***2021 Cohort Synoptic Project:***

***Abstracts Submitted April 24***

|  |
| --- |
| 1. [A Critical Evaluation of Methods for Community Detection in Peer-to-Peer File Sharing Networks](#a)
 |
| 1. [A Critical Evaluation of Network Traffic Attributes for the Identification of Spyware](#b)
 |
| 1. [A Critical Evaluation Of The Resilience Of Multi-Factor Authentication Within Constrained Industrial Environments](#c)
 |
| 1. [A Novel Approach to Analysing So4ware Features: Exploring New Ways of Automating Reverse Engineering](#d)
 |
| 1. [Applying Machine Learning to Radio Frequency Deinterleaving](#e)
 |
| 1. [An Evaluation of the Feasibility of Anonymous Communications while under Heavy Surveillance](#f)
 |
| 1. [The creation and critical evaluation of a Dynamic Binary Instrumentation evaluation framework](#g)
 |
| 1. [Evaluating the accuracy of radio monitoring techniques at the detection of radio disruption attacks](#h)
 |
| 1. [A Critical Evaluation of Hashing Techniques](#i)
 |
| 1. [The Evolution of Malware Deployment by Cyber Threat Adversaries](#j)
 |
| 1. [A Comparative Study of Load Balancing Efficacy: P4 Programmable Data Plane Switches Versus Traditional Network Switches](#k)
 |
| 1. [No abstract](#l)
 |
| 1. [A Critical Evaluation Into Social Engineering Methods Utilized By Advanced Persistent Threats](#m)
 |
| 1. [A Critical Evaluation of Ransomware Operators’ Changing Attitudes to the Healthcare Sector](#n)
 |
| 1. [Evaluation Of The Threat Of Destructive Capabilities Across The Iranian Offensive Cyber Spectrum](#o)
 |
| 1. [Analysing MacOS Log Reporting and Counter Detection Mechanisms for Enhancing Cybersecurity](#p)
 |
| 1. [A critical evaluation of using Artificial Intelligence (AI) to conduct reconnaissance to identify target vectors for a penetration test.](#q)
 |
| 1. [A Critical Analysis of Reverse Engineering Methodologies Against Mobile Applications](#r)
 |
| 1. [Evaluating Machine Learning Techniques for Anomaly Detection in Univariate Time Series Datasets](#s)
 |
| 1. [A Critical Evaluation of the Potential Impact of Compiler Optimisations on Security Integrity](#t)
 |
| 1. [Assessing the Evolution of Security Measures: A Comparative Study of IPv4 and IPv6](#u)
 |
| 1. [Critical evaluation of automated versus traditional approaches to compiling and aggregating research from multiple sources](#v)
 |
| 1. [Critical assessment of the Effects of Voltage Fault Injection on Microelectronic Devices and Their Potential Countermeasures](#w)
 |
| 1. [Comparative Analysis of the deployment of trust cues in websites](#x)
 |
| 1. [A Critical Evaluation of Geolocation Methods Within Ad-tech](#y)
 |
| 1. [Critical Evaluation of Current Encryption Standards](#z)
 |
| 1. [Critical Evaluation Of The Efficacy Of Contemporary Malware Identification Techniques](#aa)
 |
| bb) [An assessment of the Efficacy of Different Anti-Scraping Technique Implementations](#bb)  |
| cc) [Critical Analysis of Simple Network Management Protocol to](#cc)[Identify The Optimum Secure Configuration of SNMPv3](#cc) |
| dd) [An evaluation of the internet footprint of Docker containers with varied configuration options](#dd) |
| ee) A [Critical Analysis of Cybersecurity Threat Modelling](#ee) |
| ff) ) [A Critical Evaluation Of Machine Learning Powered Ddos Detection Tools](#ff) |
| gg) [A Critical Evaluation of Client Attitudes towards the Penetration Testing Process](#gg) |
| hh) [A critical evaluation of the potential of Large Language Models to democratise cybercrime](#hh) |

|  |
| --- |
| **a) A Critical Evaluation of Methods for Community Detection in Peer-to-Peer File Sharing Networks** |
| **Abstract**Peer-to-peer file sharing networks such as BitTorrent and the InterPlanetary File System (IPFS) are becoming increasingly ubiquitous, threatening to make centralised enterprise network monitoring redundant. Recent studies have identified community detection as a method for analysing users on a decentralised network to gain insight into the types of activities they perform. The purpose of this study was to evaluate modern community detection algorithms to identify the most performant technique for accurately identifying communities formed around a shared interest in peer-to-peer networks. Synthetic data from a probabilistic data generation model for peer-to-peer networks was used to assess the accuracy and execution time of multiplecommunity detection methods, spanning traditional modularity-based methods such as the Girvan-Newman algorithm to modern vector embedding models such as node2vec. The findings from this experiment reveal the spectral clustering model and the node2vec vector embedding model perform the best for identifying communities of users in peer-to-peer networks, despite taking two to four times as long to execute than the best performing traditional community detection model, the Louvain algorithm, assessed using synthetic network snapshots ranging from 500 to 7500 users. The ability to identify communities in a peer-to-peer network has the potential to be a vital step in network analysis tools as enterprise networks become increasingly decentralised, such as being an important stage in anomaly detection routines to detect users performing actions abnormal to the actions of the community they belong to. Identifying the best performing algorithms enables future work on decentralised network analysis tools by providing the best foundation algorithms upon which to develop further analysis techniques. |
| **b) A Critical Evaluation of Network Traffic Attributes for the Identification of Spyware** |
| **Abstract**In an age where an increasingly large amount of personal data is stored onindividual devices, identifying and protecting against spyware intent to steal such data is more important than ever. Modern techniques for the general identification of malware involve the usage of machine learning to create efficient and adaptive detectors of malicious activity. Spyware is a type of malware that performs reconnaissance on a personal device, before sending the collected data back over a network. This report intends to add to the research surrounding spyware detection by investigating spyware detection over a network, and identifying network-based features that are of the most importance when determining whether a network communication is related to spyware. This will allow machine learning techniques to be enhanced, since strong models will need features to be selected to achieve the best results. To achieve this, a database containing benign and malicious spyware PCAP files was analysed via six different feature selection techniques, and the results were compiled together to form a list of features which have the most importance when determining whether a packet is a spyware packet. Interpretation of these features was performed, and a reflection as well as a recommendation for further work outlined. |
| **c) A Critical Evaluation Of The Resilience Of Multi-Factor Authentication Within Constrained Industrial Environments** |
| **Abstract** Authentication is an important part of everyday life, especially in working environments. Using Multi-Factor Authentication (MFA) is important for security of sensitive information. However, there are industrial environments with unique constraints that prevent usual MFA methods from working, such as having no internet connection or requiring urgent access. The purpose of this report is to determine what MFA methods are possible and how viable they are in air-gapped industrial environments.A literature review was conducted to gather insight into what MFA is, the challenges of constrained environments, what research has already been done in the area and what MFA methods may be possible. This led to the identification of many methods that can be tested, where five were chosen for this experiment. These methods were divides between two devices – with fingerprint recognition, facial recognition and smart cards being tested on an engineering workstation (EWS), and domain user accounts, time-based one-time passwords (TOTP) and smart cards being tested on a human-machine interface (HMI). With this, a methodology was created to assess them. This methodology encompasses the testing environment, the testing process and a framework to analyse the results. Each method was configured to be the authentication method of the relevant device in the network. After this, they were tested repeatedly to determine how long each method takes to authenticate, finally the methods were analysed and discussed to see how secure and accessible they are compared to the framework defined in the methodology. Single factor authentication was tested as well as a control to see if MFA would be an improvement. The results of the experiment show that facial recognition with Windows Hello is the most effective MFA method for an EWS, being fast, secure and accessible. However, for an HMI, MFA takes significantly longer and does not improve security, therefore MFA is not recommended on an HMI. It was also discovered that key areas for future research include testing the rollout processes of each method to discover the costs and inconveniences of that process and testing with more people (such as real industry employees) in a real industrial environment. |
