Reza Rizvi
Assistant Professor
Department of Mechanical Engineering
York University

Dear Professor Rizvi,

I have prepared the following report “Machine Learning for Cybersecurity” detailing a possible solution for the Engineering Grand Challenge of Securing Cyberspace. This report will be ready for publishing by March 22, 2022.

In this report, I discuss the Engineering Grand Challenge of Securing Cyberspace and its associated problems. I then offer as a solution the development of machine learning for cybersecurity, detailing its capabilities, strengths, weaknesses, and effectiveness in making progress for the grand challenge. I intend for this report to educate and inform you of the importance of these issues and the suitability of the new technology.

I encourage you to contact me if you have questions, concerns, or any feedback. Thank you for your time.

Sincerely,

FirstName LastName
email@yorku.ca
(012) 345-6789

Machine Learning for CyberSecurity

Solving Engineering Grand Challenge of
Securing Cyberspace

FirstName LastName

March 8, 2022

YORK
UNIVERSITÉ
UNIVERSITY

Executive Summary

The internet is one of the most complex systems ever engineered. Utilizing this complexity, cybercriminals have an abundance of opportunities to wreak havoc through the internet. The options for attacks range from sending fake emails in an attempt to steal someone's password, to shutting down entire power grids. As industries become more dependent on technology and the internet, the latter case is more feasible for cybercriminals.

The engineering grand challenge of securing cyberspace addresses this problem. The challenge acknowledges the massive scope of this problem, and that it will only get worse as technology dependence increases. This challenge falls into the cross-cutting theme of security, which needs to be prioritized for these reasons. Creating a secure cyberspace is necessary for the proper functioning of industry and the prevention of costly damages.

An emerging technology that addresses this grand challenge is machine learning. Machine learning models can be trained using training data to detect patterns in new data. This is especially useful for this challenge, as current pattern recognition software for cybersecurity is programmed manually and is unable to keep up with constantly changing cyberattacks. Machine learning has an opportunity here to provide automatic detection of malicious activity that can evolve along with the evolving threats.

Initial tests and implementations of this technology are promising. MalDozer, a machine learning malware detection system for the Android operating system, has shown in experiments to be about 96% accurate with a false positive rate of about 2%. Outside of experiments, the Windows Defender Antivirus, an antivirus software developed by Microsoft, has already implemented machine learning in its production software. It has faced a cyberattack targeting over one thousand Windows users, to which it correctly identified malicious activity and blocked the attack.

Although promising, machine learning's use for cybersecurity currently has some drawbacks. One drawback is that there are not enough datasets to train the machine learning models with. If not properly trained, the models will not be effective in detecting malicious activity. Also, while machine learning receives much research, most of it is not directed to cybersecurity. As a result, the technology still needs to be researched before it can be widely adopted.

Despite these drawbacks, machine learning is a promising solution for the grand challenge. With more research and resources, this technology will be capable of solving much of the challenge and secure a large part of cyberspace.

Contents

List of Figures

1 Introduction and Background

Technology and the internet have been growing more and more pervasive over the last few decades, and this shows no sign of stopping. This comes with many benefits, like an abundance of readily available information, almost instantaneous communication, and the entire E-commerce industry. However, this also comes with consequences. Perhaps one of the most pressing issues with the growth of technology is the introduction of a new type of malicious activity—cybercrime.

Cybercrime is the use of the Internet for illegal purposes. This includes crimes targeting individuals, such as malware, ransomware, phishing, and identity theft. But with the increasing dependance of industry on the internet, cybercrime can also include crimes that target populations and large systems. For example, cyberattacks can target entire organizations, power grids, or military systems.

The engineering grand challenge of securing cyberspace seeks to address this problem. The internet is one of the most complex systems ever engineered, and the complexity of the internet leads to complexity in the cyberattacks that threaten it. Falling under the cross-cutting theme of security, this grand challenge acknowledges the massive scope of this problem. It recognizes that the effects of cyberattacks are becoming more devastating and costly, which is already being observed.

