Review

This article is a brief overview of what the future of cybersecurity is going to bring to us and what tools and technologies they are going to use to prevent hackers from attacking and gaining personal information from us. It first gives the brief overview of how the Internet of Things is severely affected by these cyberthreats which only increases due to the sheer volume of how many devices are connected to each other. When handling all this information, we recognize that this is where Big Data comes into play. With big data, cyber defense teams will now be able to recognize certain patterns with all the data points, preventing future attacks from happening. By visualizing these complex cyber-attacks with various visualizations, we can see all the predictive models and how they affect certain entry points. Yet with all this data, there comes a problem; how are we going to handle all these access points? That is where AI comes in handy.

AI is a big contributor in finding and tackling problems that seem trivial and allow the humans to focus on the bigger and more complex problems. By working together, it allows for a very productive combination in tackling these complex problems. I feel that as time goes along, we see that artificial intelligence will be used more. You see a lot of people hack into many of the companies; You see it all over the news. One of the main issues we are trying to tackle right now is securing the Internet of Things. In the article, they briefly mention that medical equipment can be hacked and be used to get critical information about patients within hospitals. By doing so, they can get ahold of information that can be detrimental to both the hospital and the patients. Therefore, the need for cybersecurity is at its peak right now. We have so far never had so many attacks with so few employees mitigating these attacks. Several other problems have popped up and really taken over and changed the way we viewed the dangers of these attacks. In 2012, a joint US-Israel created a virus dubbed “Stuxnet”, launching a cyber-attack on Iran to undermine its nuclear enrichment facilities; the virus disabled 1,000 of Iran’s centrifuges at the time. (1) We have seen Russian hackers gain access to the Democrat’s computer networks to ruin the campaign of Hillary Clinton. It has all been overwhelming and it is becoming more important for people to become aware of these problems. Otherwise people will get attacked by 3 of the most prevalent known today: Backdoor, Denial-of-Service and Direct-access.

Backdoor attacks exploit alternate methods of accessing a system that does not require the usual methods of authentication. Denial-of-service attacks prevent the rightful user from accessing the system. Direct-access attacks refer to viruses, which gain access to a system and then copy its information and modify the system. (2) We see that the sheer volume of attacks is overwhelming, and the complexity of these attacks will only get more complex. Therefore, I predict that we will come to a point where we will only need a combination of AI Scientists and Cybersecurity specialists to use machine learning alone to tackle these problems. This will ultimately save a lot of profits for several companies that need it.

(1) (2) https://medium.com/qtma-insights/the-future-of-cyber-security-one-small-step-for-man-one-giant-leap-for-ai-5133a2ab335a