Universidade do Minho
Escola de Engenharia

METI

TP2 - Modelação do Controlo de Acesso

Cibersegurança

Grupo 4

Fernando João Santos Mendes (PG55807)
Bruno Miguel Fernandes Araújo (PG55806)

Índice

Introdução

A segurança da informação em ambientes universitários exige a implementação de modelos de controlo de acesso robustos e flexíveis, capazes de proteger dados sensíveis e garantir a confidencialidade dos processos académicos e científicos. Este relatório aborda a construção e análise de um modelo de segurança baseado em rótulos (security labels) para uma universidade, utilizando os níveis de segurança P (público), C (confidencial) e SC (estritamente confidencial), bem como as categorias AS (Serviços Académicos) e ScS (Serviços Científicos).

O objetivo principal é construir a *lattice* de rótulos de segurança, aplicando os princípios do modelo Bell-LaPadula (BLP), e identificar comportamentos indesejados, como a fraude académica.

Adicionalmente, este relatório explora a viabilidade da implementação automática deste modelo em infraestruturas de tecnologias de informação e comunicação (TIC) típicas do meio universitário.

Modelo BLP

O modelo Bell-LaPadula (BLP) garante a confidencialidade da informação em sistemas de segurança multinível. Ele utiliza rótulos de segurança, combinando níveis e categorias, para controlar o acesso. A "propriedade simples de segurança" (ss-property) impede que sujeitos leiam objetos de níveis superiores, enquanto a "propriedade" (-property) impede que escrevam em objetos de níveis inferiores. Juntas, essas propriedades asseguram que a informação flui apenas para níveis de segurança mais altos, protegendo dados de forma confidencial.

Estruturação do modelo

Numa primeira abordagem e para um melhor entendimento do panorama geral foi construída a *lattice*. Através da organização dos níveis e categorias de segurança de forma hierárquica, é garantido que o fluxo de informação segue as regras de confidencialidade do modelo.