| **d) A Novel Approach to Analysing So4ware Features: Exploring New Ways of Automating Reverse Engineering** |
| **Abstract**The reverse engineering field is broad and has uses both usefully and nefariously. The rise of free reversing tools, such as Ghidra, has made Software Reverse Engineering (SRE) accessible to the masses. The sharp rise in SRE CTF (capture the flag) challenges and online learning resources has made gaining a fairly detailed understanding of the field easier. As is an emerging theme with computing there is starting to be more of a shift to automation. Tools are geQng beRer at accurately reversing binaries, but due to ever-improving obfuscation techniques this is a difficult problem. This project explores, are there any new techniques that could be utilised to aid a researcher in speeding up the process of reverse engineering?When first encountering a binary, and aRemp)ng to find out its functionality, a researcher has several ini)al avenues they could go down to successfully reverse the program. For example, they could open the program is a large piece of software like Ghidra or IDA, run various commands against it to gain some ‘low hanging fruit’. However, is there an effective tool that allows quick, efficient initial triage of a program, allowing the researcher to quickly see useful information about the program?This project explores current literature in this field and certain key-takeaways are identified that are used to inform methods that are later implemented. The result, a proof-of-concept tool that’s designed to streamline the initial stages of reversing is then tested and analysed. |
| **e) Applying Machine Learning to Radio Frequency Deinterleaving** |
| **Abstract**Radar Pulse Deinterleaving is an important task for electronic countermeasures. This report looks at the application of Machine Learning to seperating signals from different emitters referred to as the deinterleaving problem. In particular it performs an analysis of the effect of changing the size and depth of transformers and RNNs architectures on RADAR pulse deinterleaving performance as well as the affect on performance of combining the output embeddings of a transformer and an RNN model. The key findings are that firstly, as a transformers size increases so does its performance for PDW deinterleaving, and secondly, the combination of models provides better results than either model by itself. It should be noted that a synthetic dataset was used in this project and that these findings may not hold for real data. |
| **f) An Evaluation of the Feasibility of Anonymous Communications while under Heavy Surveillance** |
| **Abstract**Many people, particularly those in authoritarian regimes, are subject to unjusttreatment, censorship, and persecution. Examples given are Uyghur Muslimsin Xinjiang and Russian critics of the invasion of Ukraine. Surveillance is oftenexploited in these scenarios, to identify dissidents and suppress the transfer oftruthful information.This paper intends to provide information on how anonymous communicationscan be used in these scenarios to escape surveillance and allow thetruthful transfer of information. To this end, existing anonymous communicationsolutions are identified, and a novel solution is proposed by this paper;together these are critically evaluated to determine whether they are suitablein these situations. It is found that while existing solutions fall short of providingthe necessary assurance that communications will not be identified by surveillance,the novel solution does provide the necessary safety.Overall, this paper shows that it is possible to conduct anonymous communicationsin highly adversarial situations in order to evade surveillance andprotect users from unjust treatment. The paper proposes future work on thetopic, and advocates for future development of anonymous communicationssolutions to take into account users in such scenarios, where anonymous communicationsare typically identifiable by surveillance and such identification canresult in catastrophic scenarios for users. |
| **g) The creation and critical evaluation of a Dynamic Binary Instrumentation evaluation framework** |
| **Abstract** When reverse engineering software, the reverse engineer deploys a variety of techniques in order to gain an understanding of how either the program as a whole, or a part of the program works and is implemented (Teodoro Cipresso, 2010). Software reverse engineering is split into two paradigms, dynamic and static analysis, with dynamic analysis analysing the behaviour of a running program (Or-Meir, Nissim, Elovici, & Rokach, 2019) and static analysis analysing the characteristics of a program, without executing it (Johnson, Song, Murphy-Hill, & Bowdidge, 2013). One such dynamic analysis technique is dynamic binary instrumentation (DBI). This project seeks to identify features common to DBI tools that can influence the success of the reverse engineering process via the means of practical reverse engineering using DBI tools along with the surveying of reverse engineers. A literature review is carried out, critically exploring and evaluating concepts key to reverse engineering as well various dynamic and static software reverse engineering (SRE) techniques, before focussing in on DBI. Additionally, the methodology section details the steps undertaken to select applications, and their functionality, to be reverse engineered as well as the steps necessary to setup an environment and applications suitable for DBI. The methodology also details the survey method performed to evaluate data generated under the practical stage as well as generating new data for this project. The results and discussion section of this project presents the findings of this project. The results in this project were mixed, they reveal a number of key aspects within DBI tooling that have some level influence on the success of reveres engineering an application, but no consensus on the amount of influence is achieved. The future work section sets out what could be performed in the future to improve the quality of these results. |
| **h)** **Evaluating the accuracy of radio monitoring techniques at the detection of radio disruption attacks** |
| **Abstract** As digital systems transition to a more wireless and interconnected architecture, the vulnerabilities that exist within Radio Frequency (RF) communications systems become a more serious risk. This project has aimed to contribute to research that supports defensive monitoring as a risk management approach to RF disruption. The aim has been addressed through the summary of attacks and detection techniques captured in the literature review, followed by the development of a practical to provide tangible data reflecting the performance of radio monitoring techniques. This took the shape of a binary classification task between a GSM signal and a noise-based RF jammer. Jamming was identified as the threat to focus on because mitigations aren’t possible on a protocol level, so radio monitoring is one of the few approaches at counteracting this attack. The performance comparison between random forest-based machine learning techniques and a metrics driven approach on physical layer RF has shown that defensive monitoring is feasible with current technologies. The exceptional adaptability and accuracy of machine learning on RF has highlighted this as an important future area of research. |
