1 Student content

1.1 Doug Healy

I am starting my second year in work towards my PhD in Engineering Security, studying under Dr. Bloom. I received my Masters in Information Security Policy and Management (MSISPM) from Carnegie Mellon in 2013, and my BS in Electrical Engineering Technology back in 2003 from the Rochester Institute of Technology (RIT).

I am a avid and active supporter of Scouts BSA, volunteering much of my time in support of the program, both at the Scout (11 to 18 years old) and Cub Scout (5-11 years old) levels. Being an Eagle Scout myself, I highly believe in the values and qualities it instills in our young men and women and work very hard to make the programs successful and FUN!

For this course, I hope to become more efficient in my research. I have spent many, many hours over the summer pouring over search results from both Google Scholar and the UCCS Library. I want to learn how to hone search results, use the correct resources, to efficiently find what I am actually looking for, not what some search engine ”thinks” I am looking for. This will also require me to refine how I choose my search terms.

Secondly, I want to learn how to effectively learn to use my time in reading a scholarly document. I do not skim documents or books well; never have been able to. I want to learn how to do this more effectively and to make sure I am not missing anything. I always think I am missing important things on the page, and I want to ensure that through my skimming, I am not.

1.2 My Picture:

Figure 1: Doug Healy at Philmont Scout Ranch, Cimarron NM

1.3 Related GiT repository

First, thanks to Will for making a comment about this! I would have missed it too...

`https://github.com/stamparm/tsusen`

This repo has code for a software defined situational awareness sensor for networks. It monitors outside traffic and and logs it data into a csv file that can then be analyzed for ”spikes” in traffic and predictors of malicious intent. It flushed the csv periodically and I will need to look into it more to see how often it does that.

1.4 Q & A

1. AN: How was your experience at Carnegie Mellon? I was always curious about going there myself.

2. Carnegie Mellon was great! The ISPM program was much less intense than CMU’s CS department/degrees. I really enjoyed being downtown Pittsburg for the year and a half I was there. The professors were very knowledgeable, most worked at CERT or the SEI so picking their brains on what they could tells us was beneficial (due to the work space there was a LOT they couldn’t tell us..). Classes were a bit more intense and we had ”mini’s”, or half semester classes that flew by and you HAD to keep up. If you want to talk more offline or have more specifc questiosn (my knowledge is 7 years old though) send me an email and we can chat more!

1.5 Will Wesley

1.5.1 Introduction

In authoring *Go To Statement Considered Harmful* [1] Dijkstra is credited for giving birth to structured programming by some [2]. But, I think he set a precedent that many overlook. There are certain things that one *can* do when creating software, but for the sake of the humans involved, one *shouldn't*.

Figure 2: Will

Dijkstra said that by restricting how we enter blocks of code, we get some guarantees about what to expect of the system state inside those blocks. We use typing systems to give us some guarantees about our usage of data in a program, even though data coercion and "duck typing" have certain advantages. Functional programming gives us guarantees about the behavior of functions, while restricting our ability to assign values.

I suspect that there is another set of restrictions, or perhaps disciplines, that can be shown to also make software better with respect to the humans who have to maintain it.

My goals in this course are to develop better skills in researching and find a meaningful question to answer that relates to testing software in a disciplined manner, as I suspect doing so can be shown to yield superior software.

I am currently studying for a Master's of Computer Science, which I expect to complete this semester. I will be starting my PhD research in the spring. This fall, I will also be testing for my Second Degree Black Belt in Taekwondo.

1.5.2 Sneaky added requirement

`https://github.com/stryker-mutator/stryker-js` is a mutation testing tool for JavaScript. Mutation testing is kind of a way to test the test suite. If you have a test suite that has high code coverage, but asserts very little about the behavior of the code, how do you know it does what you want? The idea of mutation testing is to present the test suite with broken, mutated versions of your production code to see if it can detect the change. If it can't, you can be sure the test suite is insufficient.

An interesting thing to note is that research shows that software test suites with better mutation scores (detect lots of mutations) correspond to fewer bugs found in the production code[3]. Further, I believe that the practice of TDD leads to better mutation scores.

[1] E. Dijkstra, "Letters to the editor: go to statement considered harmful," Commun. ACM, vol. 11, pp. 147–148, 1968.

[2] E. N. Yourdon, Ed., Classics in Software Engineering: Go to Statement Considered Harmful. USA: Yourdon Press, p. 27–33.

[3] J. H. Andrews, L. C. Briand, and Y. Labiche, "Is mutation an appropriate tool for testing experiments?," in Proceedings of the 27th International Conference on Software Engineering, ICSE '05, (New York, NY, USA), p. 402–411, Association for Computing Machinery, 2005.