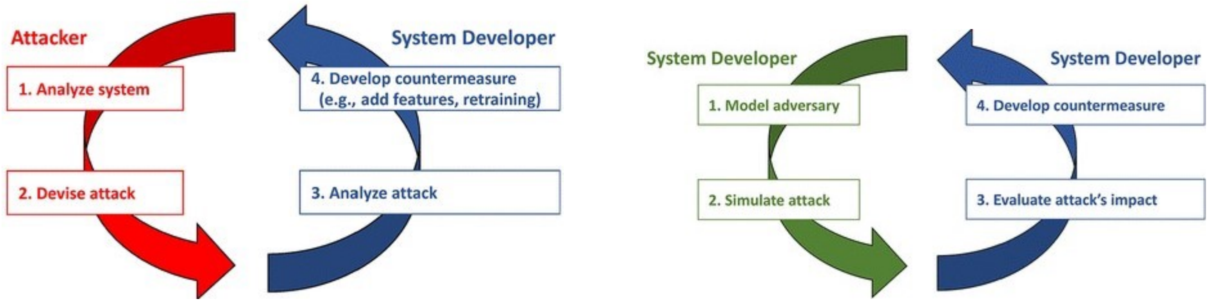
On June 1, 2020, the University of California, San Francisco, was hacked by a ransomware campaign that threatened to release confidential information, to which the university paid approximately $1.14 million to the group [1]. In fact, in 2015, cybercrime was estimated to have had a global cost of $3 trillion [2], and is predicted to reach $10.5 trillion by 2025 [3].

As is evident by successful cyberattacks of reputable organizations, the current methods of dealing with these attacks are insufficient. The main method of developing cybersecurity systems involves having successful cyberattacks occur, then learning from them to fix the vulnerability. Clearly, a much more proactive and complex cybersecurity system is needed.

2 Machine Learning's Use in Cybersecurity

Traditionally, cybersecurity algorithms were written manually from heuristics [4]. But the rapid growth of the internet and technology in general has led to constantly changing cybersecurity threats. As a result, these manually written heuristic algorithms are insufficient—they cannot keep up with the evolving threats [4]. Machine learning offers a solution to this problem.

Machine learning models are able to "learn" certain data patterns to predict behavior [4]. In this case, their goal is to predict whether some online activity is malicious or legitimate. For maximum effectiveness, this requires a change in the way these systems are developed. The development process must shift from a reactive approach to a proactive approach [5]. This is shown in Figure 1, where the system developer shifts from learning based on being attacked to learning based on models and simulations. This way, the machine learning technology will be more than just learning from cyberattacks, but also predicting new cyberattacks.



(a) Reactive Approach to Cybersecurity System Development

(b) Proactive Approach to Cybersecurity System Development

Figure 1: Reactive versus Proactive Cybersecurity Systems Development. [5]

To accomplish this, the model must be trained with training data and tested to ensure it is effective. This first involves data-centered tasks, like gathering and cleaning data [4]. This data can then be used to train the model, which may take seconds to days, depending on the algorithm chosen [6]. Once the model is trained, it must be tested to ensure it is accurately detecting malicious activity, which also takes a variable amount of time depending on the machine learning algorithm chosen [6]. Figure 1 shows a diagram of this process.

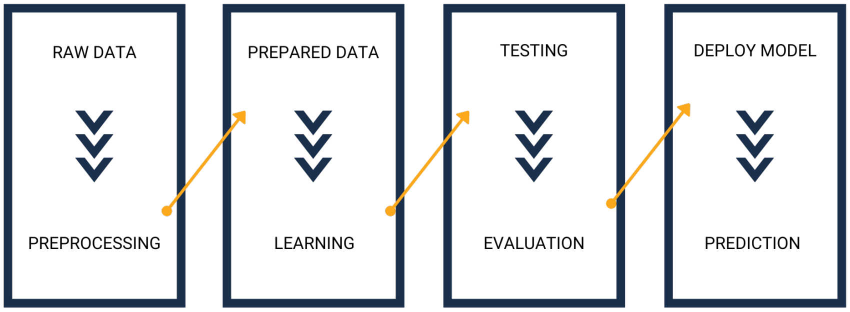


Figure 2: A Diagram of a Typical Machine Learning Process. [7]

In the context of cybersecurity, this means compiling together large datasets containing information about malware, phishing attempts, and other malicious activities. The goal of this process is that, after training and testing a machine learning model with this data, it will be able to detect cyberattacks before they occur.