| **i)** **A Critical Evaluation of Hashing Techniques** |
| **Abstract**The rapid development of artificial intelligence (AI) in recent years has provided a capability of large-scale image identification at an accuracy to rival that of humans. However, for small scale applications where there is insufficient data to provide the training a large AI model an requires. This project looked to find the most accurate image hashing algorithm for determining image similarity between company logos to an accuracy level where they are trusted in a reverse image search scenario. Relevant literature was reviewed, outlining the development of hashing algorithms and the current landscape with regards to image hashing, allowing for the identification of potential algorithms to be taken forward for future study, with the perceptual hash and wavelet hash of two different lengths each being selected for evaluation. From previous studies, four image variation techniques were selected to be applied to the images, which were randomly sampled from a dataset of company logos. Experiment and evaluation methods were applied to analyse the performance metrics gathered during the algorithm testing. The overall performance of each algorithm was considered, along with the focussed breakdown of how different image variations affected performance and whether any discrepancy between algorithms could be identified. The results of this experiment lead to the 256-bit perceptual hash being identified as the most effective algorithm, scoring highest in accuracy and collision resistance, and was taken forward for the development of the reverse image search POC. Performance evaluation of this POC revealed it showed strong performance. |
| **J)** **The Evolution of Malware Deployment by Cyber Threat Adversaries** |
| **Abstract**The evolution of malware poses significant challenges to cybersecurity professionals and industry stakeholders across the world. This paper aims to provide an analysis of malware deployment trends by using historical and modern-day data about the evolution of cyber threat adversaries. This paper does not try to solve the problem of malware deployment, rather to inform readers on the impacts malware has on the cyber world and provide insight to the direction malware deployment is heading by extrapolating from historical data.The paper contains a literary review concerning malware ranging from pre internet era to modern day commodification of malware. This reveals the many ways malware has changed and evolved from physical media and sneakernet malware into the worldwide issue that it is today. The literature review aims to inform readers on the different eras of malware and to ensure a baseline understanding of malware families so that the methodology can be easily understood.The methodology contains explanations of the practical work completed including data selection, reducing errors and bias, and the work done to analyse the processed data. Several datasets are processed and analysed to provide insight into the development of new malware families and how they impacted the cyber landscape over a 5-year period.The results showed a general increase in the amount of malware in the world and its sophistication with a particular increase in encryption based and downloader-based malware families. It is noted that a level of bias could have been introduced through the data selection and preparation stages however this is reduced where possible by scrutinising the data against global reporting and equating the results to key points of interest and major cyber incidents |
| **k)** **A Comparative Study of Load Balancing Efficacy: P4 Programmable Data Plane Switches Versus Traditional Network Switches** |
| **Abstract**This project examines the efficacy of P4 programmable data plane switches versus traditional network switches in load balancing. As networks grow and require more robust load distribution, current methods fall short. Software load balancers lag behind the speed demands of modern networks, while hardware solutions are controlled by manufacturers. This study assesses the potential of programmable switches to deploy transparent and customizable data plane algorithms for improved load balancing. After conducting a broad literature review and developing a custom P4 program, performance evaluations were carried out under controlled conditions. The results show that P4 switches not only match but occasionally surpass the performance of traditional switches, particularly in certain traffic scenarios. By demonstrating superior performance and greater distribution of traffic, P4 programmable switches represent a significant step forward in network technology, suggesting that future network infrastructure investments should consider the enhanced capabilities that programmable data plane technology offers. |
| **l)** **Feasibility of Command & Control (C&C) Channel Detection Using Machine Learning** |
| No Abstract |
| 1. **A CRITICAL EVALUATION INTO SOCIAL ENGINEERING METHODS UTILIZED BY ADVANCED PERSISTENT THREATS**
 |
| **Abstract** As the number of cyber-attacks around the world continues to increase, companies are beginning to look closely at how they can secure their systems. With threats ranging from script kiddies to advanced persistent threats, it is essential that the cyber industry remains updated on the latest techniques used by these threats to help secure the systems we rely on. The review into academic literature on the subject, identified that the most common access vector into a computer system was through social engineering. Further research concluded that out of all the social engineering methods, phishing was the most popular. During the review it was noticed that there is lots of literature for training on the prevention of social engineering attacks, but little on the tools and techniques attackers use to perform them. This review of literature, helped to inform the methods which set out to test and compare three different social engineering tools: GoPhish, Social Engineering Toolkit, and Social Fish. Each tool was setup and used to create a phishing campaign, and then assessed for which performed best on a variety of metrics: ease of use, speed to setup, quality of payload. Overall, it was concluded that GoPhish provided the attacker with the best system to launch and manage phishing campaigns, especially at scale. Completion of this project demonstrates just how simple it is to perform a social engineering attack. There are many tools out there that simplify and automate the process, allowing attackers to quickly setup and manage phishing campaigns at scale. This paper opens the potential for lots of future work, such as testing large scale campaigns or actual deployment of phishing payloads to assess how real-world users would interact with them. |
| **n)** **A Critical Evaluation of Ransomware Operators’ Changing Attitudes to the Healthcare Sector** |
| **Abstract**This synoptic project seeks to assess whether ransomware operators attitudes havechanged towards the healthcare sector. Ransomware is the major cyber threat at themoment due to its widespread use and capacity to cause havoc. This is particularlyimportant to the healthcare sector, where life or death decisions are made daily. Any impacton these systems could prove disastrous.It starts by creating a series of aims and objectives to allow for effective research. Theliterature review covers what ransomware is, how it works, and how the ecosystem around itfunctions. It also assesses the literature available on the subject of ransomware inhealthcare facilities. The experiment is laid out through the methodology and includesinformation about the two ransomware datasets that will be used. These cover bothhealthcare and wider sectors. The results uncover statistical trends within the data, includingthe fact that ransomware attacks are in general increasing, while against US healthcareproviders there are signs it could be decreasing. |
