

Modelo Bell-LaPadula

Alexandra Amaro

Bell-LaPadula

- O modelo Bell-LaPadula (abreviado BLP) é um modelo de [máquina de estado](#) usada para impor o controle de acesso em aplicações de governo e militares.
- Este modelo formal de transição de estado para políticas de segurança de computador descreve um conjunto de regras de controle de acesso que utiliza etiquetas de segurança em objetos e autorizações para os indivíduos.
- Este modelo formal de transição de estado para políticas de segurança de computador descreve um conjunto de regras de controle de acesso que utiliza etiquetas de segurança em objetos e autorizações para os indivíduos.
- O modelo Bell-LaPadula é um exemplo de um modelo onde não há uma clara distinção entre proteção e segurança

Características

- O modelo Bell-LaPadula centra-se na confidencialidade dos dados e controle de acesso à informação classificada. Neste modelo formal, as entidades em um sistema de informação são divididas em sujeitos e objetos. A noção de um "estado seguro" é definida e está provada que cada transição de estado preserva a segurança ao passar de um estado seguro para outro estado seguro, assim, por indução matemática, provando que o sistema atende aos objetivos de segurança do modelo. O modelo Bell-LaPadula é construído sobre o conceito de uma máquina de estados finitos com um conjunto de estados permitidos em um sistema de rede de computadores. A transição de um estado para outro é definida por funções de transição.
- Um estado do sistema é definido como "seguro" se apenas os modos de acesso permitidos entre sujeitos e objetos estão em conformidade com uma política de segurança. Para determinar se um modo de acesso específico é permitido, o despacho de um sujeito é comparado com a classificação do objeto (mais precisamente, a combinação de classificação e um conjunto de compartimentos, tornando-se o nível de segurança) para determinar se o sujeito é autorizado para o modo de acesso específico. O esquema de apuramento/classificação é expresso em termos de uma treliça/matrix.

