Personal Info

Name: Jingxuan Feng

Student Number: s3843790

Email: s3843790@student.rmit.edu.au

Github Repository: https://github.com/Ghost-Recon131/IIT-A1

Github Pages URL: https://ghost-recon131.github.io/IIT-A1/

Basic Background

I immigrated to Australia from China with my parents back in 2008. I've maintained a conversational level of both Mandarin and Cantonese, and it has come in helpful multiple times such as in group work or helping international students.

I am also a PC enthusiast and gamer; I've always kept myself informed with the newest hardware releases. I've built around 6 PC's both for myself and family / friends. Here's pictures of a two of them:

Another interest of mine is gaming. Currently Rainbow Six Siege has the most hours of playtime, where I also played competitively part of the RMIT team back in 2020. I've also played various COD's and Battlefield releases, War Thunder, GTA 5 and some others.

I've also done self-study on using penetration testing tools in Kali Linux and challenges on sites like Hack the Box and Try hack me over the semester breaks and holidays.

Interest in IT

What is your interest in IT? When did your interest in IT start?

My primary interest in IT in cybersecurity however it wasn't where my interest started. My interest started when the existing computer at home wasn't powerful enough to run my favourite games roughly back in 2014. I started looking at computer hardware and realised I know nothing about all the parts. Further research in this area gradually got me interested in custom PC builds. Since then, I've had to deal with all the IT problems my parents have, and they will get me to setup anything with internet or smart home capabilities.

Was there a particular event or person that sparked your interest? Outline your IT experience (if any).

Interest in cybersecurity started due to multiple events over the course of 2017. During that year, many high-profile attacks happened such as Equifax data breach that leaked details of over 147 million accounts [1]. Uber data breach that exposed personal information of 57 million accounts [2]. As well as new WannaCry ransomware, followed by Petya/ NotPetya and other "strains" of ransomware. These events sparked my interest in Cybersecurity and highlighted how important this is for the rest of the IT industry.

I don't have any formal work experience in IT but I have set up a lot of tech equipment at home. I setup the router and mesh nodes for Wi-Fi, smart home devices, security camera system, a Network attached storage (NAS) and internal network shares over SMB and FTPS. To address the issue of securely connecting to these devices from an external network, I've then setup an OpenVPN server at home which can be reached via a DDNS service.

Why did you choose to come to RMIT?

I came to RMIT for a variety of different reasons. Firstly, when comparing the subjects and going to open days for other Uni's, RMIT appeared to offer the most practical course for Computer Science, whereas Monash and Melbourne Uni have more theory. I personally prefer a degree that is closer to 'real' work, and I wanted to start working once I finish undergraduate rather than to continuing with a master's degree. My high school career advisor also said RMIT was a good choice for me.

Secondly, RMIT was in a good location for me; I can take the train or bus and get to RMIT within 30 minutes, so travelling is more of a break from work than time lost.

Lastly, most of my friend group from high school also decided to study at RMIT, although they are studying different degrees it still felt less daunting. It was especially helpful during my first year at RMIT (in 2020), which was pretty much all done online due to COVID restrictions, and I didn't have many opportunities to meet others in the Computer Science course.

What do you expect to learn during your studies?

I expect to learn a few programming languages that is currently popular in the industry now such as C++, Java, React, Python ect. As well as improving my skills on turning requirements and features into functioning code.

I also expect to learn about Cloud computing and software development processes mainly Agile / Scrum, as well as some older models like waterfall. For cloud computing, I expect to learn about hosting applications on the cloud, using AWS or Google as well as DevOps tasks.

Furthermore, I expect to learn more theory-based content from subjects like Algorithms and Analysis, computing theory to help with creating more optimised code. Finally, there AI and relevant maths as well as theory behind AI.

Ideal Job

SEEK: https://www.seek.com.au/job/56037312?type=standard#sol=ade294275

Wayback Machine Backup (Created 14/03/2022): https://web.archive.org/web/20220314033934/https://www.seek.com.au/job/56037312?type=standard

Description of position

In this position I will work as an Offensive Security Consultant. This position is appealing to me since the requirements are not extremely high, and it is likely I can apply for this within a

year, max two years after graduation. The job is also exactly what I am interested in doing - trying to find vulnerabilities in code/ app / website, report it to the client and prevent anyone from abusing the vulnerabilities. Furthermore, the cybersecurity industry is still growing and will continue to grow in the future, creating great job security. The pay for these positions is also great, with internships starting around $65000 then fill time positions ranging from $90000 - $160000 according to Seek.

