1, pp. 10:1-10:11, Jan. 2014.

[16] H.M. Government, "Data Protection Act 1998," vol. 2002, no. 2, 1998.