University of Texas Rio Grande Valley

Department of Informatics and Engineering Systems

Past Capstone Project Abstracts

Bachelor of Science in Cybersecurity

Fall 2024

Security Monitoring Systems

Armando García, Citlalli Torres, Luis Martínez, Vale Alvarez

Advisor: Dr. Jose Poveda

Abstract:

In today's dynamic digital environment, the increase of cyber threats demands strong security measures to protect vital assets and data. The foundation of the global economy, small and medium-sized enterprises (SMEs), are especially susceptible to these attacks because of their insufficient ability to protect sensitive and important data, financial limitations, and shortage of staff and cybersecurity knowledge. SIEM (Security Information and Event Management) systems have become essential instruments for keeping an eye on, identifying, and handling security events. Open-source SIEM systems have become more popular because of their affordability and accessibility for small and medium-sized businesses (SMEs), despite proprietary SIEM solutions having historically dominated the market. This capstone project offers a thorough analysis with an emphasis on open-source SIEM system evaluation. The project focuses on how well these open-source solutions can handle contemporary security issues and adhere to legal standards. Empirical testing is conducted in simulated enterprise-grade SME network environments to evaluate real-time data processing capabilities and resource efficiency. Through a thorough evaluation of the security and functionality of open-source SIEM systems, this study provides insightful information to cybersecurity professionals, businesses looking for affordable security solutions, and the larger academic community. The results clarify the benefits and drawbacks of different systems, assisting decision-makers in choosing the best SIEM solution for their unique needs and strengthening SMEs' cybersecurity posture.

MFA Capstone Project

Elena V Sanchez, Kiran Bista, Itzel Juarez, Mac Franklin

Advisor: Dr. Jorge Castillo

Abstract:

With the rise in cybersecurity threats aggravating existing and new security risks every day, our systems are more vulnerable than ever. As such, one aspect of security more essential than ever is authentication [3]. Robust authentication methods are essential for protection and security of sensitive data and systems. This project proposes a Multi-Factor Authentication (MFA) [2] system combining three individual factors: Something you know (password or PIN), something you have (One-Time Password (OTP)), and somewhere you are (geolocation verification). The MFA system is inspired by the secure multiparty computational setup where all three factors interact and validate a user in a specific order to make the system both secure and user friendly. The concept was fitting for what we set out to achieve, so we wish to use the idea of SMPC and not the system itself. The first authentication method secures users credentials using either a PIN or Password known only to the user. The second authentication factor [1] would be geolocation [4] which would happen without any user input. The third factor, the OTP, would implement a system where a user types in an email they wish to receive the OTP with. The user will insert said OTP as part of the sign on process, thereby fully authenticating users into the system entirely through a third-party system.

Phishing Campaigns for the Spread of Awareness of the Dangers of Malware

Eduardo Flores, Victor Hernandez, Steven Perez, Jeremy Soto

Advisor: Dr. Liyu Zhang

Abstract:

Malware is software designed to harm or disrupt a device, system, or network. This allows attackers access to information and/or resources they otherwise wouldn’t have access to. Despite the increasing use of online services, many people are still uninformed about the risks lurking inside a pdf or link. The intention of this project is to spread awareness about the dangers that exist even in seemingly impervious tasks, such as checking one’s emails. The method for doing this is hosting a website that will simulate several types of malwares in a closed environment to educate the user on their functions and dangers. To further lean into the theme of malware, the link to the website will be spread via an email phishing campaign aimed at UTRGV faculty and students. To reiterate, the link will not lead the victims to a malicious site nor download any code onto their machine. The spoofed email messages will be tailored to the group that we are targeting in an effort to seem as legitimate as possible. An example of this approach would be pretending that one of the links leads to a website with resources to help study for the Security+ exam. This would of course be aimed at students. We plan to host our website on Google Cloud Platform. This not only adds a level of availability and security to our website, but it will essentially be free via the free trial Google provides to new users. Additionally, we aim to collect data about which groups were most vulnerable to the phishing campaign and which channels of distribution were the most successful. The types of malwares that will be simulated on the website include ransomware, keyloggers, password-crackers, and DNS spoofing. The language we will utilize for the programs is Python, given that most of us are relatively familiar with it. Deliverables for the project are the completed website and data about the phishing campaign (more details regarding deliverables are available below).

Self-Learning DGA Filter on GCP: A Machine Learning and Cloud-Based Solution

Jorge Rodriguez, Jesús Sanchez, Wilfredo de Leon

Advisor: Dr. Mahmoud Quweider

Abstract:

The dynamic nature of cyber threats, particularly those using domain generation algorithms (DGAs), necessitates innovative detection solutions. This project proposes the development of a self-learning DGA detection system using long short-term memory (LSTM) networks, Auxiliary Loss Optimization for Hypothesis Augmentation (ALOHA), and the inclusion of side information such as WHOIS features to enhance detection accuracy. Hosted on Google Cloud Platform (GCP), the system will utilize BigQuery and cloud storage for scalable, real-time analysis and domain classification. By leveraging cutting-edge techniques from recent research on DGA detection, the system will continuously learn from emerging threats, improving its ability to detect even highly evasive DGA patterns. This solution aims to provide a robust, adaptable, and real-time defense mechanism within the ever-evolving landscape of cybersecurity.

Cyber Defenders: Rise Through the Ranks

Precious Ramos, Mia Garcia, Agustin Lara, Kayla Jimenez, Ajad Yazji

Advisor: Dr. Mahmoud Quweider

Abstract:

This project proposes the development of an interactive educational game using Pygame, a Python-based game development library. The game is designed to raise awareness about common cybersecurity threats such as phishing, malware, and social engineering by simulating real-world attack scenarios. Players will assume the role of a cybersecurity analyst, tasked with identifying and responding to various cyber threats. The game aims to educate users through engaging gameplay that reinforces best practices for recognizing and mitigating online risks. By promoting quick decision-making and problem-solving, this project will serve as a tool for both educational institutions and the public to enhance cybersecurity awareness.

AI Firewall

Matthew Stelling, Jorge Gomez, Rolando Martinez, and Ricardo Olguin

Advisor: Dr. Mahmoud Quweider

Abstract:

Current ways of preventing malicious traffic using a firewall are reactive. You can only block a connection once you know about it. In addition, this allows attacks to do damage before they can be stopped.

With TensorFlow we can train a model and allow it to make decisions based on what it was trained on to block a connection without further input from network administrators. We will use traffic from a firewall to train our model.

- Dataset: https://www.kaggle.com/datasets/tunguz/internet-firewall-data-set/data

Deep Dive into Phishing: Targeting, Payload and Targets

Micajah Martinez, Luisa Tovar, Nelson Monroy, Amadeus Dutremaine, Mark Aguilar

Advisor: Dr. Mahmoud Quweider

Abstract:

Every day we hear on the news about different “hacks”, but not much is known about how it happens to the vast majority of the public. According to reports, 91% of all acks begin with a phishing email to an unsuspecting victim. On top of that, 32% of all successful breaches involve the use of phishing techniques. Phishing takes many forms but one of the most common is emails, and with the growth of AI and automated tools for phishing it has become one of the easiest and most extensive methods of cybercrime and social engineering.