1.5.3 Q & A

1. AN: How hard was it for you to ramp up on Computer Science?

   Well, I've been playing with computers since I was eight when my mom bought me a TRS-80. So, maybe not hard, just a long time.

2.

1.6 Section 1 - About Me

From Week 1, the definition of research is “a combination of investigation.” I hope to learn everything that I can about “investigation” and common tools in accomplishing that. I believe one of my skills, like reading research papers more effectively, can be further improved. More importantly, I bring in the mentality of being curious and grit. Being curious allows me to explore and wonder while grit allows me to dig deep into certain topics that would help with my research. My mission and goal for this CS6000 course is to get the perspective in understanding elements of good research that sparks my interest and passion, while making an impact on society. I am currently in my first semester of the PhD security program here at University of Colorado, Colorado Springs. With the nature of the program, I would also like to learn on how to effectively present my ideas and convey my research to the languages of different audiences. My research topic will be close to Blockchain technology with its performances and implementation.

Some of my recent interests besides information technology would be aviation and endurance sports. I have a little more than 100 hours in a Cessna 172M model and I will be running a 50k trail run this coming October.

1.7 Section 2 - Git Repo

1.7.1 Git Repo - Research

I found this Git Repo to be useful in learning more about Blockchain. This git repo covers topic from basics of blockchain all the way to development and implementation of blockchain. `https://github.com/yjjnls/awesome-blockchain`

1.7.2 Questions and Answer

You may include your question here:

1. WW: Do you have anything interesting to share from your research into Blockchain thus far?
2. DH: Where are you doing your trail run, and is it with an organized team or an individual effort?

1.8 Andrew Nielsen

I'm working towards getting my Masters degree in Cybersecurity. My goal for this course is to be able to prepare for my PhD down the road and be able to apply the research knowledge I gain from this class herein. I'm hoping to learn how to read efficiently and quickly navigate through research documents. I'm looking to be able to understand how to research and how to narrow down a topic that will help in the future. I'm studying cyber security in the master's program.

The research area that I have been working on is ransomware with fuzzy techniques in geo-spatial systems. Part of it has been in understanding ransomware, fuzzing, and identifying gaps in geo-spatial research extending past the earth's atmosphere.

Some code that I found on GitHub that deals with ransomware was found here. This code actually simulates how ransomware behaves and encrypts all the files on a machine and stores the encryption key on a remote server so the user is not able to decrypt their files.

A picture of myself can be seen below:

Figure 3: Andrew Nielsen's Picture

1. WW: Where did you do your undergrad?
2.

DH: How soon are you looking to satrt your PhD? Directly after you Master's?

1.9 Logan Montgomery

My immediate tangible goal is to get use to being retired (27 July). Next, I want to complete my second M.S. in Computer Science. Following my second M.S., I want to pursue a PhD in Computer Science, gain meaningful employment as a University Professor, and continue research in various domains impacted by or dependent on computer science. Intangibly, “I am a lifelong learner.” I do not have an objective or completion date for my journey through curiosity, education, and research. My goal is simple, “breath, engage in life, learn, and influence change where possible.”

Figure 4: My Family and I

1.10 Related GIT - Covert Channel Through TCP Checksums Using SCAPY

I chose a random covert channel git repo. I don’t have a research area officially, but I play around with network security and data exfiltration techniques regularly. So, I though I’d share a pretty straight forward method of transferring data by crafting TCP checksums using SCAPY.

`https://github.com/mtarsel/Covert-Channel`

2 Example of Easy Tables

Time (s)	Rel. time (s)	X Pos	Rel X Pos	Raw Y Pos	Model Y Pos
43.97	0	734	528	14.22624	18.26294
44.01	0.04	731	525	14.11335	18.14345
44.04	0.07	729	523	14.03819	18.06389
44.07	0.1	726	520	13.9256	17.9447
44.11	0.14	720	514	13.70096	17.70686
44.14	0.17	718	512	13.62624	17.62774
44.17	0.2	714	508	13.47704	17.46974
44.21	0.24	711	505	13.36535	17.35145
44.24	0.27	706	500	13.1796	17.1547
44.27	0.3	700	494	12.95736	16.91926
44.31	0.34	696	490	12.8096	16.7627

Better formated Tables

Time (s)	**Rel. time (s)**	**Y Pos**
43.97	0	18.26294
44.01	0.04	18.14345
44.04	0.07	18.06389
44.07	0.1	17.9447
44.11	0.14	17.70686
44.14	0.17	17.62774
44.17	0.2	17.46974
44.21	0.24	17.35145
44.24	0.27	17.1547
44.27	0.3	16.91926
44.31	0.34	16.7627