**IT Solutions: Discovery Session Exporter**
(Technical Topic)

**How to Establish Better Standards within Cybersecurity Practices**
(STS Topic)

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Martin Salzberg

October 27, 2022

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.

ADVISORS

MC Forelle, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

# Prospectus

## Introduction

In recent history, there has been a surge of cyber-attacks on governments, businesses, and people. Because of this trend, these attacks have become increasingly difficult to combat while they only grow in complexity and magnitude, leading to losses in money, sensitive information, and personal information. Unfortunately, changes in the quality of cyber security have only been established in response to these attacks rather than in preparation for them. As a result of the pattern of various companies and institutions waiting for an attack to happen before considering the integrity of their security, many of them have fallen victim to attacks for which they otherwise could have properly been equipped.

There have been attacks on well-established companies because they hadn't properly prepared for an attack with the expected standard of security. Some prominent examples of such are the Sony shutdown hack of 2011, the Yahoo data breach in 2016, and the Microsoft hack in 2020 (Information is Beautiful, 2022). A more severe example is that of the SolarWinds attack in 2020 by Russian hackers that "successfully compromised about 100 companies and about a dozen government agencies", even including US Homeland Security (Temple-Raston, 2021). Given this context, it must be put into question of how security can be assembled in a more proactive manner than the current practice of reacting to an attack after the damage has already been done (Bedi, Boyal, Kumar, & Ritika, 2021).

ScienceLogic, an IT management software development company, has had its number of employees skyrocket within the past few years, now numbering nearly 700. Subsequently, its number of back-end software developers has also increased. When the company was in its earlier stages with fewer employees, it was a much smaller issue when they had to manually replicate data from one of their SL1 IT management systems to another. One such example would often

occur during the transfer of discovery sessions, which are records of a device's connection to a SL1 system. This process would take around 20 to 30 minutes per discovery session after taking the manual filling of fields, of which there were many, into account as well as making sure there were not any typos while doing so.

With the massive increase of employment, the time it took to perform this task increased in tandem because of the larger number of employees that had to do it, accumulating to many hours lost per week to a tedious task which that could have been better spent on something else. As a solution, I was tasked with developing an automated tool that would export discovery sessions from system to system, which both reduces the time spent down to a matter of seconds and minimizes the chance of human error occurring from a manual replication.

While developing the tool, a bug was discovered where an encrypted credential field on the source SL1 would appear in plain text after it had been transferred to the target SL1, revealing a security vulnerability of the tool. It was this occurrence that prompted the research for the STS project in establishing better cybersecurity standards.

**Technical Topic**

During the summer between my 3rd year and 4th year at UVA, I had the opportunity to participate in an internship program for ScienceLogic, an IT management software development company. Their main product is the SL1, which is a piece of software that serves as a system to assist IT professionals to perform and organize their tasks more easily, and is equipped with a large variety of tools and interfaces to do so.

One such capability of the software is its ability to automatically track discoveries, which are the connections between all hardware devices and software applications to an SL1's network.

Moreover, a discovery session is an individual record of an item's discovery, which requires an extensive list of fields that need to be filled, and was the focus of my assigned project for the duration of the internship.

My assignment was to create a tool that could export a discovery session from one SL1 instance to another. As mentioned in the introduction, a massive increase in ScienceLogic employees led to an increase in time spent by back-end developers replicating discovery sessions by hand, which was less of an issue when the company was smaller. In order to save many hours per week that were spent on a tedious task, my tool was intended to perform the operation in a matter of seconds via automation, which is a large improvement over the 20 to 30 minutes that was usually spent on each discovery session as described by my manager. In addition, by automating the process, any chance of human error was mitigated, which was also a concern for the back-end employees. I wrote a Python program using the Requests library to carry out this task.

The first step to export a discovery session is to import it to the local machine first. I made use of the source SL1's application programming interface (API), which allows for the ability to access all of that SL1's data with written code. To first import to the local machine, I used a "get" request, which takes data from the API and moves it to the local machine, to write a discovery session's information to a .json file written to the local machine. The advantage of using .json format over a .txt file is that the information would be created as a list instead of a long, continuous string of characters, which makes it easier to write code to parse the file for the necessary information for the following steps.

Next, I had to account for "dynamic" fields, which were fields within a discovery session that needed to be later exported along with and linked to the discovery session. I scanned the

.json file in the previous step for the session's dynamic fields, which were called credentials, organizations, and templates, then used the API's filter feature to search for those respective fields, which all have their own lists of data, and imported them as their own files to the local machine, also in .json format. The exhaustive list of fields is pictured below in the interface for discovery session creation.