| 1. **Evaluation Of The Threat Of Destructive Capabilities Across The Iranian Offensive Cyber Spectrum**
 |
| **ABSTRACT** The Iranian state is a well-known cyber threat that often associated with very aggressive, low sophistication attacks against their adversaries and Iranian dissidents. While their best known for their social engineering and espionage campaigns, strictly destructive attacks have also been deployed in the past, with Shamoon being one of the most infamous wiper attacks in cyber history. This project will take a deeper look into Iran’s use of destructive capabilities of which the threat will be assessed. A thematic literature review is performed covering the key concepts and areas that are relevant in order to conduct the project. The literature review will also be used to inform the methodology chapter and the presentation of results. The methodology chapter includes the processes followed at each step of the project in order to make it fair and repeatable. Covering what data will be used and how it will be analysed, as well as identifying how the results will be evaluated to answer the research questions set out at the beginning of the project. The results indicated a strong use of personas, particularly to perform destructive attacks. This use of personas make attributing each group to a wider Iranian organisation very difficult, and it is likely that personas will remain a big part of how Iran operate their cyber-attacks. Some surprising results on well-known threat actors performing destructive attacks questioned the historical evidence, however a few potential reasons for this are addressed. The findings of this project also pose implications for future academic efforts in this same area, informing what could be done next time. |
| **p)** **Analysing MacOS Log Reporting and Counter Detection Mechanisms for Enhancing Cybersecurity** |
| **Abstract**This dissertation examines the effectiveness of macOS's error reporting and counter-detection systems in enhancing cybersecurity defences. The main objective is to assess these systems, identify their advantages and disadvantages, and recommend changes to fortify macOS's security architecture. Given the increasing sophistication of cyber-attacks and the critical role operating systems play in reducing these risks, this inquiry is essential.  An intensive analysis of the literature, a detailed examination of macOS's error reporting systems, and an evaluation of its counter-detection methods are all part of the research process. The literature review establishes a theoretical foundation by outlining the state of research gaps in error reporting and counter-detection techniques across operating systems, with a particular focus on macOS's unique architecture and user base.To assess how well macOS's crash reports, error messages, and log files identify and handle abnormalities, illegal access attempts, and other possible security risks, a thorough examination of these materials is part of the empirical investigation. This study parses, analyses, and visualises data using technologies including Security Information and Event Management (SIEM) systems, specialised log analysis software, and custom scripts. This gives researchers a thorough understanding of how sensitive the operating system is to security threats. The results highlight the advantages and disadvantages of the current macOS error reporting and counter-detection systems. The dissertation provides particular recommendations targeted at improving log granularity, strengthening the system's resilience to new threats, and improving error detection systems based on these insights.In the end, this research contributes to the larger conversation about cybersecurity by offering theoretical and practical improvements that can fortify macOS against a variety of cyber threats and make users' computing environments safer.  |
| **q)** **A critical evaluation of using Artificial Intelligence (AI) to conduct reconnaissance to identify target vectors for a penetration test.** |
| **Abstract**Penetration testing is a field which can be complex and has many aspects which can be time consuming, in particular handling the vast volumes of information in the reconnaissance and scanning stages. Artificial Intelligence (AI) is a rapidly growing technology which provides the potential to help solve complex problems which require contextual understanding. Due to the novelty of AI, there is limited research on its application specifically within penetration testing. This study investigates the potential of AI to be used to enhance the penetration testing process. The existing attempts to improve penetration testing have been to utilise automation by researching these existing methods the performance of AI can be critically evaluated to identify potential areas for improvement and areas where conventional approaches are better suited. In this project AI is used to conduct the reconnaissance and scanning stages of a penetration test against sample target machines. This is done by using the GPT-4 model from OpenAI to provide commands to execute against a target machine and the results of this. In the experiment AI clearly demonstrated a potential to contextualise information discovered and how to proceed due to the information found. AI was able to achieve the required steps with minimal external assistance for easy and medium machines from HackTheBox (HTB) but was unable to succeed against a hard machine. It is clear however, that AI has the potential to greatly assist less experienced penetration testers as well as to improve the existing process. Future research should be conducted into how automation can be combined with AI to further improve upon the benefits AI and automation provide individually |
| **r)** **A Critical Analysis of Reverse Engineering Methodologies Against Mobile Applications** |
| **Abstract** The rapid expansion of portable devices over the last two decades has in turn cause an enormous growth in mobile application development. Mobile applications are now an essential tool in the majority of people’s day. Therefore, the constant need to increase the security of development is extremely important to many app developers. This paper aims not only further knowledge of reverse engineering methodologies against Android applications but also to critically compare said methodologies to evaluate their effectiveness. Furthermore, it also aims to spread the knowledge of the value of reverse engineering to application developers in the hope that it is more widely used in the development and testing phases of new applications.The literature review critically evaluated contemporary literature to introduce knowledge around Android applications and how and why reverse engineering them can be beneficial. It revealed some of the common effective methodologies used including static and dynamic analysis. It furthermore comments on the different tools that can be used for these methodologies such as JADX and Frida. The methodology outlines the methodologies used in the practical experiment and rationalizes their uses. Three methodologies were selected to be used in the practical experiment in the methodology including:- User Testing- Static Analysis- Dynamic AnalysisFinally, the results of the practical experiment reveal the effectiveness of the different methodologies and how best to use them. Although different methodologies should be considered depending on the type of target application, a general approach was suggested. This was a smooth progressive approach which incorporates all three methodologies sequentially is effective against a large number of applications. |
| **s)** **Evaluating Machine Learning Techniques for Anomaly Detection in Univariate Time Series Datasets** |