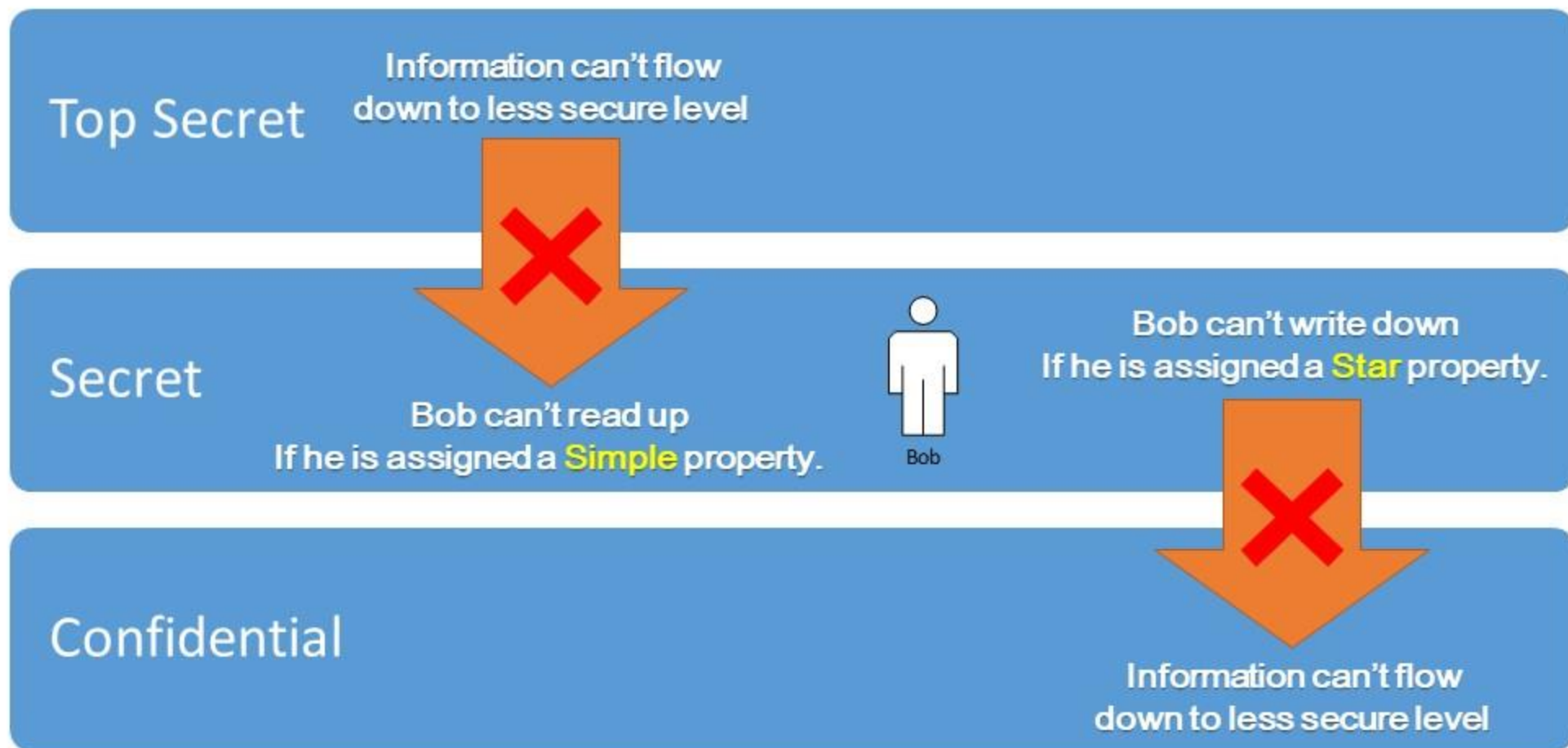
Bell-LaPadula

- O modelo define duas regras de controle de acesso obrigatório (MAC) e uma regra de controle de acesso discricionário (DAC) com três propriedades de segurança:
- Propriedade de Segurança Simples - um sujeito em um dado nível de segurança não pode ler um objeto com um nível de segurança mais alto (não ler-para-cima).
- A Propriedade-★ (leia-se propriedade-estrela) - um sujeito em um dado nível de segurança não deve escrever para qualquer objeto em um nível inferior de segurança (não escrever-para-abaixo). A Propriedade-★ também é conhecida como a propriedade de confinamento.
- A Propriedade de Segurança Discricionária - utiliza uma matriz de acesso para especificar o controle de acesso discricionário.

Bell-LaPadula

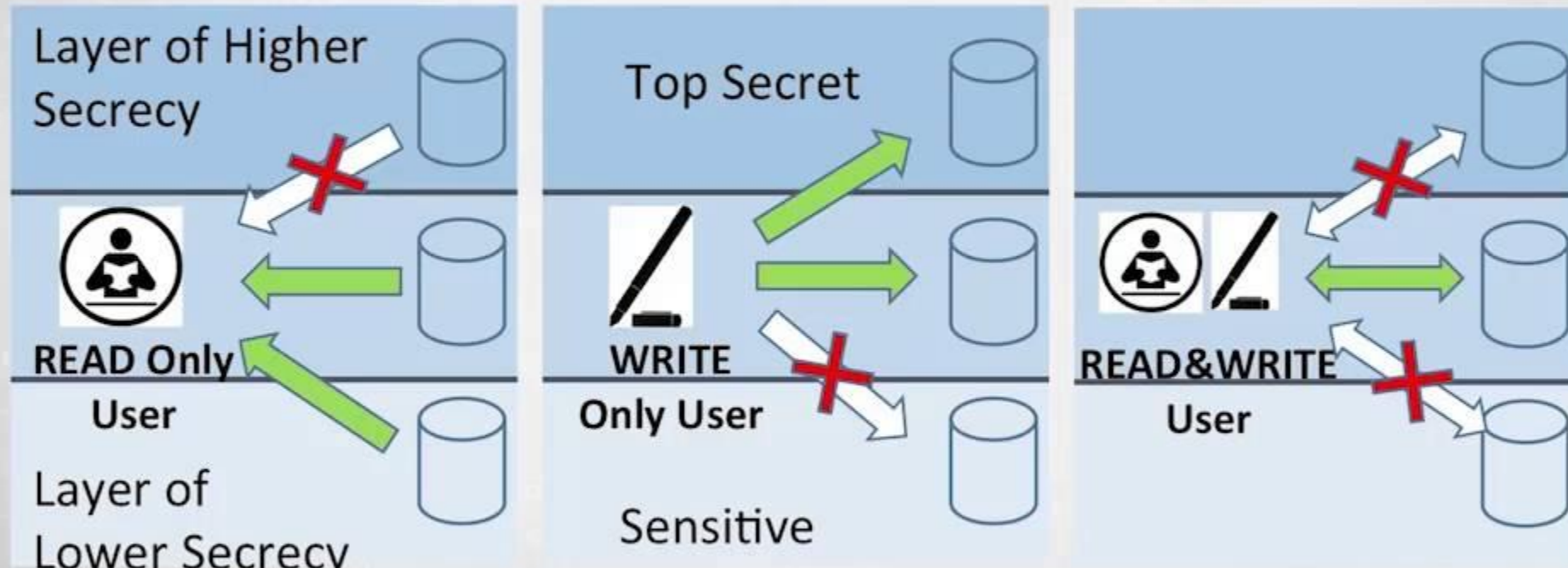
- O modelo Bell-LaPadula define seu escopo explicitamente. Ele não trata extensivamente os seguintes pontos:
- Canais secretos. A passagem de informação através de ações pré-arranjadas foi ligeiramente descrita.
- As redes de sistemas. Trabalho de modelagem mais tarde abordou este tema.
- Políticas fora da segurança multi-nível. Trabalhos no início de 1990 mostraram que MLS é uma versão de política booleana, assim como todas as outras políticas publicadas.

Bell-LaPadula Model



Bell-LaPadula Confidentiality Model - Lattice

User restriction is No read up and No write down
No stealing of Secrets – No divulging of secrets



Simple Security Property
Simple is Reading
Loading from a disk

*(star) Property
Star is writing
Saving to a disk

Strong *Property
Only same level