3 Evidence of Machine Learning's Effectiveness

Machine learning algorithms are already being developed, tested, and employed to detect cyberattacks, and the progress being made is promising—machine learning is already proving to be an effective cybersecurity technique. This is illustrated by the following case studies.

3.1 Phishing Detection Experiments with Machine Learning

A common type of cyberattack is phishing, which is an attempt to steal users' sensitive information by presenting them with a fake email or login page that appears legitimate [8]. Users, thinking that the website is real, can be tricked into entering their information, giving it to attackers. Systems exist to detect these attacks, but they often incorrectly classify legitimate websites and emails as malicious—as much as 75% of domains classified as suspicious are actually genuine [8]. Furthermore, these systems often do not update quick enough to catch new phishing attempts [8].

Machine learning is a suitable technology for this problem of classifying websites and emails as phishing attempts. Currently, many experiments and studies are exploring this area. One such study used a machine learning algorithm to generate rules for spotting phishing attempts. These rules were found to correctly identify 85.4% of emails and 83% websites as phishing attempts [8]. Another experiment used a neural-network model to categorize emails as phishing attempts at high speed. The results showed that the error rate of this algorithm was below 2% [8].

Machine learning offers clear improvements to classifying websites and emails as phishing attempts. This will operate faster than current systems, leaving less opportunities for attackers, and will prevent legitimate websites from being classified as malicious.

3.2 MalDozer—Automatic Malware Detection for Android

Android, is an open-source mobile device operating system released by Google. Partially due to its openness, Android is particularly vulnerable to malware [9]. In recent years, damage from malware on Android has been dramatically increasing.

In response, multiple machine learning technologies are being developed to protect Android devices from malware [9]. One such technology is called MalDozer. Several experiments were conducted by presenting MalDozer with datasets containing varying amounts of malware. The experimenters found that its accuracy rate was 96%-99% with a false positive rate of 0.06%-2% [9].

These experiments show exciting progress in machine learning models as a malware detection system. As the technology is refined, the accuracy rates will improve further, reducing the amount of malware on Android devices.

3.3 Windows Defender Antivirus

The Windows Defender Antivirus is not only being tested, but is actually being put in use, providing real examples of the capabilities of machine learning. In 2018, a new malware attack campaign was launched against over a thousand users of Windows 7 Pro [10]. These Windows systems featured the Windows Defender Antivirus, an antivirus software developed by Microsoft.

The Windows Defender Antivirus features lightweight machine learning models built into the client, which responded immediately to the attack [10]. These models detected a high probability of maliciousness in the requests they were receiving, so they sent data to the Windows Defender Antivirus cloud protection service, which runs more complex machine learning models [10]. Through this, the cloud protection service correctly identified the requests as a cyberattack and responded back to the clients, instructing them to block the attack [10]. Figure 3 shows a schematic made by Microsoft, providing an overview of this process, illustrating the progression from the client-side machine learning models to the complex cloud protection service.