| **Abstract**Detecting anomalies in time series is vital, with great commercial and academic interest expressedin the subject. An anomaly can indicate many things depending on the context of the data, such as a manufacturing issue, a network intrusion, or an access control failure. This project sets out to evaluate the performance of a variety of machine learning techniques, with differing complexity, on time series data. The project aimed to research machine learning models already used in time series anomaly detection and understand their implementation. It also aimed to research which datasets were used to test the models in the current academic research.A thematic literature review was used to gain a foundational understanding of time series data and anomalies. It identified the three types of anomalies used in the project. This review also covers supervised and unsupervised machine learning approaches before introducing the specific models. The models presented were the support vector machine, the convolutional neural network, and the isolation forest. The review then identifies several datasets, recommending the Yahoo Webscope S5 dataset.The evaluation metrics identified in the literature review are accuracy, precision, recall, and the F1 score. These provide a holistic view of the model performance, with particular emphasis placed on precision and recall.The methodology laid out how the models would be tested against the chosen Webscope S5 dataset.The models would be trained and tested on all 67 datasets within S5, with average scores produced for evaluation with the metrics identified in the literature review. There would also be a qualitative evaluation of the model performance for each type of anomaly. The implementation for each modelvaried and the support vector machine required deviations from the methodology to produce a working example.The results found the isolation forest performs very well at identify simple point anomalies, where they clearly lie outside of the expected data. The convolution neural network encountered issues with insufficient training data, however in the functioning examples demonstrated relatively good performance compared to the other models when identifying complex collective and contextual anomalies.The support vector machine performed worse than the two other models, producing unreliable and inaccurate results over most of the data. |
| **t)** **A Critical Evaluation of the Potential Impact of Compiler Optimisations on Security Integrity** |
| **Abstract**Compiler optimisations are used to increase the performance of executable code; however, these have been proven to introduce vulnerabilities within secure code through a variety of methods (Yang and Johannesmeyer, 2017). The unique attributes of these, such as not being able to detect them within source code, contributes to them being potentially very high impact, whilst also being hard to mitigate against.Within this project, compiler-introduced optimisation vulnerabilities are analysed to determine their effects and the risks undertaken by using both optimisation flags and optimisation levels when compiling code. This is then compared to current practice to determine the potential risks being taken within code being written by programmers of a wide range of backgrounds.A critical review of literature is conducted first to identify current knowledge on optimisation vulnerabilities. The reason behind such vulnerabilities is found, typically the handling of undefined behaviour in an unintended manner. This allows such vulnerabilities to be understood, with the methods and mitigations being analysed to inform the experiments.The methodology outlines the process of conducting all aspects of this study, such as determining the scope of the experiments and how previous research will inform experimentation. This also discusses mitigations for issues regarding the way the experiment has planned, to allow a more reliable and widely applicable result. The investigative method results revealed that most vulnerabilities are caused by undocumented optimisations, however, four compiler flags were found that were verified to introduce vulnerabilities within code. It also led to a more accurate dataset being created than that within the study by Xu et al. (2023), which the investigation was based on. Within the undocumented optimisations, there were some at O0 which presented an urgent need for mitigation as code actively chosen to have no optimisations during compilation may still have introduced vulnerabilities. The statistics of vulnerabilities per optimisation level were also determined to provide an informed risk of utilising each of them during compilation.The survey highlighted the knowledge gap about such vulnerabilities within less experienced programmers, indicating that awareness needs to be raised to ensure that the severity of the problem is well understood. The usage of optimisation levels was also analysed, showing common usage at O1 and O2. This is concerning after the wide range of vulnerabilities found within the investigation at these two levels, as vulnerable code may be regularly produced. Some mitigation strategies are used, such as language mechanisms being used by most programmers. However, literature shows that certain mitigations are not guaranteed to work, thus a combination of these are needed to effectively counter the vulnerabilities (Yang and Johannesmeyer, 2017). The survey shows that this is not being done, leading to the presence of vulnerabilities that are assumed to have been countered |
| **u)** **Assessing the Evolution of Security Measures: A Comparative Study of IPv4 and IPv6** |
| **Abstract** The Internet is a vast, global network of interconnected computer devices that facilitates the exchange of data using standardized communication rules known as protocols (Rouse, 2023). This project focuses on the two main Internet Protocols (IP) – IPv4 and IPv6 - which are the addressing protocols that define a set of rules that govern how data packets are routed, addressed, transmitted, and received (Cloud Flare, no date). IPv4 is the most common but due to the “rapid growth of internet devices” (Bajrami, 2019, no page) and IPv4’s lack of address space, IPv6 was developed to “provide a solution for the eventual exhaustion of addresses in IPv4” (BasuMallick, 2022, no page). Consequently, IPv6 has become indispensable for the future of the internet and therefore its ability to secure network traffic is heavily scrutinized. This project identifies the key security factors when comparing IPv4 and IPv6 through a thematic literature review. Specifically, this highlighted IP security (IPsec) – defined as a “set of communications, rules or protocols for setting up secure connections over a network” (AWS, no date, no page) – as a critical factor. This informed the methodology, ensuring that this project builds upon the existing work by exploring the differences in IPsec usage between IPv4 and IPv6. This is delivered by implementing the processes outlined within the methodology to create simulated IPv4 and IPv6 network environments, generate and capture network traffic and evaluate the packet captures using a variety of statistical measures to explore IPsec protocol usage. Upon evaluation, it was clear that within the simulated network environments, IPv4 displayed greater usage of IPsec, with two-thirds of the IPsec protocols having higher packet counts within the IPv4 environment, thus indicating more prevalence and negating the argument that IPv6 provides additional security in comparison to IPv4 through its usage of IPsec. |
| **V)** **Critical evaluation of automated versus traditional approaches to compiling and aggregating research from multiple sources** |
