Tolani T[redacted]

[redacted]

[redacted]

[redacted]

[redacted] Recent Events Report

NSA Cybersecurity Director Says 'Buckle Up' for Generative AI by Lily Hay Newman

In today's society, artificial intelligence and machine learning can be found present in almost all areas of life from job recruitment, to personalized advertising, your phone's virtual assistant, and even in healthcare with AI diagnosis and identification. Due to the extremely fast evolution of generative AI, specifically with the rise of AI to create misleading, false, or imitating information, photos, videos, and sound, more people are becoming wary of the technology. And in the cybersecurity field, professionals are starting to prepare for what the rise and increase in accessibility of AI and ML could mean for threat actors.

The article "NSA Cybersecurity Director Says 'Buckle Up' for Generative AI" by Lily Hay Newman features NSA cybersecurity director, Rob Joyce, and warns readers about the prospective implications of generative AI on cybercrime. One of Joyce's main concerns was that whilst AI is "game-changing technology", from a practical standpoint it can be (and is very likely to be) exploited by bad actors to propagate malware, automate attacks, and create false data to manipulate individuals and organizations (qtd. in Newman). For example, as Joyce pointed out, AI could be misused to create believable/well-written phishing emails, or develop programs to evade current detection flags and definitions. When it comes to risk management and incident response, not being able to detect and prevent incoming attacks is a major impediment to protecting one's data. The use of generative AI can assist attackers in bypassing the standard IDPS by generating malware code that consistently rewrite its signature to remain undetected, or automating injection attacks to exploit vulnerabilities in a system. Consequently, the work of professionals specializing in risk/vulnerability management and mitigation, could become intractable, if not properly prepared for.

In my opinion, artificial intelligence can be an extremely dangerous tool. With generated images, videos, and audios already deceiving millions of social media users and impersonating notable figures or ethnic groups, it's not farfetched to anticipate how AI is a significant threat to information security. As exemplified by the AI-generated songs imitating artists, it won't be long until biometric data can be replicated to hack into protected or classified systems. Furthermore, there could be myriad applications of AI to aid in cybercrimes, for instance, a program could be trained to analyze encryption strategies to crack protected servers and files, or falsify media to enhance their social engineering techniques. In principle, AI has the potential to make cyber-attacks a lot more effective and efficient.

On the other hand, AI also has the potential to be extremely beneficial. As mentioned previously, AI is already a big part of the healthcare sector, but it also plays a role in environmental science (automating climate/weather analysis), finance (generating forecasting models), transportation (optimizing routes for travel), and a growing number of fields. Specifically, in the cybersecurity sector, AI-based security programs can be used to analyze traffic and network data to detect unusual behavior, alert personnel, and automate certain response protocols.

Like hacking, which can be used maliciously or benevolently, AI has the potential to completely disrupt or shield an organization's assets. As mentioned in the *WIRED* article, there is great "potential for generative AI to aid in big data analysis and automation" and to act as an "accelerant for [cyber]defense" (Newman). However, as a cybersecurity professional, it is crucial to stay up to date on the advancements in machine learning, and maintain algorithm safeguards, to ensure the AI program's authenticity and efficiently identify evolving cyberattacks.

The Car Thieves Using Tech Disguised Inside Old Nokia Phones and Bluetooth Speakers by Joseph Cox

In today's day and age, cybersecurity is still a growing field and concept, and outside IT-based and other predominantly online corporations. Even within organizations, the importance of cybersecurity is often overlooked to prioritize budgets, time, or the company's interests. However, without cybersecurity, the risk of data loss, system corruption, or even service interruptions, can result in a much greater loss of revenue, time, and possibly reputation than investing in security personnel, tools, and protocols. One industry that could benefit from improved security measures is automotive manufacturing. According to the article "The Car Thieves Using Tech Disguised Inside Old Nokia Phones and Bluetooth Speakers" by Joseph Cox, high rates of car theft are emerging due to a new form of cybercrime and manufacturers are primarily unprepared.

Cox's article provides a detailed insight into how criminals are utilizing technology to quite easily break into and steal various vehicles. By purchasing a tiny chip embedded in a mobile phone or Bluetooth speaker, malefactors with virtually no technical background, can initiate an attack on a vehicle's control system and gain access in as little as 15 seconds. Due to the low-cost and ease of use, “the barrier of entry for stealing even high-end luxury cars is dramatically reduced” (Cox). Consequently, it’s up to the manufacturing companies to respond to the need for information security and its management.

