National College of Ireland

Project Submission Sheet – 2022/2023

Student Name:	Gbenga Fadele		
Student ID:	X21246891		
Programme:	Cyber Security	**Year:**	2023
Module:	Research in Computing		
Lecturer:	Vanessa Ayala-Rivera		
Submission Due Date:	16 April 2023		
Project Title:	Prevention and Response Strategies for Advanced Persistent Threats on BGP Routing Using Machine Learning		
Word Count:	…………………………………………………………………………………………………		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Gbenga Fadele

Date: 16/04/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Prevention and Response Strategies for Advanced Persistent Threats on BGP Routing Using Machine Learning

Gbenga Fadele
X21246891
Cyber Security
National College of Ireland

Abstract

Border Gateway Protocol (BGP) is the Internet's backbone infrastructure, a critical protocol that is used to route Internet traffic between different autonomous systems (ASes). Over the years BGP has been under constant attack for reasons ranging from Financial gains, cyber-crime, hacktivist, human configuration errors leading to route leaks/hijacks etc.

An Advanced Persistent Threat (APT) on BGP routing is a sophisticated and persistent attack designed to evade detection and remain undetected for extended periods of time and could have significant consequences for Internet users, service providers, and organizations. To address these issues, this research proposes a prevention and response framework for APTs on BGP routing using machine learning (ML) techniques.

The research identifies the weaknesses in the BGP routing protocol that enable APTs to persist and evade detection. The study then presents a machine learning-based approach that utilizes anomaly detection algorithms to monitor and classify BGP routing behavior.The proposed response strategy involves filtering out malicious BGP routes, blocking network access to suspicious IP addresses, and alerting security personnel to investigate further.We will be investigating the current state of APTs on BGP routing and examining existing prevention and response strategies. We will also identify the limitations of current network monitoring tools and proposing more effective approaches to enhance them, with the aim of preventing and responding effectively to advanced persistent threats on BGP routing

Ultimately, this research will contribute to the development of more effective prevention and response strategies for APTs on BGP routing using machine learning, which is critical for ensuring the stability, security, and resilience of the Internet.The proposed framework can assist organizations in enhancing their cyber-security posture, protecting their sensitive information, and avoiding reputation damage.

Keywords: Border Gateway Protocol, Advanced Persistent threats, Machine learning, monitoring tools.

1. Introduction

Cyber is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide (Wikipedia, 2022).

One critical component of cyber-security is the Border Gateway Protocol (BGP). The Border Gateway Protocol (BGP) is a crucial protocol enabling exchange of routing information between different autonomous systems (ASes) on the Internet. Hence, BGP can be said to be the backbone of the internet. While BGP has been instrumental in enabling the growth and evolution of the Internet, it is also vulnerable to various threats and attacks, including Advanced Persistent Threats (APTs). An APT on BGP routing is a sophisticated and persistent attack on the Internet's backbone infrastructure designed to evade detection and remain undetected for extended periods of time. A successful APT on BGP routing can lead to devastating consequences, including rerouting of internet traffic, stealing sensitive data, and launching DDoS attacks (Bahnasy et al., 2020).

The purpose of this research paper is to analyze the current status of advanced persistent threats (APTs) on BGP routing and evaluate the effectiveness of current prevention and response strategies. The study will highlight the limitations of existing approaches and propose novel strategies to enhance the prevention and response to APTs on BGP routing. Additionally, we will explore the integration of machine learning into the existing processes to bolster the security of BGP routing networks against APTs.

Ultimately, this research will contribute to the development of more effective prevention and response strategies for APTs on BGP routing, which is critical for ensuring the stability, security, and resilience of the Internet.

Previous research in this field has mainly focused on improving the BGP protocol itself, through measures such as securing the TCP session or developing algorithms to predict BGP behaviour. However, despite these efforts, there are still gaps in the security of BGP routing networks. In this paper, we propose to address these gaps by leveraging machine learning techniques. Specifically, ML algorithms can effectively analyze large volumes of data to detect anomalous behaviors, identify patterns, and predict potential threats. By learning from historical data, ML models can detect and prevent APTs before they cause significant damage. Additionally, ML can help respond to APTs quickly by automating the analysis of vast amounts of data, enabling security teams to respond to threats in real-time. Thus, we will investigate how incorporating machine learning can enhance the security of BGP routing networks against APTs.

