Capstone Review

MIDN Eshleman

Tailgating and Social Engineering:

The goal of this capstone project was to obtain data about tailgating and analyze how the concept of authority affects the success. The team defines tailgating as a cyber attack in which the attacker tries to gain access to a facility by deceiving others into letting them through an access controlled entryway. The team's hypothesis was that authority affects tailgating success and will yield a higher success if tailgating victim is lower in rank than the tailgater. The team collected data by in-person observations and camera footage of entryways within Bancroft Hall. They also took into account the rank of the midshipman tailgating and the tailgating victim, the success or failure of the tailgating and how many people were let into the facility. They concluded that authority of rank does not significantly matter to the tailgating success. Although those who were of higher rank were more likely to be tailgating victims. The success rate of tailgating was 100%.

COVID-19 Contact Tracing App Vulnerability:

During the emergency of the COVID-19 pandemic, contact tracing applications became important in tracing the paths of the virus and informing people if they had been in contact with someone known to have the virus. Using Bluetooth technology commonly found on mobile devices, to what extent can a contact tracing packet be replicated and then manipulated from a source outside of the original, and what potential implications can this have for security practices.Their attack plan was to develop an app that can advertise packets via bluetooth low energy. They then capture packets with the correct packet information and then reconfigure the packet to advertise the effects of a positive COVID trace, and then send the packet out via the app. The final results show that they were able to collect the “dummy” packets being sent out by the app. Due to the encryption of the data stored on the packets the team could not perform the suggested attack. Per LAW they could not legally spoof the data in these packets.