

1 Student content

1.1 Constance Hendrix

Greetings. My name is Constance Hendrix. I go-by Constance. I'm a wife, an electrical engineer, a 30-year Air Force veteran, and a current Engineering Security PhD student here at UCCS (see Canvas picture in Figure 1. I'm com-

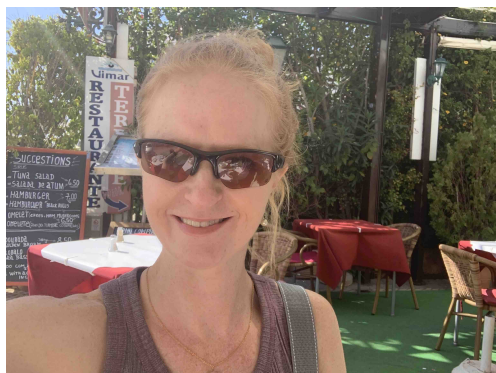


Figure 1: Constance, about to be fed, while on a overdue retreat!

ing in with a Masters of Science degree in electrical engineering with a focus in navigation systems from the Air Force Institute of Technology and a Masters of Business Administration from the University of West Florida. I'm also a licensed electrical engineer in the state of Colorado and a certified Project Management Professional. My overarching goal for graduate school is to make a significant contribution to my engineering field and lay the foundation for a future in academia. My research interests include reliable and accurate navigation, secure satellite communications, biologically-influenced design, artificial intelligence, and signal processing. I have yet to specifically identify my security research topic, but know it will include artificial intelligence, signal processing, and/or edge computing. I hope to select a topic by next semester and will be preparing for my oral qualifier next Spring as well. My goal for this course is to narrow my research focus for my degree, learn new and efficient ways to conduct research, and develop research questions. Outside of school, I work part-time as a position, navigation and timing (PNT) engineer, enjoy reading, working on stained glass creations, quilting, camping, fly fishing, hiking, cooking, and gardening. Quilting is a tradition for the women in my family. Even though I just recently started, I am excited to carry on this tradition.

Question from Jackie Hi Constance, you have a very impressive knowledge background. I do not know a lot about navigation systems, but I always have a question on how navigation works when two teams are digging an undersea tunnel toward each other and they align perfectly?

Answer to Jackie: Hi Jackie! Good question. Most of my knowledge assumes satellite navigation is available. Without Googling, one possible option

would be to map out the two locations via GPS, calculating relative bearing. Once you have the bearings you can begin. There will probably be a random drift if you used a magnetic compass, which would increase the possibility that the two boring machines won't meet up. There would have to be intermediate checks to make sure they don't drift off course. This is where my research would have to begin.

I've never been asked this – I'm sure someone has identified an optimal method. Interesting to think about. Thanks!

Question from Jordan Have you used git before? Most EEs I know end up in software at some point. I've only used Subversion before this year so git is still new to me.

Answer to Jordan: Yes, I use Git at work. I push up code on a regular basis to my team's repo. I've also used GitLab in a previous job (program manager). I only know the basics. Actually, I think I'm a rare case. I've been an engineer for about 20 years. I've been suck in program management and leadership positions during most of that time (military officer). Retired last year, so given this new freedom, I decided to get back to my roots. I have only been doing real engineering since Feb, so I'm somewhat of a novice. Never heard of Subversion... will have to look it up. Thanks for the question!

Question from Ntumphah Hi Constance, am here to congratulate you on your services to the country. You are an inspiration. My question is after 30 years, how was your transition from military life to civilian life?

Third Week's Git Assignment

September 21, 2020

Abstract

This document provide a brief introduction to Maximus' personal life, his goals, and his love for privacy.

2 Background and Objectives for This Course

Maximus a.k.a. "*Cyber Gladiator*" works in the field of cybersecurity and is currently studying security this semester to focus on CPS/IoT designs, vulnerabilities, and flaws. As a student, he loves/ obsessed with privacy, and he hopes that he will become a more effective computer science researcher focusing on CPS/IoT systems by taking computer science research course this Fall.

Maximus' main area of interest includes (but not limited to) information systems' vulnerabilities, vulnerabilities in system design and implementations, cyber risk assessment of IoT systems, and management of the risk in critical information systems in the broader context of their daily effects on individuals.

