Segurança e Auditoria de Sistemas

Autenticação

Autenticação

- Técnicas de Autenticação:
  - Usuários e grupos;
  - Técnicas de autenticação;
  - Senhas;
  - Senhas descartáveis;
  - Desafio/resposta;
  - Certificados de autenticação.

Autenticação

- Identificar as diversas entidades de um sistema computacional
  - o usuário interessado em acessar o sistema comprova que realmente é quem afirma ser.
  - Inicialmente, a autenticação visava apenas identificar usuários
    - para garantir que somente usuários devidamente credenciados teriam acesso ao sistema.
  - Atualmente,
    - identificar o sistema para o usuário,
    - ou mesmo sistemas entre si.

Autenticação

- A autenticação é o primeiro passo no acesso de um usuário a um sistema computacional.
  - Cria processos para representar o usuário.
  - Os processos interagem com o usuário e agem no sistema em seu nome.
- Sessão de usuário
  - inicia imediatamente após a autenticação do usuário (login ou logon) e
  - termina quando seu último processo é encerrado, na desconexão (logout ou logoff).

Usuários e grupos

- As credenciais do processo é o conjunto de identificadores do usuário e grupo
- Usuário
  - Permite técnicas de controle de acesso e auditoria.
  - Cada processo deve ser associado a um usuário
  - UID – User Identifier – Identificador do usuário
    - Inteiro usado como chave em uma tabela de usuários
      - /etc/passwd no UNIX
    - Usado pelo S.O. para definir o proprietário de cada entidade ou recurso conhecido.

Usuários e grupos

- Grupos:
  - Conjuntos de usuários podem ser agrupados em um único identificador GID – Group IDentifier ou identificador de grupo.
  - Grupos servem para definir políticas de acesso de forma não individual.

Técnicas de autenticação

- Três grandes grupos:
  - SYK – Something You Know (“algo que você sabe”).
  - SYH – Something You Have (“algo que você tem”).
  - SYA – Something You Are (“algo que você é”)
- Sistemas computacionais com fortes requisitos de segurança implementam mais de uma técnica de autenticação
  - Chamado de **autenticação multi-fator**.

Técnicas de autenticação

- SYK – Something You Know (“algo que você sabe”):
  - baseadas em informações conhecidas pelo usuário,
    - nome de login e sua senha.
  - São consideradas técnicas de autenticação fracas
    - A informação necessária para a autenticação pode ser facilmente comunicada a outras pessoas, ou mesmo roubada.

Técnicas de autenticação

- SYH – Something You Have (“algo que você tem”)
  - baseada na posse de alguma informação mais complexa
    - um certificado digital ou
    - uma chave criptográfica, ou
    - algum dispositivo material, como um smartcard, um cartão magnético, um código de barras, etc.
  - Mais robustas que as técnicas SYK
  - Ponto fraco
    - dispositivos materiais, como cartões, também podem ser roubados ou copiados.

Técnicas de autenticação

- SYA – Something You Are (“algo que você é”)
  - Baseada em características intrinsecamente associadas ao usuário
    - Como seus dados biométricos:
      - impressão digital,
      - padrão da íris,
      - timbre de voz, etc.
  - São potencialmente mais robustas que as anteriores.
  - Ponto Fraco
    - São técnicas mais complexas de implementar.

Senhas

- A grande maioria dos SO de propósito geral implementam a técnica de autenticação SYK baseada em login/senha.
  - Na autenticação por senha, o usuário informa ao sistema seu identificador de usuário (nome de login) e sua senha.
    - Normalmente é uma sequência de caracteres memorizada por ele.
    - O sistema então compara a senha informada pelo usuário com a senha previamente registrada
      - se ambas forem iguais, o acesso é consentido.
- A autenticação por senha é simples mas muito frágil
  - armazenamento das senhas "**em aberto**" no sistema, (arquivo ou base de dados).
    - Caso o arquivo ou base seja exposto, as senhas dos usuários estarão visíveis.
  - Para evitar o risco de exposição indevida das senhas, são usadas funções unidirecionais para armazená-las
    - Ex. os resumos criptográficos.

Senhas

- Pergunta:
  - Como usar o resumo criptográfico para senhas?
  - Como recuperar a senha? É possivel?

