Software Requirements Specification (SRS)

Introduction

This document specifies the requirements for the ***"Covert Channel Detection and Prevention"*** software. The purpose of this software is to detect and prevent covert channels, which are methods used to communicate secretly over computer networks. The intended audience for this SRS includes software developers, quality assurance testers, project managers, and other stakeholders involved in the development and deployment of the software.

Scope

The "Covert Channel Detection and Prevention" software will provide a means for detecting and preventing covert channels in computer networks. While a wide variety of covert channels exist, the focus of this project will be on detecting timing channels. The software will be designed to work with various types of network protocols and will be compatible with a wide range of hardware configurations. In addition to detecting covert timing channels, the software will be tested in a virtual environment using multiple virtual machines (VMs) and data transmission through covert timing channels. The software will also be designed to disrupt covert timing channels after they have been detected.

Functional Requirements

The following are the functional requirements for the "Covert Channel Detection and Prevention" software:

1. The software shall provide a means for detecting covert timing channels in computer networks.
2. The software shall provide two levels of detection. The first level shall involve superficial detection by analyzing delay and packet length. The second level shall involve ML-based pattern analysis to reduce false positives.
3. The software shall be compatible with BPF for network packet filtering and analysis.
4. The software shall store each packet for a given source and destination and only delete the packets once the suspicion of a covert timing channel has been cleared.
5. The software shall be tested in a virtual environment with multiple VMs and data transmission through covert timing channels.
6. The software shall be designed to disrupt covert timing channels after they have been detected.
7. The software shall use a test environment for simulating covert timing channel transmission between client and server.
8. The software shall create a dataset of training ML model.
9. The software shall use BPF code for packet analysis.
10. The software shall embed the ML model to analyze packets.

11. The software shall disrupt timing channels using random delays and other techniques.

Non-Functional Requirements

The following are the non-functional requirements for the "Covert Channel Detection and Prevention" software:

1. The software shall be reliable and accurate in detecting and preventing covert timing channels.
2. The software shall be scalable and able to handle large volumes of network traffic.
3. The software shall be secure and able to protect against unauthorized access.
4. The software shall be easy to install and configure.
5. The software shall have minimal impact on network performance.
6. The software shall be able to detect covert timing channels with a high degree of accuracy in the test environment.

Constraints

The following are the constraints for the "Covert Channel Detection and Prevention" software:

1. The software must comply with all applicable laws and regulations.
2. The software must be developed within the specified budget and timeline.
3. The software must be developed using the programming languages and tools specified by the project stakeholders.

Assumptions

The following are the assumptions made during the development of the "Covert Channel Detection and Prevention" software:

1. The software will be used for legitimate purposes only.
2. The network traffic to be monitored will be within the network administrator's authority to monitor.
3. The hardware and software requirements will be met by the target systems.
4. The test environment will accurately simulate covert timing channel transmission.

Dependencies

The following are the dependencies for the "Covert Channel Detection and Prevention" software:

1. The software will depend on BPF for network packet filtering and analysis.
2. The software will depend on ML libraries for training and embedding the ML model.
3. The software will depend on a virtual environment for testing with multiple VMs.
4. The software will depend on network protocols supported by the target systems.

Acceptance Criteria

The following acceptance criteria must be met for the "Covert Channel Detection and Prevention" software:

1. The software shall detect covert timing channels in the test environment with a high degree of accuracy.
2. The software shall prevent covert timing channels from being established in the test environment.
3. The software shall not generate false positives in detecting covert timing channels.
4. The software shall be easy to install and configure on the target systems.
5. The software shall not have a significant impact on network performance.
6. The software shall be able to handle large volumes of network traffic.

Glossary

The following terms are used in this SRS:

1. ***BPF*** - Berkeley Packet Filter, a system for filtering and analyzing network packets.
2. ***Covert channel*** - a method used to communicate secretly over computer networks.
3. ***ML*** - Machine Learning, a field of study that uses algorithms to learn patterns and make predictions based on data.
4. ***Test environment*** - a controlled environment used for testing software or hardware.
5. ***Timing channel*** - a covert channel that uses variations in timing to transmit information.

Conclusion

This SRS document provides a detailed specification of the requirements for the "Covert Channel Detection and Prevention" software. The document outlines the functional and non-functional requirements, constraints, assumptions, and dependencies for the software. The document will serve as a reference for software developers, quality assurance testers, project managers, and other stakeholders involved in the development and deployment of the software.