ECEN 5053-002 Developing the Industrial Internet of Things Hands on with Security

Description

The purpose of this assignment is to give you hands-on experience with security. You can choose from the following list of topics to explore:

The first choice is CryptoPals, see: http://cryptopals.com/. This site presents a series cryptographic challenges. You will write programs for each of the challenges. You can code your solutions to each challenge in any language you choose. I recommend python. See also the python cryptographic library: https://pypi.org/project/pycrypto/. You decide how many of these challenges you perform. At the time of this writing there are 8 sets of challenges. **To get credit for this choice** you must complete Set 1 (Basics) and Set 2 (Block crypto). In terms of hands-on experience with security, this first choice is ideal.

The second choice is a game called CyberCiege. The game was developed by the US Naval Postgraduate School. You can download the latest version here: http://my.nps.edu/web/c3o/latestv. The installer will ask for a password. The password is **grostolis**. There is a notional syllabus here: http://my.nps.edu/web/c3o/syllabus. There is a support page here: http://www.c3o.nps.edu/cyberciege/support.html. After installation to play the game, open the CyberCIEGE icon, which will start the "Campaign Player". Then select "Game Help and Getting Started" from the menu and follow the suggested steps (including a brief movie) to become familiar with the tool. Most scenarios include Lab Manuals to help guide players through the game. You decide how many of these labs you perform. **Note**: I could not get this game to run on:

- A new Windows 10 Lenovo machine
- Bootcamp, Fusion or Parallels Desktop on my Mac

Your results may vary. One student shared with me this trick: Run the application in Administrator mode. However, many students have been successful running the game on a Windows 10 machine. **To get credit for this choice** you must proceed past the Training Campaign (Stop Worms, Life with Macros, Identity Theft, Passwords) and at a minimum complete the Starting Scenarios Campaign (Introduction Scenario, Physical Security, TirePly Filter Scenario, Patches, PCA).

The third choice is to strike out on our own self-study. Here is one idea: Review presentations and papers from Black Hat (https://www.blackhat.com) and/or DefCon (https://www.defcon.org/index.html). Others are listed at: https://www.tripwire.com/state-of-security/off-topic/the-top-13-information-security-conferences-of-2017/?gclid=EAIaIQobChMIm4SKo9iD2QIV0Jd-Ch2t_wxuEAAYAiAAEgIL__D_BwE
See also: https://www.nist.gov/itl/applied-cybersecurity/nice

To get credit for this choice you must read at least 3 papers.

The assignment:

Spend time exploring one of the choices above. Explore, tinker, experiment, read, learn. Write a 5 to 6 page paper (5 or 6 pages of text, not including figures etc.). The length can be extended beyond 5 to 6 pages to include code, figures, pictures and diagrams. However, the total length of the paper should remain under 12 pages, including the title page. In this paper write about:

- What you did
- What you learned
- How what you learned in class supported or reinforced what you learned in this assignment

Format of your paper: Start with the provided template below.

To submit for grading: A single PDF file of your paper that contains all of the content of your paper. If you submit your paper in any other format, you will receive 0 points.

Note: It is super important to do your own writing. You will find that in your professional life you will do a great deal of technical writing as an engineer. Citing up to 10 or less web resources or on-line papers is fine for this assignment, but you must indicate your citations as other people's work. See the paper template provided to you to use as a starting point for your paper. Points may be taken off for any un-cited web references.