HOW ARTIFICIAL INTELLIGENCE CAN BE USED TO BOOST OUR COMPUTER SECURITY SYSTEMS

Joshua Russell

University Of Greenwich

COMP-1809-M01-2021-22 Introduction to Computer Science and Its Applications

Ali Jazdarreh

28th March 2022

Table of Contents

Introduction

Artificial Intelligence and Cyber Security are two fields that for the most part, have been separated during their development. Cyber Security was developed to protect our computers whilst A.I was made to give the computers the ability to think on their own and have the human intelligence needed to do tasks that would be done by humans. In recent years, however, the 2 sectors have been coming together, with AIs being developed to control cybersecurity to protect a system from threats and cybersecurity systems being programmed into AI to protect it. In this report, I will be going through the ways that the 2 sectors merge together as well as some examples of its uses and how effective AI-controlled cyber security systems are. There are some flaws that AI have currently, which will also be discussed.

Literature Review

"Artificial Intelligence in Cyber Threats Intelligence" by Roumen Trifonov, Ognyan Nakov and Valeri Mladenov discusses how AI is used across different IT sectors and example of how different people are using it for Cyber Security measures.

Xiaoyi Hu and Ke Wang's "Bank Financial Innovation and Computer Information Security Management Based on Artificial Intelligence" discusses how AI is used commercial banking systems and its specific role in Cyber Security.

"Role of Artificial Intelligence in Enterprise Information Security: A Review" by Madhavi Dhingra, Manisha Jain and Rakesh Singh Jadon discusses the work being done in information security and the role of Artificial Intelligence in it. It also discusses recent developments in information security, particularly information hiding techniques, then discusses how this can be improved.

Tsung-Yu Ho, Wei-An Chen and Chiung-Ying Huang's "The Burden of Artificial Intelligence on Internal Security Detection" discusses the flaws of AI in its current state.

"Recommendations Concerning the Selection of Artificial Intelligence Methods for Increasing of Cyber-Security" by Roumen Trifonov, Slavcho Manolov, Georgi Tsochev and Galya Pavlova connects Artificial Intelligence and Military defence and how Cyber Security can defend military systems.

"Artificial Intelligence Enabled Cyber Security" by Ankush Mehra and Sumit Badotra lists the different types of cyberattack then describes how the AI deals with them and the advantages of using it.

"Artificial Intelligence in Cyber Security - A Review" by Jenis Nilkanth Welukar and Gagan Prashant Bajoria is a basic rundown of how AI can be implemented into cyber security and the advantages and disadvantages of doing so.

"Combat Security Alert Fatigue with AI-Assisted Techniques" by Tao Ban, Ndichu Samuel, Takeshi Takahashi and Daisuke Inoue how an AI with a learning system would be able to distinguish genuine security to the several false calls it may receive whilst controlling a security system.

"IoT Object Authentication for Cyber Security : Securing Internet with Artificial intelligence" by Kuldeep Verma & Nishtha Jain discusses how the Internet of Things and how it can be used to detect cyber-threats.

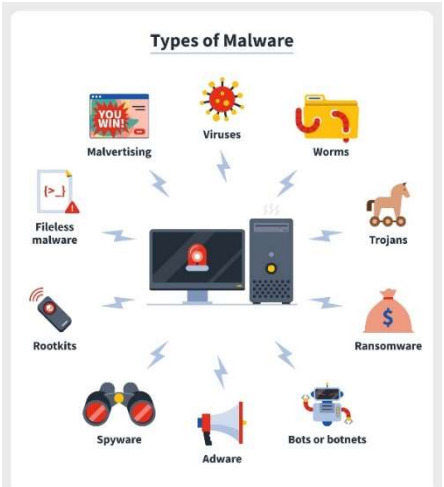
"Artificial Intelligence and Blockchain for Future Cyber Security Application" by Feng Xiaohua, Conrad Marc, Eze Elias and Hussein Khalid discusses how AI and Blockchain(a digital ledger for cryptocurrency), which has built-in cryptography and data encryption technology can be used to boost cyber-security, particularly in the NHS.

Main Discussion

The first known 'cyberattack' was in 1834, by brothers Francois and Joseph Blanc in Bordeaux, France. The brothers were attempting to gain an advantage in the Bordeaux stock exchange, which was directly linked to the stock exchange in Paris which set the pace for trading across the country. The people at the Parisian stock exchange would send info to the other regions and send information about changes in the market via telegram. The Blanc brothers bribed a telegram operator to send secret codes disguised as errors as telegrams to an end station, which had another inside man, who would translate the telegram and relay the information to the brothers. This trick lasted two years and was exposed when the operator in Tours became ill and brought a friend to take his place in the scheme. The friend instead reported the whole thing to the police and the operation was shut down. This of course wasn't the last attempt for criminals to use technology's weaknesses to their advantage and overtime, different forms of cybercrime emerged.

Bordeaux stock exchange -Place de la Bourse

"Artificial Intelligence Enabled Cyber Security" by Mehra goes into detail about the different types of cyber threats. For example, he refers to "Malware Attack:… Worms, spyware, ransomware, adware and Trojans are examples of harmful software viruses." (Mehra, 2021)These are all well known forms of malware. Worms are self-replicating viruses which then spread to other devices across a network. Spyware is a software program designed to track its host's actions. It frequently attaches itself to safer software programs in an effort to be downloaded into the system. This is similar to trojans which are essentially files containing viruses that are disguised to look like innocent software. Ransomware uses the info collected during the spyware software's actions to blackmail the target. He also states that "companies are vulnerable to denial-of-service attack." (Mehra, 2021) He then goes on to list the many benefits of AI in cybersecurity such as "AI is capable of handling a large amount of data…detection and response times are accelerated…unknown threats are spotted." (Mehra, 2021) Mehra is confident



Common types of malware used by hackers and cybercriminals

that A.I can be used effectively to deal with cybercrime due to it's ability to pick up on threats that would be ignored by humans and can run 24/7.

