Universidade do Minho
Escola de Engenharia

Universidade do Minho

Trabalho Prático 2

Controlo de Acesso/Access Control

1º Semestre – 2019/2020

Bruno Rodrigues Pg41066

Carlos Alves Pg41840

Paulo Bento a81139

Índice

Introdução 3

Controlo de Acesso & Modelo Bell-LaPadula 4

Propriedades do modelo 4

Lattice 5

Implementação do modelo numa típica infraestrutura TIC 6

Conclusão 7

Referências 8

Introdução

Este trabalho prático, sugerido em aula na unidade curricular Segurança em Redes tem como objetivo construir um modelo de um sistema de Controlo de acesso baseado no modelo *Bell - LaPadula*, isto no contexto de uma universidade.

Seguindo o enunciado, é nos mencionado os três níveis de segurança (Publico(P), Confidencial(C) e Estritamente Confidencial (SC)) e ainda as categorias (Serviços Académicos (AS) e ScS (Serviços científicos)). Deste modo é nos referido no enunciado para "seguirmos" as propriedades fundamentais do modelo *Bell – LaPadula*. Para tal, foi necessário que todos os elementos do grupo compreendessem os aspetos formais do modelo BLP.

Deste modo, a estrutura deste relatório (Trabalho prático) será a seguinte:

- Modelo *Bell – LaPadula* e Controlo de acesso;
- Controlo de acesso de uma universidade baseado no modelo *Bell – LaPadula*;
- Implementação do modelo numa típica infraestrutura TIC.

Controlo de Acesso & Modelo Bell-LaPadula

Inicialmente, o modelo de *Bell – LaPadula* nada mais é que um modelo usado para impor o controlo de acesso em sistemas/aplicações. Este modelo centra-se principalmente na confidencialidade dos dados no controlo de acesso de um sistema, sejam eles dados confidenciais.

O modelo *Bell-LaPadula* melhora o acesso de controlo definindo regras de MAC (*Mandotory acess control*) para complementar o uso de DAC (*Discretionary Acess Control*). De forma a implementar o DAC usa-se uma ACLs (*Acess Control Lists*), também designado por *Acess Matrix*. A *Matrix* serve para os utilizadores definirem as permissões de leitura e escrita de cada tipo de sujeito para um determinado objeto. Através de um *Lattice* define-se o MAC. O *lattice* é composto pelas várias *Security Labels* que estão relacionadas por uma ordem parcial que indica em que direção a informação pode fluir. Definindo, assim, os vários níveis que só podem ser comparados caso exista um caminho de um para o outro.

Propriedades do modelo

- **Simple-Security property** - Um sujeito só pode ler objetos que estão num nível inferior ou igual ao que este se encontra.
- **Star-property** - Um sujeito só pode escrever num objeto que se encontre num nível igual ao superior ao do sujeito

Utiliza uma matriz de acesso para especificar o controlo de acesso arbitrário.(Não abordado neste relatório)

Resumidamente, o modelo BLP é caraterizado por: *"não leia-para-cima, não escreva-para-baixo".*

Um exemplo para melhor compreensão é o caso do modelo militar: onde temos ***Top Secret***, ***Secret*** e ***public***. Aqui quem tiver no nível do ***Secret*** apenas pode escrever no seu nível ou para cima, mas nunca para baixo, isto é, um pesquisador pode criar arquivos ***top secret*** mas não pode criar ficheiros **públicos**. Invés disso, os usuários podem ver o conteúdo do seu nível ou abaixo do seu nível de segurança, exemplo, um pesquisador secreto pode ver arquivos secretos e públicos, mas não pode ver os arquivos ***Top secrets***.

Lattice

A **Star property** pode ser modificada para impedir modificação e destruição de objetos em níveis superiores por sujeitos em nível inferiores restringindo o *Write Acess* só para objetos no mesmo nível que o sujeito. No caso do estudo no contexto de uma universidade contempla três níveis de segurança (P-publico, C-confidencial, SC-estritamente confidencial) que tem ordem P<C<SC como visto na Figura 1.

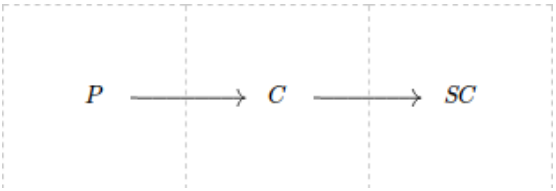

Figura 1 – Publico/Confidencial/Estritamente Confidencial lattice

Ainda podendo os objetos e sujeitos cair em duas Categorias AS (Serviços Académicos), ScS (Serviços científicos) que encontram representadas na Figura-2 todas as combinações possíveis e a sua ordem. Finalmente, combinando os dois *Lattices* anteriormente mencionados pode formar-se o *Lattice* completo presente na Figura-3.