| **Abstract**Selecting relevant sources for literature reviews is becoming increasingly difficult for technical researchers and academics due to the growing number of academic research papers published annually. This causes information overload, where the amount of information available exceeds an individual’s ability to process it effectively.This project proposes a Natural Language Processing (NLP)-enhanced semantic keyword search tool, which identifies and abstractedly summarises potentially relevant papers based on a user’s search. The project hypothesises that the tool could assist researchers by streamlining the search and pre-screening stages of the literature review process.Secondary research into existing literature critically discussed relevant NLP and machine learning (ML) theory, along with the theoretical process for undertaking a literature review during technical research. The review identified the current state of NLP infrastructure, identifying relevant existing technical solutions.Primary research was conducted to test the hypothesis. The thoughts and opinions of 20 technical researchers were gathered via an online questionnaire, collecting views on the literature review process, currently available tools, and gauging interest in a tool matching the description above. A proof-of-concept tool was designed and evaluated using a Jupyter notebook environment. The tool used a pre-trained Large Language Model (LLM) to perform document embedding, performed cosine similarity to rank papers according to relevance, and used a fine-tuned T5 model to perform abstractive summarisation on the top k papers. A demonstration was given to three researchers from the initial questionnaire sample group, and feedback was collected in 1-to-1 interviews.The research found that creating a tool to perform automation of this process is viable, however the project had limitations in speed and accuracy largely caused by lacking the right hardware. The author suggests that creating a similar tool on the cloud, for instance with AWS, with additional training on the dataset would vastly improve the project outcome. |
| **w)** **Critical assessment of the Effects of Voltage Fault Injection on Microelectronic Devices and Their Potential Countermeasures** |
| **Abstract**If the security of a computer’s hardware is incomplete then the system will always be vulnerable, no matter the overlaying software security. Voltage fault injection (VFI) is one such inexpensive hardware hacking technique that allows malicious actors and researchers to gain access to a system’s vulnerable hardware and cause it to operate unexpectedly. This unexpected behaviour enables the exposure of sensitive information and can act as a foothold to inject further attacks that can allow for unauthorised privileged code execution. Due to the high risk of this attack countermeasures have been developed through academia and industry, protecting devices at the hardware level and, secure code practices have been developed to mitigate the risk of the attack at the software level. This project evaluates the vulnerability of a STM32F103 microcontroller against VFI using a readily available embedded hardware security research platform called the ChipWhisperer-Lite to inject voltage glitches using a crowbar circuit. The results from testing the vulnerability of this device are further used to evaluate countermeasures from academia to identify mitigations to this attack. A literature review is conducted to provide a background into the technique as well as inform the methods later utilised to collect the data at the end of the project. The data collected is evaluated against findings from similar results in literature to put the results of this project into the context of wider literature. The project is concluded with issues encountered during the practical process and methods which could be utilised to improve further pieces of work on the topic of VFI.The results of this project demonstrate that the STM32F103 microcontroller is vulnerable to VFI attacks, and the attack used in this project can be mitigated by software countermeasures. |
| **x)** **Comparative Analysis of the deployment of trust cues in websites** |
| **No Abstract** |
| **y)** **A Critical Evaluation of Geolocation Methods Within Ad-tech** |
| **Abstract**Over the past two decades, the development of location GPS and Bluetooth enabled mobile devices has increased the availability of location-based data leading to increased opportunity in the location-based advertising (LBA) market. As a result, there have been several advertising technologies (Ad-Tech) developed for geolocating devices. Two major examples of geolocation methods with Ad-Tech are geofencing and beaconing. Many academic and industry published papers have accompanied the development of these geolocation methods revealing how these technologies have improved as well as the limitations they still face. These papers are explored in the literature review of this project which found that despite the availability of literature regarding this subject matter, little has been done to experiment on the theoretical limitations of each technology presented. As part of evaluating these geolocation methods, this project aimed to fill this research gap. This project uses several methods to evaluate the findings of the literature review. Method 1 evaluates the ability of geofencing to accurately track a device in open versus closed spaces by evaluating the time loss when moving between fences in different areas.Method 2 evaluates the interference of human and non-human barriers on beacon signal by comparing the RSSI (see glossary) and distance accuracy reported by a connected device.Method 3 evaluates the contemporary state and prevalence of beacon infrastructure by surveying the number of beacons in different areas.Whilst the findings of the literature suggested that geofencing was the best geolocation method in all open areas such as towns, cities and parks, The results of the methods showed beacon infrastructure is already prevalent and that beacons are still able to accurately able to track a device to within 1m within at least an 18m range so long as no human barriers stood within 4.5m of the beacon, between the beacon and target device. From the evaluation made of the results, the project concludes that beaconing is a better method of geolocation in all cases where a beacon infrastructure can be built, as even in open spaces such as a park, there was still time loss when tracking the time loss across exiting and entering geofences, proving that tracking a device across fences can lead to data loss and unreliable data. |
| **Z)** **Critical Evaluation of Current Encryption Standards** |
| **Abstract**As the reliance and use of the internet in everyday life increases, the ability toensure data is being transferred over networks securely is becoming more important. Making use of encryption when using the internet, helps to guarantee that only the intended recipients are receiving the initial data, protecting an individual’s right to privacy. With modern abilities to store petabytes of data having the intention to decrypt it later, it is also important for current encryption algorithms to remain strong against future technology.A review of current literature was carried out in order to assess the current state of encryption algorithms. The review attempts to summarise the whole history of encryption but, towards the end, has a particular focus on the encryption algorithms that are widely used on the internet today. This secondary research also delves into the different options for parameters in the experiment, including the programming language, development environment, type of attack, as well as the encryption algorithms to compare. The key findings include DES, AES and RSA being widely used, along with the environments to setup them up for the experiment. It was also found that, among other attack strategies, brute force attacks have proven particularly successful in the past.A methodology was developed using knowledge gained in the literature review, particularly for parameter selection. The methodology outlined how to test the strength of different encryption algorithms and implementations against brute-force attacks. The time to attempt decryption with a key along with the number of key combinations is recorded forthe three algorithms, DES, AES and RSA, to give an indication to how long, on average, a brute-force attack would take against them.The methodology was then carried out in the investigation, comparing DES, AES and RSA using different open-source Python libraries. Graphical representations of the recorded results were presented and analysed to conclude which algorithm was more resistant to brute-force attacks and what feature enabled its strong resistance. The results of the experiment show that the main feature needed to improve thebrute force resistance of an encryption algorithm is a long key size. The number of key possibilities increases exponentially as the key size grows, eventually making the time needed to execute a brute-force attack incomprehensible. Therefore, AES and RSA proved to be better than DES, due to their 256-bit key lengths. |
