SOP – Computer Science

Introduction:

The ***rapid*** discovery of a breach is key to minimizing the damage of a targeted attack.

Organizations today generate large amounts of data relating to security events, but waste a lot of time on analyzing false positives and misleading signals. Depending upon the environment, false positives can be numerous and difficult to verify, costing analysts a valuable time determining the significance of an event. Competitive advantage today, lies in making the best decision in as short a time as possible.

My projects and internships in cyber security analysis made me aware of such issues and discover my passion in the fields of Network Security, Data Analytics and Machine Learning. Therefore, I would like to return to school to pursue my Master's in Computer Science, to study how the fields of Big Data analysis can be integrated with Computer Security to address the emerging threats to privacy and security.

Academic Background:

In 2007, I developed an Obstacle Avoiding Robot that won the first prize in a competition for socially helpful projects. This was a prototype for an automated wheelchair that could be further developed for use of the visually challenged and physically handicapped. A perfect 100 in Computer Science (Java & Programming) in high school further cemented my desire to explore it as my major at _____ University. The courses in Algorithms, Computer Networks, Cryptography and Pattern Recognition were the ones that interested me the most in college. Graduating with a CGPA of 8.27, I achieved a Distinction.

At college, I joined FOSS (Free and Open Source-Software) club where I first began to delve into the fields of open source contribution and competitive coding. But it was another field that would keep me occupied for hours into the night; Ethical Hacking. As I explored Cryptography, Binary Exploitation and Reverse Engineering for taking part in various CTF (Capture The Flag) competitions, I learned about the various types of vulnerabilities that could be exposed in real world scenarios. This further helped me understand the required mindset and basic skills required to not only analyze these situations and detect an intrusion/anomaly but also to be prepared to tackle it.

This inspired my final year project, MDLAM (Malware Detection using Log Analysis and Machine Learning). Usually in Network Security using Log Analysis, the log data is manually analyzed by the Network Administrator to determine if the network has been compromised. I decided to improve upon this method by incorporating automated analysis of the Log data using an Unsupervised Machine Learning Algorithm (One Class SVM) that would help in classifying the malware processes, predicting

possible malware domains and reducing the false positive rate. The main objective was to assist the Network Security Administrator by reducing the time and complexity of such a process. My knowledge gained during my CCNA (Cisco Certified Network Associate) was very useful in understanding and analyzing the network architecture of the test site.

It was during this project that I picked up a strong interest in the field of Machine Learning, that motivated me to further take up the Machine Learning course by Professor Andrew Ng on Coursera and explore Data Analytics through MITx course, The Analytics Edge.

Industrial Experience:

During the Summer of 2014, I interned at Sequretek, a startup that specializes in offering IT Security solutions. As a Systems Engineering intern, I developed a web application including both front-end and back-end, for a client, using jQuery, SQL, HTML & CSS. This internship gave me an excellent insight into the workings and challenges faced by a startup as well as learning about the stages of real-life software development like requirement elicitation and analysis from clients.

My ability to learn new technologies and deliver quality software saw me getting an offer to continue as an Associate Consultant in the Information and Data Security division of Sequretek. This has given me the opportunity to work and learn more about practical security implementations at various client locations and learn firsthand about the various aspects of Network security like Security Operations Centre (SOC), Endpoint Security, Anti-Virus, VAPT (Vulnerability Assessment and Penetration Testing) and Data Loss Prevention (DLP) systems. I was also one of the only freshers to be involved in the implementation and deployment stages of a SOC (Security Operations Centre) as a L2 SOC analyst.

Extracurriculars:

I'm not only an extremely avid follower of sports, I also love analyzing the game tactics, especially in soccer. I'm fascinated by the use of Big Data in Sports, the science of sabermetrics and the growing importance of sports science in using analytics to comprehend player and statistical data, and how this can be translated into improving performances on the pitch. This interest also evolved into occasional forays into Sports journalism. I have, in the process, learned to articulate my thoughts better and developed a better understanding of the practical applications of data analytics.

Why Master's at University of _____?

While my job has been extremely rewarding and engaging, it is restrictive in scope. As I realize the increasing potential and importance of Big Data Security Analytics, I see the necessity of pursuing a Master's degree to learn in depth, through research, about how to design more robust and responsive security systems.

University of ____ with its excellent infrastructure and cutting-edge research in labs like Center for Computer Systems Security (CCSS) and DETER, would provide the most conducive learning environment. I am further excited about the ongoing projects in the Big Data Analysis group under Professor Viktor Prasanna and those in the field of ML and Data Mining in the Melady labs under Professor Yan Liu. I would like to take CSCI 530 Security Systems and CSCI 556 Introduction to Cryptography courses to help build a solid foundation to further my knowledge in these fields.

I hope the admissions committee would give me the opportunity to achieve my goals by accepting my application to ___.