**Lab 0: Initial Report**

**Marvin Newlin**

**Objective:** Receive a baseline assessment of students

**Due Date:** 2 Apr

**Instructions:** Answer the questions to the best of your ability. Please type your answers and turn them into me one week from receipt. Each question is worth the same, so answer all the questions. If you get help from other sources, cite them!

**Write-up (limit 2 sheets)**

1. Have you identified your research topic / or research question? If so, what is it?

* Yes, will be looking at methods of objectively evaluating synthetically generated data (like images or text)

2. If you have an advisor, who is it?

* Lt Col DeYoung.

3. What do you want to get out of your time at AFIT?

* Master’s degree (obviously) and an understanding of overall cyber operations.

4. What do you want to learn from this class?

* Basic understanding of mobile and SCADA devices and the threats that exist in that world

5. When it comes to academic scholarship, what are your strengths and what are your weaknesses?

* Strength is memorizing details and

6. What do you want to be when you grow up?

7. What did you study in your undergraduate degree?

* Mathematics & Computer Science

8. Do you have any programming / scripting / developer experience? If so, briefly describe your exposure?

* Undergrad CS was in Java so ~3 years of Java
* Basic python and C, C# experience
* Cursory linux scripting experience

9. Do you have any experience in embedded development or reverse engineering of mobile devices? If so, briefly describe your exposure?

* None

10. On a scale of 1 – 5 (1 novice, and 5 expert), how competent are you with the Linux command line?

* 2

11. In your own words, what is research and what is the benefit of it to the Air Force?

* Research is the process of acquiring new knowledge and it can help the Air Force because we need to continually develop new knowledge to expand our warfighting capability.

12. Identify 5 examples of SCADA systems and discuss why it is important that they be secure?

* Water treatment plants
* Power plants
* Retractable railroad bridge
* Nuclear plant
* Oil & Gas pipelines

It is important that SCADA systems be secure because the consequences of these systems being hacked or taken down can be catastrophic. For example, if a nuclear power plant SCADA system is compromised, it could lead to a meltdown or other catastrophic issue that could cause great damage.

Source: https://oleumtech.com/what-is-scada

13. Discuss 2 examples in history where the security of SCADA systems have been compromised and what, if any, where the impacts?

* 2008: Stuxnet worm destroyed the Iranian nuclear reactors which are controlled by a SCADA system. Impacts: worm caused the centrifuges to break which set back the Iranian nuclear program by several years.
* 2018: FBI reports that Russians have hacked several power plants in the US. As of yet, no impacts have come from this. However, in the Ukraine, Russia hacked power grids and manipulated them by killing power prior to military attacks.

Source: https://www.hackers-arise.com/single-post/2017/06/30/SCADA-Hacking-Why-YOU-Should-Study-SCADAICS-Hacking

14. Discuss 2 examples in history where the security of mobile devices have been compromised and what, if any, where the impacts?

* 2017: White House Chief of Staff John Kelly’s personal android phone was compromised, possibly leading the loss of sensitive data. Source: <https://www.wired.com/story/john-kelly-hacked-phone/>
* 2015: Android stagefright vulnerability led to many android phones being hacked with just a single malicious text. Impact of this was that over 950 million Android phones were vulnerable to this attack. Source: https://www.makeuseof.com/tag/priorityanyone-can-hack-android-phone-single-text/

15. What does mobile security have to do with SCADA devices? Are they mutually exclusive or is there overlap? What are the points of overlap?

* If a SCADA system can be reached from the internet, then hacking a mobile device that can access that system would lead to a compromise of the SCADA system. Additionally, if the mobile devices of the technicians that operate the SCADA systems are compromised, it could lead to information leakage about the SCADA system that would then contribute to a successful attack on the SCADA system.

16. What are your cursory thoughts on how Mobile and SCADA security could support your research (this assumes that you have answered “yes” to questions #1). If you answered “no” to question #1, then discuss a couple research interests you would have in the mobile / SCADA realm.

* Given that my research will be in machine learning and evaluating synthetically generated data, it will not have any relation to mobile and SCADA security.

17. If you had unlimited time and money to design a mobile app, what would you make? How you make it secure?

* I would design an app for Search & Rescue that would track search routes on top of a map and allow for that data to be shared with the people that are running the search.
* To secure it, I would use secure login capability, something like OAuth.

18. Over Christmas, a relative, with no security/computer background, asks you “what do I need to do to make my phone safe so that I don’t get hacked?” How do you answer this?

* Make sure to secure phone with a PIN/password.
* Keep location tracking off.
* Don’t open spam texts/emails

19. If you and some friends got lost hiking in the woods, what would you do first?

a. Stay in the same spot, wait for help to arrive, and tell stories with your friends to pass the time?

* Having been in the Search & Rescue world, stopping and waiting in the same spot for help to arrive is the correct option here.

b. Immediately head back in the direction of your car, even if this means leaving the trail and your group

c. Continue the hike, enjoy nature, and plan to run into a park ranger or find a trailhead at some point.

d. Pull out the map, identify your last known location; divide into groups to find help

e. Other, explain