

**BUSITEMA
UNIVERSITY**
Pursuing Excellence

**A Process Flow Model for Dynamic Enterprise Network Cyber Security
Analysis**

By

Mugoya Shariff

BU/GS19/MCF/1

Email: mugoyashariff@gmail.com

Tel: +256773792444 / +256701043709

**A Research Dissertation Submitted to the Directorate of Graduate Studies, Research and
Innovations in Partial Fulfillment of the Requirements for the Award of a Master of
Science in Computer Forensics Degree of Busitema University.**

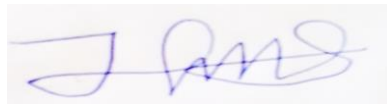
December 2023

DECLARATION

I the undersigned, declare that this research proposal is my original work, except where due acknowledgement has been made. I declare that this work has never been submitted to this University or any other institution for funding/ partial fulfillment for any award.

Student Name: MUGOYA SHARIFF

Registration Number: BU/GS19/MCF/1



Signature:

Date: 14th December, 2023

SUPERVISOR(S) APPROVAL

This research proposal has been submitted as a partial fulfillment for the award of Masters of Science in Computer Forensics of Busitema University, with my/our approval as the academic supervisor(s).

Name: Prof. SEMWOGERERE TWAIBU

Academic Qualifications: M.Sc. (Maths), PhD (Mech. Eng. Maths), MAK.

Rank: Associate Professor

Department: Computer Engineering and Informatics

Faculty: Faculty of Engineering and Technology

Signature: 

Date: 14th December, 2023

Name: Dr. ODONGTOO GODFREY

Academic Qualifications: M. Sc. (I.T), PhD (I.T, Mod)

Rank: Lecturer

Department: Computer Engineering and Informatics

Faculty: Faculty of Engineering and Technology

Signature:

Date:

DEDICATION

I dedicate this work to the Almighty Allah who has blessed me with wisdom that enabled me reach this step.

I dedicate this thesis to my loved ones.

I dedicate this work to my supervisors Prof. Semwogere Twaibu and Dr. Odongtoo Godfrey who have provided me with the academic guidance needed in the formulation of this thesis.

ACKNOWLEDGEMENT

I thank the Almighty Allah for providing me with the resources needed throughout this research process.

I would like to thank my supervisors Prof. Semwogere Twaibu and Dr. Odongtoo Godfrey for the support and guidance rendered to me during this research.

My sincere thanks go to the institutions that I work with and those that have participated in this research.

Table of Contents

Contents

DECLARATION	iii
SUPERVISOR(S) APPROVAL	iv
DEDICATION	v
ACKNOWLEDGEMENT	vi
Table of Contents	vii
ACRONYMS AND ABBREVIATIONS	x
OPERATIONAL DEFINITIONS	xi
List of Figures	xii
List of Tables	xiii
ABSTRACT.....	xiv
CHAPTER 1: INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	3
1.3 Research Objectives.....	3
1.3.1 Main Objective.....	3
1.3.2 Specific Objectives	3
1.4 Research Questions	3
1.5 Assumptions.....	4
1.6 Originality and Contribution to new Knowledge.....	4
1.6.1 Knowledge	4
1.6.2 Practice.....	4
1.6.3 Research.....	4
1.7 Significance of the Research.....	5
1.8 Scope of the Study	5
1.9 Conceptual Framework.....	6
CHAPTER 2: LITERATURE REVIEW	7
2.1 Introduction.....	7
2.2 Methods used in Combating Cyber threats faced by Enterprise Networks.....	7
2.3 Metrics for Cybersecurity Modeling.....	8
2.4 Related Works.....	9
2.5 Research Gaps.....	11

