Liam Clement

CYSE426

4/23/2023

Emergent Technologies as Relevant Cyberthreats

As the technology our world uses has developed further and further, it has brought about significant changes and advancements to numerous sectors that affect our daily lives. However, as technology continues to advance, new technologies that break the mold have begun to arise, creating new challenges, threats, and security risks that cybersecurity professionals in both private and public sectors will need to address. This essay will discuss and provide a brief overview of emerging and future technologies that cybersecurity professionals will have to address in the near future.

A very promising technology that has arisen in the public eye in recent years is Artificial Intelligence. While AI technology has been both criticized and lauded for its potential or present drawbacks or benefits, it shows serious signs both of potential as a tool for cybersecurity professionals, and potential as a threat. Language Learning Models, Adversarial Machine Learning, Artificial General Intelligence, Deepfakes, and other AI-centric systems can create serious risks as threat actors begin to exploit them to greater and greater extents within the realm of cybersecurity and cyber attacks.

Some experts agree that within 3 to 5 years, Artificial Intelligence will significantly impact the landscape of cybersecurity. Cyber threat actors will both grow vastly in numbers, as

well as in the strength of their tools, and at the same time, attack surfaces will both grow in total numbers, as well as in a variety of types, offering additional types of vulnerabilities that they can exploit. At the other end of the spectrum, Artificial Intelligence will seriously boost the overall effectiveness of cybersecurity professionals and their tools as it is implemented and integrated with increasing pervasiveness. (Bonfanti #)

Language Learning Models, such as those of the ChatGPT project, provide a unique opportunity to cyberattackers for exploitation as a social engineering tool, and to great effect. (Dash and Sharma #) Such attacks have become a great concern to cybersecurity professionals as chat based systems and similar systems become more prevalent within the digital work environment. Chat-Based social engineering (CSE) attacks using Language Learning Models have seen a significant amount of growth in a rising trend that has continued since the beginning of the COVID-19 pandemic. As digital work environments grew as a result of the pandemic, so did the attack surfaces offered to threat actors. (Tsinganos et al. #) With the growth of language models that can become more effective at obfuscating and inserting persuasive payloads into communications, as well as opportunities for persuasive payload to be delivered through services such as Discord and Slack, the ability of threat actors to quickly manipulate employees has grown exponentially.

However, with this growth in access to more powerful artificial intelligence language learning models that can generate attacks, there has also been a growth in the development of Language Learning models that have been trained and programmed to recognize these attacks. Several proof of concept models have been created using Natural Language Processing (NLP), as

well as Machine Learning (ML), and Artificial Neural Networks (ANN). Some studies on potential implementations of AI language learning models using these techniques have shown effective results in detecting social engineering attacks. While the technology is in its early stages and has not seen reported effective real-world implementations, prototyping has shown promising signs that AI based Chat Based Social-Engineering attacks may be detectable and preventable in the near future. (Lansley et al. #)

Another form of tools that threat actors may use in the near future to generate social engineering is Deepfake technology. Deepfake technology is an established form of AI models that are used specifically for image generation, creating false images that are convincing enough to be credible at a glance. Recent developments have gone further than static images, and have begun to create motion video, and even voice modulation. This poses a significant threat as a method of social engineering attack, as a combination of convincing images, videos, and sound files generated and delivered by threat actors may assist in impersonating authority figures within a target organization and thereby may assist in manipulating even trained individuals. (Dash and Sharma #)

Adversarial Machine Learning (AML) is another emerging artificial intelligence technology that cybersecurity professionals in the near future will face as a powerful and dangerous tool for threat actors to use. Adversarial Machine Learning is a technique using AI-based algorithms to generate data known as adversarial examples, which is then used to deceive machine learning models, such as those that are beginning to be used by Intrusion Detection Systems (IDS), malware detection systems, and similar AI-based cybersecurity

measures. AML attacks exist in numerous forms, one example being a technique by which the adversarial example is generated by creating minor perturbations in data that are imperceptible to human actors, but can vastly negatively impact machine learning models and their ability to classify data inputs. A more simplistic method of using similar adversarial examples to those used in cybersecurity could include using a strip of electrical tape to visually alter a speed limit sign in a manner that may cause a self-driving car using machine learning to navigate to misread or misclassify the data from the sign. Similarly, Adversarial Machine Learning algorithms can generate data that, while similar to the original data that was intended to be transmitted without interception, has been modified to prevent proper classification by AI-based cybersecurity measures.

Particularly vulnerable neural networks and similar machine learning models, while clearly not sufficient in their ability to properly classify adversarial examples, can be altered to make them more resistant to Adversarial Machine Learning attacks. One study has shown that by injecting adversarial examples into the training data applied to an Inception v3 machine learning model trained on an ImageNet dataset, the resultant artificial neural network is more resistant to adversarial examples generated using the fast gradient sign method of ALM. (Kurakin et al. #) Fast gradient sign is considered to be a one-step method of generating adversarial examples.

