Assessing Security Risk Caused By Smart Mobile Devices In A University Network Through A Web-Based Threat Matrix

Irene WanjiruWanja
School of Computer Science and Bioinformatics
Kabarak University, Private Bag 20157 Kabarak, Kenya
Email: iwanja@kabarak.ac.ke

ABSTRACT
The need by staff and students to use smart mobile devices in university network is indisputable. This is because they help them to work and study more effectively as well as achieve better work-life balance. However smart mobile devices pose a security challenge as they continue to expand the corporate network unchecked thus increasing the attack surface. The purpose of this study is to develop a web-based threat matrix that computes likelihood of threat attack. The matrix indicates risk exposure levels and provide recommendations that maximize the protection of confidentiality, integrity and availability of university data while still providing functionality and usability of smartmobile devices.

Introduction

A university local area network comprise of interconnected key departments and other offices within a university campus or campuses. Computers and other smart mobile devices use LAN connection to share resources such as a printer or network storage. The nodes are usually interconnected either through wired or wireless means. Smart mobile devices (SMD) refers to any physical object associated with computing resources and is capable of transmitting data to other similar objects either through physical transmission medium and logical protocols or with human through the device user interface (Somayya&Hema, 2016). BYOD (Bring Your Own Device) is a technology, concept or strategy for employees and in this case students prefer working with their personal smartmobile devices such as smart phones, tablet PCs and laptop computers to access corporate internal resources such as database and applications.

The use of smartmobile devices in a corporate network has introduced the need manage and control devices and data not only in an IT department inside a company but also by individual users. Hence security policies should be focused on both user-centered security policies and devices-centered security policies. With the advent of BYOD it has become necessary to supervise not only a specific point of access but also all points of access to corporate network.
To enhance the benefits brought about by use of smart mobile devices in a corporate environment security issues must be addressed. According to Miller, Voas and Hurlburt (2012) smartmobile devices contain a wealth of personal information which may be mixed with corporate information stored on the same device. This creates the need to control access to these devices to protect the privacy of information. When both organization and personal information coexist in one device, it becomes a challenge to find a balance between security control for organization's data and privacy of personal data (Ghosh, Gajar&Rai, 2013).

Problem statement

Despite of the fact that use of smartmobile devices increases convenience and efficiency of work and study, they pose a security challenge as they continue to expand the corporate network unchecked thus increasing the attack surface. One of the major reasons for increased security threats is the concern of managing disparate smartmobile devices which are heterogeneous.
In an environment where bring your own device (BYOD) policy is encouraged, it is important to consider a flexible security policy that accommodates the numerous types of terminals and their diverse use. This can easily be done if there is a threat assessment tool that can inform the level of exposure to attack and hence provide some policy review advisory notes or guideline. In addition such a tool can help to provide guidelines on technical security mechanisms or otherwise to aid in enforcing the security policy. This is the sole purpose of this study.

Research objective

(i) To develop a threat matrix to compute likelihood of threat attack ona university network and provide security requirements based on the computed likelihood of attack

Research Question

(i) How can a threat matrix that computes likelihood of threat attack be developed?

2. LITERATURE REVIEW

2.1 Smart mobileDevices Security Threats

(Goguen&Fringa, 2002) define threat as the likelihood of a particular threat-source to exercise vulnerability or a weakness that can be accidentally triggered or intentionally exploited. Computing devices connect to the Internet in a variety of ways such as wirelessly using a Wi-Fi card and a wireless internet connection or hotspot, through a broadband connection such as third generation (3G) or fourth generation (4G) wireless connections provided by a cellular network, or by tethering using a cellphone as a modem (Pinola, 2012).

The benefits of using smartmobile devices also come with various cyber security threats and vulnerabilities. These vulnerabilities can be related to the hardware of the device, the internet connections (Bluetooth or wireless), installed applications, stored data and information transfer. Threats can be rated as low, medium or high depending on the likelihood to occur and the impact to the user (Bosworth, Kabay&Whyne, 2009).

Malware threats include viruses, Trojans, worms, spyware and other malicious software which severely degrades and destroy computer's operating system. Most malware target laptops but threats against mobile phones have also increased recently(Friedman & Hoffman, 2008). Smartmobile devices with activated Bluetooth and set to discoverable mode are vulnerable to bluesnarfing attacks(Blue jacking Tools, 2012).

2.2 Security Requirement for Smart Mobile Devices

Employers need to consider this risk when drafting security policies to ensure the rules on the use or prohibition of personal devices for company purposes are spelled out. Hardware and software of the device should be known to the employer and employees they are also required to

follow minimal secure practices on their devices before accessing company websites or e-mail (NZ Business, 2011).

It is hard to prevent theft or loss of devices, but the loss of data can be minimized by encrypting the information on the device, requiring a password, biometrics, or an access key to use and configuring the device to erase data after a number of failed logon attempts. The cost of these mitigations is minimal since most operating systems offer password protection and biometric systems are also relatively inexpensive (Milligan & Hutcheson, 2008).