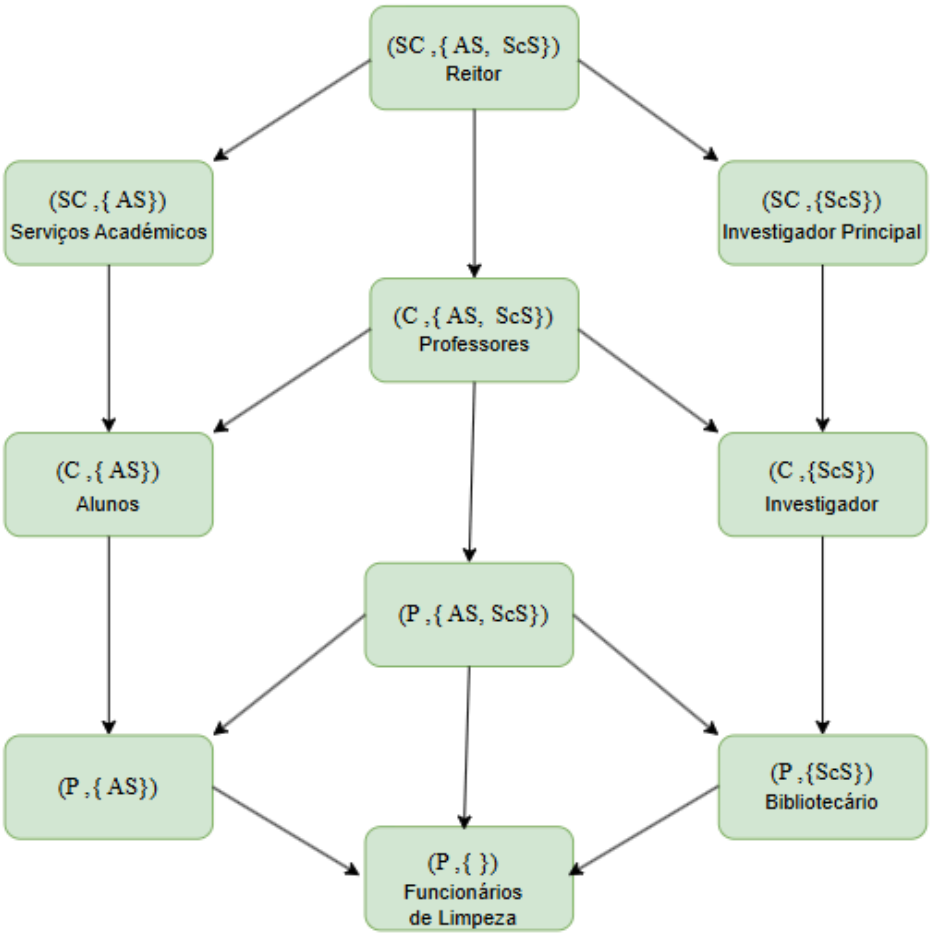

Figura 1: Lattice de labels de segurança

Após serem definidas as labels referentes aos níveis de segurança: P (público), C (confidencial) , SC (confidencial estrito) e as categorias AS (serviços académicos) e ScS (serviços científicos) designamos algumas entidades/grupos da universidade cujas etiquetas pudessem ser atribuídas (presentes na figura 1).

Reitor
Label: (SC, {AS, ScS})

O Reitor é o órgão máximo de gestão de uma universidade, responsável pela supervisão geral de todas as atividades acadêmicas e administrativas. Como tal, o nível de segurança deverá ser o mais alto derivado do acesso a informações sensíveis da instituição.

Serviços Académicos
Label: (SC, {AS})
Responsável por serviços de suporte aos alunos, como matrículas, registros e apoio acadêmico. Dado o acesso a dados pessoais e acadêmicos dos estudantes, temos associado um alto nível de segurança.

Investigador Principal
Label:(SC, {ScS})
Lidera projetos de pesquisa e iniciativas científicas, e, como tal, tem acesso a dados de pesquisa e informações científicas caracterizadas por um alto nível de segurança.

Professores
Label: (C, {AS, ScS})
Docentes dedicados ao ensino e pesquisa. Têm acesso a materiais de curso, dados de alunos e informações de pesquisa revelando-se informação importante, não tão sensível como as entidades em cima mas que requer um nível de segurança médio (confidencial).

Alunos
Label:(C, {AS})
Estudantes que recebem suporte acadêmico e administrativo cujo acesso é limitado às suas próprias informações acadêmicas cuja informação sobre os mesmos deve ser pessoal e portanto ter um nível de segurança que proteja esta sensibilidade de dados (confidencial).

Investigador
Label: (C, {SCS})
Pesquisadores envolvidos em atividades científicas (categoria de serviços científicos) que requerem um acesso privilegiado a artigos e documentos específicos que requer um nível de segurança que não comprometa a integridade do material e o acesso do mesmo, com tal adequa-se um nível de segurança C (confidencial)

Bibliotecário
Label: (P, {ScS})
Responsável pela gestão da biblioteca e recursos de informação (livros, artigos científicos). Como tal, os recursos são de fácil acesso e portanto assume-se um nível de segurança público.

Funcionários de Limpeza
Label: (P, { })
Responsáveis pela manutenção e limpeza das instalações e como tal não têm uma categoria que se adeque àquelas definidas, sendo um serviço público que não requer um nível de segurança relevante.

(P, {AS, ScS})
Não foram encontradas entidades cuja label as caracterize visto que teriam de ter contacto com as categorias de serviços académicos e científicos e ao mesmo tempo a informação/ recursos aos quais tivessem acesso não serem de grande valor.

(P, {AS})
Não foram encontradas entidades cuja label as caracterize.

