CS6000 - Computer Science Research - Git Assignment

By Duane Michael
September 20, 2020

Figure 1: A photo of Duane Michael

I am a first year PhD student in the computer science program. Professionally, I work in computer security specializing in offensive security, such as penetration testing, exploit development, vulnerability research, etc. My current academic research interests relate to the application of machine learning and artificial intelligence techniques, such as artificial neural networks and deep learning, to detect intrusions and anomalous behavior on a network or system. I am also interested in various other areas of computer security, so I am expecting my research interests to shift until I get settled into the program.

Question from IJ Olawale

Hello Michael, thank you for sharing your professional and research interests. With your decision to start a PhD program, do you see yourself transiting from your professional career to the academia? For me, I have worked in the corporate world since I graduated from college, over 20 years ago and now it is a bit of struggle getting back into the world of reading voluminous testbooks, research papers, assignments and exams! LOL...

Wishing you the best in your PhD pursuit.

Answer to IJ Olawale

Hi IJ, This is a great question and something I have thought about in depth. I can definitely see myself going towards academia at some point. My priority is advancing the state of security, and I believe there is important work to be done both in academia and industry. Getting into the swing of graduate school has been quite a whirlwind! My first few weeks of my algorithms class were pretty intense for me, but I feel like I'm finally finding my stride!

Question from Abiola Ogundeko

Hello Micheal, it is interesting to read your professional and research interest. Aside understanding the threat landscape, how do you think your professional knowledge and experience will be beneficial in your research interest? Just curious!

Answer to Abiola Ogundeko

Hi Abiola, Great question. I believe understanding the threat landscape is a crucial part of being successful in the realm of intrusion detection. It definitely also seems to be a gap in academic research. To answer your question, my professional experience is pretty well-rounded and I am lucky to be able to see many different implementations of security tools and products in different client environments. I feel that having that exposure will be beneficial in terms of researching new methods.

Question from Simeon Wuthier

Hi Michael, I'm a first year PhD student as well and find your work and research interests to be very fascinating (along with the information from the first discussion). I would love to learn more about your projects, and was just wondering if your artificial neural networks/deep learning reasearch for network anomalies is tailored towards outgoing (attack) or incoming (defense) vectors? I'm still getting settled into this program as well, I wish you the best of luck!

Answer to Simeon Wuthier

Hi Simeon, A fantastic question! I've always thought the concept of detecting attacks closer to the source is fascinating, but that has many challenges, some of which I'm not sure are feasible. For example, analyzing (from the internet) traffic patterns egressing a network to the internet would be difficult due to encrypted traffic that can't be terminated, thus losing a lot of the network artifacts used in detection. However, outbound attack patterns within a network already exist and becomes extremely useful for things like command and control traffic, botnets, etc. So, to answer your question, I am interested in both. If something is malicious on a network, whether inbound or outbound, I want to know about it and I believe the methods

to detect both are similar, with different data collections being analyzed.