Usage of Windows Event Log Analysis to Improve Cyber Defense
(Technical Paper)

Looking Towards the Future: Autonomous Vehicles and Social Consequences
(STS Paper)

A **Thesis Prospectus Submitted to the**

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Geoffrey D. Hicks
Spring, 2020

Technical Project Team Members
Rajiv Sarvepalli
Jake Smith

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

I. Introduction

Am I secure? Should I click on that email? Do I need to invest in an antivirus protection plan? These are all questions that those who are looking to protect their technological devices from foreign threats will ask themselves, and for good reason. In recent years, as the computer has advanced, it has become easier and easier for those fluent in technology to find ways to manipulate it to their advantage. This occurs in the forms of various cyber-attacks such as man-in-the-middle, denial-of-service, SQL injections, DDOS, and Malvertising. But just as the methods of attacks grow, so do the methods of defense. One particular method of defense is performed by looking at the event logs on one’s windows computer. Event logs act as a method to record various changes and activities that are being performed across a device.

Event log monitoring has many uses such as profiling normal user activity, identifying and preventing attacks, and if necessary, performing post-breach forensics and remediation. Not only is it powerful, but it’s simple as well requiring little to no technical skill. The event viewer utility, which is used to view event logs, is preinstalled on every windows computer. All one needs to do is click on the app, and they can immediately gain access to the event logs. When looking to defend against malicious attacks, event log analyzation can be an invaluable tool to add to one’s arsenal of cyber defense utilities.

Cyber-attacks have a heavy impact on society. They are responsible for causing physical, digital, economic, psychological, reputational, and social damage (Tunggal, 2019). But are these the effects that technology itself has imposed upon us as an unchangeable consequence of its’ usage, or do we as individuals have a choice in how we can control its’ power?

This thesis seeks to demonstrate how one can detect cyber-attacks early on through the observation of event logs patterns within a windows domain. It also seeks to address how technology is exploited, its’ impact upon society, and whether or not society as a whole is responsible for the consequences of its’ usage. These topics are to be observed through the lens of STS theories such as technological determinism and social determinism. These theories will allow us to perform a thorough analysis of the impact that society and technology have on each other, as well as giving us room to think about ways to mend the problems caused by either side.

II. Technical Topic

During Spring and Summer of 2019, I was a windows team member for the DARPA-funded project called Cyber Hunting at Scale (CHASE). The objective of this project is to develop distributed algorithms that detect live zero-day attacks as early as possible. This is done through global analysis that leverages the power of big data, which is collected at multiple organizations (“Real-world attack campaigns”, n.d.). The idea is that an inter-organizational globally coordinated effort will expose attacks within a short time frame when the attacks are still largely invisible to any single organization. During my time with the project, I conducted research involving the testing of various cyber-attacks and cyber-attacks techniques on windows virtual machines set up within an ESXI hypervisor.

When engaging in cyber defense, one can think of it as something akin to fighting a war. You have two sides: red (attackers) and blue (defenders). The red team focuses on using every tool they have at their disposal to attack the base of the blue team in an attempt to cause damage or gain access to valuable information. In order to launch these attacks, they need to access various weapons from a malware supply depo such as viruses, worms, trojans, spyware, rabbits, droppers, etc…. In order to defend against this bombardment, the blue team will need to use instruments of their own to detect and circumvent the attacks of the red team before any real damage can be caused. They come together and strategize, exploring various methods of attack detection such as those that are signature-based, statistical anomaly-based, and stateful protocol analysis. As a member of CHASE, my position on the blue team.

Building off my research, my technical topic explores the avenue of using signature-based attack detection in the form of windows event logs analysis to detect security threats. When a computer is being attacked and a payload is being executed, there are certain changes that are made within the architecture of the computer. As these changes are made, event logs are generated by the windows domain. For example, if a large number of files are suddenly deleted, windows event 4663 could be logged. Or if one makes changes to the user rights assignments, then event logs 4704 and 4717 will be activated. While the generation of logs themselves by Windows is a normal activity, the *type* of logs that are produced can be a telltale warning sign of malicious activity. In order to examine this in more detail, my project explores this by:

I. Setting Up a Windows Domain

In order to analyze security threats, there must exist a safe and proper environment in which one can run them in. Through the usage of the hypervisor utility *ESXI,* this can be achieved. ESXI is a tool that allows one to set up a server where multiple virtual environments can be hosted, customized, and manipulated as one sees fit. Not only that, but in order to access these virtual environments one doesn't even have to be anywhere near the server itself. If configured properly, the virtual machines can be accessed from a simple web browser making testing much more efficient.

