**Project Plan:**

David Yi

The Polytechnic School, Arizona State University

IFT520: Advanced Information Systems Security

Dr. Jim Helm

October 1, 2023

**Table of Contents**

Abstract3

Introduction4

Problem Statement5

Significance of Study5

Objective6

Tools and Requirements6

Implementation7

Scope8

**Abstract**

As technology advances and becomes more interconnected, creating secure communication channels between devices in separate networks is vital. This project outlines the scope, design, development life cycle and demonstration of an application that creates automated Virtual Private Network (VPN) connections between interconnected devices in separate networks, creating an effective, secure and encrypted connection between the interconnected devices.

**Introduction**

Protecting data and ensuring that the data is private is often treated as different aspects of security, however those two aspects are generally synonymous with each other. While the security of the data is paramount from an organizational standpoint, end users general determine their own person threat environment, and in correlation, with how their data is protected. There are several general steps that can be taken in order to protect a user’s data. According to the Federal Trade Commission (2021), the steps to ensuring that a user’s data is secure involves:

* Ensuring that any software (operating system included) is up to date with the latest security patches and versions.
* Ensuring that accounts utilized use strong passwords and/or multifactor authentication.
* Creating backups of data, using either a cloud service or an external USB storage device.

While these steps are important, there other considerations that need to be made as well. When sharing or uploading data amongst peers or online services, is the data in transit protected? How much of the users’ identifiable data is viewable by malicious actors? Is the users’ personal data protected from any malicious actor’s prying eyes? For corporations, if data at rest or data in transit is compromised, then the organization loses a significant portion of revenue and loses the trust of their consumer, however the organization isn’t affected as significantly as the individual. For an individual, if their data is compromised the impact is significantly more, as a person could lose their entire livelihood. “Identity theft occurs when someone steals your personal information and uses it to take your money, open credit accounts, file tax returns, make health insurance claims and more without your consent” (Luthi, 2022). There are several methods of protecting against data compromise, however the end user is ultimately responsible for protecting their data at rest and in transit.

**Problem Statement**

While there are several solutions in place to secure personal data, several commercially available solutions require monthly or annual payments for securing data. Most modern computers have built in encryption readily available for data that is stored locally on the machine, however there aren’t many solutions that can be obtained without purchase for protecting data while in transit. The current industry standard for protecting data while also maintain a certain level of privacy during the transit is to utilize a VPN or virtual private network. A VPN “establish[es] a protected network connection when using public networks [and] … encrypt[s] [the users’] internet traffic and disguise[s] [the users] online identity” (Kaspersky, 2023). While there are several paid solutions for VPNs, not everyone can afford to pay for a VPN service, or trust that the VPN providers’ have the end users’ best interests regarding network traffic and data security.

**Significance of Study**

The current state of data security poses a problem. The abundance of solutions that require continuous payments, for protecting data. Although modern computers come equipped with built in encryption for storing data there is a gap when it comes to affordable and accessible methods for safeguarding data while it is being transmitted. In todays interconnected society ensuring the security of data as it travels through networks and the internet is crucial. The accepted solution to this challenge is Virtual Private Networks (VPNs) which establish connections encrypt internet traffic and safeguard users’ online identities especially when using public networks. However, a major hurdle arises from the reliance on paid VPN services. Many individuals and organizations struggle with recurring costs, coupled with concerns about how VPN providers handle their data. This research project addresses the pressing need for cost reliable solutions to protect data during transit. Its objective is to make data security accessible to everyone regardless of their situation. By doing it empowers users, with effective tools to safeguard their data ultimately enhancing privacy and strengthening data security in our increasingly interconnected digital world.

**Objective**

The objective of this project is to create a user-friendly, application for any user or organization that wishes to protect their data in transit between interconnected devices. This application with automatically configure the necessary authentication, encryption, and iptables rules, while also allowing the user to specify the destination source to connect to, allowing cross-platform compatibility, while also encrypting the data in transit. This application will be written in Rust, which is an open source, memory safe programming languages that have specific protection measures against buffer overflow attacks. This application will also be easily deployable without having to run in an elevated state (requiring administrative rights).

**Tools and Requirements**

To create an easy, to use solution for safeguarding data while its being transferred I will utilize the Rust programming language, GitHub for version control and the WireGuard open-source VPN protocol.

Rust is a powerful systems programming language that prioritizes safety, performance and memory management. I've selected Rust as my coding language because of its ability to efficiently handle low level tasks making it ideal for constructing networking applications. By focusing on preventing programming mistakes like memory leaks and buffer overflows Rust aligns perfectly with my objective of building a data protection solution.