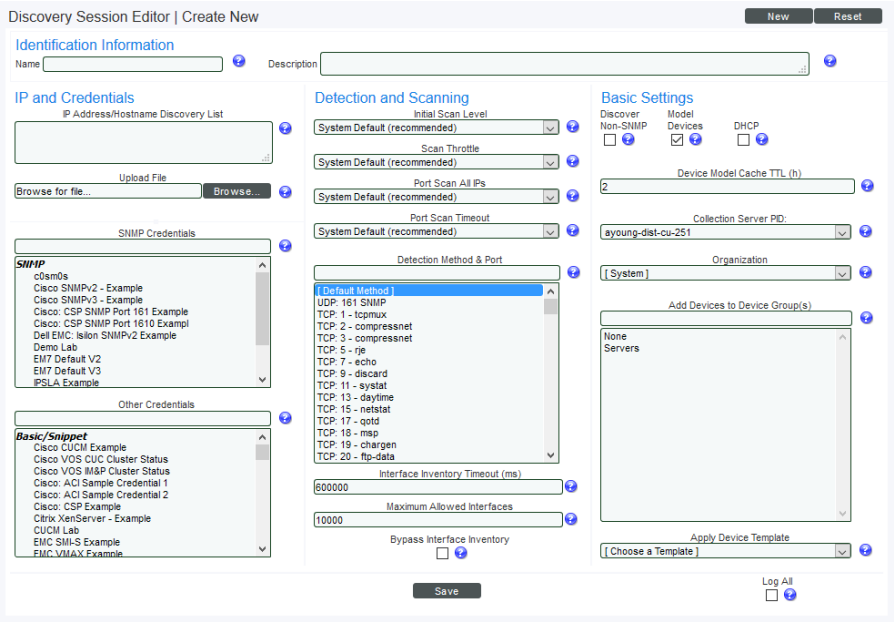


*Figure 1: Discovery Session Creation Interface* (Discovering Devices)

The next step was to then export the files that were newly imported on the local machine to the target SL1. This time, I made use of a "post" request, which moves data from the local machine to the target API, and posted the credentials, organization, and template information to the target SL1. Next, the discovery session's file was exported to the target SL1 by first performing a search on the target's API to find those exported dynamic fields, linking them to the discovery session, then finally publishing the discovery session on the target SL1.

Some types of credentials contained an encrypted field that served as a key to utilize those credentials. When viewed in the SL1's interface, a credential's information would appear hidden to any user that did not have access to the encrypted key. An issue that arose when

developing the tool was a bug that displayed the encrypted field in plain text after a credential had been exported to the target system, revealing the credential's contents to all users with access to the target SL1. The bug halted progress on the project until a new version of the SL1 was released a few days later, which correctly encrypted the credential keys during transfer, resolving the issue.

The project was developed with an agile format, with a three-person team composed of my assigned mentor, manager, and me, the project lead. Additionally, I had the opportunity to join and observe a scrum team of regular employees composed of software developers led by a scrum master, and participated in their daily scrum meetings and team bonding exercises.

The internship for ScienceLogic allowed me to apply the skills I had learned in my coursework, but also served as a learning experience with leading a team. Moreover, the project I was given allowed me to make a measurable difference for the company and its future.

**STS Topic**

As the world shifts to a more cyberspace-focused form of communication and business, cyber defense systems become increasingly necessary to protect sensitive data (Xingye, 2019). Some of the most common techniques and systems that are used to secure electronic data in its various formats are firewalls, encryption, and private keys (Cebula, Popeck, & Young, 2014; Woody, Alberts, & Wallen, 2022). The application of each of these items may change depending on whether the data is at rest, in transit, or in use, as described in a Carnegie Mellon University lecture by Rotem Guttman (2020).

The need for the implementation of said techniques and systems is a response to the existence of cyber-attacks, which are done to acquire money, steal information, gain power, and

more (Kagita, Thilakarathne, Gadekallu, Maddikunta, & Singh 2022). In other, victims and defenders are “at the mercy of cyber-attackers” (Vieane et al., 2016) whose methods of attack have shaped the way we developed and maintain our defense systems. As a result, most organizations and institutions have reached their own levels of standards regarding the level of technological advancement and integrity, many of which have kept up as technology continues to become increasingly sophisticated.

On the other hand, there are some organizations who haven’t evolved at the same rate, and have been victims of cyber-attacks that could have been avoided if they maintained security standards (Gong, 2019). One such instance is that of the 2019 data breach of Facebook, in which over 530 million of its users had their personal information exposed because of the company’s failure to cover an obvious vulnerability (Bowman, 2021). Because of the breach, it became public knowledge that Facebook had these users’ login information stored in a database in plain text, meaning that their usernames and passwords were stored exactly as they are, so the attackers then had access to hundreds of millions of accounts. With just a username and password, an attacker could view an account that contained sensitive information such as full names, email addresses, physical addresses, and telephone numbers, which can easily be utilized to further uncover more sensitive data like financial information and health information. Additionally, this also means that Facebook employees already had access to said data before the cyber-attack took place, which is a breach of privacy (Chapman, 2019). As a result, Facebook suffered a fine of $5 billion (Bowman, 2021) that could have been avoided if the company had implemented encryption into their storage system, which is a technique used to encode data during transfer and in storage, and is a practice that was established many years before the fact.

With even some of the most established companies revealing enormous vulnerabilities and suffering huge losses such as in the previous example, it must be brought into question why some organizations have failed to upkeep their cybersecurity standards, and how they can improve their standards to avoid detrimental situations (Al-Zahrani, 2022; Bhaiyat & Sithungu, 2022).