In addition to this, the study found that adversarial examples using single step methods, such as the aforementioned fast gradient sign method, have a tendency to demonstrate a property that researchers refer to as “label leaking.” This property is a noticeable regularity in adversarial example construction processes that, when used as training data, can be used by AI machine

learning processes to properly classify adversarial examples, similarly to cryptographers in the 20th century finding an unintentional, consistent anomaly in ciphertext transmissions generated using the same algorithms and exploiting them to break codes and determine plaintext. (Kurakin et al. #)

In addition, researchers found that, by using Artificial Intelligence Machine Learning models with higher capacities, meaning a higher number of parameters, have a greater resistance to adversarial examples. Thus, as higher complexity models are developed, theoretically they will have greater use as the basis of Intrusion Detection Systems and other cybersecurity tools. However, one unfortunate conclusion that the study found was that higher risk adversarial examples have reduced transferability between machine learning models. (Kurakin et al. #)

A more fanciful and science-fictional future technology that cybersecurity professionals will need to face in the future is Artificial General Intelligence (AGI). Artificial General Intelligence, or "true" AI is defined as an artificial intelligence system or model that can "perform multiple tasks autonomously by employing a degree of intelligence/rationality equal if not superior to the one displayed by human beings." (Bonfanti #) Simply put, this is a hypothetical AI model that will consistently pass the Turing Test, perform to the same degree as a cybersecurity professional, and even possibly learn from prior experiences. Effectively, this theoretical technology can fully autonomize offensive cyber operations with little very low-level scripting, allowing high-complexity cyber operations to be run with minimal human input. This supposed "Third Generation Artificial Intelligence" model does not yet exist outside the realm of popular science fiction, but as current machine learning, neural network, and similar models of

artificial intelligence advance further and further, AI researchers will come closer and closer to such models being available as both defense and attack systems.

Another emerging technology that is currently showing significant growth, as well as offering a serious threat, is Internet of Things technology. As the convenience of Internet of Things technology grows, so does its market, as well as its presence within the digital workplace and homespace environments. Currently, Internet of Things devices have expanded their market greatly from their early humble beginnings as household conveniences to reaching as far as workplace usage in the medical sector. This, unfortunately, creates a greater attack surface for threat actors to exploit, often with significantly greater consequences than those of the past. (Sadhu et al. #) As our physical interactions within the world of our workspaces merge with our digital interactions, the vulnerabilities of IoT-based industrial systems grow. However, recent studies into the vulnerability of IoT devices have revealed potential solutions to the problems cybersecurity professionals face.

One study in particular published in a Swiss open-access journal detailed particular emergent targets for threat actors in the form of proposed and future IoT applications, and summarizes several other studies that detail promising solutions to these challenges. (Sadhu et al. #) The study particularly details specific emergent applications as future vulnerable attack surfaces, and then lists a variety of studies and their findings on methods to defend these near-future technologies. (Sadhu et al. #)

A Smart City, one of the emerging technologies that the aforementioned study listed as a vulnerable technology, is an advanced metropolitan area that uses a variety of sensors, electronic techniques, and data-collection technologies to collect information that is then processed and analyzed so that it may be used to handle and control the city's assets, services, and programs. This allows effective management and maintenance of resources and systems such as road and transport infrastructure, power grids, utilities, water systems, waste management infrastructure, crime prevention and law enforcement, education infrastructure, healthcare facilities, and other programs important to the functioning of a city. However, due to the city's connectivity, a vast amount of sensitive, private, personally identifiable information is collected from residents, which must be protected. (Sadhu et al. #)

Another emergent IoT Application is a Smart Grid, which is an electrical system that uses smart technology to increase energy efficiency. These technologies can include intelligent electrical meters, intelligent power panels, smart control systems, alternative and renewable energy solutions, and other emerging technologies. A Smart Grid encapsulates an entire power generation and distribution system into a single frame, from the plant where power is produced, all the way to the end customer, allowing the grid to provide "cleaner" energy to the customer. This, like a Smart City, also collects significant amounts of user information, which must be protected from threat actors. (Sadhu et al. #)

Yet another emergent IoT Application that the study details is Internet of Vehicles. Internet of Vehicles (IoV) is a framework comprising vehicles, smartphones and wearables, and roadside equipment that is interconnected within a network using wireless technologies such as

Wi-Fi, Bluetooth, 5G, and Cellular data. The goal of such a network and technology is accident reduction, alleviating traffic congestion, providing low traffic route information, and providing other information services. The effects of IoV applications can significantly improve overall safety and significantly reduce gridlock on roads, but due to these effects, falsified data fed to IoV environments can also massively increase these problems in some areas, or totally clear roads in other areas, necessitating security against threat actors. (Sadhu et al. #)

The final emergent IoT application that the study mentions is Internet of Medical Things (IoMT). This environment consists of smart healthcare devices interlinked using wireless communication frameworks such as Bluetooth, Wi-Fi, Zigbee, 3G, 4G, 5G, etc. to exchange data with healthcare providers. Often, this environment can include wearable devices concealed within watches, belts, shoes, clothes, etc.. These devices can provide the opportunity for constant monitoring of patient information by healthcare providers, allowing immediate diagnosis and treatment. However, according to research conducted by CyberMDX in 2020, nearly 50% of all IoMT equipment is vulnerable to cyberattacks. Because IoMT devices directly impact the health and safety of patients, as well as interact with highly sensitive private and personally identifiable information, which must be protected under laws and regulations such as HIPPA. (Sadhu et al. #)