Another option is to install software that allows remote wipe of the data such as Lojack for laptops and Sophos for smartphones (Barcelo, 2011). Users may not want to take the extra steps in logging on to their devices but the pay-off is rewarding if the device is lost or stolen.

Although some phishing attacks may be hard to recognize, the best prevention strategies are to read e-mail carefully to ensure it is from a reputable source, look for grammatical errors and avoid opening attachments unless their receipt is expected (Newman, 2011).

2.3 Security Solutions for Smart Mobile Devices

According to (Antonio, 2012) there exists two main ways of addressing security concerns in a BYOD environment, this include access control where people are at the center and device control where devices are at the center. The research identifies three different security approaches that can be used to control smartmobile devices. Mobile Device Management (MDM) provides support to full device control through software solutions that companies can use to control, lock down, enforce policies and encrypt mobile devices. Mobile Application Management (MAM) according to this research acts like MDM but it is only applied to specific applications on a device. MAM can enable IT security personnel to control and secure specific corporate applications and leave the rest of the things contained on a smartmobile device to the user. Mobile Information Management (MIM) on the other hand allow files and documents synchronization across different devices to manage security.

Network Access Control (NAC) is a security framework which limits the number of connected devices while determining permissions and denying unrecognized devices access to a company's internal network (Downer & Bhattacharya, 2015). According to this research, NAC is useful in ensuring that likelihood of data leakage, infection of malware and other related attacks are avoided or minimized.

Desktop virtualization is a type of security framework which enables desktop computers, virtual machines of servers to host sessions for remotely located smartmobile devices (Downer &Bhattacharya, 2015). These models centralize resources, data as well as security management. This reduces or eliminates the need to transmit data onto smartmobile devices and hence reduces the likelihood of data leakage.

Containerization is used as a security framework to partition smartmobile device storage into different independent sections which separates personal data from work data (Rhodes, 2013). Each section has its own security policies and allows remote access for company control without affecting personal data.

Remote wiping is a reactive solution which is triggered when a device is lost or stolen or when the owner leaves the company (Downer & Bhattacharya, 2015). This is done by removing all company applications and data contained in the smartmobile device. Some MDM and MAM solutions already contain remote wiping procedures.

2.4 Research Gap

From the security solution for smart mobile devices presented in section 2.3 above, none of them integrates a threat assessment as part of their proposed solution. Before designing and deploying smartmobile device security solutions, it would be prudent to assess the security status in order to implement the most suitable solution. However there seems to be no tool designed to assess risks and threats brought about by use of smartmobile devices before proposing a solution.

Using ISO 27001best practices as benchmark framework, the researcher aimed at designing a matrix with a more comprehensive approach that comprised five of the domains of ISO 27001. This includes; information security policy, asset management, access control, operations security and communications security.

The developed security matrix will act as a risk assessment tool to determine likelihood of attack from various threats introduced to university network through use of smartmobile devices. After submitting the assessment questions included in the matrix, feasible threats and vulnerabilities will be identified. The computed likelihood of attack information will help the university determine the security controls that need to be improved or to be added to the network.

3. METHODOLOGY

3.1 Matrix implementation and discussion

The matrix which is in the form of a web-based model is developed using rapid prototyping approach which will enable testing and evaluation at an early stage. The matrix will have various module including; user registration module to allow new users to register in order to access other system functionalities. User login module to allow only authorized users to access the system functionalities after submitting the correct credentials. Assessment module to allow users to answer the assessment questions; the results are then submitted to the database and are used to compute the likelihood of attack. Reports module to allow users to view their scores and recommendations of the submitted assessment.

3.2 System Design and Testing

A logical design of the STM web-based model is presented in this section. It is comprised of several sections to expound on the system design and testing. Figures 1 to 6 presents flowcharts for the system.

3.2.1User Registration

This is the first section of the STM model where every user is expected to register in-order access the system. Personal details such as user name, email address, name of organization, user category and password are required in this interface. Figure 1 below provides flowchart of the registration process while figure 2 provides the graphical user interface of the registration module.