2.5.1 Summary of Existent Gaps	11
CHAPTER 3: MATERIALS AND METHODS	12
3.1 Research Design.....	12
3.2 Study Population.....	14
3.3 Sampling Strategy and Sample size.....	14
3.4 Data Collection Methods	15
3.5 Data Analysis and Presentations	15
3.5.1 Reliability Test.....	15
3.5.2 Validity Test	15
3.6 Ethical Consideration.....	16
3.7 Environmental and Gender implications.....	16
3.8 Limitations of the Study.....	16
CHAPTER 4: DATA ANALYSIS AND RESULTS DESCRIPTION.....	17
4.1 Data Analysis.....	17
4.1.1 Validity on Vulnerabilities as a Construct for Enterprise Networks.....	17
4.1.2 Validity on Threat Intelligence and Detection as a Construct for Enterprise Networks.....	18
4.1.3 Validity on Security Controls as a Construct for Enterprise Networks	18
4.2 Demographic Characteristics of Respondents	19
4.3 Current methods used in combating cyber threats faced by enterprise networks.....	20
4.3.1 Common Cyber Security challenges faced by Enterprise Networks	20
4.3.2 Security measures employed by Enterprise Networks.....	21
4.4 Metrics for enterprise network cyber security Modeling.....	21
4.4.1 Frequency of vulnerability assessment testing.....	22
4.4.2 Ways of Handling Security incidents/breaches	22
4.4.3 Number of times security awareness training is conducted	22
4.4.4 Source of latest Cyber Security threats and trends	23
4.5 The Proposed Model (DENCAM)	24
4.6 Experimentation.....	25
CHAPTER 5: DISCUSSION AND CONCLUSION	30
5.1 Discussion of Findings.....	30
5.1.1 Demographic Characteristics of Respondents	30
5.1.2 Current methods used in combating cyber threats faced by enterprise networks.	30
5.1.3 Metrics for enterprise network cyber security Modeling.....	30

5.2 Recommendations.....	30
5.3 Conclusion and Future Work.....	31
REFERENCES	32
APPENDICES	35
Appendix 1: Field Introductory Letter.....	35
Appendix 2: Questionnaire	36
Appendix 3: Work Plan	43
Appendix 4: Research Logframe	44
Appendix 5: Budget.....	45
Appendix 6: Factor Analysis	46

ACRONYMS AND ABBREVIATIONS

ATM – Automated Teller Machine.

DARPA – Defense Advanced Research Projects.

DENCAM – Dynamic Enterprise Network Cyber Security Analysis Model.

DFD – Data Flow Diagram.

DML – Detection Maturity Level.

DoS – Denial of Service.

DDoS – Distributed Denial of Service.

DSR – Design Science Research.

MITRE ATT & CK – MITRE Adversarial Tactics, Techniques and Common Knowledge.

NSA – National Security Agency.

OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation.

PASTA – Process for Attack Simulation and Threat Analysis.

SIEM – Security Information and Event Management.

STRIDE – Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of Privilege.

TTP – Tactics, Techniques, and Procedures.

VAST – Visual, Agile, and Simple Threat.

OPERATIONAL DEFINITIONS

Cyber Security Analysis is the examining each risk to the security of an internet connected organization's information systems, devices, and data.

Enterprise Network is a hardware and software infrastructure that connects a company's computers, servers and other devices.

Process Flow Model is a graphical representation of the steps or processes involved in a system.

Dynamic Network is a network where the topology and components of the network are constantly changing.

Scalability is the ability to be changed in size or scale.

Network Security Vulnerabilities are weaknesses or flaws within the system's software, hardware, or organizational processes.

List of Figures

Figure 1.1: Conceptual framework 6

Figure 3.1: MITRE ATT & CK matrix..... 13

Figure 3.2: A map of Uganda showing the regions of the country..... 14

Figure 4.1: Dynamic Enterprise Network Cyber Security Analysis Model 24

Figure 4.2: Beginning interface of SolarWinds ipMonitor 26

Figure 4.3: Results of Scan 27

List of Tables

Table 2: Frequency of conducting security awareness training..... 23
Table 3: Source of information about latest Cyber Security threats and trends 23

ABSTRACT

Several Enterprises are adopting Enterprise Networks due to their benefits like remote file storage, resource sharing, and improved communication. Due to a large number of target groups, cyber-attackers have exploited vulnerabilities in the Enterprise Networks to launch cyber-attacks on these networks thus resulting into data theft and financial losses to the enterprises.

To effectively address these security concerns, this study proposes a Dynamic Enterprise Network Cyber Security Analysis Model for Enterprise Network security. The proposed model caters for dynamic networks. It puts into consideration the ever changing components of enterprise networks.

This study uses Design Science Research approach and MITRE ATT & CK matrix serves as the knowledge base for information about common attacks. A sample population of 132 respondents from 10 enterprises with Enterprise Networks in Eastern and Central Uganda was studied. Purposive sampling was used to select key informants with technical knowledge about cyber security. Primary data was collected using closed-ended questionnaires and secondary data was collected from analysis of scholarly articles, books, conference papers, and journals. The research participants were required to voluntarily participate and their consent was required before being studied. SPSS version 27 tool was used to analyze the data collected.