2. Literature Review

- Detecting anomalies in Border Gateway Protocol (BGP):

These articles and research papers (Li, Rios and Trajkovic, 2022), (Paiva et al., 2021) discusses the use of machine learning algorithms and Autonomous system classification graph for detecting anomalies in Border Gateway Protocol (BGP), which is used for exchanging network reachability information among autonomous systems in the Internet. Anomalies in BGP can result from various causes, such as infrastructure failures, router misconfigurations, and network intrusions (Li, Rios and Trajkovic, 2022). The article analyzes and classifies recent BGP anomalies caused by the WestRock ransomware attack and evaluates the performance of supervised and unsupervised machine learning algorithms for detecting such anomalies (Li, Rios and Trajkovic, 2022). The article also introduces BGPGuard, a BGP anomaly detection tool that integrates various stages of anomaly detection. The experiments and performance evaluation show that gradient boosting decision tree and deep learning algorithms such as convolutional neural networks and recurrent neural networks are effective in detecting BGP anomalies.

- "A Survey on BGP Security Issues and Mitigation Techniques" (Hassan et al. 2018) - This paper provides a comprehensive survey of the security vulnerabilities in BGP routing and the mitigation techniques proposed in the literature. The authors discuss the various BGP security threats such as prefix hijacking, route leakage, and DDoS attacks and the techniques proposed to mitigate them. They also discuss the advantages and limitations of each technique and the challenges faced in implementing them. The paper provides a useful overview of the current state of research in BGP security and the mitigation techniques proposed in the lite.

- BGP Security Vulnerabilities: Analysis, Exploitation, and Protection (Zhang, Liu, and Mao 2011) - This paper provides an in-depth analysis of the security vulnerabilities in BGP routing protocol and proposes several strategies for prevention and response to APTs. The authors suggest that APTs can exploit BGP vulnerabilities such as AS path manipulation, prefix hijacking, and route oscillation to launch various attacks such as eavesdropping, interception, and denial of service attacks. The paper suggests several countermeasures to prevent APTs, such as the use of secure BGP extensions, route filtering, and path authentication mechanisms. They also propose response strategies such as dynamic path generation, filtering, and path verification to detect and isolate compromised routing paths caused by APTs. This paper provides valuable insights into the vulnerabilities of BGP routing and the strategies that can be used to prevent and respond to APTs.

- Another Relevant work related to my research question is "Securing BGP - A literature survey" by Geoff Huston, Mattia Rossi and Grenville Armitage (Huston, Rossi and Armitage, 2011). The paper provides an in-depth survey of the current state of research on securing the Border Gateway Protocol (BGP). The paper begins by discussing the design of BGP and its vulnerabilities. BGP is a distributed and dynamic protocol that relies on trust relationships between autonomous systems. This trust model is vulnerable to attacks, such as spoofing and route hijacking, that can be used to manipulate routing information and divert traffic to unauthorized destinations. The paper also discusses the potential consequences of these attacks, including disruption of network services, eavesdropping, and interception of data.

  The paper then reviews the existing approaches to securing BGP, including resource certificates, Route Origin Authorization (ROA), and BGPsec. Resource certificates are digital certificates that are issued by a trusted authority to authenticate the ownership of IP address blocks. ROA is a mechanism that allows network operators to specify the origin of their routes and authorize them to be propagated through BGP. BGPsec is a security extension to BGP that provides digital signatures for routing information, ensuring its authenticity and integrity.

  Lastly the paper also examines the challenges of implementing these security measures. These challenges include the complexity of BGP, the distributed nature of the internet, and the need for a coordinated effort by all autonomous systems to adopt these measures. The paper highlights the potential impact of these solutions on the internet routing system, including increased overhead, longer convergence times, and the risk of creating new vulnerabilities.

In conclusion, the literature suggests that APTs can exploit various vulnerabilities in BGP routing to launch attacks such as eavesdropping, interception, and denial of service attacks. To prevent and respond to these attacks, various strategies such as secure BGP extensions, route filtering, and path authentication mechanisms have been proposed in the literature. Furthermore, a comprehensive survey of BGP security vulnerabilities and mitigation techniques can provide a useful overview of the current state of research in BGP security.

2.1 Research Niche

Based on the research questions and the literature review, the research niche is investigating the effectiveness of specific prevention and response strategies against advanced persistent threats on BGP routing. This will involve evaluating the proposed strategies in a real-world or simulated environment and measuring their effectiveness in detecting, preventing, and responding to APTs.

The expected contribution of the research would be to provide a deeper understanding of the vulnerabilities in BGP routing and the most effective prevention and response strategies against APTs. By evaluating the effectiveness of specific strategies, this research could potentially identify the most effective techniques for detecting and mitigating APTs, which could be useful for network administrators, security professionals, and policy-makers. Additionally, this research could potentially contribute to the development of new and more effective prevention and response strategies against APTs on BGP routing.

