Introdução

Este artigo é focado em fornecer orientações claras, simples e acionáveis para fornecer segurança de controle de acesso em seus aplicativos. O objetivo é fornecer orientação para desenvolvedores, revisores, designers, arquitetos sobre como projetar, criar e manter controles de acesso em aplicativos da Web.

O que é controle de acesso / autorização?

Autorização é o processo em que as solicitações para acessar um recurso específico devem ser concedidas ou negadas. Deve-se notar que a autorização não é equivalente a autenticação - pois esses termos e suas definições são freqüentemente confundidos. Autenticação é fornecer e validar identidade. A autorização inclui as regras de execução que determinam quais funcionalidades e dados o usuário (ou o Principal) pode acessar, garantindo a alocação adequada dos direitos de acesso após a autenticação ser bem-sucedida.

Aplicativos da Web precisam de controles de acesso para permitir que usuários (com privilégios variados) usem o aplicativo. Eles também precisam de administradores para gerenciar as regras de controle de acesso de aplicativos e a concessão de permissões ou direitos a usuários e outras entidades. Várias metodologias de design de controle de acesso estão disponíveis. Para escolher a mais apropriada, é necessário realizar uma avaliação de risco para identificar ameaças e vulnerabilidades específicas de seu aplicativo, para que a metodologia apropriada de controle de acesso seja apropriada para sua aplicação.

Política de Controle de Acesso

Por que precisamos de uma política de controle de acesso para o desenvolvimento da web?

A intenção de ter uma política de controle de acesso é garantir que os requisitos de segurança sejam descritos claramente para arquitetos, designers, desenvolvedores e equipe de suporte, de modo que a funcionalidade de controle de acesso seja projetada e implementada de maneira consistente.

Controle de acesso baseado em função (RBAC)

No Controle de Acesso Baseado em Função (RBAC), as decisões de acesso são baseadas nas funções e responsabilidades de um indivíduo dentro da organização ou base de usuários.

O processo de definição de papéis é geralmente baseado na análise dos objetivos e estrutura fundamentais de uma organização e geralmente está vinculado à política de segurança. Por exemplo, em uma organização médica, os diferentes papéis dos usuários podem incluir aqueles como médico, enfermeiro, atendente, enfermeiro, pacientes, etc. Obviamente, esses membros requerem diferentes níveis de acesso para desempenhar suas funções, mas também os tipos de transações na web e seu contexto permitido variam muito dependendo da política de segurança e de quaisquer regulamentos relevantes (HIPAA, Gramm-Leach-Bliley, etc.).

Uma estrutura de controle de acesso do RBAC deve fornecer aos administradores de segurança de aplicativos da Web a capacidade de determinar quem pode executar quais ações, quando, de onde, em que ordem e, em alguns casos, em que circunstâncias relacionais.

As vantagens de usar essa metodologia são:

- Os papéis são atribuídos com base na estrutura organizacional, com ênfase na política de segurança organizacional
- Fácil de usar
- Fácil de administrar
- Construído na maioria dos frameworks
- Alinha-se a princípios de segurança, como segregação de funções e menos privilégios

Problemas que podem ser encontrados ao usar esta metodologia:

- A documentação das funções e acessos deve ser mantida de forma rigorosa.
- A multilocação não pode ser implementada com eficácia, a menos que haja uma maneira de associar as funções a requisitos de recursos de multilocação, por exemplo, OU no Active Directory
- Existe uma tendência para que o escorregamento de escopo aconteça, por exemplo, mais acessos e privilégios podem ser dados do que o pretendido. Ou um usuário pode ser incluído em duas funções se as revisões de acesso adequadas e a revogação subsequente não forem executadas.
- Não suporta controle de acesso baseado em dados

As áreas de cautela ao usar o RBAC são:

- Os papéis devem ser transferidos ou delegados somente usando procedimentos e assinaturas rigorosas.
- Quando um usuário altera sua função para outra, o administrador deve certificar-se de que o acesso anterior seja revogado, de modo que, em qualquer momento, um usuário seja atribuído apenas àquelas funções que precisam saber.
- A garantia para o RBAC deve ser realizada usando revisões rigorosas de controle de acesso.