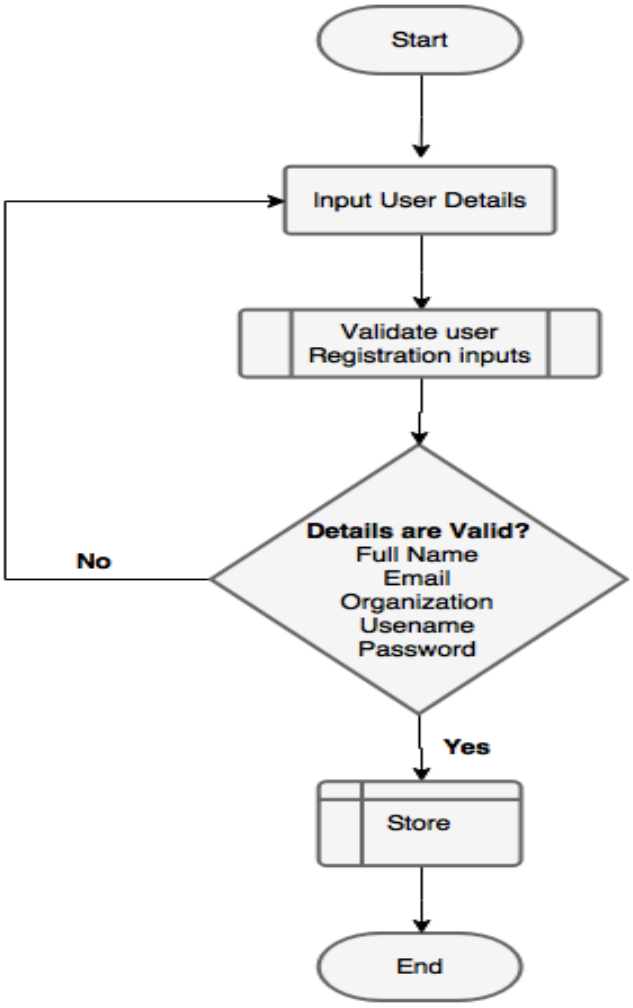


Figure 1. Registration Process Flowchart
Source: Researcher (2018)

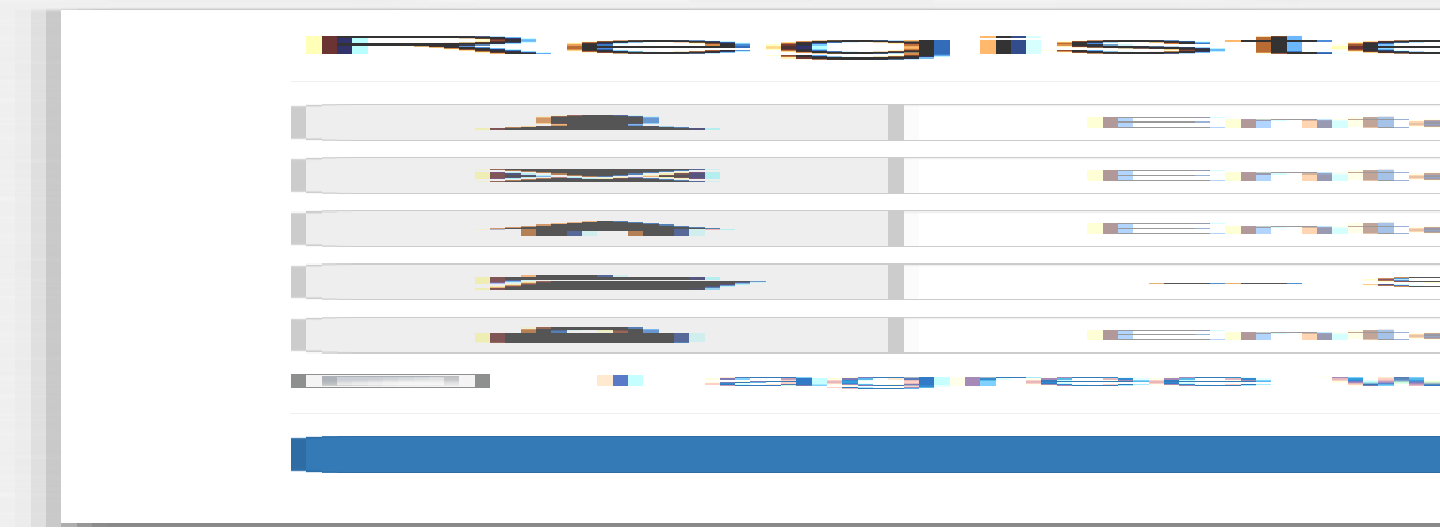


Figure 2: Registration Process GUI

Source: Researcher (2018)

3.2.2 Login Module

In this module, user sessions and logins are managed. When a user attempts to login, this module refers to the users' table in the database to determine if the user is registered or not and whether the user has provided the correct password. Figure 3 below shows a flowchart representing the logic of the login system whereas figure 4 presents a graphical user interface of the login system.