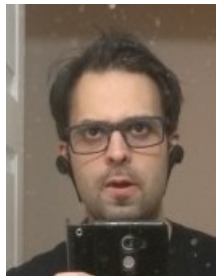


Figure 2: Maximus is currently looking at the mirror.

Question 1: Have you focused any of your research in hardware vulnerability specifically? (from Cassandra Putman)

Answer 1: Great question Cassandra; and after I read your bio, I realized why you asked me this question. Hardware security (and more broadly physical security) is one of the most important topics in IoT systems. Traditionally, security is more focused on protecting digital media in information systems; rather than focusing on physical security. In IoT, however, physical security

can be more important because it can inflict real harm on people (and it will!). This is one of my areas of interest (to study of course) but couldn't find much literature by far. I am also thinking about researching in these areas. -Maximus

2.1 James Bond(Peng)

Before I study in UCCS, I was security solution architect and software engineer. I worked for Newegg, and Hewlett-Packard. I developed security for BIOS (basic input output system) and firmware in laptops, developed infrastructure security for fraud detection systems and search systems in E-Commerce. I also served in military, for cyber operation and radar systems for Coast Guard. I studied electrical engineering and energy systems in undergraduate and high school.

My recent research interest now is signal intelligence (SIGINT), and advanced persistent threats (APTs) in embedded systems. Fields I've done are:

- adversarial machine learning (artificial intelligence, intrusion detection and operation systems)
- lightweight provenance (operating systems)
- trust execution and zero trust architecture (cloud, privacy and cryptography)
- fuzzing for satellite embedded systems (vulnerability scanning, protocol state machine, flight software)

I like not only coding, reading but also sports. I did fencing in elementary school and, after high school, Greco-Roman wrestling, boxing, cage fight, and surfing (both long board and short board). Now in the mountains of Colorado Springs, I swim instead. I am glad to learn from you guys.

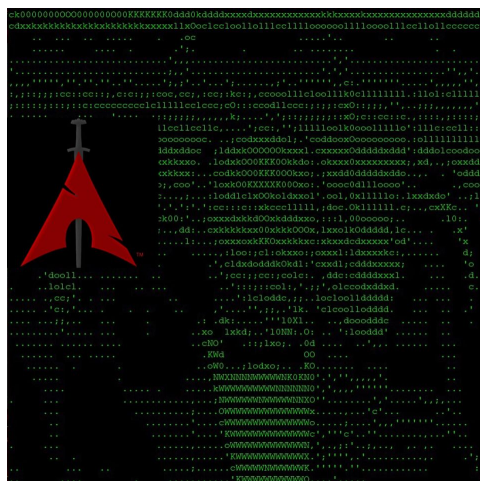


Figure 3: Profile Picture on Office360

Question for James Peng from Constance Hendrix: Hi again, James. I saw you served in the Coast Guard as a Cyber Operator – very exciting! Where have you been stationed?

Answer from James Peng to Constance Hendrix: I was not cyber operator but cyber security specialist for intelligence and counterintelligence against China, stationed in Taipei—a place near to Tokyo—very far away from here Colorado Springs. Thank you for emailing me previously; because of that, I also found your Linkedin and already sent you a friend request. Please accept it when you have time. Your career background is also very exciting to me, too: My uncle worked at US Air Force Intelligence and Personnel for his whole career until retirement—from US-Taiwan Command, German 7455th Tactical Intelligence Wing, Virginia, and NORAD—, like you. And your current employer BAH happens to be my dream company/ firm has my dream position. I hope to join your company as a vulnerability security engineer after my PhD. Should be very fun!

Question for James Peng from Lori Babyak: Hi James. Thanks for fixing my problems in Babyak.txt - I appreciate it! You've done some interesting work - I hope you can explain it to me sometime.

Answer from James Peng to Lori Babyak: Hi, sure thing, anytime and anything. Feel free to ask me on any channel. Thank you for asking me question. By the way your background is also very very cool; not gonna lie. I feel all my classmates are extraordinary, wow!

Question from Maximus to James Bond: Hi James, You have broad and diverse research interests. These are all great topics; but can I ask you why you decided to focus more on SIGINT and APTs for your research among all these topics you studied?