| **aa)** **Critical Evaluation Of The Efficacy Of Contemporary Malware Identification Techniques** |
| **Abstract**Malware is a threat to almost all modern computer systems, capable of causingdamage to individuals and companies in a wide variety of ways. With malwarethreats on the rise and ever increasing in complexity, it is necessary for cybersecurity researchers to have access to the best tools available to identify andanalyse samples of new malware when they crop up to best understand andimplement defensive measures against new threats. This project criticallyevaluates the efficacy of contemporary malware identification techniques, thereby offering cyber security researchers a justified selection of the best techniquepossible for malware identification.The literature review of this project discusses and evaluates the varying types ofmalware and the threat they pose, as well as the different levels of complexitymalware can come in and the evasion techniques implemented by malwaredevelopers in order to avoid identification. The literature review also criticallyevaluates the differing tools and techniques available to cyber securityresearchers and how successful they are at counteracting malware evasiontechniques to deliver the most reliable results.The methodology of this project outlines a standardised testing environment tocritically evaluate different tools and their capabilities against a randomised threat database, as well as a justified selection of contemporary malware identification tools to be evaluated. The results of this project show that dynamic analysis is a superior method of malware identification to static analysis, however the results also show that dynamic analysis is significantly slower on average suggesting that static analysis is not entirely invalid as a technique for some use cases. |
| **bb)** **An assessment of the Efficacy of Different Anti-Scraping Technique Implementations** |
| **Abstract**Web scraping has both positive and negative consequences. Whilst it is a great tool for the collation and categorization of information, it also poses a risk to the average user of the internet. Unmoderated web scraping can result in the theft of personally identifiable information, corporate secrets and copyrighted data. To combat these issues, a variety of techniques exist that can be used to prevent scraping from taking place on a website.A literature review was performed to develop a standard base of knowledge on relevant topics and inform the methodology used to gather the primary research needed to meet this report's goal. Also, the development of the literature review aided in determining areas where knowledge is lacking and where future work should be conducted. The knowledge gained from the literature review included various web scraping tool configurations and features, as well as the techniques used to prevent these tools from being used. Additionally, the review highlighted the history of scraping, as well as the legal and ethical concerns associated with the practice.A method was developed for the experimentation section and evaluation of data. These methodologies provided overviews on how an experiment would be conducted, including the techniques to be tested, the environment they would be tested in, and the systems implemented to limit the risk of bias and error. Evaluation methodologies outlined the systems and metrics used to evaluate and analyze the data in accordance with the aims and objectives of the report to meet the aim most appropriately.The results gathered from this project showed that of the tested technique configurations, the implementation of rate-limiting and CAPTCHA together was the most effective for preventing the use of scraping tools on a website. However, this conclusion was reached using only a single comparison metric and without testing every technique available for the prevention of scraping. Whilst the conclusions made were supported by the literature obtained during the literature review, the results also highlighted areas where further work can be conducted, such as testing different techniques like honey-potting and automated traffic detection, as well as using different metrics of comparison. |
| cc) **Critical Analysis of Simple Network Management Protocol to****Identify The Optimum Secure Configuration of SNMPv3** |
| **Abstract**Network management is a critical component of ensuring the seamlessoperation of IT infrastructure. However, the evolving threat landscape hashighlighted the need for an ever stricter security approach. Approachingthis problem, a comprehensive overview of the security concepts and bestpractices of the SNMP protocol, exploring its use of SNMPv3 in relationto the User Security Model (USM) and Transport Security Model (TSM)is proposed. The research builds upon previous research conducted withinthis field providing recommendations for the optimum secure implementationof the SNMPv3 protocol.Initially, a comprehensive literature review is undertaken with the aimto find common themes and areas of research to pay close attention towhen considering security implications. This has resulted in considerableresearch into the security of data in transit. Notable researchers withinthis field include Taha Albakour, Georgios Smaragdakis who build uponthe grounding research of cryptography researchers who publish on behalfof NIST and influence subsequent publications by the National CyberSecurity Centre.The primary research conducted builds upon the findings within theliterature review, defining a repeatable methodology to test concerns raisedwithin the earlier works. Further consideration has been given to emergingthreats that previously were not discussed. Analysing them usingqualitative methods.The findings resulted in a number of recommendations, enabling animplementation of SNMP which would be deemed secure. However, thisresearch further outlines new areas of study including the recommendationsfor deeper analysis into TCP for SNMP |
| **dd)** **An evaluation of the internet footprint of Docker containers with varied configuration options** |
| **Abstract**Enterprises are rapidly migrating legacy applications and webservers to run inside of Docker containers, in order to improve application security. Docker takes a unique approach to running applications; rather than taking a binary released by your OS’s maintainers which is released according to an arbitraryschedule, Docker allows the core application developers to provide whole ‘containers’ including their application and it’s dependencies, directly to users of the application, skipping out a step in the release progress and providing ubiquitous images that run on any operating system.These ‘containers’ benefit from advanced security features and isolation from the rest of the host machine. They share the Linux kernel with the host, but the filesystem, network, memory space, process ID space, and users/groups are entirely isolated. This improves security as malicious processes insideof containers cannot have access to important system logs, user’s files, or keys for other applications,nor can they maliciously bind to ports or create network connections not explicitly allowed. However, in bringing an entirely different approach to networking, Docker containers introduce a different footprint onto the internet. Connections into Docker containers go through a number of different steps including routing, firewalling, network address translation, and proxying. This can create a signature which can be detected and traced, potentially allowing a malicious user to find other servers ran by the same organisation by actively or passively scanning internet address space.A methodology was developed which involved using a variety of testing scripts in order to gather information about the webserver and the network environment, then these scripts were executed against Docker & Base webservers running on 3 different operating systems.The results showed that containers include a number of these finger printable differences, from intricacies in TCP packet headers to varied HTTP response headers. However, none of the results showed a way to fingerprint a specific enterprise’s usage of Docker, unless manual configuration changes were madeby it. Additionally, using Docker allowed masking of some underlying operating system differences and also allowed the latest version to be deployed, therefore on balance it seems to hold a positive impact on application security. |