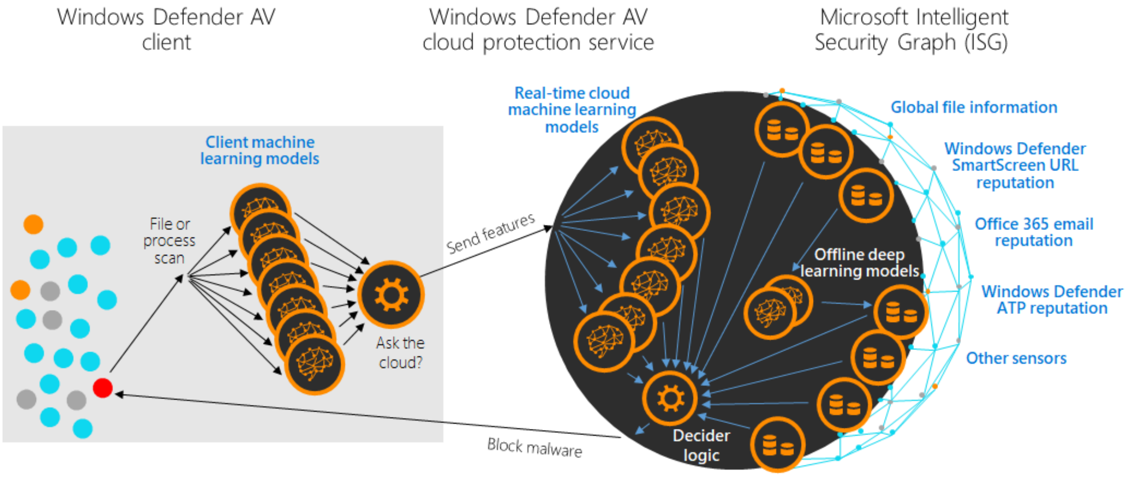

Windows Defender AV client
Windows Defender AV cloud protection service
Microsoft Intelligent Security Graph (ISG)
Client machine learning models
File or process scan
Ask the cloud?
Send features
Block malware
Real-time cloud machine learning models
Decider logic
Offline deep learning models
Global file information
Windows Defender SmartScreen URL reputation
Office 365 email reputation
Windows Defender ATP reputation
Other sensors

Figure 3: Overview of the Cyberattack Detection Process use by Windows Defender Antivirus. [10]

Demonstrated by this event, machine learning is effective not only in tests, but also in real cyberattacks. The use of machine learning algorithms were able to protect thousands of users from a cyberattack with no human intervention.

4 Drawbacks of Machine Learning for Cybersecurity

In its current state, machine learning has many drawbacks for use in cybersecurity, some of which make it infeasible for many organizations to use.

4.1 Low Availability of Adequate Datasets

Since cyberattacks can be complex and varied, extensive and high quality datasets are needed to train the machine learning models to ensure they can protect against all attacks. This is not the case with existing datasets.

Current datasets contain lots of old data and redundant information [6]. This can be somewhat improved after cleaning the data, but even then there is the issue of volume—there is not enough data to properly train the models [6]. As a result, the machine learning models are not totally equipped for identifying new cyberattacks. This also introduces a barrier of entry, as larger organizations may be able to work around these issues, but smaller organizations do not have the resources to do so.

4.2 Lack of Research and Adoption

While the field of machine learning receives lots of research, this research is mainly focused on deep-learning algorithms for applications like self-driving cars [11]. Machine learning for cybersecurity purposes has yet to receive this same amount of attention. Due to this lack of research, widely adopted machine learning models for cybersecurity are limited, using mostly rule-based techniques [11].

Furthermore, this lack of research introduces inconsistency across organizations [11]. To be most effective, cybersecurity models need to have consistent behavior for any attack that may occur. This requires cooperation and research to keep all parts of the internet secure.

5 Discussion

Machine learning has promising applications in cybersecurity. It has proved to be accurate and effective in testing scenarios, being able to determine malicious online activity from legitimate activity. Outside of tests, machine learning proves effective in real cyberattack situations, being able to detect real cyberattacks and block them with no human intervention. As a technology, machine learning is well equipped for making progress on the engineering grand challenge of securing cyberspace.

These machine learning technologies are still in the early stages of development, requiring much research. Due to this, many organizations do not have the resources to utilize this technology. However, as more research is conducted and industry standards start to form, the barrier of entry to using machine learning for cybersecurity will start to vanish.

When this technology is more accessible to organizations and, as a result, more organizations start to use it, the cybersecurity industry will grow further. More parts of the internet will be protected much more securely, leaving less opportunities in general for cyberattackers. These are all important advancements for securing cyberspace.

6 Conclusion

The engineering grand challenge of securing cyberspace has a level of complexity and difficulty that is daunting. However, this complexity and difficulty can be matched with machine learning.

With the ability to find patterns in data, machine learning shows potential as a detection system for malicious activity. Even though the cyberthreats it must respond to are constantly evolving, machine learning models will remain effective because they can evolve with the threats. This has been shown both in experimental settings and in real cyberattacks.

