Introdução

No âmbito da unidade curricular de Segurança de Redes foi-nos proposto a realização de um trabalho com o objetivo de desenhar uma política de controlo de acesso num contexto de ensino universitário.

Os mecanismos de controlo de acesso têm como objetivo principal a autorização ou bloqueio de acesso a recursos consoante o que a entidade tenta aceder. Alem disso, permite ainda distinguir o tipo de permissões que cada entidade possui sobre diferentes objetos, como por exemplo, acesso apenas de leitura ou de leitura e escrita.

Conceitos Importantes

Discretionary Acess Control

É um tipo de [controlo de acesso](https://pt.wikipedia.org/wiki/Controle_de_acesso) definido como um meio de restringir o acesso a objetos com base na identidade dos sujeitos e/ou grupos aos quais eles pertencem. Os controlos são discricionários no sentido em que o sujeito com uma certa permissão de acesso seja capaz de passar esta permissão (talvez indiretamente) para qualquer outro sujeito.

Mandatory Acess Control

É uma estratégia de controlo de acesso que restringe a possibilidade que os proprietários têm para permitir ou negar acesso a serviços num sistema de ficheiros.

Os critérios MAC são definidos pelo administrador do sistema e são impossíveis de sofrerem alterações por parte do utilizador normal ou comum.

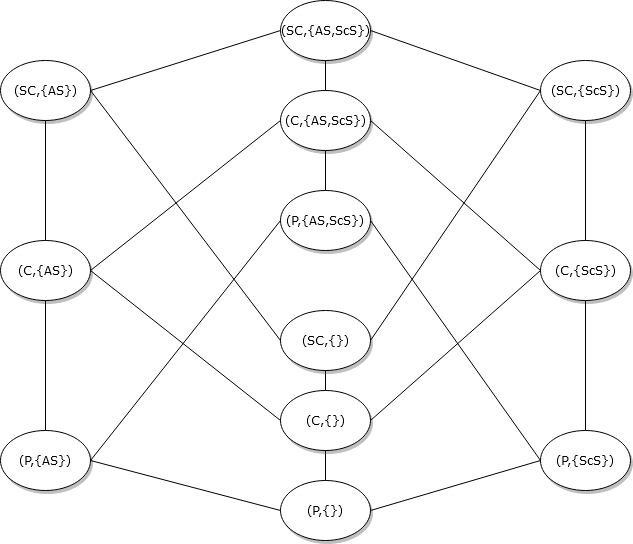
Esta estratégia é predominantemente implementada por organizações governativas ou militares e funciona baseando-se na designação de classificações para cada objeto como por exemplo Confidential, Secret ou Top Secret e cada utilizador tem um nível de acesso semelhante podendo aceder apenas a objetos que a sua designação o permite.

Modelo Bell-Lapadula

O modela foca-se na confidencialidade de dados e no controlo de acesso á informação privada onde as entidades de um sistema são divididas em processos/objetos.

Neste modelo é definido a noção de nível de segurança, onde se demonstra que numa transição de nível para outro se preserva a segurança. Este nível de segurança é só considerado totalmente seguro se os acessos aos objetos de um sistema estiverem de acordo com a política de segurança implementada.

Os utilizadores que estejam sujeitos a este modelo apenas podem criar/escrever conteúdo no seu nível de segurança ou o nível acima, mas apenas podem ver conteúdo no seu nível ou abaixo.



LATTICE PEDIDA

É-nos pedido no trabalho, que consideremos duas condições importantes na construção da lattice, as labels de aluno (C, {AS}) e professor (C, {AS,ScS}).

É importante também referir que é necessário que as labels de um nível superior têm de ter um nível de segurança mais restrito e conter a informação de uma label abaixo sempre garantindo a dominância entre labels diferentes.

No caso específico de aluno e professor, uma vez que estão ambos no nível confidencial, o aluno não tem permissão para ler ou escrever nesse nível na label do professor, logo não é possível o aluno modificar objetos inseridos pelo professor.

Para a atribuição de notas pelo professor e necessário também que este possua uma label (C, {AS}) equivalente á do aluno.

**É possível um aluno ser fraudulento para com o Professor?**

Tendo em consideração a lattice acima, numa primeira vista, parece ser praticamente impossível um aluno ser capaz de ser fraudulento. No entanto, isto pode não ser verdade. Partindo do princípio que os utilizadores podem criar/escrever conteúdo no seu nível de segurança ou o nível acima e apenas podem ver conteúdo no seu nível ou abaixo, podemos simular o seguinte caso.

Um professor (C,{AS,ScS}) escreve as notas finais para um nível de acesso superior(Serviços Academicos). Após a aprovação por parte dos serviços académicos, estes irão divulgar, sob domínio publico, as notas, de forma a que os alunos possam ter acesso.

Posto isto, uma das formas de ser fraudulento, seria o chamado blindwrite, segundo o qual, o aluno poderia escrever na pauta das notas, antes de esta ser aprovada pelos funcionários dos serviços academciso, uma vez que está a escrever para um nível de segurança superior, sendo então possível apagar os dados todos, ou alterar a sua própria nota, sendo isto algo complexo de concluir com sucesso.