Mark Migdal 12/5/25
CYSE200T

Analytical Reflection Paper

In this paper, we will review authentication, encryption, and cybercrime, examining their effects on cybersecurity and how they relate to one another.

Authentication

Authentication is a vital part of cybersecurity. It ensures that only authorized users can access the system, blocking potential attackers. The actual definition of authentication, especially within computing, is “the process or action of verifying the identity of a user or process”. There are multiple authentication methods and versions. The first, and most commonly used, is knowledge based authentication. This is passwords, pins, and security questions. These are typically picked by the user, and if used incorrectly, can be very vulnerable to attackers. The second type of authentication is biometrics. This type of authentication uses something that is unique to the user and is typically pretty strong against attackers. Some examples of biometrics are face, fingerprint, eye, and voice identifications. One weakness within biometrics is the recent advancement of artificial intelligence. Generative AI now has the ability to replicate voices with enough precision to pass a biometric voice authentication. Another type is certification based authentication. Certification based authentication, or CBA, is basically a digital paper that your device shows to authenticate itself. They have a private key built into it, which is the actual certification aspect of them. One risk, although very rare, is CBAs being stolen and used to infiltrate certain applications. One example of CBAs being stolen was during the Stuxnet attack on the Iranian Nuclear Program. This allowed the Stuxnet worm to get way further into the systems without being detected. Lastly, hashing. Hashing ties closely with the next topic of encryption. Hashing is a form of encryption, typically used to store passwords. While this could

be tied into Knowledge based encryption, it ties very closely to encryption, which is the next major topic.

Encryption

The definition of encryption is “the process of converting information or data into a code, especially to prevent unauthorized access”. Encryption is a major part of cybersecurity and its role in protecting information and data. Encryption is very closely related to authentication and is equally important. Typically, the information that requires authentication is encrypted while stored, or usually it should be. A perfect of them working together is hashing, which was covered in the previous section. A major part of encryption is that it can protect sensitive data at all points. As stated in the IBM article, “Encryption can protect data at rest, in transit and while being processed”. The way encryption actually works is that there are two different parties, the sender and receiver. The sender uses an encryption algorithm, or a public key, to hide their information, and the receiver has a private key, which allows only them to decrypt the message. Current day encryption algorithms can take millions of years to crack, but with quantum computing getting closer to being commercialized, these algorithms will no longer be good enough. These algorithms make man-in-the-middle attacks far less effective, as any intercepted data remains encrypted. Encryption is also an essential part of the CIA triad, being closely associated with confidentiality. In the event of a data breach, if the data is encrypted, the data will still be safe because all the attackers will get is a jumble of letters and numbers.

Mark Migdal 12/5/25
CYSE200T

Cyber Crime

Both of the previously mentioned topics are a small but important part of the prevention of cybercrime. The definition of Cyber Crime is “criminal activities carried out by means of computers or the internet”. Cybercrime is bigger than ever and will continue to grow as the development of technology continues. And in conjunction with AI, cybercrime has never been easy to do and harder to defend. Most cybercrimes are usually done for some kind of financial gain. Things like romance scams and general fraud, which directly make money for the user, or stealing data through things like ransomware, man in the middle attacks, and general infiltration attacks, which allow the user to sell data for a profit. On the higher end of cybercrime, you start to see attacks that are less financially motivated and more politically motivated or military driven. A perfect example of this is the Stuxnet attack on the Iranian Nuclear Program in 2010. It was done with no financial gain in mind, and the perpetrators were never officially discovered, although it was believed to be an attack from the United States government. Usually, attacks on a large scale are financially motivated in some way, like the Colonial Pipeline cyber attack.

The Need to Rethink Cyber Policy Amid Rapid Technological Change

It would be unrealistic to assume that current cyber policies are fully adequate today or will remain effective with the rapid development of technology. Before this class, I had never even thought about this type of “policy change”. There are many topics within the cyber world that need a policy overhaul, but there are a few that need it more than most. Gene editing and the cybersecurity surrounding it, Artificial Intelligence, and Social Media. AI and social media are

the two that I believe need the most attention as soon as possible. AI is rapidly learning and advancing with very few regulations and rules in place. Social media is currently how most youth interact with each other, get news, get entertainment, and much more. The national regulation around it is minimal, considering the amount of people who use it today.

Conclusion

Even though it may not seem like it, all topics in cybersecurity are in some way related to each other. These three topics relate heavily to each other, but it would have been easy to substitute another topic in place of any of these. They show how important the collaboration between them is, and that if just one system fails, it can cause an entire system to crumble. Authentication fails without encryption, encryption means little without protection from cybercrime, and cybercrime itself evolves in response to gaps in both. Overall, it just shows how interconnected cybersecurity is and that most systems are equally important in their own way.

Sources

Authentication Types

What Is Authentication? Definition and Methods | Microsoft Security. (2025). Microsoft.com. https://www.microsoft.com/en-us/security/business/security-101/what-is-authentication?msockid=0fa2eecc4d8b6d0b1fd5f8994c306c61

Certificate based authentication

GeeksforGeeks. (2024, April 11). What is Certificatebased Authentication? GeeksforGeeks.

https://www.geeksforgeeks.org/computer-networks/what-is-certificate-based-authentication/

Encryption

IBM. (2021, July 14). What is encryption? Ibm.com.

https://www.ibm.com/think/topics/encryption

McKay, D. (2023, October 23). What Is Encryption, and How Does It Work? How-to Geek.

https://www.howtogeek.com/33949/htg-explains-what-is-encryption-and-how-does-it-work/

All sources used to reinforce topics learned in class

Appendix A - Reasoning Notes

All three of the topics I covered were topics I was pretty well acquainted with, so there wasn't very much that surprised me. The one that I wasn't totally sure about was encryption, more specifically, public and private key encryption. After a little bit of research, it became clear to me that the idea of encryption is pretty simple, although encryption itself is not. Moving on to AI, the only program I used was ChatGPT because I am familiar and comfortable with it. All ideas are original, and I really didn't use them very much. One of the ways I used it was to help with some poorly worded sentences that didn't really fit into this paper. The other major way I used it was to try and poke holes in my paragraphs and ensure that my information was accurate.

Mark Migdal 12/5/25
CYSE200T