Secure Software Development Project
Software Security Course – 2024-25
Polytech Nice Sophia Antipolis

This small project aims at experiencing the overall activities supporting the secure software development lifecycle (SSDLC). It also constitutes a recap of the different activities that were undertaken during the course labs. You will be playing both the role of the developer and of the security expert.

Introduction

Your mission, should you accept it, is to develop SecTrans, a secure transfer application working in client-server mode. This application should make it possible for the company employees to securely transfer files to a server where they would be stored. It should also make it possible for the employee to query the server for the presence of a given file and to possibly retrieve this file. The server will be deployed on the company's premises and will be accessible to employees from their office and from their home.

Your work will be evaluated based on the software production but also, and more importantly, based on the security evaluation and documentation you will produce.

Specification phase

This part of the work will first require you to determine the system architecture as well as the security architecture. Your system architecture will have to cope with a major requirement: your boss has selected a client server communications library from Macrohard Corporation as a middleware for implementing data transfers, which you must incorporate into your design. Unfortunately, this library does not implement any security mechanism.

Your security architecture will have to describe how security countermeasures are introduced into the system architecture and how they interact. The security countermeasures will be determined based on the threat model that you also have to establish. Such countermeasures typically include access control and cryptography. The threat model will investigate security and privacy threats to the application and will also have to be documented.

You will also have to develop a preliminary risk analysis in order to understand where to investigate potential vulnerabilities. You may for instance try to define an attack tree for the architecture you are drafting.

Development phase

Your software will be developed in C and will run on Linux 20, the same distribution as the SEED Labs virtual machine. You will have to implement the following command-line options (which you may complete with your own):

sectrans -up file	Upload file to the server
sectrans -list	List the files stored by the employee on the server
sectrans -down file	Download file from the server

The Macrohard framework relies on two C libraries, libclient.so, and libserver.so. You have access to the client.h and server.h files which provide you with a very basic description of the API for transferring data.

Security Analysis phase

You also must analyze the security of your application when it is finished, based on the approaches used in the labs (typically fuzzing and reverse engineering). Your report should contain a detailed report of the analysis you will perform on the finished application.

Based on that analysis, you may validate the product, suggest recommendations about the security architecture, or even decide to modify part of the application code if necessary. If your recommendations encompass the use of another language like Rust, you will have to clearly explain where and what for you would use the language and its specific features.