Identificação de fraquezas no modelo

Ao aplicar as propriedades Sem Leitura para Cima e Sem Escrita para Baixo do modelo BLP, o sistema de controle de acesso multinível impede eficazmente que os alunos cometam fraudes com os professores. As relações de dominância entre as etiquetas de segurança garantem que os alunos não podem aceder ou manipular dados confidenciais dos professores, no entanto conseguimos perceber que embora a confidencialidade seja garantida neste modelo, é possível identificar que não existe nenhuma condição que impeça o aluno de escrever numa etiqueta acima do mesmo, e, como tal, a integridade dos dados pode ser comprometida. Desta forma é possível que o aluno consiga alterar ou inserir dados no professor que visem de alguma forma ajudar ou permitir que o mesmo tenha uma gratificação com isso (batota). Um exemplo seria o aluno editar as notas/pautas para poder obter uma nota consoante a sua intenção.

Implementação

Optamos por desenvolver um programa em python onde pudéssemos refletir , de forma simplória, o comportamento das permissões de cada entidade, com o principal objetivo de ajudar na compreensão de ferramentas mais avançadas.

Inicialmente pretendíamos representar a lattice com algo similar a VLAN's mas acabamos por usar pastas agrupando-as tendo em conta o nível de segurança, sendo assim , as diretorias destas ficaram da seguinte forma:

|-- Universidade
| |-- SC
| | |-- AS
| | |-- ScS
| |-- C
| | |-- AS
| | |-- ScS
| |-- P
| | |-- AS
| | |-- ScS
| | |-- Empty

A aplicação que desenvolvemos funciona da seguinte forma: após a escolha do grupo (simular um login), seleciona-se onde se pretende ler ou escrever e, por fim, define-se a ação a realizar. Todas as escolhas são posteriormente registadas numa pequena caixa de texto (logs).

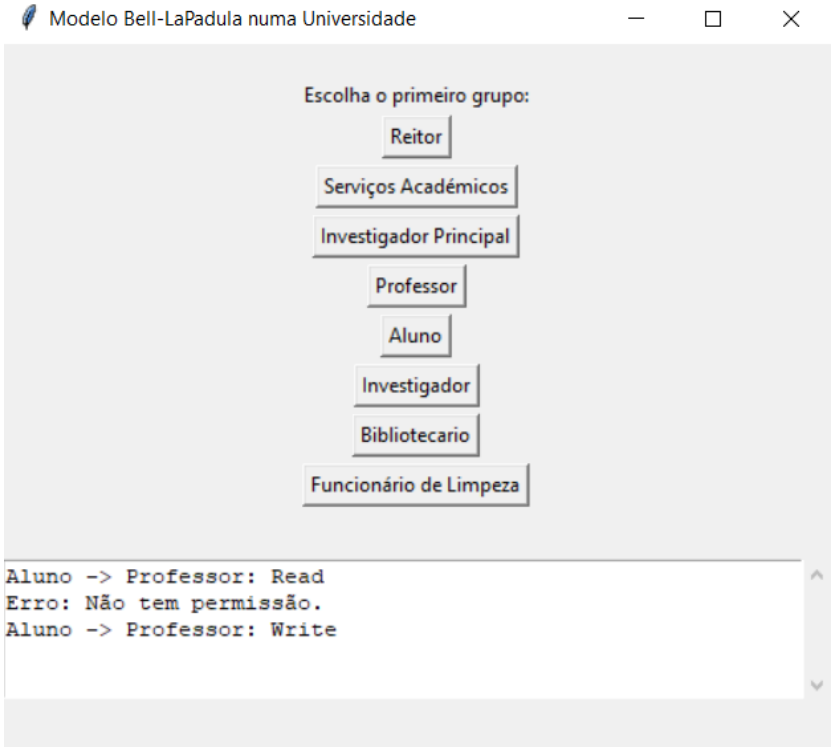

Figura 2 : Interface da aplicação.

