6.0 - Controles de Acesso

prof. Fábio Engel

fabioe@utfpr.edu.br

Controles de Acesso

- **Controles de Acesso** são métodos usados para restringir acesso a certos ítens, como automóveis, casas, computadores ou mesmo telefone celular.
  - É o processo de proteger um recurso de modo que ele seja usado somente por aqueles com permissão. Eles protegem um recurso contra uso não autorizado.

Controles de Acesso

- Empresas utilizam controles de acesso para controlar o que funcionários podem ou não fazer.
- Controles de acesso definem quem são usuários (pessoas ou processos computacionais), o que eles podem fazer, quais recursos podem acessar e que operações podem realizar.
- Sistemas de controle de acesso utilizam várias tecnologias, incluindo senhas, geradores de códigos (tokens) de hardware, biometria e certificados.
- Acesso pode ser concedido a ativos físicos, como prédio ou salas, e a sistemas computacionais e dados.

As quatro partes de controle de acesso

- As quatro partes de controle de acesso são:
  - **Autorização** - Quem está aprovado para acessar e o que, exatamente, eles podem usar?
  - **Identificação** - Como eles são identificados?
  - **Autenticação** - Suas identidades podem ser verificadas?
  - **Responsabilização** - Como as ações de um indivíduo são acompanhadas de modo a garantir que a pessoa que faz mudanças em dados ou sistemas possa ser identificada? Esse processo de associar ações a usuários para posteriores relatórios e pesquisas é conhecido como **responsabilização**.

As quatro partes de controle de acesso

- Essas quatro partes são divididas em duas fases:
  - **A fase de definição de política** - Determina quem tem acesso e quais sistemas ou recursos podem usar. O processo de **autorização** opera nesta fase.
  - **A fase de imposição de política** - Concede ou rejeita solicitações de acesso com base nas autorizações definidas na primeira fase. Os processos de **identificação**, **autenticação** e **responsabilização** operam nesta fase.

Os dois tipos de controle de acesso

- Organizações controlam acesso a recursos em, principalmente, dois níveis:
  - **Controles de acesso físico** - Estes controlam entrada em prédios, áreas de estacionamento e áreas protegidas. Por exemplo, você provavelmente tem uma chave para a porta de seu escritório, que controla o acesso físico ao lugar.
  - **Controles de acesso lógico** - Estes controlam acesso a um sistema computacional ou rede. Sua empresa provavelmente exige que você informe um nome de usuário e uma senha exclusivos para efetuar acesso em computadores da empresa. Esse nome de usuário e essa senha permitem que você use o sistema computacional e recursos de rede da organização.

Os dois tipos de controle de acesso

- Controle de acesso físico
  - Por exemplo, um funcionário pode ter um cartão inteligente, programado com seu número de identificação, que lhe permite abrir uma porta para o estacionamento e passá-lo no elevador para sair do seu andar. E também passá-lo para entrar em seu escritório. Ou seja, a política de autorização da organização concede a este funcionário acesso físico a certos lugares.

Os dois tipos de controle de acesso

- Exemplos de Controle de acesso lógico
  - Decidir que usuários podem entrar em um sistema;
  - Monitorar o que o usuário faz nesse sistema;
  - Restringir ou influenciar o comportamento do usuário nesse sistema.

O Núcleo de Segurança

- O Núcleo de Segurança:
  - O núcleo (*kernel*) de segurança é a parte central de hardware, software e firmware de um ambiente de computação que impõe controle de acesso a sistemas computacionais.
  - Fornece um ponto central de controle de acesso e implementa o conceito de **monitor de referência**.

O Núcleo de Segurança

- O kernel atua como mediador para toda solicitação de acesso e permite acesso apenas quando as regras ou condições apropriadas são atendidas. Por exemplo:
  1. O sujeito solicita acesso a um objeto específico. O núcleo de segurança intercepta a solicitação.
  2. O núcleo de segurança consulta sua base de regras, também conhecida como **banco de dados do núcleo de segurança**. Ele usa essas regras para determinar direito de acesso, definidos de acordo com as políticas de sua organização.
  3. O núcleo permite ou nega acesso com base nas regras de acesso definidas. Toda solicitação de acesso tratada pelo sistema é registrada (*logged*) para posterior acompanhamento e análise.

