INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

105 ANOS
REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909-2014

Redes de Computadores

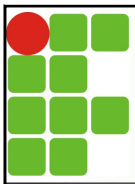
Segurança de Redes
Parte I

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>

Agenda

- Parte I
  - Segurança da Informação
- Parte II
  - Segurança em Redes de Computadores

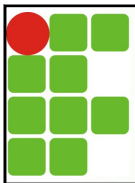
2



Agenda – Parte I

- Parte I
  - Introdução
  - Tendências
  - Incidentes
  - Arquitetura de Segurança
  - Ataque à Segurança
  - Serviço de Segurança
  - Mecanismo de Segurança
  - Modelo

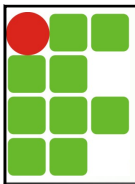
3



Agenda – Parte II

- Parte II
  - Comunicação Segura
  - Ataques
  - Criptografia
  - Chaves Simétricas e Públicas
  - Função de Resumo, Assinatura Digital
  - SSL
  - IPsec
  - Redes Privadas Virtuais (VPNs)
  - Firewall, IDS

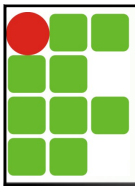
4



Introdução

- Nas últimas décadas as organizações passaram por importantes mudanças
  - Processamento das informações
    - Passado: realizado por meios físicos e administrativos
    - Presente: processamento massivo automatizado (uso de computadores)
  - Modelo de segurança
    - Passado: uso de robustos armários com fechaduras
    - Presente: mecanismos e ferramentas automatizadas de proteção (uso de computadores)

5



Introdução

- A introdução dos sistemas distribuídos também provocou grandes mudanças para a segurança das informações
  - Novas medidas de segurança precisam ser implantadas para proteger os dados durante a transmissão
    - Desenvolvimento de mecanismos e ferramentas para proteger os dados na rede (Segurança na inter-rede)
    - Desencorajar, impedir, detectar e corrigir violações de segurança

6

Introdução

- Exemplo de violação de segurança (1)
  - O usuário **A** transmite um arquivo ao usuário **B**
  - O arquivo contém informações confidenciais (ex.: folha de pagamento) ou dados sensíveis (ex.: informações médicas) que devem ser protegidos contra violações
  - O usuário **C**, que não está autorizado a ler o arquivo, é capaz de monitorar a transmissão e obter uma cópia do arquivo durante a transmissão

7

Introdução

- Exemplo de violação de segurança (2)
  - Um gerente de rede, **D**, transmite uma mensagem a um computador **E** sob seu gerenciamento
  - A mensagem instrui o computador **E** a atualizar um arquivo de autorização para incluir as identidades de diversos novos usuários que devem receber acesso a esse computador
  - O usuário **F** intercepta a mensagem, altera seu conteúdo incluindo e/ou excluindo entradas, e depois encaminha para **E**
  - **E** aceita a mensagem como se tivesse vindo do gerente **D** e atualiza o arquivo de autorização conforme solicitado

8

Introdução

- Exemplo de violação de segurança (3)
  - Em vez de interceptar uma mensagem, o usuário **F** cria sua própria mensagem com as entradas desejadas e transmite a mensagem ao computador **E** como se ela partisse de **D**
  - O computador **E** aceita a mensagem como se ela tivesse vindo de **D** e atualiza seu arquivo de autorização conforme solicitado

9

Introdução

- Exemplo de violação de segurança (4)
  - Um funcionário é demitido sem aviso
  - O gerente do RH envia uma mensagem ao servidor para invalidar a conta do usuário
  - Quando a invalidação é realizada, o servidor deve enviar um aviso ao arquivo como confirmação da ação
  - O funcionário é capaz de interceptar a mensagem e adiá-la por um tempo necessário para fazer um último acesso ao servidor e obter informações confidenciais
  - A mensagem é então encaminhada, a ação tomada e a confirmação postada

10

Introdução

- Exemplo de violação de segurança (5)
  - Uma mensagem é enviada de um cliente a uma corretada com instruções para a realização de diversas aplicações
  - Depois disso, os investimentos perdem valor e o cliente nega ter enviado a mensagem

11

Tendências

- Nas últimas décadas a segurança da informação passou a ocupar um lugar de destaque na área de informática
  - Virou uma área ? Empresas especializadas, cursos, certificações, ...
  - Já existem graduações e pós-graduações
    - Tecnologia em segurança da informação, Gestão de segurança da informação, Especialização em segurança da informação, ...
  - Diversos cargos no mercado de trabalho
    - Security Officer, Analista em segurança de redes de dados, Projetista de soluções de segurança em TI, ...
  - Normas
    - BS 7799, ISO 27001, NBR 17799 -> "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."