3 Section 1

My name is Lori Babyak. I am a first year Computer Science PhD student at the University of Colorado, Colorado Springs. I hold a Bachelor's Degree in Computer Science from UT Austin and a Master's degree, also in Computer Science, from Texas State University. My goals for this course - CS 6000 Computer Science Research Methods- are to learn to research, read, and eventually produce research papers on subjects of interest in Computer Science. Additionally, I am looking forward to getting to know other students in the class and work collaboratively towards goals. Something personal about myself is that I have three grown children, two of whom live in the Denver area. Also, I took an extended vacation with a couple of friends in August. We visited Colorado Springs, Wyoming and South Dakota. In South Dakota, we visited Mt. Rushmore, the Crazy Horse Sculpture, and Custer State Park - where we saw free-roaming bison in their natural environment. I am happy and excited to be part of the UCCS community, and my hope is to make significant contributions to the field.



Figure 4: A photo of Lori Babyak in front of Crazy Horse sculpture, outside Custer, SD, August 2020

Question to Lori Babyak from Constance Hendrix: I traveled to Wyoming and South Dakota in July. Did you have the chance to see Devils Tower?

Answer to Question from Constance Hendrix: We drove through Wyoming and stopped in Torrington. We only had a couple of days in SD, so we visited Mt. Rushmore, the Crazy Horse Sculpture and Custer State Park. I don't think we saw Devil's Tower. There's so much to see there!

Question from Jackie Hi Lori, thanks for sharing. I went to those places twice. The first time was in 2013, and the second time was in 2018. To be

honest, I did not see much progress on the Crazy Horse. My questions would be: since you are in Colorado Springs, are you going to snow ski? If you already did, how much you enjoy the mountain views at the top? the cog train is a fun ride, too.

Answer to Jackie from Lori Babyak: Hi Jackie, I guess I never mentioned that I actually live in Austin, Texas and am doing everything remote this semester! As far as skiing, I have not skied in CO Springs. I have skied Keystone, Breckenridge, Copper Mountain, Vail and Park City, Utah. I am not an expert by any means, and I mostly enjoy the outdoors on the trips. I took the train to the top of Pike's Peak, and the views are amazing (but, it's very cold up there). I think my favorite mountain top view was in SW Colorado, in the four-corners area, where I got a view of 4 states at once - maybe it was in Mesa Verde? Anyway, I really enjoy travelling and CO!

4 Something About Me

I am a first year PhD student in the UCCS. I am a photographer in my leisure time. I started this hobby from 2012. Throughout the past few years, I have helped friends recording the moments for their wedding, graduation parties, newborn baby, housewarming party, Halloween party, etc. When I travel, I enjoy capturing the beautiful nature. Beyond this, I like to disassemble and reassemble things then make improvements that fit my needs. If the product does not exist, I create my own. I sometimes play games with friends; this is a way of getting out of the busy life and relaxing and rebounding with friends. Snow ski and water ski are the two sports I enjoy. One is for winter and the other for summer. Here is a picture of me taken by myself.



Figure 5: Portrait of Kelei Zhang

Question from Jordan: When I first read this, I missed the bit about you being a photographer. I was confused because it seemed like grad school was a hobby from 2012! :) What is the coolest picture you have taken? Answer to Jordan: Hi Jordan, thanks for asking the question. I think one of the coolest pictures I had taken was the Big Boy Steam Train. 2019 was the 150th anniversary of Big Boy on the railway. and it was snowing on the day I took the picture. With the team engine and the snowy day, it was quite a beautiful and unforgettable scene.

Question for Zhang from James Peng: Hi, Zhang, that's awesome to obtain an ability of photography. I'd like to know how you guys capture or design the "composition" of certain moment? For example, in like 3 seconds, you need to decide what moment and how much and what things should be in your frame. This is amazing. How do you guys improve your decision making on the matter? Answer to James: Hi James, this is a very good question. I think the most important thing to take a good picture is to learn your camera and master the basic operation. Photography is split into different fields: portraiture, landscape, event, studio, action, etc. I think your question is more about event and action/sports photography where the person has to capture the subject very quickly and also compose perfectly. Well, that almost never happens. For these situations, either the photographer take a series of pictures to capture then select the best one, or they pre compose and wait for the moment. Sometimes, they sit still hours after hours, just like snipers. When they have a clear image, they usually crop to make a better composition.