Políticas de Controle de Acesso

- **Políticas de Controle de Acesso**
  - Uma política de controle de acesso é um conjunto de regras que permite a um grupo específico de usuários realizar um conjunto específico de ações sobre um conjunto específico de recursos.
  - Se os usuários não forem autorizados, não terão acesso a funções ou recursos de sistema.
  - Você utiliza políticas de controle de acesso para reduzir e controlar riscos de segurança. Tanto processos automatizados como seres humanos usam essas políticas.

Políticas de Controle de Acesso

- Você precisa entender quatro elementos centrais de acesso para gerenciar bem políticas de controle de acesso:
  - **Usuários** - Pessoas que usam o sistema.
  - **Recursos** - Objetos protegidos do sistema. Recursos só podem ser acessados por sujeitos autorizados e usados de formas autorizadas.
  - **Ações** - Atividades que usuários autorizados podem realizar sobre os recursos.
  - **Relacionamentos** - Condições opcionais que existem entre usuários e recursos. Relacionamentos são permissões concedidas a um usuário autorizado, como leitura, escrita, execução.

Definindo uma política de autorização

- Definindo uma política de autorização:
  - Para controlar o acesso é necessário criar uma política para definir regras de autorização, processo de decidir quem tem acesso a que recursos computacionais e de rede.
  - Na maioria das organizações, autorização baseia-se em funções de cargos, filtragem de perfil e quais requisitos de governos.
  - Essas condições ou políticas são decididas principalmente por uma **política de inclusão em grupo** ou uma **política em nível de autoridade**.

Definindo uma política de autorização

- Em uma **política de inclusão em grupo**, autorização é definida pelo(s) grupo(s) do(s) qual(is) você faz parte. Por exemplo, talvez apenas os cartões de segurança do pessoal do departamento de TI deem acesso à sala na qual o equipamento de computação é armazenado. Se você não for um membro desse grupo de TI, seu cartão de segurança não permitirá que você entre nessa sala.
- Em uma **política em nível de autoridade**, você precisará de um grau maior de autoridade para acessar certos recursos. Por exemplo, talvez apenas um membro de nível sênior do grupo de TI tenha permissão para entrar na sala que hospeda servidores. De modo que uma política pode especificar que somente um membro do pessoal sênior poderá entrar na sala de servidores.

Métodos e Diretrizes de identificação

- Métodos e Diretrizes de identificação
  - Uma vez que tenha definido as regras de autorização em uma política de autorização, você poderá impô-las. Todas vez que um usuário solicitar acesso a um recurso, os controles de acesso o concederão ou negarão com base na política de autorização.
  - O primeiro passo ao impor uma política de autorização é a **identificação**, método que um sujeito utiliza para solicitar acesso a um sistema ou recurso. Existem vários métodos normalmente utilizados para identificar sujeitos, veremos alguns a seguir.

Métodos de identificação

- Métodos de identificação
  - Um nome de usuário é o método de acesso mais comum para identificar um usuário em um sistema e pode estar na forma de um ID de usuário, um número de conta ou um número de identificação pessoal (PIN).
  - Alguns aplicativos identificam um usuário por meio de um cartão inteligente, que pode ter a forma de um cartão de crédito de plástico.
  - Biometria é outro método de controle de acesso para identificar sujeitos, usada para reconhecimento de pessoas com base em uma ou mais características físicas ou comportamentais. Exemplos, impressão digital, reconhecimento facial, de voz, DNA e retina.

Métodos e Diretrizes de identificação

- Diretrizes de Identificação
  - Para garantir todas as **ações** executadas em um sistemas computacional possam estar associadas a um usuário específico, cada usuário precisa ter um identificador exclusivo.
  - O processo de associar uma ação com usuários para posterior relatório ou análise é chamado de auditoria (*accounting*).
  - Você deverá manter atualizados os dados usados para identificar sujeitos e monitorá-los de perto e deverá desativar os IDS de usuários que saiam da organização ou que estejam inativos por um período prolongado.

