Sistemas de controle de acesso

No início dos tempos da computação, pode-se dizer que a segurança não era prioridade na lista de tarefas de ninguém. Na verdade, na maioria dos casos, a segurança nem sequer era uma ideia existente. A triste verdade sobre segurança é que ela saiu de uma postura reativa e foi feito pouco esforço de forma proativo até recentemente.

Isso não quer dizer que ninguém tenha tentado. Na realidade, em 1983, o Departamento de Defesa dos EUA viram a necessidade de proteção da informação (governamental) e trabalharam com a NSA para criar o National Computer Security Center (NCSC). Este grupo reuniu-se e criou todos os tipos de manuais de segurança e etapas, e publicou-os em uma série de livros conhecida como a "Rainbow Series". A peça central deste esforço saiu o "Orange Book", que realizou algo conhecido como o Trusted Computer System Evaluation Criteria (TCSEC).

O TCSEC era um padrão do Departamento de Defesa do Governo dos Estados Unidos (DoD), com o objetivo de estabelecer requisitos básicos para testar a eficácia dos controles de segurança do computador incorporados em um sistema de computador. A ideia era simples: se seu sistema de computador (rede) fosse lidar com informações classificadas, ele precisava cumprir com as configurações básicas de segurança. TCSEC definiu como avaliar se esses controles estavam sendo aplicados. As configurações, avaliações e avisos no Orange Book foram bem pensados (para o seu tempo) e provaram seu valor ao longo do tempo, sobrevivendo até 2005. No entanto, como qualquer um em segurança pode dizer, nada dura para sempre.

TCSEC eventualmente deu lugar ao Common Criteria for Information Technology Security Evaluation (também conhecido como Common Criteria, ou CC). Os CC tinham realmente existido

desde 1999 e, finalmente, tiveram precedência em 2005. Forneceu uma maneira para os fornecedores de fazer alegações sobre a sua segurança, seguindo um conjunto de padrões de controles e métodos de testes, resultando em algo chamado Nível de Garantia de Avaliação (Evaluation Assurance Level – EAL). Por exemplo, um fornecedor pode criar uma ferramenta, aplicativo ou sistema de computador e deseja fazer uma declaração de segurança. Seguiriam então os controles e os procedimentos de teste para ter seu sistema testado no EAL (níveis 1-7) que desejaram ter. Assumindo que o teste foi bem sucedido, o fornecedor poderia reivindicar "Testado com êxito na EAL-4".

Common Criteria é, basicamente, um padrão de teste projetado para reduzir ou remover vulnerabilidades de um produto antes de ser lançado. Além de EAL, três outros termos estão associados que precisamos lembrar:

- Target of Evaluation (TOE) – O que está sendo testado;
- Security target (ST) – A documentação que descreve o TOE e os requisitos de segurança;
- Perfil de proteção (PP) – Um conjunto de requisitos de segurança especificamente para o tipo de produto testado.

Embora haja muito mais, basta dizer que o CC foi projetado para fornecer uma garantia de que o sistema é projetado, implementado e testado de acordo com um nível de segurança específico. É usado como a base para certificações do governo e é testado geralmente para agências de governo dos E.U.A.

Por fim, em nossa excursão através de terminologia e história sobre segurança e testes, temos alguns termos para lidar. Um deles é o conceito geral de controle de acesso em si. Controle de acesso basicamente significa restringir o acesso a um recurso de alguma maneira seletiva. Aqui, vamos apenas falar sobre algumas maneiras de implementar o controle de acesso: obrigatório e discricionário.

Controle de acesso obrigatório (Mandatory Access Control – MAC) é um método de controle de acesso onde a diretiva de segurança é controlada por um administrador de segurança: os usuários não podem definir controles de acesso próprios. No MAC, o sistema operacional restringe a capacidade de uma entidade acessar um recurso (ou executar algum tipo de tarefa dentro do sistema). Por exemplo, uma entidade (como um processo) pode tentar acessar ou alterar um objeto (como arquivos, portas TCP ou UDP, e assim por diante). Quando isso ocorre, um conjunto de atributos de segurança (definido pelo administrador da diretiva) é examinado por uma regra de autorização. Se os atributos apropriados estiverem no lugar, a ação é permitida.

Em contrapartida, o controle de acesso discricionário (Discretionary Access Control – DAC) coloca uma grande parte deste poder nas mãos dos próprios usuários. O DAC permite que os usuários definam controles de acesso nos recursos que possuem ou controlam. Definido pelo TCSEC como um meio de "restringir o acesso a objetos com base na identidade de sujeitos e/ou grupos aos quais eles pertencem", a ideia é que os controles são discricionários no sentido de que um sujeito com uma certa permissão de acesso é capaz de passar essa permissão (talvez indiretamente) para qualquer outro objeto (a menos que restringido pelo controle de acesso obrigatório). Alguns exemplos de DAC incluem permissões NTFS em máquinas Windows e o uso de usuários, grupos e permissões de leitura-gravação-execução do Unix.

Sugestões de livros: