Saket Upadhyay's

Statement of Purpose

8 Dec 2021

Problem Statement

With the exponential rise in computation power in past decades, the world has witnessed the most advanced and intricate cyber-attacks. As powerful computational machines become more accessible to the public, we need to devise robust and effective security standards, protocols, and strategies to defend future generation computer systems. These topics will remain hotspots of research and discussion even after my doctoral degree and we can continue to expand our work further.

This is the problem that I am intended to work on and hopefully will be able to solve to some extent. My primary research interest is in adaptive and resilient cyber/network security. With rapid developments in machine learning and its better-than-ever integration with cybersecurity, concepts like "self-healing", "adaptive networks" and "dynamic deployment" are catching more eyes than ever. I've been trying to create a stable ground for this topic by integrating a nature-inspired approach with cybersecurity in a new field called Nature Inspired Cyber Security (NICS) for the past 3 years at my current academic institution with my professor Dr. Shishir K. Shandilya by collaborating with well-established professors and professionals from around the world [Prof. Nagar (Liverpool Hope University-UK), Prof. David (Soongsil University-South Korea), and Dr. Neal Wagner (Complex Systems Scientist, STResearh) to name a few].

My Research Experience

My exposure to research started when my supervisor asked me to experiment with the existing network testbed to implement and compare certain security algorithms. Later, he encouraged me to design my own testbed, which I created in Network Simulator NS-2 to facilitate the implementation and verification of nature-inspired cyber security algorithms. This work resulted in a paper titled "AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis" which is published in "Future Generation Computer Systems" which has an impact factor of 7.187. One of the most interesting challenges in this work was to find the most suitable network architecture which can cover all basic topologies used in enterprise applications and to create a modular structure so that we can easily debug or enhance the quality of its individual components and integrate future prototypes of NICS algorithms.

After creating a working prototype of the testbed, I was curious to test and know its capabilities with the actual NICS strategies, so I have attempted to work on early intrusion detection that can assist the existing intrusion detection systems. Inspired by the fireflies for feature selection and optimization, we implemented firefly's characteristics at the network level to detect suspicious nodes. The major challenge in this research was the implementation and redesign of the existing firefly algorithm and translating their behavior to computer networks application. Another hurdle was creating a base structure that should easily integrate with current IDS solutions and can be used as an add-on in the existing network setup. While working with Indian and South Korean Professors on this work, we have got an Australian Patent granted.

My Professor invited me to write a chapter for an edited book titled "Advances in Nature-Inspired Cyber Security and Resilience" which will be published by Springer. I wrote a chapter titled "Nature-inspired malware & anomaly detection in android-based systems" in which I have discussed the developments in NICS strategies, its history and existing malware detection methods for android devices, and how we can ultimately combine these two domains to create more robust malware detection strategies in Android-based devices to counter more sophisticated attacks. After a thorough review, this chapter got final acceptance to be included in the book.

During my induction into the academic research and procedures, I've had the honor to be part of two patents, four copyrights, and three quality publications where I was one of the principal contributors in all the projects.

Co-Curricular Activities

I've been actively taking part in security conferences and trying to give back to the community and learn as much as possible. Started with IEEE Big-Data Conference 2019, LA, where we presented my very first research titled "PACE: Platform for Android malware Classification and threat Evaluation". After that, I took part in multiple conferences including DefCon 25 Safemode, DERPCON 2020, DevSecOps 2020, and PyCode Conference 2021. I've also given guest lectures in high schools in our state, teaching students about security and privacy in general.

The thing I like the most about security conferences is the diversity of professionals we get to meet there; this interaction always inspires me to try something new and helps me with my ongoing research in one way or another.

My vision for future research

Having experienced a little bit of both academic and enterprise research, I want to continue my research in academia and develop solutions beyond prototypes that I've been creating so far. I want to explore more about self-healing and adaptive defense systems and experiment with various scenarios to check their applicability at the enterprise level.

My prime purpose behind doing this Ph.D. is to explore deeper in the domain and ultimately, in coming years, I see myself as a well-established professor in academia and a good researcher, giving all the knowledge back to people and making the subject a little bit easier and less intimidating for the students.

At Texas A&M University, I found Dr. Nitesh Saxena's work is close to my vision. The work he and his students do in SPIES lab in the domain of "Mobile Systems and IoT Security" and "Privacy and Anonymity" can be seamlessly integrated with my idea of network security and resilience and I can see us working together in these domains.

Dr. Guofei Gu and his "SUCCESS" Lab's interest in "Intrusion detection, anomaly detection", "Internet malware/botnet/APT detection, defense and analysis" and "Network and system security" and their research on "CyberProbe", "Shadow Attacks" and "AutoProbe" aligns with my work and interest, and I can see myself working under their supervision for my final thesis.