Tecnologias de Segurança

Trabalho Prático #3

Controlo de acesso a um sistema de ficheiros virtual baseado em libfuse com regras automáticas e autorizações explícitas

8 de Maio de 2023

Introdução

Neste trabalho pretende-se implementar uma componente de software capaz de intercetar e, eventualmente, negar ou autorizar operações de acesso a objetos do sistema de ficheiros num sistema virtual de ficheiros baseado em libfuse e integrar com a infrraestrutura de logs rsyslog. A negação ou a autorização de acesso deverá poder ser aplicada de forma automática com base em regras previamente definidas. Deverá também ser possível definir regras que obriguem a uma autorização explícita recorrendo a um mecanismo de OTP.

1 Descrição da funcionalidade

A componente a desenvolver deverá intercetar o acesso a cada um dos objetos do sistema de ficheiros virtual, negando ou autorizando a operação de acesso em função das regras definidas.

As regras poderão ser tão flexíveis quanto se queira, tendo em consideração, por exemplo, o utilizador que pretende aceder ao objeto, o tipo de operação, e o objeto propriamente dito.

Relativamente ao objeto do sistema de ficheiros, as regras poderão ter em conta padrões do nome e caminho do objeto, datas de criação, modificação e acesso, identificação do utilizador e grupo dono, etc.

As regras poderão autorizar ou negar imediatamente, ou poderão requerer a autorização explícita do utilizador responsável, por exemplo, o dono do objeto que se pretende manipular numa dada operação.

Quando requerida, a autorização explícita implicará pois o envio de um código OTP por parte do utilizador responsável. A necessidade de autorização poderá ser sinalizada por envio de e-mail, SMS, ou por um outro qualquer mecanismo entendido adequado. O OTP deverá ser enviado à componente a desenvolver também, por exemplo, via e-mail ou HTTP GET. Se desejar também poderá recorrer à utilização de uma aplicação do tipo Google Authenticator.

Note que o processo de notificação e receção de OTP será despoletado pela invocação de uma operação de acesso a um objeto do sistema de ficheiros virtual, mas sem qualquer envolvimento ou mesmo co-

nhecimento do utilizador que a invocou. Durante este processo a execução da operação ficará bloqueada (suspensa). O tempo máximo para a conclusão deste processo de autorização poderá ser um parâmetro de configuração da componente que deverá ser desenvolvida para este projeto.

Tenha ainda em atenção que, como será necessário contactar de alguma forma os utilizadores responsáveis por autorizações, deverá ser possível especificar (ou gerir) esses mesmos contactos.

No desenvolvimento da sua solução, por uma questão de simplificação do trabalho, poderá desenvolver o sistema de ficheiros virtual recorrendo ao espelhamento de uma parte de um sistema de ficheiros existente. Dependendo do nível de abstração utilizado – poderá ser suficiente a interceção das chamadas ao sistema `open()` e/ou `read()` e `write()`.

No desenvolvimento desta componente poderá querer ter em conta os exemplos de utilização e programação de libfuse disponíveis em passsthrough.c ou passthrough_fh.c, servindo-se deles como seu ponto de partida.

Na realização deste trabalho, deverá ter em conta uma adequada definição de permissões associadas ao(s) ficheiro(s) onde serão definidas as regras e os contactos dos utilizadores envolvidos.

Submissão do trabalho

A data-limite de entrega do trabalho será o dia 27 de maio (23:59) e será submetido via a página da UC no sistema de elearning.

O trabalho deverá ser submetido num arquivo zip contendo todos os ficheiros de código-fonte, ficheiros de projecto (p. ex: Makefile) necessários à geração dos programas executáveis, e um relatório de até 6 páginas (identique claramente os membros do grupo).

O relatório deverá descrever a arquitetura e estrutura da solução desenvolvida, os aspectos relacionados com eventuais dependências de biblioteca e com a sua instalação, e os aspectos relacionados com segurança que possam ter sido tidos em consideração.

Garanta que a solução ao problema tem em atenção a existência de vulnerabilidades conhecidas (CVE) e os tipos de fraquezas mais comuns (CWE) no desenho e implementação do seu código. Apresente e discuta como estes aspectos foram contemplados no trabalho.

O trabalho poderá ser desenvolvido em qualquer linguagem que permita a integração com o libfuse (note, contudo, que a implementação de referência está escrita em C).