3. Research Method & Specification

3.1 Research Method

The proposed solution to the research question of preventing and responding to APTs on BGP Routing Using Machine Learning (ML) entails developing a machine learning-based system that can detect and respond to APTs on BGP routing. This system will analyze network traffic and detect anomalies in BGP routing using ML algorithms. When an anomaly is discovered, the system will either block the malicious traffic or notify the network administrator. To improve its detection of APTs, the system will be trained on historical network traffic data, including both benign and malicious traffic.

Here are some potential use cases:

Anomaly detection: One of the key challenges in preventing APTs on BGP Routing is identifying abnormal traffic patterns that may indicate a security breach. ML models can be trained on historical traffic data to learn what is normal, and then used to detect anomalies in real-time. AI-based systems can further enhance anomaly detection by analyzing large amounts of data and identifying patterns that would be difficult for humans to detect.

Threat intelligence: ML models can be used to analyze and categorize threat intelligence feeds to help identify potential threats and vulnerabilities in BGP Routing. By using ML to automate the analysis of large amounts of data, analysts can save time and quickly identify threats that may be difficult to detect otherwise.

Incident response: In the event of a security breach, ML and AI can be used to help automate the incident response process. For example, an AI-based system could automatically isolate the affected network segment and prevent further spread of the attack, while ML models could help identify the root cause of the breach and recommend appropriate remediation steps.

Predictive analysis: ML models can be used to predict potential APT attacks on BGP Routing by analyzing historical data and identifying patterns that may indicate an upcoming attack. By identifying potential attacks in advance, security teams can take proactive measures to prevent the attack from occurring.

Network segmentation: ML models can be used to help segment BGP networks into smaller, more manageable sections, making it easier to detect and respond to security breaches. By breaking up the network into smaller segments, security teams can better control access to critical systems and limit the impact of any potential security breaches.

In summary, ML models and AI will be used to enhance prevention and response strategies for APTs on BGP Routing by automating key tasks, analyzing large amounts of data, and predicting potential attacks. By leveraging these technologies, security teams can better protect their networks and respond quickly in the event of a security breach

3.2 Expected Steps and Activities

Data collection: Collect data on APTs on BGP Routing, including historical traffic data, threat intelligence feeds, and incident response data.

Data preparation: Prepare the data for analysis, including cleaning and preprocessing the data as needed.

ML model development: Develop machine learning models to analyze the data and identify anomalies, predict potential attacks, and segment the network.

AI-based systems: Investigate the use of artificial intelligence-based systems, such as natural language processing and computer vision, to enhance APT prevention and response strategies.

Validation: Validate the effectiveness of the ML models and AI-based systems in preventing and responding to APTs on BGP Routing through simulation or testing in a real-world scenario.

3.3 **Test data identified for research and validation.**

Data sources: The research will identify and collect data from a variety of sources, including:

1) Network traffic data from BGP routers
2) Threat intelligence feeds from third-party sources
3) Incident response data from previous security breaches

4) Open-source data on APTs and cyber attacks

3.4 Evaluation

Data analysis: Analyze the data using appropriate ML techniques, such as anomaly detection, predictive modeling, and network segmentation. The analysis should will to identify patterns and trends in the data that can be used to develop effective prevention and response strategies.

ML model development: The ML models will be developed based on the data analysis that can be used for anomaly detection, predictive analysis, and network segmentation. The models should be trained on historical data and validated on new data to ensure their effectiveness.

AI-based systems: This research will investigate the use of AI-based systems, such as natural language processing and computer vision, to enhance APT prevention and response strategies. This may involve developing new AI-based tools or using existing tools that have been adapted for cyber-security purposes.

Validation: This research will validate the effectiveness of the ML models and AI-based systems in preventing and responding to APTs on BGP Routing through simulation or testing in a real-world scenario. This may involve setting up a test environment to simulate an attack and measuring the effectiveness of the prevention and response strategies developed in the study.

Overall, this research methodology and specification would involve collecting and analyzing data on APTs on BGP Routing, developing ML models and AI-based systems to enhance prevention and response strategies, and validating the effectiveness of these tools in a real-world scenario. The study would aim to identify best practices for using ML and AI in cyber-security, particularly in the context of APTs on BGP Routing

3.5 ETHICAL CONSIDERATIONS

Ethical consideration must be considered during any research process, and I have highlighted a few issues that would be associated with the research for this particular study.

- **Protecting data privacy:** This research will ensure that the data used and collected will be used in way that respects the privacy of the individual or organization.
- **Using machine learning responsibly:** The use of machine learning in research can have both positive and negative consequences. This research will use machine learning responsibly, considering its potential impact on society and ensuring that its application adheres to ethical standards.
- All data and datasets sources would be cited in order to register the use of that party's intellectual property.

