Thesis Project Portfolio

BLUESPAWN Design and Architecture

(Technical Report)

The Unforeseen Cost of Offensive Cyber Capabilities

(STS Research Paper)

An Undergraduate Thesis

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

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

James McDowell

Spring, 2020

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

A gas shortage spanning the entire East Coast of the United States. Hospitals unable to operate. Power grids across Ukraine failing. Elections compromised. These examples, though there are many, many more, all serve to show the importance of ensuring computer are safe and secure. Computer systems are rapidly growing and integrating to every part of our lives. Nearly every industry has adopted computers in one way or another, and they are vital to the continued growth and success of these industries. Unfortunately, as computers become more vital to businesses, they become targets for bad actors, who leverage their importance and sensitivity to steal information, gain financial data, or pursue political motives. The field of cybersecurity is growing to combat this, but as it advances in understanding how to defend against attacks, so too do malicious actors in understanding how to get past these defenses. Constant vigilance and improvement is always needed to stay ahead of cyber attacks.

These improvements can take many forms: more secure software, better security tools, improved network defenses, and many more. This research focuses on the development of new and better security tools and how such development impacts the field of cybersecurity as a whole. Security tools can serve in both defensive and offensive capacities when used by benevolent actors; antivirus products identify and remove malware, threat emulation software allows benevolent actors to assess a network's defenses, some tools give insight to a current system's state, network scanning tools allow network engineers to understand the state of their network, and thousands of other tools allow people to do thousands of other things. This research will explore BLUESPAWN, one such tool, allowing a security analyst to scan a system for evidence of malicious activity. This research will also explore the impacts of offensive tool development and examine how bad actors can sometimes use these well-intentioned offensive tools for malicious purposes.