INFRAESTRUTURA PARA SISTEMAS DE SOFTWARE

Controle de Acesso e Mecanismos de Autenticação

ROTEIRO

- Introdução
- Definições
- Classificação do Controle de Acesso
- Identificação, autenticação, autorização
- Mecanismos de autenticação
- Modelos de Controle de Acesso
- Gerência de Identidades

INTRODUÇÃO

- O controle de acesso é um importante mecanismo para a segurança de aplicações
  - Atualmente, aquelas implantadas em nuvens computaciona

- Responsabilidade:
  - Quais recursos podem ser acessados
  - Quais operações podem ser realizadas sobre os recursos
  - Quais os componentes estão autorizados a desempenhar determinadas operações

DEFINIÇÕES

- O controle de acesso pode também ser definido como um método ou conjunto deles, cujo objetivo é restringir a utilizaçã determinados recursos a um sistema por certos usuários ou grupos de usuários

- Visa limitar as ações que um usuário de um sistema pode rea no ambiente

- Capacidade de permitir ou negar a utilização de algo por algu

- Prevenir que o sistema/aplicação esteja em ou vá para um estado inseguro.

DEFINIÇÕES

- Alguns requisitos básicos de segurança da informação que também se aplicam ao desenvolvimento de software na nuvem envolvem:
  - Disponibilidade
    - Ter certeza de que os dados estão acessíveis quando forem necessários e onde forem necessários
  - Integridade
    - Ter certeza de que os dados não foram modificados intencionalmente ou acidentalmente
  - Confidencialidade
    - Somente os indivíduos autorizados a acessar os dados podem fazê-lo

DEFINIÇÕES

- **Elementos para garantir:**
  - Disponibilidade
    - Redundância
    - Backup
  - Integridade
    - Assinatura digital
  - Confidencialidade
    - Criptografia e controle de acesso

CLASSIFICAÇÃO DO CONTROLE DE ACESSO

- Baseada em:
  - Hosts
    - Controle de acesso aos recursos do sistema operacional
    - Proteção de arquivos e objetos
    - Controla recursos via rede
  - Sistemas
    - Atuam dentro de hosts (composto por uma interface e um banco dados)
    - Com mecanismos próprios de controle
  - Rede
    - Implementados por meio de firewalls: filtros de pacotes e prox
    - Roteadores, switches

IDENTIFICAÇÃO, AUTENTICAÇÃO, AUTORIZAÇÃO

- É importante destacar alguns componentes que fazem parte do controle de acesso e o que eles representam
  - Sujeito
    - Aquele que solicita acesso a algum tipo de informação. Exemplo: hosts e usuários
  - Objeto
    - O que é acessado pelo sujeito
      - Exemplo: arquivos, dados nos bancos de dados
- Monitor de Referência
  - Usado para mediar um acesso
  - Ter controle que garanta a integridade do seu funcionamento

IDENTIFICAÇÃO, AUTENTICAÇÃO, AUTORIZAÇÃO

- Etapas para realizar o acesso a um objeto
  - Identificação
  - Autenticação
  - Autorização
  - Prestação de Contas/Responsabilidade

IDENTIFICAÇÃO, AUTENTICAÇÃO, AUTORIZAÇÃO

- Identificação
  - Identificar um sujeito junto a um objeto
  - Responsabilizar individualmente por ações no sistema
    - Identificar por: username, PIN
- Autenticação
  - Confirma a identidade
    - Tecnologias:
      - Algo que o usuário sabe (senha)
      - Algo que o usuário tem (token, smart card, certificado digital)
      - Alguma característica do indivíduo (traço físico/comportamen (biometria)

IDENTIFICAÇÃO, AUTENTICAÇÃO, AUTORIZAÇÃO

- Autorização
  - Determina se o sujeito está autorizado a acessar um recurso particular
  - Faz parte de qualquer sistema operacional e é desejável em aplicações
    - Exemplo: Usuário autenticado no Active Directory ou no Servic LDAP, tem acesso a uma página ou a um arquivo no servidor local

- Sistema Operacional verifica permissões com base em critérios d acesso
  - Horário, tipo, localização física

MECANISMOS DE AUTENTICAÇÃO

- Senhas Estáticas
  - String de caracteres para autenticação de usuários
  - É um dos mais utilizados
    - Problemas: Senha fraca pode ser quebrada
- Senhas Dinâmicas
  - On Time Password
    - Válida uma única vez
    - Usada como segundo fator de autenticação e pode ser implementada hardware/software
- Chaves Criptográficas
  - Usada para comprovar a identidade do emissor
  - Assinatura digital: tecnologia que utiliza chave privada para encriptar ur