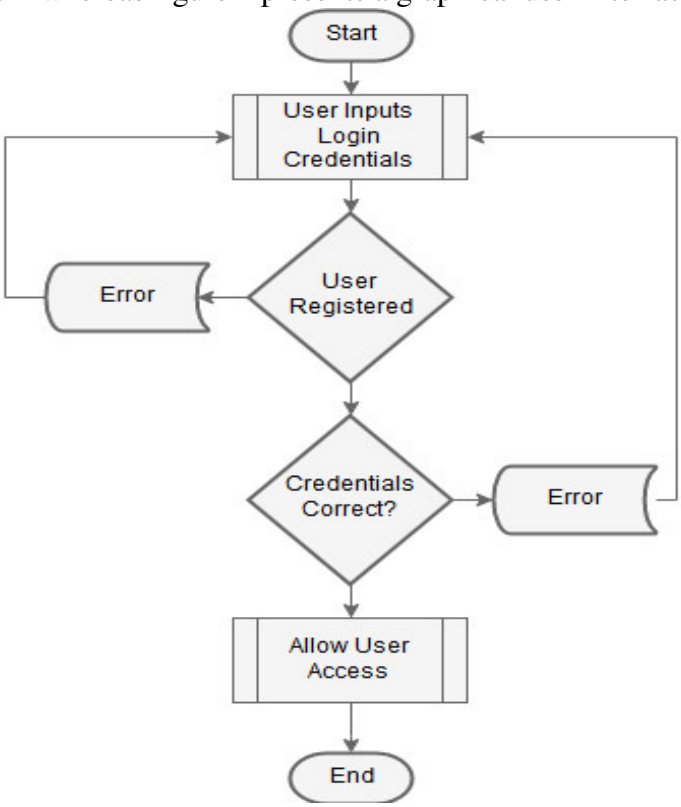


Figure 3: Login Process Flowchart

Source: Researcher (2018)


Login

Figure 4: Login GUI
Source: Researcher (2018)

3.2.3 Threat Assessment Module

This is a self-assessment module for staff and students in which the system displays questions which are retrieved from the database and has five choices to allow the user to select their preferred choice. Once the user has completed the assessment they are allowed to submit the results in the database from which the likelihood of attack is computed. Figure 5 below shows a flowchart presentation of the assessment logic whereas figure 6 is the presentation of the graphical user interface of the risk assessment module.

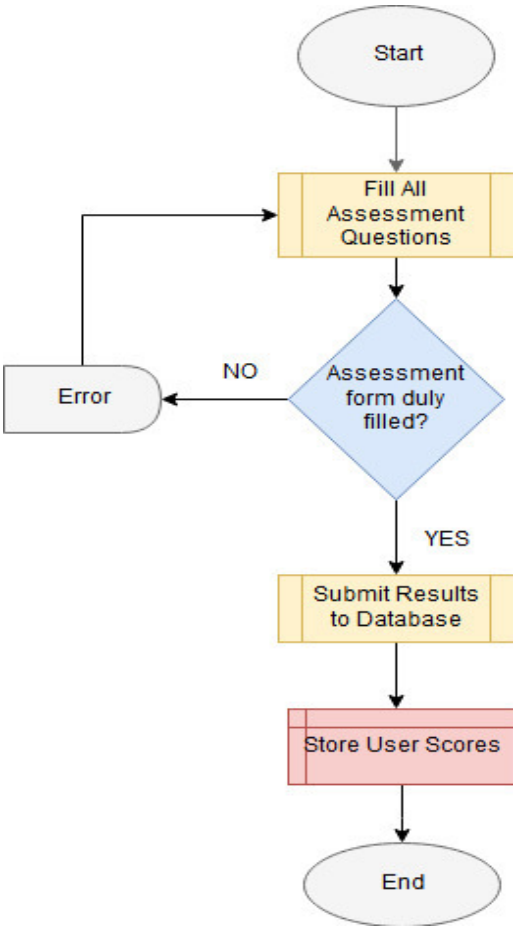
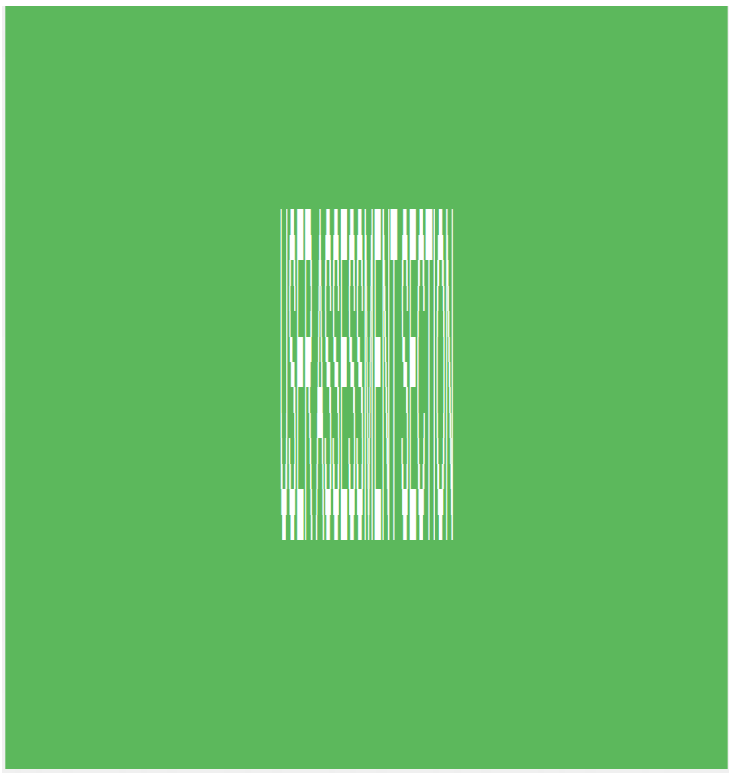


