Name: Matthew Young

**Take Home Midterm Exam**

1. (5 pts) Using the recent FBI warning[[1]](#footnote-1),[[2]](#footnote-2) about SMS weaknesses, create a summary of some of the ways that SMS-based two factor authentication solutions can be defeated. *200-300 words*

**Answer: While Multi-Factor Authentication is 99.9% effective at stopping attacks1 there are a few ways around it. Before I start listing these methods, know that these attack methods have yet to be automated1 effectively – meaning they are not able to use a bot to enact them effectively yet. The first method of getting around SMS authentication is an attack “called SIM swapping”1. In this attack the attacker ports the victim’s number to a phone the attacker owns and asks for information from the victim’s phone company to “complete a SIM swap”1. After having completed the SIM swap the attacker then can call services that the victim uses – e.g. a Bank, Healthcare Provider, etc. – and uses the victim’s phone number as a way to avoid security in order to get information or perform actions with the victim’s account1.**

**Another method of attack is to avoid the SMS authentication entirely. The attacker can do this by exploiting the login site, manipulating the URL to make the site believe that the computer being used to login has been used to login in the past in order to avoid any security checks for an unrecognized device1. This can also be done by using man-in-the-middle attacks, session hijacking, and phishing in order to avoid SMS verification completely1.**

1. (5 pts) Tell in your own words how Russia bugged an American Embassy’s Typewriters[[3]](#footnote-3) and peek at the declassified NSA report[[4]](#footnote-4). What lessons can we apply to our world today? *200-300 words*

**Answer: Back in the Cold War the US embassy in Moscow discovered an antenna hidden in the embassy building. At the time of the discovery, the exact use for this antenna was unknown but the ones who discovered it believed it to be used to transmit or relay some form of signal (as an antenna is meant to do). After the initial discovery was made an electrical engineer working for the US National Security Agency (NSA) named Charles Gandy went to work to figure out the exact use of the antenna. After years of searching for the signal that the antenna might be used to transmit, Gandy was issued a “cease and desist” by the Central Intelligence Agency (CIA)3 which, at the time, had operational authority over the embassy. Later on, Gandy was given a letter of authorization from President Ronald Regan3 to continue his investigation and decided to send the electronics that were used in the embassy to be taken apart and x-rayed in the US. They uncovered what is essentially a magnetic key-logger and transmitter that was rigged up to be hidden inside the supports of the typewriters used at the embassy for typing out sensitive documents. The transmitters themselves were also tuned into the same frequencies that the Russian TV broadcasted with which allowed the signals to be masked by the TV broadcasts3.**

**Now for what lessons we can gather from this story. One lesson I personally gather from this is the good old phrase “You’re not paranoid, if they’re actually out to get you”. Security should always be at the forefront of your mind, and if you see a (figurative) smoking gun then there is usually a bullet somewhere waiting to be found – it may even take years to find it.**

1. (5 pts) Summarize in your own words (in about *200-300 words)* the warnings contained in the NYT article by Mr. Gerstell, the general counsel of the National Security Agency[[5]](#footnote-5).

**Answer: Substituted Question 7**

1. (5 pts) Based on the report from CISA (part of DHS) below[[6]](#footnote-6), provide a summary and recommendations for a small business that might be a target of such a state actor. *200-300 words*

**Answer: The Cybersecurity and Infrastructure Security Agency (CISA) has noted that Chinese Ministry of State Security (MSS) affiliated cyber attackers have used “publicly available information sources and common, well-known tactics, techniques, and procedures (TTPs) to target U.S. Government agencies”6. In addition, they believe that the information used by these MSS affiliates are being sourced from cites such as Shodan, the CVE database, and the NVD. The information used seems to be a combination of publicly accessible information (through Shodan) and vulnerabilities in software (through the CVE database and the NVD)6.**

**As for recommendations for a small business, the most parroted method to avoid attacks and exploitations is to frequently update your software applications, security, and operating systems. Keeping things updated makes it harder for attackers to exploit your systems due to the systems changing so frequently and patching out any obvious methods of attack. Aside from that, it is a very good idea to use the same services for public information (Shodan, the CVE database, and the NVD)6 that the attackers use to see if any of your systems or software are actively exploitable and to perform a rollback if necessary to secure your systems and applications. Note that should you choose to continually update your systems it is best practice to check new updates for vulnerabilities before implementing them, and while this may not be easily practiced in smaller-scale businesses it is definitely something to keep in mind for future growth.**

1. (5 pts) In *200-300 words*, summarize the trends in ransomware[[7]](#footnote-7), how it is deployed, who gets attacked, and whether victims get access to their (decrypted) data. Provide a short list of recommendations for small businesses to prevent or deal with ransomware.

**Answer: In Q4 of 2019 ransomware attackers began taking data from companies and threatening its release to the public should the ransom not be paid7. This new tactic meant that the average payout of ransomware attacks rose from $41,198 in Q3 of 2019 to $84,116 in Q47 of the same year across all types of ransomware and ransomware targets. Paying the ransom yields a 98% rate of return for the encrypted data stolen by ransomware attackers7. The average downtime of effected systems is 16.2 days7. The most common method of attack varies by the type of ransomware, but for the Phobos ransomware the most common is a Remote Desktop Protocol (RDP) Compromise and for Ryuk the most common is Email Phishing, which, both happen to be the most common attack methods overall7. Currently, the most common targets of these attacks are businesses with less than 2,000 employees and averaged at around 610 employees, but that number has decreased from Q3 to Q4 in 20197.**

**For small businesses who would like to increase their protections against ransomware attacks there are quite a few options. The most highly recommended ways to prevent ransomware attacks are to maintain antivirus software, train employees on security, backup all data, patch often, and restrict admin abilities[[8]](#footnote-8). Some of these may seem obvious but every implemented precaution helps.**

1. (10 pts) Summarize in your own words (*300-400 words*) the major findings from Mandiant/FireEye about the Ghostwriter Influence Campaign[[9]](#footnote-9). Also provide some recommendations about how governments should respond, and how people can avoid misinformation.