Description of skills needed for position

Based on my understanding, the following skills are needed for this position:

- Attention to detail
- Good communication and a team player
- Open minded and always seeking to learn something new
- Determined and persistent
- Has at least 1 year of experience working by myself on penetration testing
- Can deliver small / medium tasks in a timely manner
- At least 1 year of penetration testing experience on web applications or mobile applications
- At least 1 year of experience using mix of internal and external penetration testing methods
- Know of and can perform attacks on Microsoft Active directory, Linux systems and web / mobile systems
- Some form of a recognised security certificate.

Description of skills I currently have

Currently I have all the 'soft' skills required such as attention to detail, work well in team or individually etc. I've also done 'Security Testing' an elective which gave me more theory on protecting services / websites and apps as well as common attack vectors and vulnerabilities to look for. I am confident in using Kali Linux as well as some of the built-in tools. I also have some experience on performing penetration testing on Websites, and static code analysis on program source code, which may contain security flaws such as not validating input or could allow a stack overflow resulting in information being leaked. Moreover, I can also use a combination of Nmap / Wireshark and other tools to look for vulnerabilities at a network level.

Plan for how to obtain the skills

I currently don't have the 1-year experience in performing penetration testing on Web apps and mobile apps, as well as missing a recognised security certificate. To obtain these skills, I will do more self-teaching / studying then sign up for OSCP and CISSP programs, then take the respective exams to obtain both certificates, which will likely take 6 months. According to my lecturer for Security Testing, these two certificates are more useful for working in Australia. These certificates will teach more penetration testing methods as well as give me more experience on Websites, Mobile apps, and network security.

I will then look for an internship placement which is hopefully 6-12 months long. This is mainly to increase the experience I have in the penetration testing field and start using my knowledge on real world scenarios, thus meeting the 1-year minimum experience required. Ideally, there the internship also covers switching between blue and red team (defending and attacking) during simulated attacks, which is an important aspect in penetration testing. Following the internship, I should have all the required skills to apply for a full time Penetration tester role.

As a backup, in case I am still mission some skills, I will try stay in the company I did my internship as a part-time or full-time employee and continue to build my experience. If that is not possible would try look for a penetration testing job with lower entry requirements (and lower pay) and increase my experience, there.

Profile

What do the results of these tests mean for you?

All three tests sort of point to me to theorist / consul type personality and learning styles pointing me at a leadership type role. These are mostly accurate, and it would mean I tend to be supportive and outgoing with others and will try help others when they are having trouble. But the Myers-Briggs Test results show that I lean more towards feelings, judging and assertive. Whereas the learning styles test suggest I tend solve problems logically and value rationality and objectivity. I reckon that the learning styles results are closer to reality as I do work strictly off rubrics and requirements, whereas feelings on a certain subject or group will not affect my performance or work quality.

The Myers-Briggs Test also suggests I lean towards extraverted personality; however, this is not very true. Generally, I do not actively try to make friends, nor do I walk up to someone I don't know and start a conversation. I only start leaning towards an extraverted personality when I am with close friends.

The leadership styles test is fairly accurate; I have had to act as the team leader or the one keeping others on task on several group projects. Though, I also don't try to seek to be the leading role, especially if someone else wants the role.

How do you think these results may influence your behaviour in a team?

I think these results make me a versatile team member, because I can adapt to many roles. Such as acting as group leader, or someone who helps members stuck on a task. The results also suggest I tend to be more logical and observant, thus I might also be one of the planners or reviewers of the group work when we discuss how to do the group assignment as well as doing checks over the course of and at the end of the assignment. Overall, I should be able to work with team members of any other personalities.

How should you take this into account when forming a team?

When forming a team, I will try to look for teammates who tend to be more extroverted, as it would be easier to get along with them which also helps get group projects going. Other than that, I'm used to working with people with various personalities, and I will be more

focused on other aspects, such as going to try to for a high grade, whether we have similar interests etc.

Project Idea – Fully integrated AI cybersecurity software

Overview

This project will propose the use of AI models and machine learning to boost cybersecurity defence for an organisation. By using all endpoints (individual computers / devices for each employee), server usage data and running alongside applications, the AI model will have far more data to work with compared to current antivirus or business security solutions. Thus, will help circumvent with attacks that rely on compromised accounts or zero-day attacks in addition to the usual malware attacks. The necessary hardware is already available, currently 'only' an AI model and time is needed. There is also a demand for using AI to enhance cybersecurity, thus making this product profitable once all technical details are worked out and a fully developed product is ready to hit the market.

