Michael Liam Sinclair

Professor Davis

CSCI 412

18 November 2023

Presentation Responses

Joshua Greff: End-to-End Encryption (E2EE)

Josh presented end-to-end encryption as it is used in messaging applications. Josh explained how E2EE is extremely important for privacy and security since digital communication is currently the most common form of communication. He defined the Signal Protocol which is an open-source security protocol that is used to enable E2EE how it was developed and how it is currently used. Josh also went over applications, disadvantages, and security concerns for E2EE. I believe Josh did a great job with his presentation, as it came off as very conversational and more of a discussion, which I enjoyed. His style of explaining things made them very easy to understand and comprehend. My only criticism is that he could have included more information on the slides/screen itself for others to be able to follow along easier though I did not find this to be an issue personally. I only had a vague idea of E2EE, so Josh's presentation made it much easier for me to understand moving forward.

Ariya Seng: Software Defined Networks in the Modern Era

Ariya presented on software-defined networking as it is today. In her presentation, she covers what SDN is and how it is software-based over the traditional hardware-based techniques. The figures she provided made it easier to visualize her topic and what she was going over, so I found them very helpful. She did a great job going over the disadvantages of SDN, though my presentation topic was also SDN I found these disadvantages somewhat hard to find and learned that controller placement can also present itself as a disadvantage or challenge. Overall, I found Ariya's presentation very easy to follow and I really liked her coverage of Google's Orion and Cisco's ACI. I believe expanding upon how SDN works on a technical level would have elevated her presentation and would help viewers follow along better and support the advantages and disadvantages she provides.

Tom Tran: Splunk in System Networking

Tom presented on Splunk in the system network, as well as an introduction going over SIEM. Tom had a strong focus on security and how Splunk uses machine data. I found his presentation a little hard to follow since I couldn't read his slides very easily though I do believe he did a great job at explaining the concepts within his presentation. I liked that he provided evidence supporting Splunk and his organized breakdown of information. I didn't really know anything about Splunk before watching his presentation, and I enjoyed learning about it. Tom's discussion on the cons of Splunk could have used a bit more thorough discussion, such as offering some examples of competitors to Splunk. Overall, I believe Tom did a great job at explaining Splunk for security in system networking, and his graphics as well as charts were very helpful for understanding it.

Brandon White: Application Layer Protocol HTTP/HTTPS

Brandon's presentation was an overview of HTTP and HTTPS. He discusses what HTTP is and how its role as a protocol for web communication and data transfer over the Internet. He also did a great job discussing TCP though I think it would’ve been helpful if he spent more time defining what TCP is for those who may not be as familiar. Given the class that this is for I’d hope that everyone has a strong idea of what TCP is though. His graphic for this section was very helpful for visualizing his talking points, specifically the three-way handshake. His slides were very dense with information, which would make sense if he was reading off the slides however, he was not, so I think the slides could’ve done with just key points and graphics. Despite these minor criticisms, Brandon was very informative and formal in his presentation, and his explanation of the HTTP request-response process was very thorough. Though I knew the information covered in the presentation before viewing Branding modeled it in a way that made it easy to follow and understand the process as a whole.

Kelvin Tims: Malware and Its Effects

Kelvin provides a broad discussion of malware as well as some different types of malware and the effects malware can have on a system user, etc. Kelvin's discussion of trojan horses, ransomware, and computer worms was well-done and I learned a lot from the examples of them as well as the methods of dispersing them. Eric also provided ways to protect against common malware types that anyone could find helpful regardless of technological background. I don’t think he needed as much information on the slides themselves since he did a great job discussing each topic without using the slides. An expansion on antivirus software works would be very helpful for those following along, though his general prevention tips were very strong, and the specific examples of each that he provided strongly support each point. Overall, Kelvin’s presentation was very thorough, and his discussions were very relevant to issues that anyone with an internet connection faces today.

James Robinson: Google Dorking

James covered Google dorking in his presentation which is exploiting Google searches to find private information such as passwords, configuration files, and even IOT devices. I found his discussion of this fascinating and while I had a general idea of what it was beforehand, I had no idea how serious of an issue this really is and how easy it is for hackers to use. The example queries provided were almost scary to see since most people would never think about how this information is exposed to a simple Google search. The examples of exposed webcams he had access to are crazy, especially the government camera examples he provided. James did a fantastic job explaining Google Dorking and exploring how it is used as well as the risks associated with it. I really learned a lot from his presentation, and I would've loved a deeper dive into how system administrators and IT specialists can better protect themselves from this. I think the end of his presentation might've gotten cut off though (at least for me), which is a shame since I really would have loved to hear more.

Juan Arismendy: WannaCry Ransomware Presentation

Juan covers the WannaCry ransomware that infected computers and networks in 2017. The ransomware encrypted files, locked down computers, and demanded compensation in Bitcoin. Juan also discussed how it infected through EternalBlue and how the exploit was done by the NSA via the SMBv1 protocol. I had known of WannaCry beforehand, but I didn't know anything about the NSA-developed EternalBlue. This was interesting to learn about, and I found it fascinating how Marcus Hutchins just registered the secret domain and was able to disable it from there. Juan did a great job explaining the history, functions, and technical aspects of

WannaCry, and I found his explanation interesting and easy to follow. Expanding more on how WannaCry was spread would be a great addition to this presentation, though I really felt like I got the full picture from his presentation alone and enjoyed his discussion on a very interesting piece of cybersecurity history.

Jacob Milam: AI and Cybersecurity

Jacob's presentation was a thorough discussion of the relationship between artificial intelligence and cybersecurity. Jacob did a great job cultivating a more casual discussion on his topic and making it very understandable and follow. He covered specific security risks that artificial intelligence introduces such as deepfakes, biases (specifically racial biases) that artificial intelligence models can have, and how artificial intelligence enhances malware. Jacob's discussion of WormGPT was something I did not know of previously, and I found it very interesting to learn about. His presentation may have been a bit too thorough, and his presentation fell on the longer side and felt a bit disorganized at times, though while watching this did not pose an issue to me since I found his discussion very intriguing. Jacob's coverage of model injection and specifically the pickle exploits also opened my eyes to something I really knew nothing about beforehand. I believe including more information on how individuals can protect themselves and their data would be very beneficial for this presentation. Overall, however, Jacob presented a great discussion on the relationship between artificial intelligence and cybersecurity, and I learned a great deal on several current issues related to artificial intelligence.