**Answer: The Ghostwriter Influence Campaign is a series of action sets believed to be related to one another involving what is essentially an international disinformation campaign directed against the United States (US) and the North Atlantic Treaty Organization (NATO) in favor of Russia. The disinformation ranges from false quotes to fabricated images and general misinformation regarding US and NATO operations in Eastern Europe. Currently affected countries include Lithuania, Latvia, and Poland. The Ghostwriter Influence Campaign primarily targets news websites by leveraging sites into creating an “inauthentic persona”9 which they use to publish fabricated news articles and documentation. A second activity set that is similar, but notably separate, from the Ghostwriter Influence Campaign is an activity set called “Secondary Infektion”9. Notably, what sets “Secondary Infektion” apart from the Ghostwriter Influence Campaign is the way in which they leverage sites – with Ghostwriter creating inauthentic users based on real people9 and Secondary Infektion creating one-off accounts that don’t impersonate anyone, as well as Ghostwriter using more traditional cyber threat activity9 compared to Secondary Infektion not using any cyber threat activities. Sites affected by the Ghostwriter Influence Campaign all have ties to the country they are targeting for disinformation. Their tactics differ from each incident, the only pattern seems to be a creation of fabricated content, addition of fabricated “evidence”, and then spreading said content to legitimate news websites through fabricated personas9. Some personas will coordinate with one another in order to make the others seem more legitimate as well.**

**The governments of the effected nations have begun flagging the fabricated articles as misinformation9 and issuing statements disproving them to the general public. As recommendations to any potentially effected nation in the future I would suggest keeping close tabs on, and communication with, news outlets to help verify any suspected disinformation as quickly as possible. Any news outlet thought to be a target for the Ghostwriter Influence Campaign should take precautions to avoid the creation of potential fake accounts and should be encouraged to communicate any suspicious activity with their government to hopefully keep the effect of the disinformation to a minimum as well as monitor the spread of the campaign.**

**QUESTIONS BELOW ARE FOR GRADUATE STUDENTS ONLY** although undergrads can substitute 1-2 questions from above with 1-2 questions from below (for 5 pts a piece).

1. (5 pts)Based on this news story by the AFCEA[[10]](#footnote-10) and the underlying report[[11]](#footnote-11), summarize the major concerns. What has been observed so far? What are the trends? How bad could this get? Max of *200-300 words.*

**Answer:**

1. (10 pts) In *300-400 words*, create a summary of what is known so far about the involvement of foreign entities (countries, nation-states) in running campaigns of disinformation about the Coronavirus. What impact are such disinformation activities having on a global scale? Which countries/populations are most impacted? Provide at least 2 sources from 2020.

**Answer:**

1. FBI warns about attacks that bypass multi-factor authentication (MFA) | ZDNet <https://www.zdnet.com/article/fbi-warns-about-attacks-that-bypass-multi-factor-authentication-mfa/> [↑](#footnote-ref-1)
2. PDF of FBI Cyber Criminals Use Social Engineering and Technical Attacks to Circumvent Multi-Factor Authentication <https://www.sc.edu/study/colleges_schools/law/centers/cybersecurity/_docs/fbi_cyber_pin/2019/fbi_pin-20190917_multi-factor_authentication.pdf> [↑](#footnote-ref-2)
3. The Crazy Story of How Soviet Russia Bugged an American Embassy’s Typewriters - IEEE Spectrum <https://spectrum.ieee.org/tech-history/silicon-revolution/the-crazy-story-of-how-soviet-russia-bugged-an-american-embassys-typewriters#.XhDXFzgGN8I.facebook> [↑](#footnote-ref-3)
4. See declassified NSA report “Learning from the Enemy – The Gunman Project” in D2L Exam folder [↑](#footnote-ref-4)
5. I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution <https://link.mnsu.edu/gc> [↑](#footnote-ref-5)
6. Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity | CISA <https://us-cert.cisa.gov/ncas/alerts/aa20-258a> [↑](#footnote-ref-6)
7. Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate?format=amp> [↑](#footnote-ref-7)
8. Ransomware Protection & Removal: How Businesses Can Best Defend Against Ransomware Attacks https://digitalguardian.com/blog/ransomware-protection-attacks [↑](#footnote-ref-8)
9. Ghostwriter Influence Campaign | Mandiant/FireEye <https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf> [↑](#footnote-ref-9)
10. Cheap Cyber Weapons Threaten Unintended Consequences | SIGNAL Magazine <https://www.afcea.org/content/cheap-cyber-weapons-threaten-unintended-consequences> [↑](#footnote-ref-10)
11. Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar <https://nsiteam.com/social/wp-content/uploads/2019/11/191119-AEP_Commodification-of-Cyber-Capabilities-Paper.pdf> [↑](#footnote-ref-11)