Machine Learning and Security

Anthony Meza anthony.meza02@utrgv.edu

Feburary 8 2019

Proposal

Security remains a core discussion among technology enthusiasts and has been a growing sector of research. Individuals, schools, and businesses care about their security and how it impacts our daily use of technology (regardless of our usage of traditional computers, smartphones, tablets, or even home automation setups). Security must be kept up to date against hackers and their ever-growing tactics of stealing personal data. Thankfully, machine learning has the ability to adapt for security measures and further enhance the systems. This paper aims to explain what machine learning can do to implement security on modern devices (such as understanding what the algorithms are about for successful implementations). The topics in discussion are in hopes that machine learning can be better explained for it's purposes of computer science and how it can contribute towards successful safeguard protection of our personal private data.

Background

In recent years there has been breaches of credit card information and trade secrets released to public view. Inadequate security systems (those without any encryption and where the data source is usually displayed in plaintext) are usually the causes of these breaches. Without security there is no safeguard if your data has been stolen (aside from reporting to banks that a person's credit card is stolen). The best anyone can do if their data is stolen is to find a better system to hide the data in. There is also malware to be weary of as it can be hidden from plain sight and requires insight from security experts to detect (however there even being a malware in the first place is unpleasant for individuals and groups). There is potentially a vast number of solutions machine learning can build security for these systems to protect against hack attacks. One could be learning passwords so that over time a strong password (of numbers, letters, and special symbols) will be required for new users who want to depend on the strong security system. Another could be executing safeguards or sudden self-repair when the machine learning algorithm (if programmed as such) scans and finds an "suspicious" programs inside the system (such as a keylogger that records and sends password entries to the attacker). A more recent practice among security firms they recommend everyone to consider implementing is encryption. While not absolute, encryption is one of the best methods to protect systems from breaches or service disruptions. Machine learning can be capable of encryption (although it must be done correctly or else the system will be easier to infiltrate).

Goal and Objectives

The purpose of this research paper is to convince programmers to consider machine learning as a viable technique for the sake of security. The difficulty and algorithms involving machine learning must be understood to successfully have programs execute machine learning instructions. This also requires an endgame purpose for what the programs are designed for as machine learning typically can only be used for specific purposes (for instance, UI design cannot depend on machine learning algorithms as that is a separate matter for the programmer to create). An improper machine learning algorithm for a security typically results in the program performing worse than without it (which is why it is important to understand the flaws of machine learning and program workloads).

Data and Methods

Because machine learning can self-learn the more it is utilized, there is much data to be added for the system to learn from. It must consider what is good or bad for the system (which falls under the responsibility of the programmer to define) and understand what the final result should be. Even if it'll never perform the final result itself, machine learning can try it's very best to provide the data as needed. However, even with all the data it can accept as input, the execution of the machine language must be performed to optimal levels. Complex algorithms must be sought out for machine learning to perform as intended and must process all the data it is intended for. While it is not limited to the following, machine learning accepts this sort of input: numbers, letters, graphs, user behavior.

References

- A User-centric Machine Learning Framework for Cyber Security Operations Center
- Android mobile security by detecting and classification of malware based on permissions using machine learning algorithms
- Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey