Segurança e Auditoria de Sistemas

Autenticação

Autenticação

- Técnicas de Autenticação:
  - Técnicas biométricas;
  - Kerberos.

Técnicas biométricas

- Técnicas biométricas ou biometria (biometrics) identifica apartir de:
  - Características físicas ou
  - Características comportamentais de um indivíduo,
    - Impressões digitais
    - Timbre de voz.

Biometria

- Diversas características podem ser usadas para a autenticação biométrica.
- Princípios básicos [Jain et al., 2004]:
  - **Universalidade**: a característica biométrica deve estar presente em todos os indivíduos que possam vir a ser autenticados;
  - **Singularidade** (ou unicidade): dois indivíduos quaisquer devem apresentar valores distintos para a característica em questão;
  - **Permanência**: a característica não deve mudar ao longo do tempo, ou ao menos não deve mudar de forma abrupta;
  - **Mensurabilidade**: a característica em questão deve ser facilmente mensurável em termos quantitativos.

Sistema biométrico

- Um sistema biométrico típico é composto de [Jain et al., 2004]:
  - Um sensor,
    - responsável por capturar dados biométricos de uma pessoa;
  - Um extrator de características,
    - processa os dados do sensor para extrair suas características mais relevantes;
  - Um comparador,
    - Compara as características extraídas do indivíduo sob análise com dados previamente armazenados, e
  - Um banco de dados
    - contem as características biométricas dos usuários registrados no sistema.

Sistema biométrico

- O sistema biométrico pode funcionar de dois modos:
  - Modo de autenticação,
    - verifica se as características biométricas de um indivíduo correspondem às suas características biométricas previamente armazenadas.
  - Modo de identificação,
    - identifica o indivíduo a quem correspondem as características biométricas coletadas pelo sensor, dentre todos aqueles presentes no banco de dados.

Kerberos

- O sistema de autenticação Kerberos foi proposto pelo MIT nos anos **80** [Neuman and Ts'o, 1994].
- Utilizado para centralizar a autenticação de rede em vários S.O., ex.: Windows, Solaris, MacOS X e Linux.
- O sistema Kerberos se usa tickets
  - Clientes pedem tickets a um serviço de autenticação e
  - Tickets são usados para acessar os demais serviços da rede.
  - Os tickets são cifrados (criptografia simétrica DES) e têm validade limitada, para aumentar sua segurança.

- Os principais componentes de um sistema Kerberos são:
  - o Serviço de Autenticação (**AS** - Authentication Service),
  - o Serviço de Concessão de Tickets (**TGS** - Ticket Granting Service),
  - a base de chaves,
  - os clientes e
  - os serviços de rede

- O **AS** e o **TGS** constituem o Centro de Distribuição de Chaves (**KDC** - Key Distribution Center).
- O funcionamento básico do sistema Kerberos:

1. o cliente se autentica junto ao **AS** (passo 1) e
2. obtém um ticket de acesso ao serviço de tickets **TGS** (passo 2).
3. solicita ao **TGS** um ticket de acesso ao serviço (servidor) desejado (passos 3 e 4).
4. Com esse novo ticket, ele pode se autenticar junto ao servidor desejado e solicitar serviços (passos 5 e 6).

- No Kerberos,
  - Cada cliente **c** possui uma chave secreta **kc** registrada no servidor de autenticação **AS**.
  - Cada servidor **s** também tem sua chave **ks** registrada no **AS**.
  - As chaves são **simétricas**, somente são conhecidas por seus respectivos proprietários e pelo **AS**.
  - Usa cifragem **DES**.

Funcionamento do Kerberos 1/6

- O funcionamento do Kerberos versão 5 [Neuman and Ts'o, 1994]: (6 passos)

  1 – Um cliente **c** quer acessar um servidor **s** envia uma **solicitação m1** de autenticação ao serviço de autenticação (**AS**) com:

  - sua identidade (**c**),
  - a identidade do serviço desejado (**tgs**),
  - um prazo de validade solicitado (**ts**) e
  - um número aleatório (**n1**), usado para verificar se a resposta do **AS** corresponde ao pedido efetuado:

$$m1 = [c\ tgs\ ts\ n1]$$

Funcionamento do Kerberos 2/6

2 - A resposta do **AS** (mensagem **m2**) contém duas partes:

1. a **chave de sessão** a ser usada na comunicação com o **TGS** (**kc—tgs**) e o número aleatório **n1**,
   - ambos cifrados com a chave do cliente **kc** registrada no **AS**;
2. um ticket (TGT - *Ticket Granting Ticket*)
   - cifrado com a chave do **TGS** (**ktgs**), contendo:
     - a identidade do cliente (**c**),
     - o prazo de validade do ticket concedido pelo **AS** (**tv**) e
     - uma chave de sessão **kc—tgs**, para a interação com o **TGS**:

m2 = [{kc—tgs n1}kc Tc—tgs] ➔ Tc—tgs = {c tv kc—tgs}ktgs

Funcionamento do Kerberos 3/6

3- A seguir, o cliente envia uma solicitação ao **TGS** (mensagem ***m3***) para obter um **ticket** de acesso ao servidor desejado ***s***. Essa solicitação contém:

- a identidade do cliente (***c***) e
- a data atual (***t***), ambos cifrados com a chave de sessão ***kc—tgs***,
- o ticket **TGT** recebido em *m2*,
- a identidade do servidor ***s*** e
- um número aleatório ***n2***:

$$m3 = [\{c\ t\}kc—tgs\ Tc—tgs\ s\ n2]$$

Funcionamento do Kerberos 4/6

4- Após verificar a validade do ticket **TGT**, o **TGS** devolve ao cliente uma mensagem ***m*4** contendo:

- a chave de sessão ***kc—s*** a ser usada no acesso ao servidor ***s*** e
- o número aleatório ***n*2** informado em ***m*3**, ambos cifrados com a chave de sessão ***kc—tgs***, e
- um ticket ***Tc—s*** cifrado com a chave do servidor, que deve ser apresentado ao servidor *s*:
  $m4 = [\{kc—s\ n\}kc—tgs\ Tc—s]$ onde $Tc—s = \{c\ tv\ kc—s\}ks$

Funcionamento do Kerberos 5/6

5- O cliente usa a chave de sessão ***kc—s (m4)*** e o ticket ***Tc—s (5m)*** para se autenticar junto ao servidor ***s*** através da mensagem ***m5***. Essa mensagem contém:

- a identidade do cliente (***c***) e
- a data atual (***t***), ambos cifrados com a chave de sessão ***kc—s***,
- o ticket ***Tc—s (m4)*** e
- o pedido de serviço ao servidor (***request***), que é dependente da aplicação:

$$m5 = [\{c\ t\}kc—s\ Tc—s\ request]$$

Funcionamento do Kerberos 6/6

6- Ao receber ***m5***, o servidor ***s***

- decifra o ticket ***Tc—s*** para obter a chave de sessão ***kc—s*** e
- a usa para decifrar a primeira parte da mensagem e confirmar a identidade do cliente.
- Feito isso, o servidor pode
  - atender a solicitação e
  - responder ao cliente, cifrando sua resposta com a chave de sessão ***kc—s*:**

$$m6 = [\{reply\}kc—s\,]$$