No que diz respeito às ações de leitura e escrita, se um elemento com um nível de segurança inferior tentar ler informações de outro com um nível superior, esse acesso será recusado. No entanto, caso tente escrever, para simular o comportamento de uma escrita "cega", será criado ou manipulado um ficheiro de texto com um nome aleatório (Nome seguido de um valor aleatório entre 1 e 10). Por fim, esse ficheiro terá como conteúdo, a frase "Um (Nome do elemento) manipulou este ficheiro.".

Considerando o problema deste modelo mencionado anteriormente, para explicar o funcionamento desta aplicação iremos mostrar os resultados obtidos quando um aluno tenta ler ou escrever num ficheiro de um professor.

Figura 3: Logs após um aluno tentar ler um ficheiro de um professor.

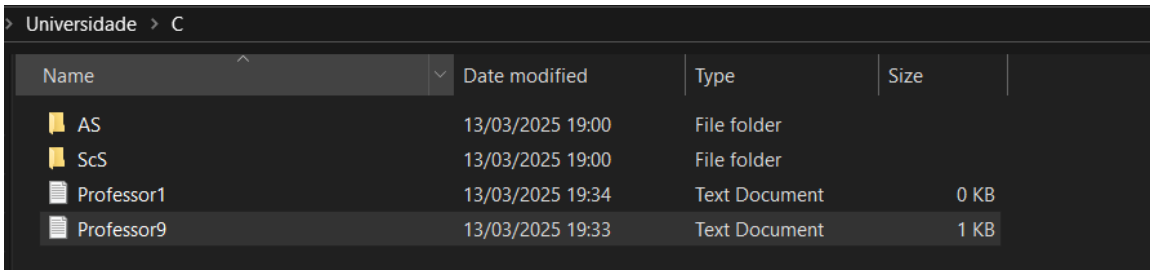

Figura 4: A diretoria dos Professores após uma escrita de um aluno.

Na figura 4, podemos verificar que apareceu um novo ficheiro "Professor9" (o Professor1 já existia e era o alvo do aluno), ilustrando que a escrita cega do aluno, não correu como ele pretendia.

Em comparação com as ferramentas nativas dos sistemas operativos, que permitem atribuir permissões diretamente às entidades, o nosso programa revela-se bastante limitado e estático. O número de diretorias disponíveis é pouquíssimo, o que compromete a sua escalabilidade. Além disso, dispõe apenas de duas ações possíveis , ler e escrever, uma abordagem simplificada em comparação com as diversas operações/ações presentes num sistema operativo.

Implementação automatizada

Utilizando as ACLs do Linux, seguimos a estrutura de diretorias previamente definida. Criamos grupos correspondentes aos níveis de segurança (**SC, C, P)** e às categorias (**AS, ScS**), recorrendo ao comando **groupadd**. Em seguida, procedemos à criação dos utilizadores, como professores, alunos , etc.. associando-os aos grupos adequados através do comando **usermod**. Com a estrutura de grupos estabelecida, atribuímos as permissões de read e write aos utilizadores, utilizando o comando **setfacl**. Por fim, é possível testar as permissões com o comando **sudo -u (utilizador) ls (diretoria)** .Desta forma, asseguramos que cada utilizador apenas acede aos recursos permitidos pelo seu nível de segurança e categorias atribuídas, respeitando os princípios de **no read up** e **no write down** do modelo BPL.

Distribuição de Tarefas:

Ambos os membros do grupo contribuíram de forma equitativa para este projeto, investindo aproximadamente 10 horas cada, significativamente maior que o trabalho prático anterior. Grande parte desse tempo foi dedicada à implementação do modelo, à estruturação da lattice e ao desenvolvimento deste relatório.

Referências:

1. **Draw.io**. (s.d.). Disponível em: https://draw.io
2. **Cornell University**. (2011). *NL Access Control*. Disponível em https://www.cs.cornell.edu/courses/cs5430/2011sp/NL.accessControl.html
3. **University of North Carolina**. (1996). *Notes on Protection*. Disponível em https://www.cs.unc.edu/~dewan/242/f96/notes/prot/node1.html
4. Slides fornecidos pelo educando.