II. Gaining Access to Cyber Attacks

The next step in observing cyber-attacks is to run them within the environment. To do this, one method would be to create and launch them ourselves. However, this would be far too complicated of a procedure, not to mention time consuming and expensive. A simpler method would be to use an online tool that runs the attacks for us. For my project, the attack generation tool that is used is called *APT Simulator*. It is a windows batch script that "uses a set of tools and output files to make a system look as if it was compromised and making it think that it was being actually attacked" ("Customers tested our scanners", n.d.).

III. Running attacks and Recording data

Once the attacks are accessible and the appropriate windows environment is chosen, they must then be run within the domain to produce event log data. This data is gathered primarily from the event viewer application that comes pre-installed on every windows machine. Depending on the actions performed on the computer, the event viewer produces various logs which are categorized as Application, Security, and System. The application logs are "events logged by applications or programs" ("You can view event logs", n.d.). The Security logs contain "events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files or other objects" ("You can view event logs", n.d.). The system logs mainly contain "events logged by Windows system components" ("You can view event logs", n.d.), such as when there is a driver or system component failure when logging on. For the tools that are being run, the main logs that need to be analyzed will be the ones from System and Security.

IV. Investigating Information

The event log information related to every cyber-attack that is run during the testing phase will be collected and exported to an excel spreadsheet. There, the various information belonging to each log will be separated into different categories like event IDs, examples, and compatible operating systems. Various factors regarding these logs will be analyzed such as how often each log occurred during testing, their patterns of appearance, and how the type of log collected may relate to more malicious cyber-attacks.

III. STS Topic

Technology is a rapidly advancing phenomenon which has over the years deeply sown itself into the fabric of modern society. It’s put into practice almost every day through its implementation by various outlets such as medicine, entertainment, business, education, and more. However, just as we reap the benefits that technology has to offer it also has the ability to be exploited often to the detriment of others. This STS thesis seeks to explore the impact that the exploitation of technology has on society and whether we have the ability to prevent these exploitations or not.

To address these topics, I have chosen to use both the technological and social determinism theories. Technological determinism is the theory that “technology is an autonomous force that changes society” (Goguen, 2001). This theory makes the assumption that whatever the effect technology has on others is a necessary byproduct of the availability of the technology itself. Technological determinism suggests that society should accept that there will always be detriments that comes with the usage of the hardware/software that’s available to them, and that the best we can do is work around them instead of opting to prevent them completely. This theory pushes the idea that it is technology that controls us and our actions.

Social determinism, on the other hand, is a theory which asserts that “society is an autonomous force that changes technology” (Goguen, 2001). This theory implies that technology itself is a tool, and that we as society can determine how that tool is used whether it be with good or bad intentions. Social determinism suggests that just as technology can be used maliciously, we also have the ability to deny their usage as well. If we want our technology to be developed with flaws in mind, then we can do so. If we want to use our technology in an immoral way, then we can also do that. But if we want to use or design our technology to be used in such a way that it promotes ethical behavior instead of evil, then we also have the power to do that. Social determinism gives us choice.

There is a clear separation that can be made between these two theories, as each offers various ideas which falls on the opposite end of the other’s spectrum. However, this is not without a purpose. To find a solution to a problem, one must first understand the problem itself. By exploring the dichotomy between the theories, this thesis can help one better think about the effects that society and technology have on each other. An analysis will be conducted between the two, weighing their strengths and weaknesses. Regarding society, this analysis will explore concepts such as the influence that cultural norms, politics, and economic pressure have on the technology that we create. On the technological side of things, concepts regarding weaponization, job automation, and economic impact will be looked into as well.

The overall goal of this thesis is to be provide an understanding to the underlying question: Does society shape technology or does technology shape society? Employing the use of technological and social determinisms, various aspects of the populace and technology as a whole will be explored and analyzed in order to better address this.

IV. Bibliography

Customers tested our scanners. (n.d.). APT Simulator. Retrieved December 1, 2019 from https://github.com/NextronSystems/APTSimulator

Goguen, J. (2001, January 16). Technological Determinism. Retrieved December 1, 2019 from https://cseweb.ucsd.edu/~goguen/courses/275f00/s2.html

Real-world attack campaigns. (n.d.). P-CORE: Privacy Enhanced Coordinated Enterprise Defense via Temporal and Topological Representation Learning. Retrieved December 1, 2019 from https://cyberinnovation.virginia.edu/p-core

Tunggal, A. (2019, November 1). What is a Cyber Attack. Retrieved December 1, 2019 from https://www.upguard.com/blog/cyber-attack

You can view event logs. (n.d.). Windows Event Logs – Event Log FAQ. Retrieved December 1, 2019 from https://eventlogxp.com/essentials/windowseventlog.html