In its early stages, this technology is proving to be accurate and effective, and this will only improve with research. As barriers to entry fade and more research and datasets are compiled, machine learning will be imperative for securing cyberspace.

References

[1] D. Winder, “The University Of California Pays $1 Million Ransom Following Cyber Attack,” *forbes.com*, Jun. 29, 2020. [Online]. Available: https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=5628ae8618a8 [Accessed March 6, 2022].

[2] Microsoft Secure Blog Staff, “The Emerging Era of Cyber Defense and Cybercrime,” *Microsoft*, Jan. 27, 2016. [Online]. Available: https://www.microsoft.com/security/blog/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/ [Accessed March 7, 2022].

[3] S. Morgan, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” *cybersecurityventures.com*, Nov. 13, 2020. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [Accessed March 7, 2022].

[4] I.H. Sarker, A.S.M. Kayes, S. Badsha, “Cybersecurity data science: an overview from machine learning perspective,” J Big Data, Jul. 1, 2020. [Online]. Available: https://doi.org/10.1186/s40537-020-00318-5 [Accessed February 28, 2022].

[5] D. Dasgupta, Z. Akhtar, S. Sen “Machine Learning in Cybersecurity: A Comprehensive Survey,” *The Journal of Defense Modeling and Simulation*, pp. 57-106, Sep. 19, 2020. [Online] Available: https://journals.sagepub.com/doi/10.1177/1548512920951275 [Accessed March 21, 2022].

[6] Y. Xin et al., “Machine Learning and Deep Learning Methods for Cybersecurity,” *IEEE Access*, vol. 6, pp.3 5365-35381, 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8359287/citations?tabFilter=papers [Accessed March 7, 2022].

[7] Echosec Systems, “How Is Machine Learning Used in Cybersecurity?,” *Echosec Systems*. [Online]. Available: https://www.echosec.net/blog/how-is-machine-learning-used-in-cybersecurity [Accessed March 7, 2022].

[8] I. Qabajeh, F. Thabtah, F. Chiclana, “A Recent Review of Conventional vs. Automated Cybersecurity Anti-Phishing Techniques,” *Computer Science Review*, Volume 29, Pages 44-55, Aug. 2018. [Online]. Available: https://doi.org/10.1016/j.cosrev.2018.05.003 [Accessed March 22, 2022].

[9] Dongliang Chen, Paweł Wawrzynski, Zhihan Lv, “Cyber security in smart cities: A review of deep learning-based applications and case studies,” *Sustainable Cities and Society*, Volume 66, Mar. 2021. [Online]. Available: https://doi.org/10.1016/j.scs.2020.102655 [Accessed March 8, 2022].

[10] Microsoft Defender Security Research Team, “How artificial intelligence stopped an Emotet outbreak,” *Microsoft*, Feb. 14, 2018. [Online]. Available: https://www.microsoft.com/security/blog/2018/02/14/how-artificial-intelligence-stopped-an-emotet-outbreak/ [Accessed March 7, 2022].

[11] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, T. Tran, “Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity,” *Computer*, vol. 52, no. 12, pp. 45-52, Dec. 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8909930 [Accessed March 8, 2022].

Appendix: Feedback Summary

The feedback from the first peer mentioned some errors with grammar and sentence flow. They annotated the report to point out these errors, most of which I agreed with and fixed. One comment I did not agree with is that the reviewer mentioned not capitalizing the word Internet in the Introduction and Background section, where I write “the Internet”. I argue that this should stay capitalized because I am referring to the Internet as a proper noun, not as an adjective. The reviewer also noted that I did not include a List of Figures section, so I added that.

The feedback from the second peer was not very descriptive, as they basically just said to include more information and topics. However, after reading my report over, I identified that there may be a lack of evidence. To fix this, I found a study on machine learning’s use in detecting phishing attempts, and included that as a subsection of the evidence section in the main topics.

The feedback from the third peer was very short and vague. They said to add more pictures within the text, which I agreed with and added a diagram of a reactive vs. proactive approach to cybersecurity. The only other piece of feedback was that there were grammar errors, without telling me where they were. Luckily, the feedback from the first peer highlighted many of the grammatical errors, and I was able to find some myself, so the grammar of this report was improved in this revision process.