One solution to emergent threats to IoT environments and applications that studies have shown is Machine Learning based data-centric misbehavior detection models, similar to Machine Learning-based Intrusion Detection Systems. This proposed method is somewhat straightforward in manner of implementation. (Sadhu et al. #) Another, more complex solution, is using a Public Key Infrastructure-based method. This method has several different variations, but

near-universally, almost all studies specifically show that its implementation is far more suited to very large scale networks, such as “smart cities,” as opposed to smaller scale work environments or consumer households. (Sadhu et al. #) One smaller scale solution, specifically proposed for use in the healthcare industry, is a MAC-based authentication system, using a framework based on smart cards authenticated by an IoMT device based on public key cryptography. While this proposal and subsequent studies that have amended it to increase its potential effectiveness shows promise, concerns have been shown about the lack of user-anonymity. (Sadhu et al. #)

Another proposed solution to threats to emerging IoT technologies is a blockchain-based solution to IoV technology. Numerous studies have been conducted with the intention of creating many different proposals for implementation, such as 5G wireless transmissions between vehicles to update the blockchain used for security, as well as using Elliptic Curve Cryptography (ECC) in combination with blockchain for authentication services. One of these studies, in particular, concluded that Identity-Based Encryption (IBE) was vulnerable to key-abuse issues, and in response proposed using a certificateless cryptography solution for generation of public keys. Following this, Pseudonym Based Cryptography (PBC) is used to hide user identities. Following this, depending on what communications are being made between what types of devices in what points of the network topography, mutual authentication is made using various methods. (Sadhu et al. #)

Beyond the aforementioned proposals, other proposals include an Attribute Based Encryption (ABE) based authentication, as well as solely Elliptic Curve Cryptography based solutions, and Physically Unclonable Function (PUF) based solutions. These solutions, along

with the aforementioned ones within the study, are believed to have significant potential in curtailing future threats to IoT environments and applications. A combination of these solutions, as well as emerging communication and computation technologies, such as 5G, quantum computing, AI, etc., will likely define the operations, threats, and solutions of the near future that cybersecurity professionals must adapt to. (Sadhu et al. #)

The emergence of new technologies that existed only within the realm of popular science fiction when the field of cybersecurity first began to arise has brought forth new challenges that cybersecurity professionals have had to rapidly adapt to in vastly uncomfortable ways, often with little foresight. However, the nature of advancements within computer science naturally demands yet more advancement and adaptation within cybersecurity to protect end users of such aforementioned advancements, or potential cyberattack victims from these advancements. As Artificial Intelligence technology becomes more powerful and more available to users, and as IoT devices become more pervasive in our daily lives, cybersecurity professionals will need to remain vigilant and adaptable in the face of new advancements. Fortunately, with the benefit of hindsight, professionals within cybersecurity have gained the ability to look forward to emergent threats exploiting near-future technologies.

Works Cited

Bonfanti, Matteo E. “Artificial intelligence and the offense-defense balance in cyber security.” *Cyber Security Politics: Socio-technological Transformations and Political Fragmentation*, edited by Myriam Dunn Cavelty and Andreas Wenger, Routledge, 2022,

p. 64, Library.oapen.org/bitstream/handle/20.500.12657/52574/1/9781000567113.pdf. Accessed 23 April 2023.

Dash, Bibhu, and Pawankumar Sharma. “Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review.” *International Journal of Engineering and Applied Sciences*, vol. 10, no. 1, 2023, researchgate.net/profile/Bibhu-Dash-5/publication/368838115_Are ChatGPT_and_Deepfake_Algorithms_Endangering_the_Cybersecurity_Industry_A_Review/. Accessed 24 April 2023.

Kurakin, Alexey, et al. “Adversarial Machine Learning at Scale.” 2017. arxiv.org/pdf/1611.01236.pdf. Accessed 24 4 2023.

Lansley, Merton, et al. “SEADer++: social engineering attack detection in online environments using machine learning.” *Journal of Information and Telecommunication*, vol. Four, no. Three, 2020, pp. 346-362. *Taylor & Francis Online*, tandfonline.com/doi/epdf/10.1080/24751839.2020.1747001. Accessed 23 April 2023.

Sadhu, Pintu K., et al. “Internet of Things: Security and Solutions Survey.” *Sensors*, vol. 22, no. 19, 2022. *MDPI*, mdpi.com/1424-8220/22/19/7433. Accessed 23 April 2023.

Tsinganos, Nikolaos, et al. “Utilizing Convolutional Neural Networks and Word Embeddings for Early-Stage Recognition of Persuasion in Chat-Based Social Engineering Attacks.” *IEEEAccess*, 2022, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9915571. Accessed 23 April 2023.