| **ee)** **A Critical Analysis of Cybersecurity Threat Modelling** |
| **Abstract**In the modern digitally driven environment we find ourselves in, cybersecurity remains a pressing issue for all types of organisations. This project focuses on threat modelling, a systematic process designed to better understand and address cyber risks before they result in a breach. A plethora of applications have been developed to assist security architects and engineers undertake threat modelling during the design and accreditation of a system. This project seeks to evaluate the effectiveness of the open-source tools that are freely available and confirm the knowledge in the subject area that proactive measures can enhance cybersecurity posture.A literature review is performed that covers the problem at hand, relevant theory and the key existing work that has been undertaken by researchers. From this, the domain specific methods were derived and key points that the tools were to be evaluated against were extracted.Furthermore, the methodology defines how a baseline comparison was achieved before a trial was conducted through the creation of a model based on a cloud three-tiered architecture. This architecture-based model was then translated into the different required input forms the tools require, before them being processed individually for analysis.To further evaluate the tools, a newly emerged network attack type was chosen. The HTTP/2 attack type was first widely reported in October 2023, and fitted in with the aim to test the tools against network-based threats. The result of incorporating this attack, and the other comparisons that were drawn both against other tools and from the literature, lead to the preliminary conclusion confirming the current knowledge and thinking in the field of threat modelling and saw the tools show a level of success in identifying the threat posed to the drawn system. |
| **ff)** **A Critical Evaluation Of Machine Learning Powered Ddos Detection Tools** |
|  |
| **Abstract**Over recent years, Distributed Denial of Service (DDoS) attacks have grown exponentially in size and simultaneously increased in complexity. DDoS detection tools exist as step one for mitigating these attacks and recent advancements in Artificial Intelligence (AI) have led to the creation of Machine Learning (ML) powered DDoS detection tools. This project assessed two popular open-source ML DDoS detection tools acquired via GitHub to determine whether ML tools are improving DDoS detection in terms of accuracy and resource consumption.A literature review outlined relevant theory surrounding DDoS Attacks, DDoS attack detection, ML, and the use of ML in DDoS detection. The accuracies achieved by commercial detection and academic research models are outlined. The methods used by the researchers in the explored papers are synthesized to provide a framework for testing the open-source detection tools in a controlled environment.Primary data collection revealed issues with the existing popular tools such as outdated code dependencies and a limited number of functional tools. After significant troubleshooting two of the nine identified tools were usable, PoCInnovation’s ‘Smart Shark’ and James Quintero’s DDoS Detection Tool ‘Quintero’. These tools were tested with 3 open-source DDoS tools (HULK, Golden Eye and RUDY) and 3 benign tests (No user traffic, manual browsing of the website and low-rate traffic generation using curl). Within these tests, data was collected on each tool’s detection accuracy and resource consumption.The data from these tests was analysed and it was revealed that the AI tools did not outperform existing commercial tools or academic models regarding accuracy. The resource usage for all tests is also recorded to provide a benchmark for future researchers. |
| **gg)** **A Critical Evaluation of Client Attitudes towards the Penetration Testing Process** |
| **Abstract**The evidently increasing reliance on digital systems in modern society has brought into the spotlight the security, or lack thereof, of these systems. Penetration testing has demonstrated itself to be an instrumental tool in improving an organisation’s security posture, as evidenced within various contemporary literature sources, in which the authors discuss some of the key reasons for which penetration testing is necessary, such as regulatory compliance and a level of granularity which cannot be achieved with more rudimentary vulnerability assessments.While it is agreed that penetration testing is important, this paper explores how existing penetration testing processes could be improved in order to provide a more accurate assessment of organisational security. This is achieved through rigorous analysis of customer feedback surveys, from which actionable insights are extracted and recommended for implementation. The methodology section of this research paper discusses the implementation of experimental methodologies to ensure valuable responses are garnered for analysis.The research conducted within this paper identifies critical areas where existing penetration testing methodologies and processes fall short, offering an insight into where, and how, improvements can be made. The findings reveal that while penetration testing is crucial for cyber security, there is a pressing need to refine these tests to provide an outcome which is more closely aligned with the expectations of the surveying organisation’s customers.In the bigger picture, the findings and recommendations of this research offer a catalyst for improving the efficacy of penetration testing. This research also leaves open the possibility of additional research; conducting the same research following the implementation of the aforementioned recommendations can provide insight into the effectiveness of the suggested changes. |
| **hh)** **A critical evaluation of the potential of Large Language Models to democratise cybercrime** |
| **Abstract**While the advent of Large Language Models (LLM) and their revolutionary applications has been groundbreaking, the need to understanding the implications this may have on our cybersecurity remains at an all-time high. The primary focus of this research is to investigate the impact LLMs will have on malware creation, and whether the barriers to entry for cybercrime have been reduced. The aim is to assess the efficiency and quality of phishing emails generated using both manual methods and AI-assisted methods. Phishing remains a significant cybersecurity threat, making it imperative to understand how different technologies can influence the creation of deceptive email content.The method will include participants being tasked with composing 2 phishing emails. Once using only traditional methods and then again using AI assistance using Chat-GPT. A sample size of 10 participants was recruited, provided with a specific scenario and objectives for email creation. The duration of both tasks was logged, alongside participants' overall feedback. Subsequently, these phishing emails underwent subject matter expert evaluation to assess their credibility. These experts were also asked to distinguish between automated and human-generated content. The study found that AI-assisted emails were faster to create than manual ones. Experts struggled to differentiate between human and bot-generated content, perceiving bot-written emails as more credible. Bots simplified the creation process, though AI-generated emails lacked personalization and were verbose, contrasting with the contextually sophisticated but slower traditional methods.The key takeaway from this research is understanding this experiment is a trial run which offers only a glimpse into the capabilities of LLMs. It emphasises the need for continued research aimed at producing more conclusive research. Such results are pivotal in influencing cybersecurity policies, ensured the relevant organisations are primed to confront the wave of cybercrime, which is likely to intensity as LLMs become more powerful |