Figure 5: Threat Assessment Flowchart
Source: Researcher (2018)



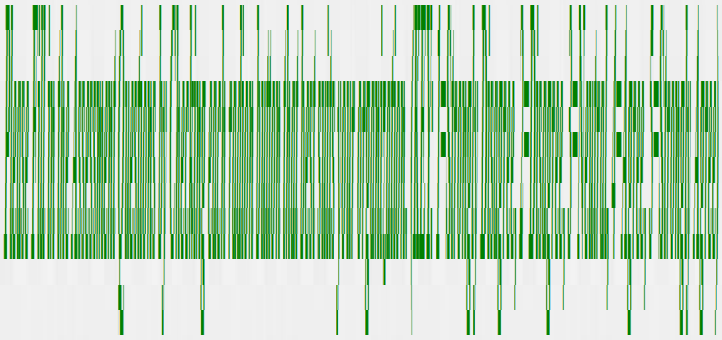


Figure 6: Threat Assessment GUI
Source: Researcher (2018)

3.2.4Likelihood of Attack Assessment Module
This module computes likelihood of threat attack depending on the scores obtained from the submitted assessments. Likelihood of attack was computed as a function weight derived from chapter 4 of this document as demonstrated below;

Likelihood of Attack =5.233 + (-0.084*Information Security Policy) + (0.199*Asset Management) + (-0.003*Access Control) + (-0.101*Operations Security) + (-0.530*Communications Security) + 0.335. Equation 1

A threat is very likely to attack the university network if the user scores 1 for all the 45 assessment questions. Similarly a threat is very unlikely to attack if the user scores 5 for all the assessment questions. Possible likelihood of attack is achieved is the user scores 3 in every assessment question. Figure 6 shows a flowchart presentation of likelihood of attack computation and figure 8 displays its GUI representation.

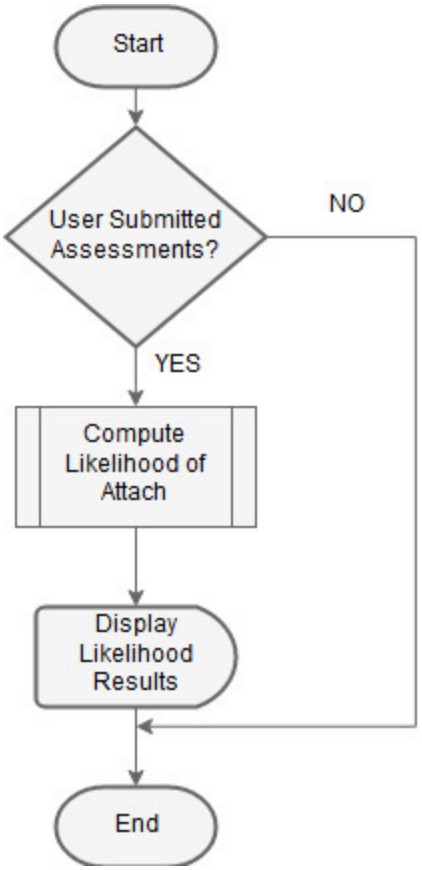


Figure 7: Likelihood of Attack Computation
Source: Researcher (2018)

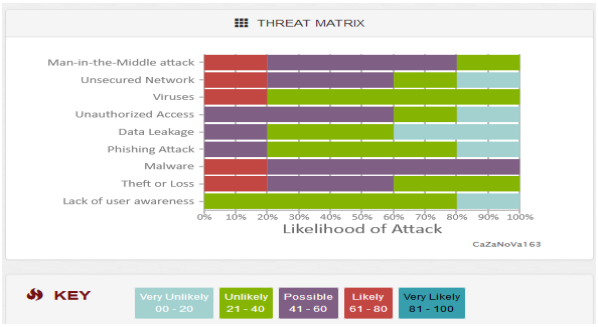


Figure 8: Threat Matrix GUI
Source: Researcher (2018)

3.2.5 Recommendations Component

Based on the user or professional assessments, this module suggests a number of recommendations necessary to mitigate threats resulting from use of smartmobile devices. This module filters the recommendations for all the questions whose user assessment scores goes below the threshold and allows the user to download the recommendations in printable document format (pdf). The figures 9 and 10 shows logic flowchart and GUI presentations respectively.

