Tecnologias de Segurança

Trabalho Prático #3

Deteção de Modificações Não-Autorizadas no Sistema Operativo

9 de Maio de 2022

Objetivos e funcionalidade

Neste trabalho pretende-se implementar uma componente de software capaz de detetar modificações não-autorizadas num conjunto de ficheiros considerados críticos para a segurança de um dado sistema operativo Linux (p. ex: configurações de sistema, de serviços, programas executáveis, etc). Essa componente deverá poder funcionar ou de forma assíncrona, como serviço, ou em tempo-real, como sistema de ficheiros virtual.

Num momento inicial – num estado que se assume como seguro – a componente a desenvolver deverá recolher o conjunto de metadados considerados relevantes, metadados esses que deverão incluir, entre outros, atributos como permissões, utilizador e grupo dono do ficheiro, hash do seu conteúdo, etc. O conjunto dos metadados deverá de seguida ser preservado em meio acessível apenas para leitura (assuma, por exemplo, a gravação em CD-ROM ou DVD-ROM).

O mecanismo a desenvolver poderá ser concretizado tanto sob a forma de um serviço integrado com a respectiva infraestrutura de gestão do systemd, como sob a forma de um novo sistema de ficheiros baseado em libfuse.

Na forma de operação como serviço, esta componente deverá periodicamente verificar a integridade dos ficheiros de interesse. Esta monitorização deverá ser realizada a períodos regulares configuráveis. O serviço deverá ainda reportar o resultado da sua monitorização através da infraestrutura de gestão de logs, rsyslog.

Na forma de sistema de ficheiros, a componente deverá interceptar o acesso a cada um dos ficheiros de interesse, negando a abertura em caso de modificação não-autorizada. Opcionalmente, um acesso a um ficheiro alterado poderá ainda assim ser autorizado mediante a introdução, por parte de um utilizador previamente designado – ou, em alternativa, do utilizador dono do ficheiro – de um código OTP enviado por um segundo canal. A esse respeito, o código poderá ser enviado por SMS, ou mesmo utilizando uma aplicação do tipo Google Authenticator. Note que poderá ser necessário manter o registo de todos os utilizadores responsáveis ou proprietários dos ficheiros a proteger. Esse registo deverá mapear os seus identificadores e a respetiva forma de contacto. Ainda relativamente a esta componente de sistema de ficheiros virtual, note que – dependendo do nível de abstração utilizado – deverá ser suficiente a intercepção da chamada ao sistema `open()` e/ou `read()`. No desenvolvimento desta componente poderá querer ter em conta os exemplos de utilização e programação de libfuse disponíveis em passthrough.c ou passthrough_fh.c, servido-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 mantidos esses registos e, em geral, de utilizador e grupo de utilizador associados a este serviço.

Submissão do trabalho

A data-limite de entrega do trabalho será o dia 7 de Junho (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 arquitectura 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).