Controle de Acesso Discricionário (DAC)

Discretionary Access Control (DAC) é um meio de restringir o acesso a informações com base na identidade dos usuários e / ou membros de determinados grupos. As decisões de acesso geralmente são baseadas nas autorizações concedidas a um usuário com base nas credenciais que ele apresentou no momento da autenticação (nome de usuário, senha, token de hardware / software, etc.). Na maioria dos modelos típicos de DAC, o proprietário da informação ou qualquer recurso é capaz de alterar suas permissões a seu critério (daí o nome).

Uma estrutura DAC pode fornecer aos administradores de segurança de aplicativos da Web a capacidade de implementar controle de acesso refinado. Este modelo pode ser uma base para implementação de controle de acesso baseado em dados

As vantagens de usar este modelo são:

- Fácil de usar
- Fácil de administrar
- Alinha-se ao princípio dos privilégios mínimos.
- O proprietário do objeto tem controle total sobre o acesso concedido

Problemas que podem ser encontrados ao usar esta metodologia:

- A documentação das funções e acessos deve ser mantida de forma rigorosa.
- A multilocação não pode ser implementada com eficácia, a menos que haja uma maneira de associar as funções a requisitos de recursos de multilocação, por exemplo, OU no Active Directory
- Existe uma tendência para que o escorregamento de escopo aconteça, por exemplo, mais acessos e privilégios podem ser dados do que o pretendido.

As áreas de cautela ao usar o DAC são:

- Ao conceder trusts
- A garantia para o DAC deve ser realizada usando revisões rigorosas de controle de acesso.

Controle de Acesso Obrigatório (MAC)

O Controle de Acesso Obrigatório (MAC) garante que a aplicação da política de segurança organizacional não depende da conformidade voluntária do usuário do aplicativo da web. O MAC protege as informações atribuindo rótulos de sensibilidade às informações e comparando-as com o nível de sensibilidade em que o usuário está operando. O MAC é geralmente apropriado para sistemas extremamente seguros, incluindo aplicações militares seguras de vários níveis ou aplicativos de dados de missão crítica.

As vantagens de usar essa metodologia são:

- O acesso a um objeto é baseado na sensibilidade do objeto
- Acesso baseado na necessidade de saber é estritamente respeitado e o escopo do escopo tem possibilidades mínimas
- Apenas um administrador pode conceder acesso

Problemas que podem ser encontrados ao usar esta metodologia:

- Difícil e caro para implementar
- Não é ágil

As áreas de cautela ao usar o MAC são:

- Classificação e atribuição de sensibilidade a um nível adequado e pragmático
- A garantia para MAC deve ser realizada para garantir que a classificação dos objetos esteja no nível apropriado.

Controle de Acesso Baseado em Permissão

O conceito de chave no Controle de Acesso Baseado em Permissão é a abstração de ações do aplicativo em um conjunto de *permissões* . Uma *permissão* pode ser representada simplesmente como um nome baseado em string, por exemplo "READ". As decisões de acesso são feitas verificando se o usuário atual *tem* a permissão associada à ação solicitada do aplicativo.

A *tem* relacionamento entre o utilizador e autorização pode ser satisfeito através da criação de uma relação directa entre o utilizador e autorização (chamado uma *concessão*), ou um indireto. No modelo indireto, a *concessão de* permissão é para uma entidade intermediária, como *um grupo de usuários* . Um usuário é considerado um membro de um *grupo de usuários* se e somente se o usuário *herdar* permissões do *grupo de usuários* . O modelo indireto facilita o gerenciamento das permissões para um grande número de usuários, já que a alteração das permissões atribuídas ao grupo de usuários afeta todos os membros do grupo de usuários.

Em alguns sistemas de Controle de Acesso com Base na Permissão que fornecem controle de acesso de nível de objeto de domínio refinado, as permissões podem ser agrupadas em *classes* . Neste modelo, assume-se que cada objeto de domínio no sistema pode ser associado a uma *classe* que determina as permissões aplicáveis ao respectivo objeto de domínio. Em tal sistema, uma classe "DOCUMENT" pode ser definida com as permissões "READ", "WRITE" e DELETE "; uma classe" SERVER "pode ser definida com as permissões" START "," STOP "e" REBOOT ".

Autores e Editores Principais

Shruti Kulkarni - shruti.kulkarni@owasp.org

Adinath Raveendra Raj - adinath@acciente.com

Mennouchi Islam Azeddine - azeddine.mennouchi@owasp.org

Jim Manico - jim@owasp.org