**Research question and methods**

To explore these questions, cases of historically significant cyber-attacks will be analyzed for their contexts and impacts, and an extensive review of literature on related research topics. Additionally, cybersecurity professors and experts at the University of Virginia will be interviewed to gather information about the technical side of these attacks because some have practical experience working in the field, and often cover the topic of historical cyber-attacks in their courses. I will utilize the STS framework of infrastructure as described by Star in *The Ethnography of Infrastructure*, in which organizations, cyber-attacks, and cyber defense techniques can each be analyzed as their own infrastructure.

Each of the mentioned parties have stark differences in scale in terms of the number of personnel involved, but the impact each one has levels out their significance within the context of cybersecurity. The varying scalability of organizations, cyber-attacks, and cyber defenses motivates the choice to interpret each one as its own infrastructure for ease of analysis and comparison because all actors are considered as infrastructures regardless of their components, functions, and purposes.

## Conclusion

The technical project will result in a measurable improvement on the productivity of ScienceLogic employees because it significantly reduces the amount of time spent on replicating discovery sessions between SL1 systems and minimizes the possibility of human error while doing so. With this tool, a previously tedious and mundane task can now be streamlined and optimized with automation.

The STS portion will bring light to an issue that many institutions and organizations have ignored to a fault, and have experienced losses as a consequence. By studying this issue, the reasoning behind their reluctance to evolve technologically can be revealed, and by doing so, a solution may become apparent to protect against cyber-attacks that can have serious negative impacts on institutions, businesses, individuals, and governments.

## Bibliography

Abdalla M., Jarrah M., Abu-Khadrah A. & bin Arshad, Y. (2021). Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia. *International Journal of Advanced Computer Science and Applications (IJACSA), 12*(11), 804-810. http://dx.doi.org/10.14569/IJACSA.2021.0121191

Al-Zahrani, A. (2022). Assessing and Proposing Countermeasures for Cyber-Security Attacks. *International Journal of Advanced Computer Science and Applications, 13*, 885-895. http://dx.doi.org/10.14569/IJACSA.2022.01301102

Bedi, P., Boyal, S. B., Kumar, J., & Ritika (2021). Cyber Security Management Model for Critical Infrastructure and Improving the Security Level on Transferring Digital Data. *Innovations in Bio-Inspired Computing and Applications, 1372*, 525-534. https://doi.org/10.1007/978-3-030-73603-3_49

Bhaiyat, H. Y., Sithungu, S. P. (2022). Cyberwarfare and its Effects on Critical Infrastructure. *Proceedings of the International Conference on Information Warfare and Security (ICCWS), 2022*, 536-543. https://doi.org/10.34190/iccws.17.1.68

Bkakria. A., Yaich, R., & Arabi, W. (2022). Secure and Robust Cyber Security Threat Information Sharing. *International Symposium on Foundations and Practice of Security (FPS) 2021*, 3-18. doi: 10.1007/978-3-031-08147-7_1

Bowman, E. (2021). After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users. *NPR*. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). Taxonomy of Operational Cyber Security Risk Version 2. *National Technical Reports Library, U.S. Department of Commerce*. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA609863.xhtml

Chapman, G. (2019). Facebook admits storing passwords in plain text (Update). *Phys.org*. https://phys.org/news/2019-03-facebook-passwords-plain-text.html

Discovering Devices. *ScienceLogic API Documentation*. https://docs.sciencelogic.com/latest/Content/Web_Monitoring_Tools/Discovery_and_Credentials/discovery_managing.htm

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences, 11* (10), 4580, pp. 30. https://doi.org/10.3390/app11104580

Gong, N. (2019). Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study. *Systems Engineering Technical Center, The MITRE Corporation*. https://doi.org/10.1007/978-3-030-01177-2_49

Guttman, R. (2020). *How to Secure Electronic Data and Communications* [Powerpoint Slides]. *Carnegie Mellon University*. Retrieved from https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1110438.xhtml

Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2021). A Review on Cyber Crimes on the Internet of Things. *Signals and Communication Technology*, 83-98. doi: 10.1007/978-981-16-6186-0_4

Morales, J. A. (2018). Current Malware Trends. *Carnegie Mellon University*. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1087017.xhtml

Plakosh, D. (2015). Increasing Adoption of Secure Coding. *Carnegie Mellon University*. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1145865.xhtml

Star, S. L. (1999). The Ethnography of Infrastructure. *The American Behavioral Scientist, 43*, 377-391. doi: 10.1177/00027649921955326

Temple-Raston, D. (2021). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. *NPR*. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., Wickens, C. (2016). Addressing Human Factor Gaps in Cyber Defense. *Colorado State University, Fort Collins*. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1021939.xhtml

Woody, C., Alberts, C., Wallen, C. (2022). Cyber Terminology Discussion. *Carnegie Mellon University*. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1168362.xhtml

Xingye, L. (2019). The big data impact and application study on the like ecosystem construction of open internet of things. *Cluster Computing, 22*, 3563-3572. doi: 10.1007/s10586-018-2206-z