Figure 6: Jordan Scott

5 CS6000 Journal - Jordan Scott

Contact Info: jscott21@uccs.edu
<https://www.linkedin.com/in/jordan-cancer-scott/>
<https://github.com/jordanmscott/uccs>

About Me I am just starting my PhD in Security program. My goal for this course is to get into a research frame of mind, learn the modern tricks and tips, and help refine my dissertation topic.

I am really interested in learning more about zotero and latex. I gained some experience with zotero last year, but previously I've only been aware of manual tracking and editing. It's nice to know that technology has evolved quite a bit with research and data management.

I have done stand-up comedy twice. My set was mostly cybersecurity related and I received a number of laughs. I'm not sure if my comedy career will continue, but my career will definitely be full of comedy.

Questions Question and Answers

Question 1 - Hi Jordan, I am just beginning my PhD program this year also! I am learning a lot, trying to wrap my head around many things. Dr. Kalita is my faculty advisor and I am studying AI. I don't have a definite plan of study yet. I'm learning so many things from this class about research. Another learning curve. I don't know about you, but I am spending endless hours figuring out LaTeX and github. I'll get there, though. What are your impressions so far?

Answer 1 - I like how the research methodologies have used software best practices to advance. The learning curve definitely exists though. I think this class has done a great job in getting us on the same page and moving towards using the tools properly. I suspect it will be a huge help later down the line when we are in a hundred page document with hundreds of references.

Question 2 - Question for Jordan Scott from James Peng: Hi, Jordan, I

would like to ask you what is the most challenging experience/ things when you are in comedy industry? I always feel you guys are awesome, like "positive/ joy-sharing version of lawyers", very good at public speaking, rhetoric, and know very well with the "jury".

Answer 2 - Comedy is some awkward balance of saying what is on your mind, taking risk regardless of opinions, timing, and getting people into a mood. I think it probably has some of the same science behind it as music. Instead of beats per minute, its laughs per joke. My biggest challenge is memory though. I have a hard time remembering a script so I do more reading than natural delivery like the pros. I can talk and just keep going without a script, but the timing and order of things matter enough to where scripts have advantages. I think that's something I will just have to keep working on.

Merge Conflict Notes: Not having access to the project seemed frustrating and took a bit to even figure out that was the problem. For my setup, I chose to use TeXstudio on a virtual box. The git clone part was easy. Getting the Assignment3 file to build was not. There were dependencies I needed to download/install into TeXstudio which was a challenge in itself, all related to the csvsimple function. Eventually got all that working. Then trying to figure out git itself... Got the commit part, the pull, the merge (had to install and configure a compare tool), and then the push. It's all working now and I definitely have a better understanding of git. The branches and stuff will get more interesting too. Anyways, I think I'm ready to start developing reports using this IDE/Git setup instead of manually transferring from overleaf.

Question from Maximus to Jordan: Hi Jordan, glad you can make jokes from a topic such as cybersecurity. One of the surprising things I discovered in these discussions, as I am reading through the comments, is we have people with really different backgrounds and interests in this field and they are mostly competent. How do you think your passion for comedy would contribute to research in a logical field like cybersecurity?



6 Maria Psarakis

I am in the master's program studying cybersecurity. I am currently in the process of a career transition; my previous job was as a Russian and French linguist. I am planning on graduating in May 2021, with the main goal of combining the skills I am getting now in this program in cybersecurity with the foreign languages I know.

In terms of research, I spent the summer doing the first three credits of my master's thesis, and I am looking to complete and defend it during this Fall semester. I am investigating the vulnerabilities of internet voting, comparing different implementations, and testing the code in one open-source implementation to see if it is in fact secure in terms of the security properties it claims to ensure.

To tell you a bit more about my background, I've lived in many different countries, mainly in Western Europe. I've had the opportunity to travel to Africa and Central Asia. I was also a "human test subject" at NASA, and tested exercise equipment that is now on the International Space Station.

Outside of my career pursuits, I am passionate about animal rescue, and have been a volunteer at the Humane Society for nearly five years.