MECANISMOS DE AUTENTICAÇÃO

- Smart Cards
  - Armazena e processa informações
  - Contém circuitos
  - Realiza operações criptográficas
  - Tipos
    - Sem contato: antena em forma de bobina enrolada
    - Com contato: leitor transmite energia com contato
- Biometria
  - Valida um comportamento ou traço físico do usuário (impressã
    digital, geometria da mão, reconhecimento facial, voz, íris, retin
  - Fácil de usar

MECANISMOS DE CONTROLE DE ACESSO

- Criam normatizações de como o sujeito/usuário acessa os objetos
- Tecnologias são usadas para reforçar objetivos do modelo
- Exemplos:
  - **DAC – Discretionary Access Control**
  - **RBAC – Role Base Access Control**

MECANISMOS DE CONTROLE DE ACESSO

- **DAC – Discretionary Access Control**
  - O proprietário do recurso é responsável por atribuir permissões
  - Tipos
    - ACL – Access Control List
    - Tabelas de Capacidades
- **RBAC – Role Base Access Control**
  - Todas as permissões são atribuídas a papéis
  - Os papéis representam funções
  - Usuários são atribuídos aos papéis

MECANISMOS DE CONTROLE DE ACESSO

- Controle Centralizado
  - Ponto central de controle
    - Radius
      - Mais usado em autenticação simples
      - Encripta somente a senha
      - Autenticação baseada em EAP, PAP, CHAP

GERÊNCIA DE IDENTIDADES

- O objetivo é automatizar as tecnologias de identificação, autentic
  e autorização

- Questões envolvidas
  - O que cada usuário pode acessar?
  - Quem aprova o acesso?
  - Como o acesso é controlado de forma centralizada?
  - Como utilizar controle de acesso para diferentes sistemas
    operacionais e aplicações?

GERÊNCIA DE IDENTIDADES

- **Ferramentas para a gerência**
  - **Diretórios**
  - Gerência de senhas
  - Gerência de contas
  - SSO

GERÊNCIA DE IDENTIDADES

- **Diretórios**
  - É um catálogo que possui informações centralizadas de usuário recursos
  - O formato de dados é hierárquico (protocolo X.500)
  - Protocolo de acesso é o LDAP
    - Nele os usuários requisitam informações de recursos e as aplicações requisitam informações dos usuários
    - Objetos são gerenciados pelos serviços de diretório
      - O administrador pode configurar e gerenciar (identificar, autenticação e autorizar recursos)

GERÊNCIA DE IDENTIDADES

- **Diretórios**
  - **LDAP**
    - Uma das principais utilidades é a de centralizar as informaçõ do usuários
    - A base é um serviço de diretórios, que é um banco de dados, otimizado para leitura e que suporta sofisticados métodos de busca
    - É ajustado para dar respostas rápidas a grandes volumes de dados
    - É oriundo do modelo X.500 que:
      - É mais conhecido como DAP (Directory Access Protocol)
      - Dita como as transações, ocorrem em um serviço de diretóri

GERÊNCIA DE IDENTIDADES

- **Diretórios**
  - **OpenLDAP**
  - Inicialmente desenvolvido pela Univ. of Michigan
  - Baseado no X.500
  - Executa na pilha de protocolos TCP/IP
  - Pode guardar informações como:
    - Nome
    - UserID
    - Passwords
    - Emails
    - Fotos
    - Local de trabalho
    - Etc.

GERÊNCIA DE IDENTIDADES

- **Diretórios**
  - **OpenLDAP**
    - As informações são organizadas em um estrutura hierárquica em árvore
    - Elas são referenciadas segundo o RFC 2253 – LDAPv3
      - Exemplo: dn: uuid=jcezar, ou=Laboratorio, o=USP, c=BR
        - Segundo o RFC (algumas infos apenas):
          - CN – commonName
          - L – locality name
          - ST – state or province name
          - O - organizationName

GERÊNCIA DE IDENTIDADES

- **Diretórios**
  - **OpenLDAP**
  - A busca é feita em determinadas áreas ou na árvore toda
  - As informações são protegidas para acessos não autorizados po meio de:
    - Autenticação
    - Controle de listas de acessos
  - Suporta IPV4 e IPV6
  - Pode atender a múltiplos bancos de dados simultaneamente
  - Faz replicação de base de usuários
  - Alto desempenho para diversas chamadas ao diretório (buscas)

REFERÊNCIAS

- https://pt.wikipedia.org/wiki/OpenLDAP
- https://www.linux.ime.usp.br/~cef/mac499-06/monografias/erich/html/ch01s09.html
- https://www.openldap.org/

INFRAESTRUTURA PARA SISTEMAS DE SOFTWARE

Controle de Acesso e Mecanismos de Autenticação