Processos e Requisitos de Autenticação

- Processos e Requisitos de Autenticação
  - Na parte de controle de acesso conhecida por **autenticação**, um usuário valida ou prova a identidade fornecida durante a identificação.
  - A autenticação responde à pergunta: Os usuários são realmente quem dizem ser? A autenticação prova que o sujeito que solicita o acesso é o mesmo que recebeu direito de acesso.

Processos e Requisitos de Autenticação

- **Tipos de autenticação**
  - **Conhecimento** - Algo que você saiba, como uma senha, uma frase secreta ou um PIN.
  - **Propriedade** - Algo que você tenha, como um cartão inteligente, uma chave, um crachá ou um token.
  - **Características** - Algo exclusivo a você, como suas impressões digitais, sua retina ou sua assinatura. Como as características envolvidas normalmente são físicas, esse tipo de autenticação às vezes é definido como “algo que você é”.

Processos e Requisitos de Autenticação

- Cada tipo de autenticação pode ser facilmente comprometido por si só.
- O uso de controle de apenas uma categoria é conhecido como **autenticação de fator único**.
- Sistemas com informações sensíveis ou críticas deverão usar pelo menos dois dos três fatores.
  - O uso de técnicas de duas ou mais dessas categorias é chamado de **autenticação de fator duplo (TFA - Two Factor Authentication)** e fornece um nível mais alto de segurança que apenas um fator.

Autenticação por conhecimento

- **Autenticação por conhecimento**
  - Baseada em algo que você sabe, como uma senha.
  - Senhas são o método mais antigo e comum de autenticação para sistemas computacionais e também o método mais fraco.
  - Atacantes podem quebrar senhas a partir de:
    - Ataque de força bruta
    - Ataque de dicionário

Autenticação por conhecimento

- Melhores práticas de senha:
  - Não use senhas fracas.
  - Não guarde uma cópia escrita da senha, exceto se absolutamente necessário.
  - Nunca compartilhe senhas com outros.
  - Use diferentes senhas para importantes e diferentes contas de usuários.
  - Se você acha que uma senha foi comprometida, mude-a imediatamente.
  - Cuidado ao salvar senhas em computadores.
  - Escolha senhas difíceis de descobrir.

Autenticação por conhecimento

- Políticas de bloqueio de conta
  - Muitos sistemas são configurados para desativar um ID de usuário após certo número de tentativas de acesso fracassadas.
  - Em muitos casos, contas do usuário são desativadas após três a cinco tentativas. O número de tentativas de acesso fracassadas que dispara uma ação na conta é chamado de **limite (threshold)**.
  - O usuário pode ficar bloqueado por alguns minutos, algumas horas ou até que a conta seja reativada por um administrador de segurança.
  - Tome cuidado ao definir uma política de bloqueio de senha. Uma política rigorosa pode bloquear usuários autorizados não intencionalmente, o que pode ser frustrante e dispendioso.

Autenticação por conhecimento

- Auditoria de eventos de acesso
  - Um método de acompanhar quem está acessando sem ambiente de computação é auditar eventos de acesso, o que dará a você um registro de quando cada usuário entra ou sair em um computador.
  - Se um usuário não autorizado roubar a senha de um usuário e efetuar o acesso a um computador, você poderá determinar quando essa brecha de segurança ocorreu.
  - Ao fazer a auditoria você poderá ver se o evento de falha foi devido a usuário não autorizados ou a atacantes que tentaram acessar um computador ou sistema.

Autenticação por conhecimento

- Reativação e armazenamento de senha
  - Quando um usuário esquece uma senha ou quando ela precisa ser reativada pela central de atendimento, a nova senha deverá ser valida somente para um único acesso e deverá expirar em um curto período.

Autenticação por propriedade

- **Autenticação por propriedade**
  - É o segundo tipo de verificação e é baseada em algo que você tenha, como um cartão inteligente, uma chave, um crachá ou um token. Tokens podem ser síncronos ou assíncronos.
- **Tokens síncronos**
  - Usa um algoritmo que calcula um número tanto no servidor de autenticação como no dispositivo.
  - Ele mostra o número na tela do dispositivo, e o usuário informa esse número como um autenticador de acesso, da mesma forma que usaria uma senha.