With the DENCAM, SolarWinds ipMonitor network monitoring tool was used to monitor changes in the components of enterprise networks, then MITRE ATT & CK provided knowledge about the possible attacks that can be launched on the enterprises as a result of the changes in the enterprise network components and the possible remedies. Once preventive measures were put in place to deter the projected attacks, simulation attacks were launched on the enterprise network using Cymulate threat emulator. The network was able to resist such attacks. This will ensure security of enterprise networks thus enabling achievement of Uganda's Vision 2040 which aims at using ICT to provide an opportunity to improve national productivity by making government and business enterprises more efficient, effective, and globally competitive.

CHAPTER 1: INTRODUCTION

1.1 Background

Of recent the use of smart phones, internet and computers is so popular in our lives. This is both for individuals and organizations. As of January 2024 there were 5.35 billion internet users worldwide which represents 66.2% of the world population [1] and according to [2] there are 6.93 billion smartphone users worldwide.

Organizations and enterprises have embraced networking of Computers thus coming up with Enterprise networks. This is attributed to the benefits like resource sharing, remote file storage, and improved communication that come with the networking of computers.

However, since access to the server computer affects activities of all computers on the network, cyber-attackers have highly targeted networked computers by exploiting network vulnerabilities thus plunging enterprises into huge financial losses and data losses. Most of the attacks have been as result of errors on the enterprise employees' part.

Cyber-attacks can lead to significant financial losses for large enterprises. The exact amount of losses varies depending on various factors such as the nature of the attack, the size of the organization, the industry sector, and the effectiveness of the organization's security measures. Here are a few notable examples of large enterprises and the losses they have experienced due to cyber-attacks:

In 2013, Target, a major U.S. retailer, suffered a cyber-attack that compromised payment card information of approximately 40 million customers. The attack also exposed personal information of around 70 million customers. The breach cost Target an estimated \$162 million, including expenses related to investigation, remediation, legal fees, and settlements [3].

In 2014, Sony Pictures Entertainment experienced a highly publicized cyber-attack attributed to North Korea. The attack resulted in the theft and release of sensitive company data, including employee information and unreleased films. Sony Pictures estimated the total cost of the attack to be approximately \$15 million, including remediation efforts, investigation, and legal fees [4].

In 2017, Equifax, one of the largest credit reporting agencies, experienced a massive data breach that exposed personal information of approximately 147 million people. The breach resulted in significant financial losses for Equifax, including legal settlements, remediation costs, and damage to its reputation. The estimated total cost of the breach exceeded \$1.4 billion [5].

In 2017, Maersk, a global shipping company fell victim to the NotPetya ransomware attack, which affected its IT infrastructure worldwide. The attack resulted in significant disruptions to Maersk's operations, including the shutdown of critical systems and the loss of data. The company reported losses of around \$300 million due to the incident [6].

REFERENCES

1. Statista. (2024). Internet user population. Retrieved from <https://www.statista.com/statistics/617136/digital-population-worldwide/> Accessed on January 16th, 2024, at 4:30 P.M.
2. HOW MANY SMARTPHONES ARE IN THE WORLD? (2024). Retrieved from <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world>. Accessed on January 17th, 2024, at 8: 16 A.M.
3. M. McGrath (2014). Target Data Breach Spilled Info On As Many As 70 Million Customers. Retrieved from <https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=df3f7cce7954>. Accessed on January 17th, 2024, at 8:29 A.M.
4. A. DeSimone, and N. Horton. (2015). Sony's Nightmare Before Christmas.
5. M. Hill (2023). The biggest data breach fines, penalties, and settlements so far. Retrieved from <https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>. Accessed on January 17th, 2024, at 8:46 A.M.
6. M. Mcquade. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> Accessed on January 17th, 2024, at 8:52 A.M.
7. PurpleSec. (2022). Conti Ransomware Attack: Summary of the Attack. Retrieved from <https://purplesec.us/security-insights/conti-ransomware-attack/#:~:text=Summary%20of%20The%20Attack,by%20Conti%20in%20April%202022.&text=agencies%20have%20since%20been%20attacked,attack%20has%20been%20leaked%20online>. Accessed on November 8, 2022, at 2:53 P.M.
8. BBC News. (2019). WhatsApp discovers 'targeted' surveillance attack. Retrieved from <https://www.bbc.com/news/technology-49125853>. Accessed on November 10, 2022, at 4:30 P.M.
9. Uganda Police Force. (2022). Annual Crime Report. Retrieved from <https://www.upf.go.ug/>.
10. Cobalt Lab, Inc. (2021). Business Cost of Cybercrime. Retrieved from <https://www.purplesec.us/common-network-vulnerabilities>. Accessed on November 8, 2022, at 1:30 P.M.
11. Cyber Security Ventures. (2022). Cyber Security Almanac. Retrieved from <https://www.cybersecurityventures.com/cybersecurity-almanac-2022/>. Accessed on November 8, 2022, at 2:36 P.M.
12. Schrenier, B. (1999). "Attack trees." *Dr. Dobb's Journal*, 24(12), 21-29.
13. Phillips, C., & Swiler, L. P. (1998). A graph-based system for network vulnerability analysis (pp. 71-18).
14. Faraz,Z., et al (2014). Analysis and Visualization of Dynamic Networks.
15. Faraz, Z., Chris M., and Arnaud, S. (2007). Analysis and Visualization of Dynamic Networks.
16. S. Yusuf Enoch et al. (2021). Model-based Cyber Security Analysis: Past Work and Future Directions
17. United Nations. (2015). Sustainable Development Goals.
18. National Planning Authority. (2013). Uganda Vision 2040.