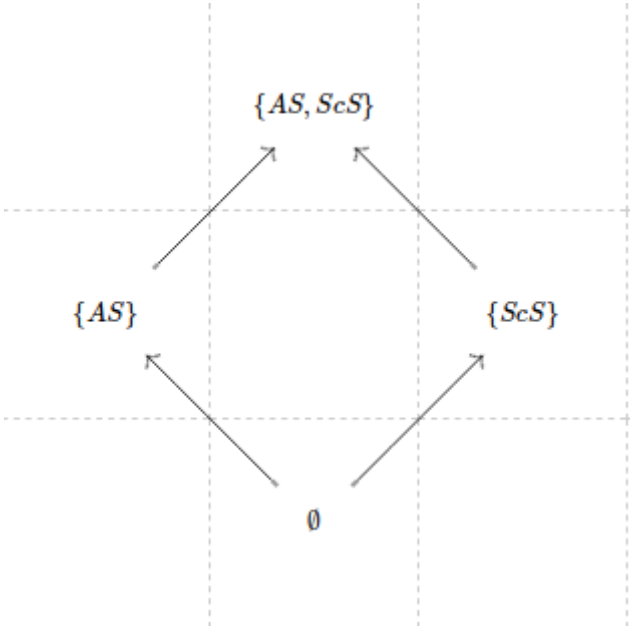

Figura 2 - Categorias

O *Lattice* completo contem várias ligações que neste contexto podem fazer ou não sentido. Dado que as combinações entre níveis e categorias não são muitas, considerar-se-á todos os possíveis. Podendo assim gerar o *Lattice* presente da Figura 3. A relação representada no *Lattice* é A -> B (A é dominado por B). A imagem "aumenta" o nível de segurança na horizontal da esquerda para a direita. E "adiciona" categorias na vertical.

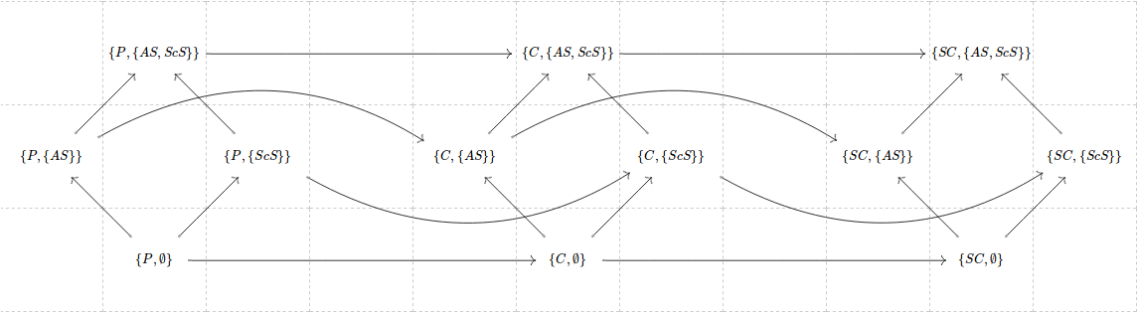

Figura 3 – Lattice Completo

Implementação do modelo numa típica infraestrutura TIC

Para implementar este modelo numa infraestrutura podia se usar como suporte a linguagem XACML para definir as diferentes *Labels* que existem. Usando as designações da linguagem definia-se os diferentes *Roles* correspondentes a cada *Label*. Posteriormente, podia-se, por exemplo, criar um script que le o XACML anteriormente criado. Esse script criaria (Assumindo um sistema UNIX) vários grupos relativos a cada *Role*/*Label* definido no **XACML** como também *Access Control Lists* para cada *Label* do modelo. Finalmente cada novo utilizador criado, pertenceria a um destes grupos que poderia realizar a operação requerida, conforme estivesse definido na ACL. Por exemplo, um ficheiro na *Label* {C,{AS,ScS}} teria um ACL associado com este conteúdo:

```
# file: example.txt
# owner: user1
# group: P_AS_ScS
user::rw-
group::rw-
group:P_AS:-w-
group:P_Scs:-w-
group:P_:-w-
group:C-AS-ScS:r--
group:SC-AS-ScS:r--
other::---
```

Figura 4 - ACL para um ficheiro da Label {C,{AS,ScS}}

Conclusão

Concluindo este trabalho prático, sugerido em aula na unidade curricular Segurança em Redes que tinha como objetivo construir um modelo de um sistema de Controlo de acesso baseado no modelo *Bell - LaPadula*, isto no contexto de uma universidade. Achamos que foi de grande valia, pois tivemos a oportunidade de aprofundar os nossos conhecimentos nos aspetos formais do modelo BLP, e ainda em Controlo de acessos.

Inicialmente surgiram algumas dificuldades em saber se estávamos a fazer o que era pretendido, mas principalmente na questão da implementação do modelo numa infraestrutura TIC.

Por fim, achamos que atingimos todos os objetivos pretendidos a alcançar neste trabalho, deste modo, conseguimos apresentar uma visão geral do modelo em questão, dos Controlos de Acessos e isto no contexto de uma universidade.

Referências

Clarkson, M. (2001). *cs. cornell.* Obtido de http://www.cs.cornell.edu/courses/cs5430/2011sp/NL.accessControl.html

University Purdue. (s.d.). Obtido de University Purdue: https://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/handouts/426_Fall10_lect21.pdf