- **Communicating research findings accurately and honestly to the public:** This research will present its findings in a clear and accurate manner, avoiding any exaggeration or misrepresentation of the results.

3.5 Project Plan

The following is a Gantt chart illustrating the project schedule that will enable the research project to be finished is provided below:

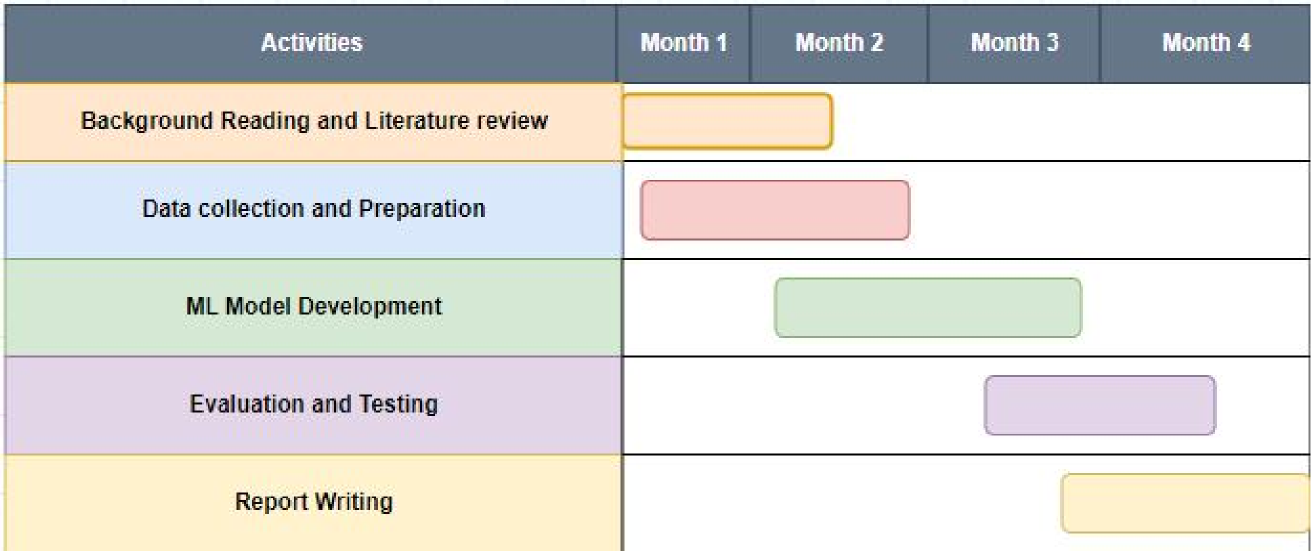

FIGURE 3.5

REFERENCESF

Alshamrani, A. and Chowdhary, A. (2019). *A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities*.

Bahnasy, M., Li, F., Xiao, S. and Cheng, X. (2020). DeepBGP. *Proceedings of the Workshop on Network Meets AI & ML*. doi:https://doi.org/10.1145/3405671.3405816.

Butler, K., Farley, T.R., McDaniel, P. and Rexford, J. (2010). A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE*, [online] 98(1), pp.100–122. doi:https://doi.org/10.1109/jproc.2009.2034031.

Engel, T. (2018). *The State of Affairs in BGP Security: A Survey of Attacks and Defenses*.

Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K. and Aparicio-Navarro, F.J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, 89, pp.349–359. doi:https://doi.org/10.1016/j.future.2018.06.055.

Huston, G., Rossi, M. and Armitage, G. (2011). Securing BGP — A Literature Survey. *IEEE Communications Surveys & Tutorials*, 13(2), pp.199–222. doi:https://doi.org/10.1109/surv.2011.041010.00041.

Li, Z., Rios, A.L.G. and Trajkovic, L. (2022). Machine Learning for Detecting the WestRock Ransomware Attack using BGP Routing Records. *IEEE Communications Magazine*, pp.1–7. doi:https://doi.org/10.1109/mcom.001.2200215.

Paiva, T.B., Siqueira, Y., Batista, D.M., Hirata, R. and Terada, R. (2021). *BGP Anomalies Classification using Features based on AS Relationship Graphs*. [online] IEEE Xplore. doi:https://doi.org/10.1109/LATINCOM53176.2021.9647824.

Wikipedia. (2022). *Computer security*. [online] Available at: https://en.wikipedia.org/wiki/Computer_security#cite_note-:2-1.

Zhang, Y., Liu, Y., & Mao, J. (2011). BGP security vulnerabilities: Analysis, exploitation, and protection. IEEE Communications Surveys & Tutorials, 13(3), 539-557. (n.d.).