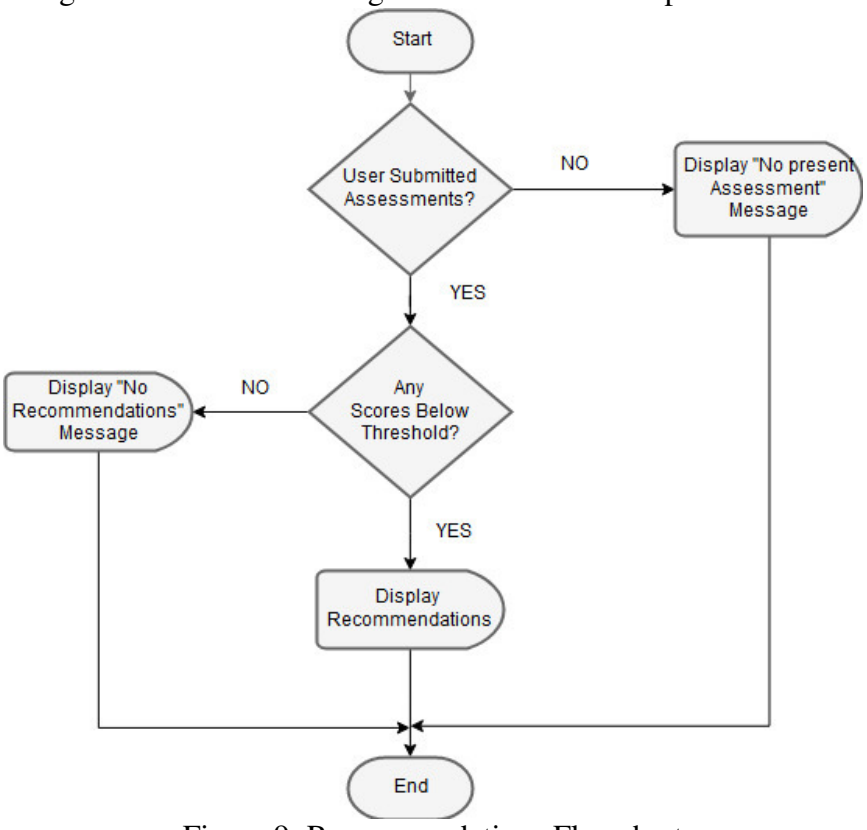


Figure 9: Recommendations Flowchart
Source: Researcher (2018)

Figure 10: Recommendations GUI
Source: Researcher (2018)

3.2.5 Proof of Concept

The STM system prototype was developed as a proof of concept using MySQL as the database engine and PHP as server side-scripting language. Bootstrap 4 which is a framework of CSS was used to style user interface for the purpose of user interaction with the system. phpStormwas used as program editor to write and test the code. Apache web server assisted in running the application locally. The application was later deployed online and is accessible through www.irenewanja.com

4. CONCLUSION

The study sought to assess security threats introduce to the university information systems and data through use of smartmobile devices. A Threat Matrix which was a web-based model was developed to show levels of likelihood of attack for various threats that were found to be common. This assisted in determining the security gap that needed to be addressed to enhance security of the university network. The matrix also provided recommendations on security requirements that were needed to improve the security status of the university network.

4.1 Suggestions for Further Research

4.1.1 Likelihood of Attack versus Impact Assessment

The main purpose of the developed Threat Matrix was to determine the possibility of threat attack to the university network. To advance the system operations, further research on how to compute the impact created by the threat in the event that it succeeds in launching the attack. This would help the university ICT security experts to prioritize on the risks that have high impact while employing the countermeasures.

References

Abdelrahman, O. H., Gelenbe, E., Görbil, G., &Oklander, B. (2013). Mobile network anomaly detection and mitigation: The NEMESYS approach. In *Information Sciences and Systems 2013* (pp. 429-438). Springer, Cham

Abomhara, M., &Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Systems (PRISMS), 2014 International Conference on* (pp. 1-8). IEEE.

Arabo, A., &Pranggono, B. (2013, May) malware and smart device security: Trends, challenges and solutions. In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on* (pp. 526-531). IEEE.

AT&T State of IoT Security survey, (2015). *Exploring IoT Security*. The CEO's guide to securing the Internet of Things. Volume 2 retrieved from https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf(accessed 10th march, 2017)

Aware, W. T. A., Documentation, T. P. S., & Logical, C. (2005). Information technology–Security techniques–Information security management systems–Requirements.

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), 2011 2nd International Conference on* (pp. 1-5). IEEE.

Barcelo, Y. (2011, September). Insecurity. *CA Magazine*, pp. 36-38.

Beach, A., Gartrell, M., & Han, R. (2009, August). Solutions to security and privacy issues in social networking. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 4, pp. 1036-1042). IEEE.

Bernabe, J. B., Hernández, J. L., Moreno, M. V., & Gomez, A. F. S. (2014, December). Privacy-preserving security framework for a social-aware internet of things. In *International Conference on Ubiquitous Computing and Ambient Intelligence* (pp. 408-415). Springer International Publishing.