Madhavi Dhingra discusses the use of Artificial Intelligence for Cyber Security purposes. She starts by describing what Artificial Intelligence is, saying it is "the study of using machines just like human brains. The thinking and activities of humans is simulated by the machine." (Madhavi, 2016) Currently, Artificial Intelligence is being developed to think like humans in order to do human jobs, such as manual labour and transport. It's also being developed to handle computer systems, such as the developments as being used for cybersecurity. Dhingra mentions how "one of the major benefits of AI is that it is (an) automatic updating system that evolves through it lifestyle and can update itself accordingly." (Madhavi, 2016) This essentially means that Ais are self-sufficient and can rapidly self-improve itself in order to do its job properly, such as finding new defences for a computer system against cybercrime, something that it useful considering the fact that 450,000 new malware programs are created everyday and a cyberattack occurs every 39 seconds, according to a study by the University of Maryland in the United States. With cybercrime as prevalent as it is, an AI that can adapt on its own unsupervised is a good idea.

AI are constantly learning new things which can help it run more smoothly

Xiaoyi Hu discusses how Artificial Intelligence is used in commercial bank's cyber security systems. The main information collected by banks relates to the bank's funds and the confidential user financial information (i.e., Account details). Hu first refers to A.I being used for customer services, most services can be done by a computer, such as displaying a user's account details or transferring money into or out of their account. He states that "through people-to-people communication, the customer's dependence on bank staff has gradually deepened and the customer's stickiness has been strengthened." (Hu, 2020) This essentially means that the customers have spent more time than they need to in the bank, due to it taking a longer period of time for the bank employees taking a while to find the necessary information and paperwork need for certain tasks. With an A.I system, the process runs smoother as the bank A.I could pull up the necessary details almost immediately and would be "one of the important means for banks to increase asset income, expand other income, reduce operating costs and improve profitability." (Hu, 2020) In relation to cyber security specifically, he mentions how the A.I needs to be able to "Scan and analyze the network system regularly with various system vulnerability detection software to find out the potential security risks and repair them in time." (Hu, 2020) An Artificial Intelligence which can automatically scan for threats is an effective system, particularly for a bank which would require 24-7 surveillance of threats. according to a report by the Boston Consulting Group, "Financial services firms are 300 times as likely as other companies to be targeted by a cyberattack." (Hu, 2020) Therefore, it makes sense to have an AI that can monitor security threats for a high-valued target. Xiaoyi makes a strong case for using A.I in banks to allow the system to run smoothly whilst also being very secure.

"Recommendations Concerning the Selection of Artificial Intelligence Methods for Increasing of Cyber-Security" discusses the use of A.I-controlled Cyber Security systems for Military uses. The report describes how to a computer system for military would need to "(produce) an immediate repulsion of attacks…predict the actions of a possible opponent… (and) troubleshoot consequences caused by Cyber-attacks - this can be referred to as so-called Incident Handling." (Trifonov, 2020) It goes on to list the actions that a computer system would need to be monitoring such as "attempts to

use services blocked by firewalls…unexpected encrypted messages…improper or suspicious use of administrative functions… (and) significant changes in the user's usual activities." (Trifonov, 2020) Trifonov shows that AI has the capability to protect military systems from attack with strong detection and prevention protocols. The report fails to mention what happens after any attempts at attack implying that a retaliation system hasn't been designed, which could be a slight flaw for the system but one that could be resolved within the next few years.

"The Burden of Artificial Intelligence on Internal Security Detection" by Tsung-Yu Ho discusses some of the flaws in A.I. Tsung-Yu states that on average there is a "0.99% accuracy" for A.I when reading through DNS queries(a demand for information sent from a user's computer (DNS client) to a DNS server), meaning that "there are still ten thousand queries that may be misleading, such as classifying benign patterns as malicious." (Tsung-Yu, 2020) This is a clear issue as it can lead to people being unable to access things on a network that they otherwise would and could lead to actual dangers to the system being ignored. There is also an issue of whether the A.I can be understood Tsung-Yu mentions how "mostly the output of AI can not be explained…Some suspicious DNS queries can be evaluated on how close to the known malicious patterns, but customers only care whether these patterns should be blocked or not according to the service's suggestion…but there is still a (chance that this could be incorrect)." (Tsung-Yu, 2020) This means that the AI system is difficult to understand for the average person, and certain warnings could be ignored by the users. Overall, there are still some flaws in Artificial Intelligence as explored by Tsung-Yu.

Conclusion

In conclusion, Artificial Intelligence has reached a stage where it can be implemented in Cyber Security as something which monitors the computer system it's installed into and frequently updates its system, amongst other things. Examples include its use in banks and for military defence, which predicts the methods of the enemy. However, there is still some flaws such some issues with accuracy and shutting down threats. As technology is constantly changing, I personally feel that over the next decade or two, these issues will be resolved, and Artificial Intelligence will begin to rise in popularity and be more efficient at running computer systems.

References

Hu, X., 2020. *Bank Financial Innovation and Computer Information Security Management Based on Artificial Intelligence.* Taiyuan, s.n.

Madhavi, D., 2016. *Role of Artificial Intelligence in Enterprise Information Security: A Review.* Waknaghat, s.n.

Mehra, A., 2021. *Artificial Intelligence Enabled Cyber Security.* Solan, s.n.

Trifonov, R., 2020. *Recommendations Concerning the Selection of Artificial Intelligence Methods for Increasing of Cyber-Security.* Ruse, s.n.