Senhas descartáveis

- Um problema importante relacionado à autenticação por senhas reside no risco de roubo da senhas.
- Por ser uma informação estática, caso uma senha seja roubada, o malfeitor poderá usá-la enquanto o roubo não for percebido e a senha substituída.
- Para evitar esse problema, são propostas técnicas de senhas descartáveis (OTP - One-Time Passwords).
  - Uma senha descartável só pode ser usada uma única vez.
  - Perde sua validade após esse uso.

Senhas descartáveis

- Problema:
  - O usuário deve então ter em mãos uma lista de senhas pré-definidas, ou uma forma de gerá-las quando necessário.
  - Há várias formas de se produzir e usar senhas descartáveis, entre elas:
    - Armazenar uma lista sequencial de senhas (ou seus resumos) no sistema e fornecer essa lista ao usuário, em papel ou outro suporte.
      - Quando uma senha for usada com sucesso, o usuário e o sistema a eliminam de suas respectivas listas.
    - Uma variante da lista de senhas é conhecida como algoritmo **OTP** de Lamport
      - Consiste em criar uma sequência de senhas $s_0, s_1, s_2, \cdots, s_n$ com s_0 aleatório e $s_i = \text{hash}(s_i\text{-}1)\ \forall i > 0$, sendo hash(x) uma função de resumo criptográfico conhecida.
    - Gerar senhas temporárias sob demanda, através de um dispositivo ou software externo usado pelo cliente
      - As senhas temporárias podem ser geradas por um algoritmo de resumo que combine uma senha pré-definida com a data/horário corrente.

Desafio/resposta

- Em algumas situações o uso de senhas é indesejável,
  - pois sua exposição indevida pode comprometer a segurança do sistema.
  - Um exemplo disso são os serviços via rede:
    - caso o tráfego de rede possa ser capturado por um intruso, este terá acesso às senhas transmitidas entre o cliente e o servidor.
  - Uma técnica interessante para resolver esse problema são os protocolos de desafio-resposta.

Desafio/resposta

- A técnica de desafio-resposta se baseia sobre um segredo ***s*** previamente definido entre o cliente e o servidor (ou o usuário e o sistema),
  - Pode ser uma senha ou uma chave criptográfica, e um algoritmo de cifragem ou resumo *hash*(*x*).
    1. No início da autenticação, o servidor escolhe um valor **aleatório *d*** e o envia ao cliente, como um ***desafio***.
    2. O cliente recebe esse desafio, o concatena com seu segredo ***s***, calcula o resumo da concatenação e a devolve ao servidor, como *resposta* ($r = hash(s + d)$).
    3. O servidor executa a mesma operação de seu lado, usando o valor do segredo armazenado localmente (s') e compara o resultado obtido $r' = hash(s' + d)$
    4. Se ambos os resultados forem iguais, os segredos são iguais ($r = r' \Rightarrow s = s'$) e o cliente é considerado autêntico.

Certificados de autenticação

- Certificados digitais é cada vez mais frequente na autenticação.
  - é cada vez mais frequente o uso de certificados para autenticar os próprios usuários.
    - Nesse caso, um smartcard ou um dispositivo USB contendo o certificado é conectado ao sistema para permitir a autenticação do usuário.
- Certificado digital é um documento assinado digitalmente
  - Através de técnicas de criptografia assimétrica e resumo criptográfico.
  - Os padrões de certificados PGP e X.509 definem certificados de autenticação (ou de identidade)
    - Objetivo é identificar entidades através de suas chaves públicas.

Certificados de autenticação

- Um certificado de autenticação conforme o padrão X.509 contém as seguintes informações [Mollin, 2000]:
  - Número de versão do padrão X.509 usado no certificado;
  - Chave pública do proprietário do certificado e indicação do algoritmo de criptografia ao qual ela está associada e eventuais parâmetros;
  - Número serial único, definido pelo emissor do certificado (quem o assinou);
  - Identificação detalhada do proprietário do certificado;
  - Período de validade do certificado (datas de início e final de validade);
  - Identificação da Autoridade Certificadora que emitiu/assinou o certificado;
  - Assinatura digital do certificado e indicação do algoritmo usado na assinatura e eventuais parâmetros;