Question (from Cassandra Putman): You went from learning different human languages to learning different programming languages. Which one do you find more challenging to learn? **Answer to Cassandra Putman from Maria Psarakis:** Thanks for your question! I think I would have to say programming languages, mainly because I haven't had as much practice. That may be the key to both, is just lots of practice.

Question from Duane Michael: Hi Maria, it sounds like you've had a

fascinating life! It sounds like what you have in mind for a career transition is very interesting. I find cyber threat intelligence particularly interesting, which is what I thought of when I read the first line of your bio. Do you plan on pursuing that type of work? If not, what type of security work are you interested in and how will you use your foreign language skillset? **Answer to Duane Michael:** I am definitely *hoping* to use my foreign languages in my work, but am not sure if I can find that niche. I'm also interested in digital forensics.



7 Introduction

7.1 My Background

My name is Cassandra Putman. My background has focused in mathematics and systems engineering. Recently, I have decided to branch out into computer science and obtain a Master of Engineering in Cyber Security with an intent of focusing on hardware security. I have a 17 year career in Department of Defense space systems including launch vehicles, space vehicles and most recently the ground systems that support the space vehicles. System security, including software, hardware and physical security are of utmost importance to all the space programs I have worked, as they are often national security asset systems.

7.2 My Research Interests and Course Goals

I intend to focus my research in supply chain security with a focus on hardware security. While I'm fairly new to the computer science field and only recently started learning about blockchain, I do see a great utility and applicability being possible in applying blockchain technology to improve hardware supply chain security. It appears, in my initial research, that applying blockchain technology to an IT supply chain, especially a supply chain that is as controlled as those that exist in government contracting, is both feasible and capable of providing great security benefits to the system, the user, and ultimately the security of the nation. I hope to narrow my research topic during this course and develop a focused and novel idea in the area of hardware supply chain security.

7.3 My Personal Interests

While I enjoy math and often read math related books, I also love to volunteer with a shar pei rescue. I volunteer by performing temperament evaluations, transporting and fostering dogs and performing home checks for potential fosters and adopters. I have fostered 100+ dogs in the 12 years I have been volunteering with the shar pei rescue. Beyond dog rescue, I also enjoy reading, hiking and doing crafts such as sewing and knitting. My love for travel has taken me to over 20 countries in the world, and I have plans to hit many more. Figure 1 is a picture of me.

Question from Maria Psarakis to Cassandra Putman: I'm so impressed with your DoD background, did it have you living in lots of different places in the world? I'm equally impressed with everyone who quilts, sews, knits...how did you get started knitting?

Answer to Maria: When I first joined the Air Force I had big dreams of seeing the country and going overseas, travelling the world. Instead, I lived in a cubicle in Los Angeles Air Force Base. I was lucky that I had amazing jobs, because LA was not what I had in mind. But satellites and especially launch vehicle work made it worth it! Since I didn't get to do any serious travel with the military, I made a goal to go somewhere international at least once each year. Until this year (thanks to COVID), I've kept that goal and I've been to 20 countries (Republic of Georgia on the top of that list if you ever get a chance!)

Maria: When I first joined the Air Force I had big dreams of seeing the country and going overseas, travelling the world. Instead, I lived in a cubicle in Los Angeles Air Force Base. I was lucky that I had amazing jobs, because LA was not what I had in mind. But satellites and especially launch vehicle work made it worth it! Since I didn't get to do any serious travel with the military, I made a goal to go somewhere international at least once each year. Until this year (thanks to COVID), I've kept that goal and I've been to 20 countries (Republic of Georgia on the top of that list if you ever get a chance!) As far as knitting (and sewing) go, I got started in high school. My best friend's grandmother taught her and she taught me. I still have the first blanket I knitted, in the heat of summer between my junior and senior year of high school. Imagine being that cool!

Question from IJ Olawale: Hello Cassandra, it is amazing and awesome how advances in technology is helping to resolve some of the challenges industries face. Talking about distributed ledger technologies a.k.a blockchain, it has caught the industries attention as it has the potential to increase the traceability and trustworthiness of information along the chain. However, when it comes to the application of blockchain to government systems, I am a bit skeptical. Do you think that the public sector will readily accept and adopt this technology given that there is not much governance, regulatory or legal frameworks to support the adoption of blockchain-based technology for government systems? Thank you for your post.

