Trabalho Prático 3

Instruções

- O trabalho prático deverá ser feito em grupo de, no máximo, 3 membros;
- A submissão deverá ser feita por apenas um dos integrantes do grupo, exclusivamente, via blackboard;
- Deve ser entregue o código fonte, Makefile e um relatório de até 10 páginas (A4, 11pt) no formato PDF (excluindo capas e anexos);
- No relatório deverá apresentado e discutido o espaço de desenho da solução, a implementação da solução proposta, e eventuais limitações e valorizações;
- O prazo de submissão será 23h59 do dia 28/05/2025;
- Será marcada, posteriormente, uma sessão onde cada grupo discutirá a sua abordagem e implementação.

Objetivos

Na aulas teóricas foram apresentados e discutidos de forma relativamente breve vários modelos de controlo de acesso, modelos esses focados na garantia de diferentes propriedades de segurança. De entre os modelos discutidos, destaca-se pelo seu caráter seminal, o modelo Bell~LaPadula (BLP), centrado na proteção da confidencialidade em sistemas se segurança multi-nível.

Como sabemos, o BLP é um modelo teórico com uma aplicação direta muito limitada. Por exemplo, os níveis de classificação e compartimentação de informação e de utilizadores são entendidos como estáticos e não é indicado um mecanismo concreto que permita passar informação de um nível superior para um inferior de classificação. Várias abordagens podem ser seguidas no sentido de serem resolvidas algumas destas limitações, por exemplo, introduzindo a noção de utilizadores de confiança (*trusted users*). Esses utilizadores poderem partilhar com um nível inferior de segurança, documentos classificados de nível de segurança superior mediante um processo de filtragem (expurgação) de informação considerada sensível. Adaptações ao modelo original introduzem, no entanto, e de um modo geral, fragilidades que obrigam, por seu turno, a mecanismos de mitigação e/ou de auditoria. Outro aspeto que não é endereçado pelo BLP -- em grande medida devido ao seu caráter estático -- , é a gestão de utilizadores e atribuição do nível de segurança que lhes é associado (*clearance*).

Neste projeto, pretende-se ver discutidas e implementadas as adaptações necessárias à concretização deste modelo de controlo de acesso suportada ou pelo sistema de ficheiros (e infraestrutura de serviços) do Unix, ou por uma base de dados chave-valor à escolha. A este respeito, a autenticação de utilizadores e monitorização do funcionamento da solução também devem ser discutidas e objeto de implementação.

O espaço de desenho deste projeto é flexível, não só em termos de resolução das limitações do modelo original, como da sua implementação propriamente dita. Dito isto, este trabalho deverá ser desenvolvido em Python e, tipicamente, deverá incluir uma biblioteca e aplicação cliente, e uma componente de servidor.