Thesis Project Portfolio

The Utilization of Sandboxing to Prevent SQL Injection Cyber-Attacks

(Technical Report)

An Actor Network Based Examination of the Healthcare Cybersecurity Crisis

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Gabriel Edwards

Spring 2022

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Cybersecurity is a wildly complex issue that has evolved to become one of the most important of the 21st century. As computers and Internet of Things (IoT) devices have become more and more ubiquitous since the 1990's, cyber-attacks and information breaches have grown exponentially in both prevalence and severity. This is especially true for businesses and organizations, as many have adopted sprawling computer networks to manage mountains of data, creating lucrative targets for cyber-criminals. Between the ever growing diversity of attack methods, sophistication of attacks, and surface area for attacks, security officials at these organizations are increasingly unable to protect users' data. The following theses examine different means through which some organizations can bolster their cybersecurity and mitigate the risk of attack.

The technical thesis proposes a unique solution to one of the most common forms of cyber-attack, the SQL injection. It suggests applying the concept of sandboxing to detect SQL injection attacks. Specifically, the effect of a prospective SQL query is meant to be tested on a copy of a target database, which is then compared against the original to discover any malicious changes. In addition to proposing this idea, the thesis lays out an experiment with the goal of determining both the effectiveness and efficiency of this idea. The expected results of this testing point to a positive ability to detect injection attacks, but with potentially noticeable delays for the large data sets representative of real world databases.

The STS thesis examines one of the world's most currently vulnerable industries: healthcare. With thousands of facilities hacked and millions of patient records stolen globally each year, healthcare is facing a cyber-crisis that is seemingly unsolvable. The vast complexity of hospital data networks is widely cited as the primary reason for their vulnerability; as such, the Actor Network Theory is applied to untangle the web of humans and devices that make up these networks. ANT is

applied to examine the relationships between these actors, in search of vulnerabilities that arise from failings in these relationships; meaningful changes to the system are then offered to secure these vulnerabilities.

Both projects provided a valuable insight into the world of cyber-security. The technical thesis, while not providing any concrete results, offered a promising new direction for cyber-security relating to one specific topic. In doing so, it brings to light the idea that no topic is fully understood, and that finding new solutions is very valuable in the fight to secure cyberspace. To provide concrete results, the proposed experiment should be expanded to test larger datasets, so as to fully determine the efficiency of the proposed idea. The STS thesis provided very promising results, determining that the rise of telehealth and remote patient monitoring following the Covid-19 pandemic have dramatically changed the landscape of healthcare data-networks, shifting attackers focus outside of the hospital. Examinations of these new remote actors and their interactions with existing actors have revealed many potential sources of positive change, and given convincing evidence that the problem is, in fact, manageable.