Autenticação por propriedade

- Em um **sistema de sincronização baseado em tempo**, a hora atual é usada como valor de entrada. O token gera uma nova senha dinâmica (normalmente, a cada minuto), exibida na janela do token. Esse sistema requer que o relógio (*clock*) do token permaneça em sincronismo com o do servidor de autenticação. Se o relógio sair de sincronismo, o servidor poderá verificar por três ou quatro minutos antes ou depois da hora para detectar um deslocamento. Se a diferença se tornar muito grande, você terá de sincronizá-los novamente.

Autenticação por propriedade

- Em um **sistema de sincronização baseado em evento**, evita o problema de sincronismo de tempo, aumentando o valor de um contador a cada uso. O contador é o valor de entrada. O usuário pressiona um botão para gerar uma senha de única vez e depois a insere com seu PIN na estação de trabalho. Um problema comum com sistemas de sincronismo baseados em evento é que, quando um usuário cria uma senha usando o token, mas não usa a senha para acesso, o contador do servidor e o do token ficam fora de sincronismo.

Autenticação por propriedade

- **Autenticação continua** é usada por sistemas que validam continuamente o usuário. Isso em geral é feito com cartões de proximidade ou outros dispositivos que se comunicam continuamente com o sistema de controle de acesso. Se o usuário se afastar de seu computador e sair do alcance do detector de controle de acesso, o sistema bloqueará o computador.

Autenticação por propriedade

- **Tokens assíncronos** se parecem com calculadoras, sendo normalmente, do tamanho de um cartão de crédito. O servidor de autenticação emite um número de desafio, que o usuário digita. O token calcula uma resposta para o valor fornecido pelo servidor de autenticação. O usuário, então, responde ao servidor com o valor exibido no token.

Autenticação por propriedade

- **Tokens USB**
  - Utilizam tecnologia de infraestrutura de chave pública (PKI - *Public Key Infrastructure*) - por exemplo, um certificado assinado por uma autoridade de certificação confiável - e não oferecem senhas de única vez.
  - É um dispositivo de hardware, codificado com sua assinatura digital, que você conecta na porta USB do seu computador. Com ele, você não precisará digitar nada.
  - A presença da assinatura digital no token é suficiente para fornecer a prova de posse (algo que você tem).

Autenticação por propriedade

- **Cartão inteligente**
  - É um token com forma de um cartão de crédito, que contém um ou mais chips de microprocessadores que aceitam, armazenam e enviam informações por meio de uma leitora.
  - A informação contida no cartão inteligente fornece informações de autenticação.
  - IDs e dados de autenticação não são transmitidos para um servidor remoto, evitando assim o problema do "caminho confiável".

Autenticação por características

- **Autenticação por Características/Biometria**
  - Biometria envolve medir várias partes exclusivas de anatomia ou de atividades físicas de uma pessoa e pode ser usada para identificação (biometria física) e autenticação (biometria lógica).
  - As oito medidas biométricas comuns pode ser divididas em:
    - Estática (por exemplo, fisiológica) - O que você é. Inclui reconhecimento de digitais, granularidade da íris e assim por diante.
    - Dinâmica (por exemplo, comportamental) - O que você faz. Inclui inflexões de voz, toques de teclado e movimentos de assinatura.

Autenticação por características

- Preocupações em torno de biometria:
  - Precisão - Dispositivos biométricos não são perfeitos.
  - Aceitação - Certas medições biométricas, como varredura de retina, são mais questionáveis para alguns usuários.
  - Tempo de reação - Tempo para que o sistema verifique uma identidade e dê uma resposta.

Autenticação por características

- Tipos de biometria:
  - Impressão digital - Examina o padrão de cristas e vales na ponta de um dedo. Altamente preciso.
  - Impressão da palma - Examina a estrutura física da palma da mão. Altamente preciso.
  - Geometria da mão - São necessários duas câmeras para analisar comprimento, largura, espessura e o contorno dos dedos. Altamente preciso.
  - Varredura de retina - Analisa o padrão de vasos sanguíneos da parte posterior da área do olho, conhecida como retina. Altamente precisa, porém, suscetível a mudanças na condição física como aquelas causadas por diabetes, gravidez e ataques do coração.