19. National Planning Authority. (2020). Third National Development Plan (NDP III) 2020/21 – 2024/25.
20. Kumar, A., et al. (2017). Enterprise Network System. *International Journal of Computer Engineering and Technology*, 8(4), 71-78. Article ID: IJCET_08_04_008.
21. TechTarget. (2023). Cyber-attack. Retrieved from <https://www.techtarget.com/searchsecurity/definition/cyber-attack/>. Accessed on November 8, 2022, at 12:50 P.M.
22. A. Siddique (2021). Threat Modeling Methodologies for Network.
23. PurpleSec. (2022.). Common Network Vulnerabilities. Retrieved from <https://www.purplesec.us/common-network-vulnerabilities/>. Accessed on November 8, 2022, at 1:30 P.M.
24. Zhao, Z. (2023). National and Enterprise Cybersecurity Countermeasures. In *Proceedings of the 2022 7th International Conference on Modern Management and Education Technology (MMET 2022)* (pp. 180–187). Atlantis Press SARL. https://doi.org/10.2991/978-2-494069-51-0_24.
25. Maglaris, V., Koutepas, G., & Maglaris, B. (2002). Detection and Reaction to Denial of Service Attacks. <https://www.researchgate.net/publication/235890300>.
26. Cisa, Fbi, & Ms-isa. (2022). Understanding and Responding to Distributed Denial of Service Attacks.
27. Tang, D., & Kuang, X. (2019). Distributed Denial of Service Attacks and Defense Mechanisms. *IOP Conference Series: Materials Science and Engineering*, 612(5). <https://doi.org/10.1088/1757-899X/612/5/052046>.
28. Internet Society (2015). Addressing the challenge of IP spoofing.
29. Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). SANDIA REPORT Cyber Threat Metrics. <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>
30. Jaquith, A. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Upper Saddle River, NJ: Addison-Wesley, 2007
31. M. J. & P. P. Bhol S G, "Cyber Security Metrics Evaluation Using Multi-Criteria Decision Making Approach," *Smart Intelligent Computing and Applications*, vol. 1, no. 1, pp. 665-675, 2019
32. Abbadi, Z. (2006). *Security Metrics What Can We Measure?*
33. Ocen, G. G., et al. (2019). An Algorithm and Process Flow Model for Extracting Digital Forensic Evidence in Android Devices. *International Scientific Journal Theoretical and Applied Science*, 72(Issue 04).
34. Microsoft. (2016). The STRIDE Threat Model.
35. McMillan, R. (2012). The World's First Computer Password? It Was Useless Too. Retrieved from <https://www.wired.com/2012/01/computer-password/>.
36. Shostack, A. (2014). *Threat Modeling: Designing for Security*. John Wiley & Sons Inc: Indianapolis.
37. Amoroso, E. G. (1994). *Fundamentals of Computer Security Technology*. AT&T Bell Labs. Prentice-Hall: Upper Saddle River. ISBN 9780131089297.
38. Schneier, B., et al. (1998). *Toward a Secure System Engineering Methodology*.
39. Alberts, C. (2003). *Introduction to the OCTAVE® Approach*.

40. Stillions, R. (2014). The DML Model.
41. L., Kohnfelder, and G., Praerit. (1999). Threats to Our Products.
42. Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017, 2017-January, 91–98. <https://doi.org/10.1109/EISIC.2017.20>
43. Ucedavélez, T., and Marco, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis.
44. M., Eddington; B., Larcom, and E., Saitta (2005). Trike v1 Methodology Document.
45. Software Engineering Institute. (2018). The Hybrid Threat Modeling Method. Retrieved from <https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/>. Accessed on October 15, 2022, at 12:50 P.M.
46. C. B. Perry R, Hinton, Isabella McMurray. (2014). SPSS Explained Second Edition.