Tecnologia de Segurança

Trabalho Prático #3

Autorização de Operações ao nível do Sistema de Ficheiros

16 de Dezembro de 2018

Objectivos e funcionalidade

Neste trabalho pretende-se complementar os mecanismos de controlo de acesso de um sistema de ficheiros tradicional do sistema operativo Linux com um mecanismo adicional de autorização de operações de abertura de ficheiros. O mecanismo a desenvolver deverá ser concretizado sob a forma de um novo sistema de ficheiros baseado em libfuse.

O mecanismo deverá autorizar a operação de abertura apenas depois da introdução de um código de segurança único enviado ao utilizador que a despoletou. O código de segurança poderá ser enviado via SMS (ou usando uma qualquer API de comunicação instantânea) ou, em alternativa, via correio electrónico.

Para o efeito, deverá ser mantido o registo de todos os utilizadores que poderão aceder ao sistema de ficheiros a desenvolver. Esse registo deverá mapear os seus identificadores e a respectiva forma de contacto. Note que poderá ser necessário ter em conta uma adequada definição de permissões associadas ao(s) ficheiro(s) onde serão mantidos esses registos.

Quando invocada a operação de abertura de ficheiros `open()`, essa operação deverá retornar: com sucesso quando tiver sido recebido o código de segurança enviado ao utilizador; ou com insucesso quando tiver sido ultrapassado o limite de tempo de 30 segundos para o utilizador comunicar o código referido.

A comunicação do código de segurança por parte do utilizador poderá ser realizada por sua introdução, por exemplo, num servidor trivial com interface web (e com o qual o mecanismo de autorização a desenvolver deverá comunicar).

O desenvolvimento deste mecanismo deverá ter por base a biblioteca libfuse, podendo utilizar os exemplos passthrough.c ou passthrough_fh.c como ponto de partida.

Submissão do trabalho

A data-limite de entrega do trabalho será o dia 16 de Janeiro (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

duas/três páginas. O relatório (que deverá identificar os membros do grupo) 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.

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

Sugestão de trabalho alternativa

Suportado na mesma base tecnológica – nomeadamente no uso libfuse – implemente um serviço de identificação de ataques de injecção de malware ou de rasomware. Para o caso da detecção de malware, poderá recorrer ao software de código aberto clamav. No caso da detecção – e desejável impedimento – de ataques de ramsonware, poderá recorrer ao cálculo da entropia dos blocos lidos e subsquentemente escritos.

Estas sugestões alternativas apresentam um desafio técnico adicional, pelo que tal será tido em consideração na avaliação do trabalho desenvolvido.