Thesis Project Portfolio

Historical Archived IP List: Leveraging AWS to Persist Slack Security Data

(Technical Report)

Analyzing the Effectiveness of Gamification in Cybersecurity Trainings for Organizations

(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

Jason Yu

Spring, 2023

Department of Computer Science

Table of Contents

Executive Summary

To defend against cyberattacks, companies must consider both the technical dimensions and social dimensions of cybersecurity. For example, companies must harness cybersecurity tools (technical aspect) as well as train their employees to implement proper security practices (social aspect). The technical report of this portfolio relates to the technical aspects of cybersecurity by detailing Historical Archived IP List (HAIL), a project completed for the Slack product security tooling team. HAIL is a software tool that keeps a historical record of facts and findings related to Slack's Amazon Web Services (AWS) infrastructure, providing valuable insight into Slack's attack surface and security posture. This technical portion details the relevant security considerations, the implementation process, and the final outcomes. The STS research paper focuses on the human aspect of cybersecurity, namely cybersecurity trainings for employees to mitigate poor security practices and social engineering attacks. Gamified approaches to cybersecurity training are increasingly popular, but the effectiveness of such methods remains an open question. By examining academic literature and applying the Social Construction of Technology (SCOT) framework, the STS research portion delivers findings that help shed light on the effectiveness of gamified approaches in order to ultimately improve the future of cybersecurity trainings. Taken together, the technical report and the STS research paper highlight two complementary approaches to cybersecurity.

Technical Report. The technical report centers around the implementation of the Historical Archived IP List (HAIL) during my summer internship at Slack. The Slack security team uses a tool called RAINS (Rapid Analysis, Internal Network Scan) to provide visibility into Slack's AWS infrastructure in order to alert engineers about unauthenticated services and defend against subdomain takeover attacks. However, RAINS does not keep an historical log of facts and findings, making it difficult to determine the cause of a potential security incident. To solve

this problem, HAIL stores results from RAINS, and it consists of a database to store RAINS findings and a backend API, allowing users to query past results. I leveraged AWS Relational Database Service (RDS) for the data layer, created the backend service using Flask, and used AWS Lambda and Simple Storage Service (S3) in conjunction with the Risk and Compliance team's Security Data Warehouse project, enabling users to easily view RAINS results. I also modified the RAINS codebase (written in Go) to call the Flask backend and pass the findings to RDS. By the end of the internship, I successfully deployed HAIL to a production environment and configured metrics and dashboards using Prometheus and Grafana. One area for future improvement of the project is configuring default querying options within Security Data Warehouse, simplifying the process of extracting insights from historical RAINS results.

STS Research Paper. Traditional cybersecurity trainings are notoriously boring and ineffective, yet organizations have historically relied on traditional security education and training to mitigate cyberattacks. Across the board, employees struggle to retain and apply what they learn in cybersecurity trainings to their everyday work lives. In an attempt to make cybersecurity education more engaging and effective, employers are increasingly turning to gamification methods. Gamification is the use of game mechanics and game thinking to engage users in solving problems and to motivate them by introducing elements of competition and reward. While gamification is increasingly popular among employers, the effectiveness of gamification is not well-documented. This STS paper applies the Social Construction of Technology framework to answer the question of how effective gamification is in cybersecurity training for organizations. To answer this question, this paper uses documentary research methods by compiling and analyzing research from a variety of scholarly articles ranging from articles detailing the current cybersecurity landscape to individual case studies of gamified

approaches to cybersecurity training. By pinpointing the strengths and weaknesses of each approach, this paper seeks to understand whether gamification is an effective approach to cybersecurity trainings. This paper carries implications for the fields of STS and cybersecurity since it analyzes the cybersecurity training landscape from an STS perspective, and the paper's findings help inform the design of future cybersecurity trainings.

Concluding Reflection. I completed the technical portion of this project during my summer internship at Slack. During this internship, I was required to complete various cybersecurity modules and attend virtual trainings. Through this experience, I came to appreciate how cybersecurity trainings and latent knowledge of proper security practices do not necessarily impact employee behavior, and this realization ultimately gave rise to the research question in the STS paper. Additionally, the internship experience allowed me to familiarize myself with the cybersecurity training landscape firsthand. Completing the technical project and the STS research portion in tandem gave me a deeper appreciation for the complexity of cybersecurity; effective cybersecurity involves both the creation of technical tools to defend against cyberattacks as well as properly motivating employees to implement safe security practices.