Motivation

According to a study by Stanford University, "88% data breach incidents are caused by employees' mistakes" (CISOMAG, 2020). As human error is the primary cause of cybersecurity incidents, there is a market for more advanced cybersecurity software beyond the usual email, links and virus scans most existing solutions offer. Another aspect is improving Protection against 0-day attacks. As documented in Google's report (Maddie Stone and Clement Lecigne, 2021), there has been a consistent uptick in 0-Day vulnerabilities detected following 2018. Furthermore "Estimates indicate that the market for AI in cybersecurity will grow from US $1billion in 2016 to a US $34.8 billion net worth by 2025" (Taddeo, McCutcheon and Floridi, 2019), thus making this a financially viable investment.

Description

First, this product needs to reach feature parity with current business cybersecurity solutions. Such as offering malware/ virus scans, firewall, email and link scanning, and a behaviour analysis module using a combination of a signature-based detection and a generalised AI. This will also be the main line of defence for an organisation data is collected on all the endpoint devices belonging to the organisation, as well as their servers. Endpoint data will contain usage data, permissions, usage times, access times, actions taken etc. These can then be used to train the AI on the usage patterns of each employee. The same can be done on the organisation's servers and deployed programs, also monitoring how they are used and the usual traffic, throughput, and dataflow.

Training the AI to fit the organisation's uses is time and resource intensive. To minimise the time needed, "Adaptive Deep Reuse" can be used as outlined in (M2 Presswire, 2019), which can reduce training time by around 60%, depending on the datasets, without loss in quality. This AI model then works though detecting anomalies such as sudden change in usage patterns or access times, missed by relying on signature-based detection alone (Stevens, 2020). However, the primary complication in creating a reliable Anomaly-based

detection is getting data that is known to be free from attacks. This step likely requires manual validation of all the data to ensure the training model does not become 'poisoned'.

The product will also integrate Specification based detection, which is used to complement the Anomaly-based detection. This detection method uses "manually developed specifications that characterize legitimate behaviours rather than relying on machine learning algorithms" (Sikos, 2019). But this also increases complexity to setup but will reduce the number of false positives from the AI model.

Once in operation, the AI would be able to detect attacks using compromised employee accounts, such as sudden increase in data access, or trying to visit unknown sites or servers. The model should also detect malicious activity from the employee themselves, such as trying to access and copy company intellectual property. Furthermore, there will be additional protection against human error, such as improper configuration by system admins. When detected, a persistent warning will be issued until the problem is rectified, likely preventing an Equifax 2017 style data breach. Where "Equifax had crucially failed to renew an encryption certificate on one of their internal security tools" (Fruhlinger, 2020), thus allowing the attackers to steal data while Equifax system admins had no idea that anything was wrong.

Another crucial feature is offering clients the ability to integrate some protecting into their program via an API. The protection is aimed at detecting potential breaches due to vulnerabilities due the way it is coded or flaws in the program dependencies. It is not aimed to replaces source code analysis tools like "FlawFinder, RATS, ITS4" (Source Code Analysis Tools | OWASP Foundation) etc. Security vulnerabilities that arise due to the program's dependencies is prevalent such as Apache Struts CVE-2017-5638 which allowed for remote code execution (RCE) on the program's servers (Syme, 2017). Late last year, Log4j also had a RCE vulnerability. This month, the author of Node-IPC added malicious code in their package which essentially deletes all files on the server if the IP address of the server is physically in Russia or Belarus (NVD - CVE-2022-23812). Thus, the features are aimed at detecting, blocking, and doing some basic analysis on these attacks.

The product will also offer network intrusion detection. This feature is aimed at protecting devices on the organisation's internal network and countering attackers who have evaded anomaly and specification detection. It is also using behaviour-based detection, but the AI will mainly focus on the user and internet packets to detect attacks. Malware detecting using electromagnetic waves (Ashley Whittaker, 2022) could also be integrated into the product.

The product needs to have built in logging tools. This feature is responsible for logging all the usage data for all the endpoints and servers. It will collect data in the background and require no human interaction. The logs are then sent to a separate machine for storage before it is passed to a machine learning model to train the AI. This feature will also do some data cleaning where necessary to ensure the logs are fully usable.

Finally, a management program is needed for system admins to control the software. This frontend will tie in with all features offered by the product. This will allow system admins to

manage organisation wide deployment of our endpoint software, as well as control the API if needed by their DevOps team. All warnings, notifications and requests for the admin to act will also be viewed and dealt with in the management program. It will also allow for tinkering with manually defined specifications used for Specification based detection. Any action taken by the system admin also requires a hardware 2FA token, such as a Google or Yubico Security key. This requirement will prevent an attacker from performing any action on the admin panel remotely, as the hardware security keys require a physical touch before they authenticate its user (Stina Ehrensvard, 2018).