From my point of view, it is paramount that the automobile industry prioritizes its security protocols and regulations. One example that is at the heart of the issue, is the controller area network receptor. As highlighted in the article, the main reason these attacks are so successful is because the vehicles’ control boards aren’t equipped to verify incoming messages and the controllers or keys aren’t able to encrypt outgoing messages. By implementing encryption methodologies, manufacturers can protect their products’ data and data transmission, preventing the attacker from hijacking the entry system. In addition, manufacturing companies may also benefit from investing in vulnerability and security testing to identify potential susceptibilities to be addressed, as well as provide regular security firmware updates to patch the vulnerabilities. Furthermore, from a consumer perspective, it may be very alarming to discover that it’s virtually impossible to protect oneself from this form of car theft. When it comes to the legal, ethical, and professional side of the issue, it is important and the responsibility of the manufacturers to defend their users from these types of threats. Without proper incident detection, response, and contingency, a company cannot efficiently prepare for, predict, or mitigate threats. Therefore, it may also be essential for automobile regulations to be updated to encourage companies to be vigilant about their security procedures.

In conclusion, the *VICE* article serves as a call to action for the automobile industry and illustrates the value of strong cybersecurity management. In order to create a secure product and build reliability and trust with their customer base, organizations have to ensure that not only are their merchandise is engineered with security in mind, but also maintained to keep up with evolving threats.

Metaverse Version of the Dark Web Could Be Nearly Impenetrable by Jai Vijayan

Metaverse is a term used to describe a virtual space or world powered by virtual reality and augmented reality where users can socialize, shop, play games, work, and more in a 3D iteration of the real (or a fictional) world, all from the comfort of their own home. Whilst potential versions of a metaverse seem to have problems of their own, there may be a greater peril to anticipate. The article "Metaverse Version of the Dark Web Could Be Nearly Impenetrable" by Jai Vijayan presents as a warning to readers that the development of the metaverse could contribute to a malignant parallel, referred to as the darkverse.

The darkverse would act as an extension of the dark web that will most likely be embedded in an unindexed portion of the metaverse. “The space [would] offer a safe haven for criminal spaces, extremist spaces, purveyors of child pornography, and those seeking to harass others” (Vijayan). And perhaps even more concerning, an unindexed darkverse could potentially protect criminals from persecution as metaverse access controls could obstruct law enforcement investigations. With bad actors “already talking about how to make a profit in the metaverse”, the darkverse is certainly an emerging threat that cybersecurity professionals and law enforcement must keep an eye out for. In addition, Vijayan’s article addresses the prospective implications the legal metaverse may pose. As businesses start idealizing how they might use the metaverse to leverage their companies, more and more vulnerabilities have to be considered. For example, companies that plan to utilize a virtual work environment for their employees to complete their work virtually may be susceptible to bad actors gaining access to these environments to steal from or disrupt the organization. Another business application mentioned in the article, was the creation of virtual stores to allow consumers to retail shop in a similar fashion as they would in a physical store. However, this could also leave both retailers and shoppers alike vulnerable to credit card fraud, IP theft and imitation, and social engineering.

Personally, I am in favor of not proceeding with metaverse development. I say this because there are too many risks that may come from its implementation that are too significant to be overlooked, and possibly too vast to contain all of them. Consequently, the metaverse may not be worth its ramifications. From my perspective, I don’t necessarily see a need for a metaverse in society, except perhaps to increase accessibility for individuals with disabilities or impairments with functions such as working ‘in-person’ and other tasks that may not be practical in the real world. Therefore, I believe that the metaverse concept would benefit substantially from prolonging the development process to ensure that all vulnerabilities are thoroughly assessed and addressed.

Whilst the metaverse is a very compelling concept, it is not without its hazards and drawbacks. The possibility of a darkverse emerging from the metaverse is disconcerting and as discussed in the *Dark Reading* article, presents an immense threat to everyone. And despite the metaverse potentially being a great business opportunity, its applications may unintentionally expose organizations and their clientele to fraud and cyberattacks. With these risks in mind, it is understandable why researchers are hesitant to sign on for the metaverse, especially before all concerns are addressed. Ultimately, whether the benefits of the metaverse exceed the risks is a question of personal preference. However, it is critical to proceed with caution in order to avoid the negative consequences of ignoring potential hazards.

Works Cited

Newman, Lily Hay. “NSA Cybersecurity Director Says “Buckle Up” for Generative AI.” *Wired*, 27 Apr. 2023, https://www.wired.com/story/nsa-rob-joyce-chatgpt-security.

Cox, Joseph. “The Car Thieves Using Tech Disguised Inside Old Nokia Phones and Bluetooth Speakers.” *VICE*, 18 Apr. 2023, https://www.vice.com/en/article/v7beyj/car-thieves-tech-hidden-old-nokia-phones-bluetooth-speakers-emergency-engine-start-keyless.

Vijayan, Jai. “Metaverse Version of the Dark Web Could Be Nearly Impenetrable.” *Dark Reading*, 26 Apr. 2023, https://www.darkreading.com/cloud/metaverse-version-dark-web-nearly-impenetrable.