Introdução aos Protocolos de Comunicação

- Protocolos
  - **Sequência de passos, envolvendo duas ou mais partes, projetados para realizar uma tarefa específica.**
  - **Sequência: início e fim.**
  - **Característias:**
    - Todos os passos devem ser conhecidos,
    - Sem ambigüidades,
    - Completo: uma ação para cada situação.

Introdução aos Protocolos de Comunicação

- Requisitos de Segurança
  - **Autenticidade**
    o sistema pode verificar a identidade do usuário
  - **Confidencialidade, ou sigilo**
    informação acessível somente ao usuário autorizado
  - **Integridade,**
    recursos modificados somente pelo usuário autorizado
  - **Disponibilidade,**
    recursos disponível ao usuário e ao sistema

Introdução aos Protocolos de Comunicação

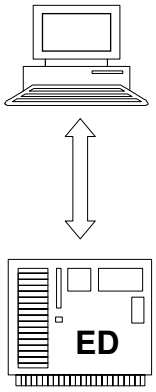
Sistema de Tomada de Decisão

agente expressa decisão (1)
ataques de autenticidade

decisão enviada ao servidor (2)
ataques de confidencialidade

servidor recebe decisão (3)
ataques de integridade

decisão armazenada (4)
ataques de integridade
ataques de autenticidade
ataques de disponibilidade



Introdução aos Protocolos de Comunicação

- Solução ?
  - **Proteger a informação**
    - **Privacidade**
    - **Originalidade** (integridade e autoria)
    - **Sistemas seguros e confiável** (prevenção a fraudes)

Introdução aos Protocolos de Comunicação

Sistemas Seguros

Baseados em protocolos criptográficos,
isto é; baseados no princípio de que nenhuma das entidades envolvidas é presumivelmente confiável.

- Protocolos Criptográficos
  - Protocolos que utilizam criptografia.
  - Partes: amigos e adversários.
  - Mais que originalidade e segredo.

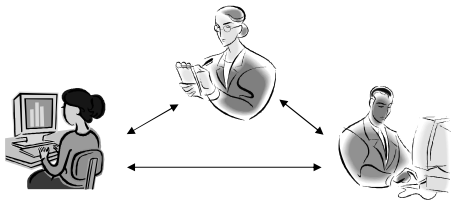
Introdução aos Protocolos de Comunicação

- Participantes:
  - Partes envolvidas (Alice, Bob, C, D, ...)
  - Escuta as escondidas
  - Malicioso (ataca o protocolo)
  - Juiz (arbitro confiável)
  - Guarda (garante segurança as partes envolvidas)
  - Provador (demostra a verdade por prova)
  - Verificador (verifica a correta execução)

Introdução aos Protocolos de Comunicação

Tipos de Protocolos

1. Protocolo Arbitrado



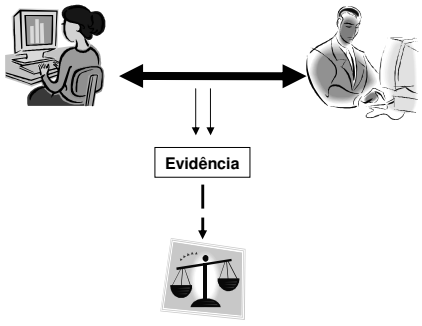
Alice vende um carro a Bob

(1) **Alice** entrega carro ao Arbitro
(2) **Bob** entrega cheque a **Alice**
(3) **Alice** deposita o cheque
(4) Se cheque Ok, **Alice** autoriza arbitro a entregar carro a Bob
(5) Se cheque ruin, arbitro devolve o carro a **Alice**

Introdução aos Protocolos de Comunicação

Tipos de Protocolos

1. Protocolo Adjudicado



Alice vende um carro a Bob

(1) Alice e **Bob** assinam um contrato
(2) Alice entrega carro a **Bob**
(3) Bob entrega cheque a **Alice**

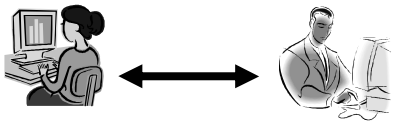
Executado no caso de disputa

(4) **Alice** e **Bob** apresentam-se ao **Juiz**
(5) **Alice** apresenta suas evidências
(6) **Bob** apresenta suas evidências
(7) **Juiz** julga as evidências

Introdução aos Protocolos de Comunicação

Tipos de Protocolos

1. Protocolo Auto-garantido



Imune a falhas

- Não é necessária nenhuma entidade de garantia
- Contruído de forma a não haver possibilidade de disputa
- Não observação de uma etapa do protocolo é imediatamente detectada e o protocolo para.

Introdução aos Protocolos de Comunicação

- Ataques a Protocolos:
  - Passivos
    - Ataque não afeta o protocolo
    - Observa e adquire informação
    - Deve-se previnir o ataque
  - Ativos
    - Afetam o protocolo
    - Todos podem ser maliciosos

Introdução aos Protocolos de Comunicação

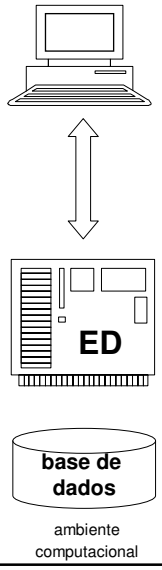
Sistema de Tomada de Decisão

agente expressa $E_{KU_{ED}}$ **[** decisão **]** (1)
ataques de autenticidade

[decisão **]** enviada ao servidor (2)

servidor recebe $D_{KR_{ED}}$ **[** decisão **]** (3)
ataques de integridade

decisão armazenada (4)
ataques de integridade
ataques de autenticidade
ataques de disponibilidade



Introdução aos Protocolos de Comunicação

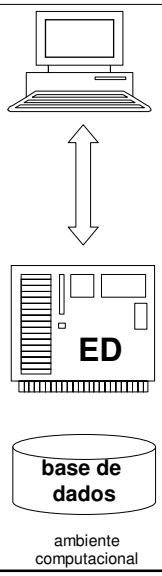
Sistema de Tomada de Decisão

agente $E_{KU_{ED}}$ **[** $E_{KR_{AG}}$ **{** decisão **}]** (1)

[{ decisão **}]** enviada ao servidor (2)

recebe $D_{KR_{ED}}$ **[** $D_{KU_{AG}}$ **{** decisão **}]** (3)

decisão armazenada (4)
ataques de integridade
ataques de autenticidade
ataques de disponibilidade



Introdução aos Protocolos de Comunicação

Sistema de Tomada de Decisão

agente $E_{KU_{ED}}$ **[** $E_{KR_{AG}}$ **{** decisão **}]** (1)

[{ decisão **}]** enviada ao servidor (2)

recebe $D_{KR_{ED}}$ **[** $D_{KU_{AG}}$ **{** decisão **}]** (3)

$E_{KR_{AG}}$ **{** decisão **}** armazenada (4)

ataques de disponibilidade