For version control and collaborative development purposes I will rely on GitHub. It provides features for tracking changes, managing issues. Promoting collaboration among team members as well as the wider open-source community. GitHub’s popularity and accessibility will ensure that my project remains transparent and available to both contributors and users. This approach allows me to maintain a documented solution that can be continually improved upon.

At the heart of my solution lies the integration of the WireGuard open-source VPN protocol. Renowned for its simplicity, security and efficiency in encrypting data while offering tunneling capabilities. This decision is, in line with my objective to offer users a VPN protocol without the need for subscriptions. Moreover, the lightweight and efficient design of WireGuard supports my aim of providing a solution that doesn't compromise performance.

By utilizing the Rust programming language GitHub for version control and adopting the WireGuard VPN protocol my project strives to create a secure and open-source solution, for safeguarding data during transmission. These tools and requirements will empower me to develop a solution that prioritizes user privacy and data security.

**Implementation**

To create a user data protection solution that guarantees data transmission I will follow the steps outlined below using the Rust programming language. Moreover, I will take advantage of GitHub, for version control. Incorporate the WireGuard open-source VPN protocol.

1. Setting up the Project Repository on GitHub: Firstly, I will establish a GitHub repository as a hub for collaboration and version control. It is essential to maintain documentation within the repository including a README file that offers insights into the projects purpose, installation instructions and usage guidelines.
2. Utilizing Rust Programming for Data Protection: Next my focus will be on building the functionality of our data protection solution using Rust. By harnessing Rusts safety features, memory management capabilities and performance optimization techniques we can ensure encryption and transmission of data. Throughout this process I will prioritize implementing measures that prevent programming errors like memory leaks and buffer overflows in line with Rusts safety objectives.
3. Incorporating WireGuard Integration: Lastly, I will seamlessly integrate the WireGuard open-source VPN protocol into our solution to provide encryption and secure tunneling capabilities. The simplicity and efficiency offered by WireGuard will play a role, in achieving this goal.
4. Creating User Interface (UI): I will design a user interface (UI) that allows users to easily set up and activate their VPN connections.
5. Documentation and User Guides: I am committed to keeping the project documentation on GitHub up to date providing users with information on how to install configure and effectively use this solution. I will also create user guides and tutorials to assist users in setting up and maximizing the benefits of this data protection tool.

By following this implementation plan using Rust programming language utilizing GitHub for version control and integrating with WireGuard VPN protocol my aim is to develop an open-source data protection solution. This solution will empower users to secure their data during transmission while prioritizing privacy and security, in todays interconnected world.

**Scope**

My main objective, for this project is to develop a data protection solution that's both source and secure. The aim is to empower users by providing them with a way to safeguard their data during transmission without any constraints. User privacy and data security are my priorities as I strive to enhance the protection of information while communicating and sharing data online.

**Utilizing Rust Programming Language**

I will leverage the capabilities of Rust to effectively handle low level tasks while prioritizing safety, performance and memory management. The core focus of the project will revolve around developing a networking application in Rust that guarantees data protection.

**Employing GitHub, for Version Control and Collaboration**

I will establish a version control system using GitHub to track code changes manage project related issues and facilitate collaboration among team members as the wider open-source community. By adopting this approach, we ensure transparency and accessibility throughout the project enabling contributions, from an audience.

**Integrating WireGuard Open-Source VPN Protocol**

The solution will incorporate the WireGuard VPN protocol to enhance encryption and enable tunneling capabilities. This integration will prioritize simplicity, security and efficiency in both data encryption and transmission. Users can benefit from a VPN protocol without having to bear subscription charges. Moreover, this solution aims to maintain an efficient design in order to deliver performance while upholding data security.

Key Deliverables:

1. Developing a data protection solution using the Rust programming language.
2. Setting up a version-controlled repository on GitHub complete with documentation.
3. Successfully integrating the WireGuard VPN protocol into the solution.
4. Designing user friendly interfaces that make it easy for users to configure and utilize the data protection solution.
5. Continuously maintaining the open-source project on GitHub while welcoming contributions from the community.

Throughout this project I will adhere to industry practices in software development, cybersecurity and open-source collaboration. The goal is to create a tool that provides support, for protecting data during transmission.

**References**

Donenfeld, J. A. (n.d.). *WireGuard: fast, modern, secure VPN tunnel*. https://www.wireguard.com/

Federal Trade Commission. (2021, May). *Protect your personal information and data*. Consumer Advice. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

Github. (n.d.). *Build software better, together*. GitHub. https://github.com/about

Kaspersky. (2023, July 31). *What is VPN? How It Works, Types of VPN*. www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Luthi, B. (2022). What is identity theft and how do I make sure it doesn’t happen to me? *www.experian.com*. https://www.experian.com/blogs/ask-experian/what-is-identity-theft/

*Rust Programming Language*. (n.d.). https://www.rust-lang.org/