To try to increase usability of this product for even beginner system admins, the management program will need a windows style design. Where it does not look daunting for the user and has pre-configured settings for common cases but allow for power user to tinker with any setting they need.

Tools and Technologies

There are two options for the organisation when it comes to which tools to use. The program could be deployed on the organisation's own hardware or servers, entirely on cloud solutions or a mix of both.

Onsite solution

Hardware recommendation based off (algorithmia, 2018) and (Ben-Zvi, 2022). When all the hardware is onsite, a minimum of one server setup is needed. The server will run off a data centre style CPU such as AMD's Epyc line-up, mainly needed for the increased memory channels and PCIe lanes. ECC memory would be optimal, and all the machine learning will be done over multiple GPUs such as the Nvidia A100. The usage logs will be stored on a separate NAS preferably running off SSD's only, as log files are a few megabytes maximum, when accessing thousands of these, the random reads for small files of SSD's will save the server a lot of time, rather than have it wait for the data. The CPU will handle turning the log files into cleaned datasets for the Machine learning (ML) model. Preferably there are Uninterrupted power suppls for the NAS and server rack to protect against data loss and corruption during a blackout or brownout. Additional NAS devices offsite to store backup data will also help in event of data loss. If an organisation wants the AI model to be trained sooner, the can then invest in multiple servers.

Cloud solution

(Using AWS as primary example so no need to repeat the same competing products from Microsoft, Google etc)

When using cloud computing, things become simpler. A program will be deployed using Elastic Beanstalk, which handles, cleans, and passes the log files as a usable dataset to EC2 G3 instances. These instances will have the ML model use to train the AI. Data will be stored on using a mix of Elastic Block Storage and S3. Network access to configure and control this process will be configured with VPC, direct storage and Route 53. (Qiang Fu, 2022).

It is also possible to use a mix of onsite and cloud computing such as offload all computing needs to AWS while keeping all the data for the AI stored locally within the company.

Skills Required

This project is extremely complex to implement and is likely impossible for a single developer to make a useable product in a short period of time. A team of data scientists, cybersecurity experts and a team of programmers will be needed.

Programming team needs to be able to create bundle of software that this project discuses which contains the separate AI detection modules for endpoints / servers, API for developers and software that controls the machine learning process. They will receive input or help directly from cybersecurity experts and data scientists to do this.

The software the runs on endpoints and servers will be written in C++, for its speed and ability to have programmer managed memory. The API could be built in Spring (Java) or Django (Python) as both are widely used (Cucciniello, 2017). Finally, the software for managing and performing the machine learning process will be built on Python, as it has the largest library of machine learning tools such as sklearn, TensorFlow etc. UX and font end developers will also be needed to create the front end for end users for managing all the software.

Finding the skills and knowledge is easy as stated by (Nguyen et al., 2019) however it will be a costly process. A large investment must be obtained before the project can proceed. The hardware required is can also be easily acquired.

Outcome

Once the project is successful, the chances of successful attack using zero-day vulnerabilities should be significantly reduced or even eliminated at the cost of more false positives. Once the effectiveness is proven and more organisation uses this software, there will be sizable profits to be made. The original problem of relying on signature and generalised AI models for protection will be replaced by specialised AI models that use all the data available to help secure an organisation. This should result in far less cases of human error leading to data being compromised and cases of RCE. But hackers will likely try creating more advanced techniques to breach organisations resulting in a constant “arms race” and continued improvements and updates are needed for the project.

References (Project Idea)

1. CISOMAG (2020) *“Psychology of Human Error” Could Help Businesses Prevent Security Breaches*, *CISO MAG | Cyber Security Magazine*. Available at: https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/ (Accessed: 19 March 2022).
2. Maddie Stone and Clement Lecigne (2021) *How we protect users from 0-day attacks*, *Google*. Available at: https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/ (Accessed: 19 March 2022).
3. Nguyen, N.T. *et al.* (eds) (2019) *Computational Collective Intelligence: 11th International Conference, ICCCI 2019, Hendaye, France, September 4–6, 2019, Proceedings, Part II*. Cham: Springer International Publishing (Lecture Notes in Computer Science). doi:10.1007/978-3-030-28374-2.
4. Stevens, T. (2020) ‘Knowledge in the grey zone: AI and cybersecurity’, *Digital War*, 1(1–3), pp. 164–170. doi:10.1057/s42984-020-00007-w.