Bluejacking Tools. (2012). *Phone Spy.* Retrieved from Bluejacking Tools: http://www.bluejackingtools.com/bluesnarf--spy/-phone-spy/(accessed 11th September, 2017)

Bosworth, S., Kabay, M., &Whyne, E. (2009). Physical Threats to the Information Infrastructure. In F. Platt, *Computer Security Handbook.* New York: John Wiley & Sons Inc.

Business Insider, (2016). IoT-Ecosystem, what is the internet of things, retrieved from http://www.businessinsider.com/iot-ecosystem-what-is-the-internet-of-things-2016(accessed 4th March,2017)

Calder, A. and Watkins, S. (2008). *IT Governance: A Manager's guide to Data Security and ISO27001/ISO 27002, 4th Edition*. London: Kogan Page Limited.

Cisco.com (2014). *Cyber Threat Management from the Boardroom Risk*: Retrieved from blogs.cisco.com: https://blogs.cisco.com/security/cyber-threat-management-from-the-board-room-risk-lost-in-translation(accessed 8th November, 2017)

Cisco.com (2017) *LAN Solutions Guide for Higher Education/Universities.* Retrieved from Cisco.com:https://www.cisco.com/c/en/us/products/wireless/-office-net-software/index.html (accessed 11th September, 2017)

Computer Weekly. (2010, July 12). *iTunes hack could affect thousands, say experts.* Retrieved from Computer Weekly: http://www.computerweekly.com/news/1280093237/iTunes-hack-could-affect-thousands-say-experts(accessed 11th September, 2017)

Delac, G., Silic, M., &Krolo, J. (2011, May). Emerging security threats for mobile platforms. In *MIPRO, 2011 Proceedings of the 34th International Convention* (pp. 1468-1473). IEEE.

Ernst & Young Global Limited, (2015). *The multiplying effect of today's cybersecurity challenges*. Cybersecurity and the Internet of Things.

Friedman, J., & Hoffman, D. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, 159-180.

Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., &Lyberopoulos, G. (2013, June). Security for smart mobile networks: The NEMESYS approach. In *Privacy and Security in Systems (PRISMS), 2013 International Conference on* (pp. 1-8). IEEE.

Hossain, M. M., Fotouhi, M., &Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *Services (SERVICES), 2015 IEEE World Congress on* (pp. 21-28). IEEE.

Huang, X., Craig, P., Lin, H., & Yan, Z. (2015). SecIoT: a security framework for the Internet of Things. *Security and Communication Networks*.

IEEE Standard Association, (2015). *Executive summary*, Internet of Things (IoT) Ecosystem study retrieved from http://standards.ieee.org/innovate/iot/study.html(accessed 4th March, 2017)

Infosecinstitute.com (2014). Cyber Threat Analysis: Retrieved from: http://resources.infosecinstitute.com/cyber-threat-analysis/#gref(accessed 8thNovember,2017)

Jha, A., & Sunil, M. C. (2014). Security considerations for Internet of Things. *L&T Technology Services*.

Kim, D. H., Cho, J. Y., Kim, S., & Lim, J. (2015). A Study of Developing Security Requirements for Internet of Things (IoT). *Advanced Science and Technology Letters*, *87*, 94-99.

Kim, J. T. (2015). Requirement of Security for IoT Application based on Gateway System. *International Journal of Security and Its Applications*, *9*(10), 201-208.

Kim, J., & Lee, J. W. (2014, March). OpenIoT: An open service framework for the Internet of Things. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on* (pp. 89-93). IEEE.

Koh, E. B., Oh, J., &Im, C. (2014). A study on security threats and dynamic access control technology for BYOD, smart-work environment. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 2, pp. 1-6).

KPMG, (2015). *Focus on Security, Privacy and Trust*. Security and the IoT Ecosystem

Lee, Y., & Kim, D. (2015). Threats Analysis, Requirements and Considerations for Secure Internet of Things. *International Journal of Smart Home*, *9*(12), 191-198.

Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In *Connectivity Frameworks for Smart Devices* (pp. 23-41). Springer International Publishing.

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). Cyber threat metrics. *Sandia National Laboratories*.

Miller, K. W., Voas, J., &Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*, *14*(5), 53-55.

Milligan, P. M., & Hutcheson, D. (2008). Business Risks and Security Assessment for Devices. *Information Systems Control Journal*, 1-5.

Mohammed, L. A. (2010). ICT Security Policy: Challenges and Potential Remedies. *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements: Trends, Issues and Advancements*, 337.

Newman, J. (2011, June 3). *4 Security Tips Spurred by Recent Phishing Attacks.* Retrieved from PC World: http://www.pcworld.com/article/229361/4_security_tips_spurred_by_recent_phishing_attacks_on_gmail_hotmail_and_yahoo.html(accessed 12th September, 2017)

NIST, G. S., Goguen, A., &Fringa, A. (2002). Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*.