Autenticação por características

- Tipos de biometria:
  - Varredura da íris - Usa gravador para registrar padrões exclusivos na parte colorida do olho, conhecida como íris, causada por estrias, buracos, fissuras, fibras e assim por diante. Altamente preciso.
  - Reconhecimento de face - Câmeras de vídeo medem certas características da face, como a distância entre os olhos, a forma do queixo e do maxilar, o comprimento e a largura do nariz, a forma dos ossos da face e assim por diante.
  - Padrão de voz - São capturados até sete parâmetros dos tons nasais, vibrações de laringe e garganta e pressão de ar da voz. Não é preciso pois pode ser replicado por software.

Autenticação por características

- Tipos de biometria:
  - Dinâmica de toque na tecla - Aqui, um usuário digita uma frase selecionada em um modelo de referência. A dinâmica de toque na tecla mede o tempo de permanência de cada tecla (tempo pressionada) e o tempo de vôo (tempo entre toques de tecla). É considerada muito precisa e funciona bem para autenticação de fator duplo.
  - Dinâmica de assinatura - Com esse tipo de biometria, sensores em uma caneta ou tables são usados para registrar velocidade, direção e pressão de traçado da caneta. É precisa e usuários aceitam bem.

Autenticação por características

- Vantagens da biometria:
  - Uma pessoa precisa estar fisicamente presente para autenticar;
  - Não há o que lembrar;
  - Biometria é difícil de falsificar;
  - IDs perdidos ou senhas esquecidas não são problema.

Autenticação por características

- Desvantagens da biometria:
  - Características físicas podem mudar;
  - Usuários com deficiência podem ter dificuldade com alguns sistemas biométricos;
  - Nem todas as técnicas são igualmente efetivas, e normalmente é difícil decidir qual é a melhor para determinado uso;
  - Tempos de resposta podem ser lentos;
  - Custo da tecnologia.
  - Questões de privacidade

Single Sign-On (SSO)

- Uma estratégia de assinatura única (SSO - *Single Sign-On*) permite que usuários sejam autenticado em um computador ou rede uma vez e tenham sua identificação e credenciais de autorização permitidas em todos os computadores e sistemas nos quais estejam autorizados.
  - Eles não precisam entrar com vários IDs de usuários ou senhas.
  - A SSO reduz erro humano.

Single Sign-On (SSO)

- Vantagens de SSO incluem:
  - Ser um processo eficiente de acesso, usuário acessa apenas uma vez.
  - Pode lidar com senhas mais fortes, uma vez que o usuário precisa lembrar de apenas uma senha.
  - Fornece nova autenticação contínua e clara. O servidor SSO permanece em contato com a estação de trabalho e monitora sua atividade.
  - Fornece limites e bloqueios para tentativas de acesso com falha.
  - Fornece administração centralizada.

Single Sign-On (SSO)

- As desvantagens de SSO incluem:
  - Uma senha comprometida permite que um intruso entre em todas as áreas abertas ao proprietário da senha.
  - Senhas estáticas fornecem segurança muito limitada. Deve-se utilizar autenticação de fator duplo.
  - Incluir SSO em computadores isolados ou sistemas legados na rede pode ser difícil.
  - O servidor de autenticação pode se tornar um único ponto de falha para acesso a sistemas.

Single Sign-On (SSO)

- Alguns exemplos de processos de SSO são o processo Kerberos e o SESAME.
  - **Kerberos** - Protocolo de autenticação de rede. Permite autenticação segura em uma rede não segura.
  - **SESAME** - Sistema Europeu Seguro para Aplicativos em um Ambiente Multivendedor (*Secure European System for Applications in a Multi-Vendor Environment*) - é basicamente uma extensão do Kerberos e oferece capacidades de criptografia de chave pública.

Políticas e Procedimentos de Responsabilização

- Neste ponto já vimos como usuários são autorizados, identificados e autenticados. Chegamos a última parte do processo de controle de acesso: responsabilização.
- **Responsabilização** é o acompanhamento da ação de uma pessoa ou processo para saber quem fez as mudanças no sistema ou nos dados.
- Isto é importante para auditorias e investigações, bem como para rastrear erros e enganos.