5. Taddeo, M., McCutcheon, T. and Floridi, L. (2019) 'Trusting artificial intelligence in cybersecurity is a double-edged sword', *Nature Machine Intelligence*, 1(12), pp. 557–560. doi:10.1038/s42256-019-0109-1.
6. CISOMAG (2021) *Log4j Explained: How It Is Exploited and How to Fix It*, *CISO MAG | Cyber Security Magazine*. Available at: https://cisomag.eccouncil.org/log4j-explained/ (Accessed: 19 March 2022).
7. *M2 Presswire* (2019) 'New Technique Cuts AI Training Time By More Than 60 Percent', 8 April. Available at: https://www.proquest.com/docview/2204757656/citation/A0CBC24657254BE5PQ/1 (Accessed: 19 March 2022).
8. Sikos, L.F. (ed.) (2019) *AI in Cybersecurity*. Cham: Springer International Publishing (Intelligent Systems Reference Library). doi:10.1007/978-3-319-98842-9.
9. Fruhlinger, J. (2020) *Equifax data breach FAQ: What happened, who was affected, what was the impact?*, *CSO Online*. Available at: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (Accessed: 20 March 2022).
10. *Source Code Analysis Tools | OWASP Foundation* (no date). Available at: https://owasp.org/www-community/Source_Code_Analysis_Tools (Accessed: 20 March 2022).
11. Syme, M.Z., Julia Karpin, Ilya Chernyakov, Dylan (2017) *From DDoS to Server Ransomware: Apache Struts 2 – CVE-2017-5638 Campaign*, *F5 Labs*. Available at: https://www.f5.com/labs/articles/threat-intelligence/from-ddos-to-server-ransomware-apache-struts-2-cve-2017-5638-campaign-25922 (Accessed: 20 March 2022).
12. *NVD - CVE-2022-23812* (no date). Available at: https://nvd.nist.gov/vuln/detail/CVE-2022-23812 (Accessed: 20 March 2022).
13. Ashley Whittaker (2022) 'Detect malware with electromagnetic waves and Raspberry Pi', *Raspberry Pi*, 1 February. Available at: https://www.raspberrypi.com/news/detect-malware-with-electromagnetic-waves-and-raspberry-pi/ (Accessed: 20 March 2022).
14. algorithmia (2018) *Hardware for Machine Learning*. Available at: https://www.algorithmia.com/blog/hardware-for-machine-learning (Accessed: 20 March 2022).
15. Ben-Zvi, N. (2022) *A 2021-Ready Deep Learning Hardware Guide*, *Medium*. Available at: https://towardsdatascience.com/another-deep-learning-hardware-guide-73a4c35d3e86 (Accessed: 20 March 2022).
16. Qiang Fu (2022) 'Lecture 2 Amazon Web Services', 7 March. (RMIT lecture slide)
17. Cucciniello, A. (2017) *What are the best programming languages for building APIs?*, *Packt Hub*. Available at: https://hub.packtpub.com/what-are-best-programming-languages-building-apis/ (Accessed: 20 March 2022).
18. Stina Ehrensvard (2018) 'What is FIDO2?', *Yubico*, 24 May. Available at: https://www.yubico.com/blog/what-is-fido2/ (Accessed: 23 March 2022).

References (tools and websites used)

1. Bootstrap 5 Text/Typography (2022). Available at: https://www.w3schools.com/bootstrap5/bootstrap_typography.php (Accessed: 21 March 2022).
2. Bootstrap Navbar - examples & tutorial (2021) MDB - Material Design for Bootstrap. Available at: https://mdbootstrap.com/docs/standard/navigation/navbar/ (Accessed: 21 March 2022).
3. contributors, M.O., Jacob Thornton, and Bootstrap (2022) Colors. Available at: https://getbootstrap.com/docs/5.0/utilities/colors/ (Accessed: 21 March 2022).
4. Mark Otto, Jacob Thornton, and Bootstrap (2022) Colors. Available at: https://getbootstrap.com/docs/5.0/utilities/colors/ (Accessed: 21 March 2022).

5. 'How to change navigation bar color in Bootstrap ?' (2019) GeeksforGeeks, 30 August. Available at: https://www.geeksforgeeks.org/how-to-change-navigation-bar-color-in-bootstrap/ (Accessed: 22 March 2022).
6. *Introduction | Consul (ESFJ) Personality* (2022) *16Personalities*. Available at: http://www.16personalities.com/esfj-personality (Accessed: 24 March 2022).
7. *Learning Styles Quiz* (2022). Available at: http://www.emtrain.eu/learning-styles/ (Accessed: 24 March 2022).
8. USC Price School of Public (2022) *Leadership Style Quiz: 12 Clever Questions to Identify your Style*. Available at: https://eml.usc.edu/leadership-style-quiz (Accessed: 24 March 2022).