Answer to IJ: IJ, I look at the problem the other way around... the gov-

ernment is always about 10 years behind in adopting anything remotely cutting edge. I assume the government will be the slow ones to adopt blockchain and they will only do so after industry uses it prevelantly enough that they are almost forced to adopt it. But I may be jaded after working DoD acquistions for so long. One thing of interest is ISO is in the process of developing blockchain standards now. They have 3 (if my memory serves correctly) already out and available to read and others documents in the queue. I know terminology definitions, blockchain uses, and smart contracts were amongst the topics already covered in the released documents (generalizing the topics, as I haven't looked at them in detail yet). Other supply chains (food/agricultural, automotive, pharmaceutical, etc) have started to utliize blockchain in their supply chains. It is really a matter of figuring out what problems it can solve and which it can't. Great question!



7.4 My Background and Goals for CS 6000

My names are Ijeoma Olawale and I go by IJ. I am in my second semester and third class as a PhD student in Security in the College of Engineering and Applied Sciences. I have had an exciting career for over 12 years in GRC, IT Risk management, IT Security Audit and Compliance working in the financial industry, government and consulting services. For CS 6000 class, I hope to learn about the research methods and publishing tools in Computer Science and how to effectively read, write and present research papers. With this knowledge gained, I hope to be able to develop my thesis proposal and write an acceptable thesis and research papers.

7.5 My Research Interests

My research interest is in the security of IoT and wearables; understanding the threats and attack surfaces that connected things like cars and healthcare gadgets face. As a security risk professional, I am concerned about the security and privacy issues that are prevalent with connected devices. These lack of security and privacy principles presents the potential for data integrity abuse, access control, authentication, authorization and non-repudiation issues. I hope that with the knowledge gained from CS 6000 I would be able to write a paper that can significantly contribute to the body of knowledge.

7.6 My Personal Interests

To spice up my life, I love taking road trips, going to the movies and attending live Christian concerts. I also love to volunteer because I believe that it is my little way of giving back and a chance to 'pay it forward'. I volunteer as a Sunday school teacher at Crossroads Community Church, Parker CO and as a support crew with Winter Shelter Networks, Douglas county. I have vol-

unteered as a DBA for Colorado Association of Black Professional Engineers and Scientists (CABPES) and I am exploring the opportunities to mentor and encourage middle and high school girls to take on careers in computer science and information security.

Question from Abiola Ogundeko Have you been able to identify novel problem areas in your area of research interest that would be impactful to research community? I am more than willing to work with you once you have a problem area that you think is worthy of contribution.

Answer to Abiola Ogundeko: Novel problems!!! hahahaha I am still taking baby steps and learning how to read the research papers and do survey on the papers related to my research interests. So far, I am trying to identify gaps in the existing technologies and tools for special needs people and trying to figure out if there are potential areas for me to research on. As for novel...I will let the reviewers that review my papers to decide... Thanks Abiola.

Question from Maria Psarakis: Where do you like to take road trips to? Have you taken any recently? (Answer to Maria Psarakis: For leisure trips within the US, I love to drive rather than fly. For Christmas 2019 I drove to California with my children, the scenic views are incredible and awesome! Stopped over at Las Vegas to break the trip. This July, drove to Houston. There wasn't much to see on that route, but still we loved the fact that we could leave home, talking and singing loudly and just taking in the wonders of nature! We are planning on doing the the Grand Canyon or Hawaii for Summer next year, God willing.

8 Simeon Wuthier

8.1 Goals for the Course

Hello, I am Simeon. I enrolled in CS 6000 with the intention to improve my research habits and make them better suit my degree. I hope to learn more about how to use \LaTeX and other research tools, so that I can put my work into words and create something publishable. Figure 7 is a picture of me.



Figure 7: An image of me.

I am working on my PhD in Cybersecurity with Dr. Chang, and have been working with him since my undergrad years, which included researching and applying my knowledge to his research projects. Throughout my time working with him, I have built a few big cryptocurrency simulations and got my feet into the water of the official Ethereum and Bitcoin source code.

[11pt]article palatino, url, hyperref, cite, setspace, amssymb, amsfonts, amsmath, graphicx, enumerate, float

CS6000 - Computer Science Research - Git Assignment

By Duane Michael
September 21, 2020



Figure 8: 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 textbooks, 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 research 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.