NZ Business. (2011, September). Are mobile devices compromising your business security? *NZ Business*, p. 60.

O'Dell, J. (2010, April 13). *New Study Shows the Web Will Rule by 2015.* Retrieved from Mashable: http://mashable.com/2010/04/13/-web-stats(accessed 11th September, 2017)

Open Web Application Security Project (OWASP) IoT Top Ten Vulnerabilities. 2014. DOI https://www.owasp.org/ images/ 7/71/Internet_of_ Things_Top_Ten_2014- OWASP.pdf

Pinola, M. (2012). *Internet Access Comparison.* Retrieved from About.com Office Technology: Pros and cons of different Internet-on-the-Go options:

http://office.about.com/od/wificonnectivity/a/wireless-internet-comparison.html (accessed 12th September, 2017)

PTC Cloud Services, (2016). *Seven Steps to Minimize IoT Risk in the Cloud.* Securing the Internet of Things. White paper

Rahman, A. F. A., Daud, M., &Mohamad, M. Z. (2016, March). Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework. In *Proceedings of the International Conference on Internet of things and Cloud Computing* (p. 79). ACM.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., &Bouabdallah, A. (2013, May). A systemic approach for IoT security. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on* (pp. 351-355). IEEE.

Sabale, R. G. &Dani, A. R. (2012). Comparative study of prototype model for software engineering with system development life cycle. *IOSR Journal of Engineering*, 2(7), 21-24.

Saif, I., Peasley, S., &Perinkolam, A. (2015). *Being secure, vigilant and resilient in the connected age*. Safeguarding the Internet of Things. *The Internet of Things*, 41retrieved from https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html (accessed 10th March, 2017)

Shafagh, H., &Hithnawi, A. (2014, May). Security Comes First, A Public-key Cryptography Framework for the Internet of Things. In *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on* (pp. 135-136). IEEE.

Shukla, I. (2011, September 21). *Advantages of Computing*. Retrieved from Buzzle.com: http://www.buzzle.com/articles/advantages-of--computing.html(accessed 13th September, 2017)

Sopori, D., Pawar, T., Patil, M., &Ravindran, R. (2017) Internet of Things: Security Threats.

Souppaya, M., &Scarfone, K. (2013). Guidelines for managing the security of devices in the enterprise. *NIST special publication*, *800*, 124.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on* (Vol. 3, pp. 648-651). IEEE.

TechTarget.com (2016).*Managing Online Risk*. Retrieved from Techtarget.com: http://searchsecurity.techtarget.com/feature/Managing-Online-Risk(accessed 8th November, 2017)

TechTarget.com. (2007). *Search Security Policy.* Retrieved from Techtarget.com: http://searchsecurity.techtarget.com/definition/security-policy(accessed 2nd October, 2017)

TechTarget.com. (2012). *Search Computing.* Retrieved from Techtarget.com: http://searchcomputing.techtarget.com(accessed 11th October, 2017)

TechTarget.com. (2017). *Search Mobile Computing*. Retrieved from Techtarget.com: https://searchmobilecomputing.techtarget.com/definition/nomadic-computing(accessed 11th October, 2017)

Trendmicro.com (2015). *The Increasing Cyberattack Surface*. Retrieved from trendmicro.com: https://blog.trendmicro.com/the-increasing-cyberattack-surface/(accessed2ndOctober, 2017)

U.S. Department of Homeland Security, (2016). *Prioritizing IoT security*. Strategic principles for security Internet of Things (IoT) version 1.0retrieved from

https://www.dhs.gov/.../Strategic_Principles_for_Securing_the_Internet_of_Things-(accessed 11th march, 2017).

Vermesan, O., &Friess, P. (Eds.). (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.

Warwick, A. (2010, July 30). *Millions downloaded suspicious Android wallpaper.* Retrieved from Computer Weekly: http://www.computerweekly.com/news/1280093401/Millions-download-suspicious-Android-wallpaper(accessed 11th October, 2017)

Westervelt, R. (2011, December 8). *Android app security: Study finds developers creating flawed Android apps.* Retrieved from SearchSecurity: http://searchsecurity.techtarget.com/news/2240112235/Android-app-security-Study-finds--developers-creating-flawed-Android-apps(accessed 11th October, 2017)

Westervelt, R. (2011, December 9). Top 5 phone security threats in 2012. Retrieved from Search Security: http://searchsecurity.techtarget.com/news/2240112288/Top-5--phone-security-threats-in-2012 (accessed 11th October, 2017)

Youker, B. W. (2014). Goal-free Evaluation and Goal-Based Evaluation.*The Foundation Review 5(4) 50-61.*

Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A Survey on Security for Smartphone Device. *International Journal of Advanced Computer Science and Applications-2016*.

Zhao, K., &Ge, L. (2013, December). A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on* (pp. 663-667). IEEE.