Políticas e Procedimentos de Responsabilização

- Arquivos de Histórico:
  - Arquivos de histórico (*log files*), os registros que detalham quem acessou um sistema, quando e quais recursos ou informações foram usados, são um ingrediente-chave para responsabilização.

Retenção de dados, descarte de mídia e requisitos de conformidade

- Retenção de dados
  - Muitos países possuem medidas para proteger muitos tipos de dados. Por exemplo:
    - Para proteger a privacidade de dados de saúde pessoal, oferecendo certos direitos ao pacientes em relação as essas informações.
    - Exigindo que qualquer entidade que mantenha dados pessoais de consumidores para fins comerciais os destrua antes de descartá-los.

Retenção de dados, descarte de mídia e requisitos de conformidade

- Requisitos de descarte de mídia
  - É importante garantir que nenhum dado vaze de uma organização em mídia descartada.
  - Formas para o descarte:
    - Destruição física;
    - Desmagnetizando (para discos magnéticos);
    - Escrita repetida.

Modelos Formais de Controle de Acesso

- Como existem muitas maneiras de restringir acesso a diferentes recursos, é útil referir a modelos para ajudar a projetar bons controles de acesso.
- Existem vários modelos formais de controle de acesso, incluindo os seguintes:
  - **Controle de acesso discricionário (DAC - Discretionay Access Control)** - O proprietário do recurso decide quem entra e muda permissões conforme a necessidade. O proprietário pode delegar essa tarefa a outros.
  - **Controle de acesso obrigatório (MAC - Mandatory Access Control)** - A permissão para entrar em um sistema é mantida pelo proprietário e não pode ser dada a outros. Isso torna o MAC mais forte que o DAC.
  - **Controle de acesso não discricionário** - São monitorados de perto pelo administrador de segurança e não pelo administrador de sistema.
  - **Controle de acesso baseado em regra** - Uma lista de regras, mantidas pelo proprietário dos dados, determina que usuários têm acesso a objetos.

Controle de Acesso Centralizado e Descentralizado

- Controle de Acesso Centralizado
  - Abordagem na qual uma única entidade comum decide quem pode entrar em sistemas e redes.
  - Os controles de acesso são gerenciados de forma central em vez de no nível local.
  - Proprietários decidem que usuários podem chegar a que objetos.
  - Serviços de autenticação centralizados são aplicados e impostos pelo uso de servidores de autenticação, autorização e auditoria (AAA - *Authentication, Authorization, Accounting*).

- **RADIUS**
  - É o serviço de AAA mais popular. É um servidor de autenticação que usa dois arquivos de configuração:
    - Um arquivo de configuração de cliente contém seu endereço e o segredo compartilhado para autenticação de transação.
    - Um arquivo de configuração de usuário contém os dados de identificação e autenticação de usuário, bem como as informações de conexão e autorização.

Controle de Acesso Centralizado e Descentralizado

- RADIUS segue estas etapas no processo de autenticação:
  1. O servidor de acesso à rede (NAS - *Network Access Server*) decifra a solicitação de acesso de UDP de usuário;
  2. O NAS autentica a origem;
  3. O NAS valida a solicitação de acordo com o arquivo de usuário;
  4. O NAS responde, permitindo ou rejeitando acesso ou solicitando mais informações.

Controle de Acesso Centralizado e Descentralizado

- Controle de acesso descentralizado
  - O controle está nas mãos das pessoas, como gerentes de departamento, mais próximos dos usuários do sistema. Solicitações de acesso não são processadas por uma entidade centralizada.
  - Normalmente resulta em confusão, pois, pode levar à perda de padronização e a à sobreposição de direitos, o que pode causar lacunas no projeto de controle de acesso. Por outro lado, elimina o problema de um único ponto de falha.
  - Exemplos mais comums:
    - PAP - *Password Authentication Protocol* - usa nomes de usuários e senhas em texto claro;
    - CHAP - *Challenge-Handshake Authentication Protocol* - Fragmenta (hashes) a senha com um número de desafio de única vez, a fim de combater ataques de retransmissão baseados em interceptação

Referências

- Fundamentos de Segurança de Sistemas de Informação - David Kim; Michael G. Solomon