12

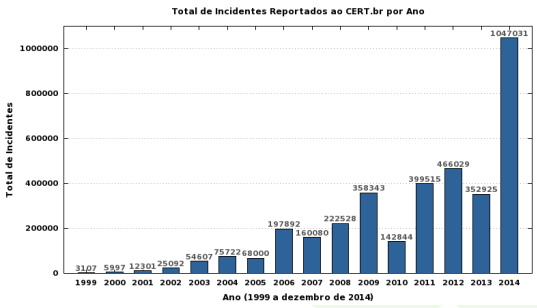
Tendências

- Em 1994 o Internet Architecture Board (IAB) emitiu um boletim intitulado "Segurança na Arquitetura da Internet" (RFC 1636)
  - IAB – (https://www.iab.org)
  - [RFC 1636] – 1994 (https://tools.ietf.org/html/rfc1636)
- Os centros de resposta a incidentes (CSIRTs) foram criados e monitoram incidentes de segurança na internet
  - CERT.br – (http://www.cert.br)
  - Em Natal/RN : Naris – (http://naris.info.ufrn.br)

13

Incidentes

- O CERT.br mantém estatísticas sobre notificações de incidentes a ele reportados
  - Estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os reportam



14

Incidentes

- Classificação dos incidentes no CERT.br (1)
  - **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
  - **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
  - **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
  - **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

15

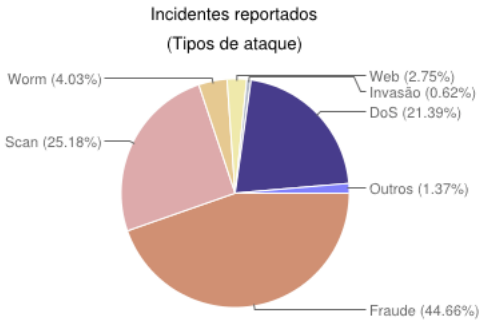
Incidentes

- Classificação dos incidentes no CERT.br (2)
  - **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
  - **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
  - **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

16

Incidentes

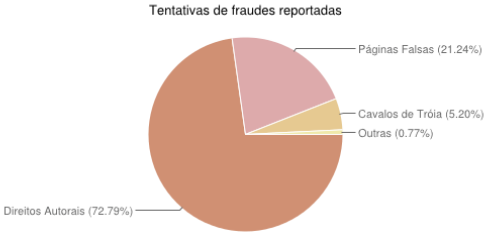
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014



17

Incidentes

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014



- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- **Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Direitos Autorais**: Notificações de eventuais violações de direitos autorais.
- **Outras**: Outras tentativas de fraude.

18

Arquitetura de Segurança

- As organizações precisam de algum meio sistemático para definir os requisitos de segurança e caracterizar as técnicas para satisfazer a esses requisitos
- A recomendação X.800 da OSI (Open Systems Interconnection) oferta uma arquitetura de segurança sistemática definindo os seguintes focos:
  - Ataque à segurança
  - Mecanismo de segurança
  - Serviço de segurança

19

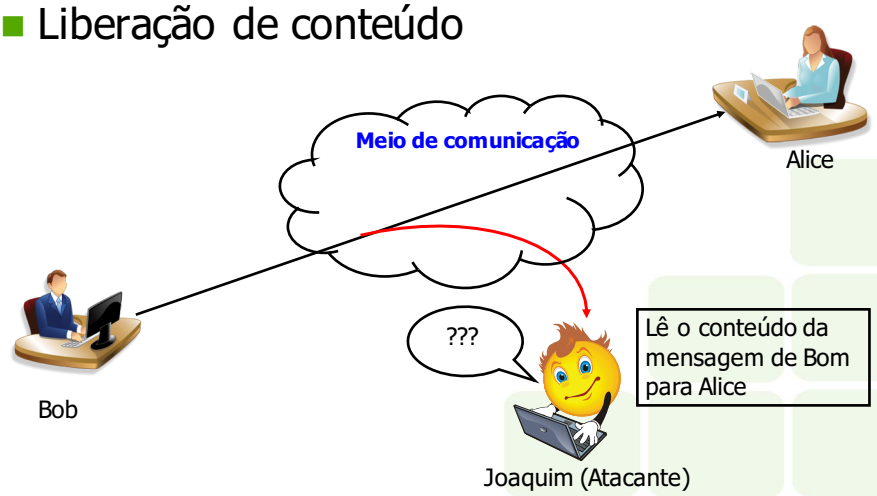
Ataque à Segurança

- Qualquer ação que comprometa a segurança da informação pertencente a uma organização
- Os ataques são classificados como:
  - Ataques passivos : leitura não autorizada de mensagem, análise de tráfego
  - Ataques ativos : modificação de mensagens, negação de serviço

20

Ataque à Segurança - Passivo

- Liberação de conteúdo



21

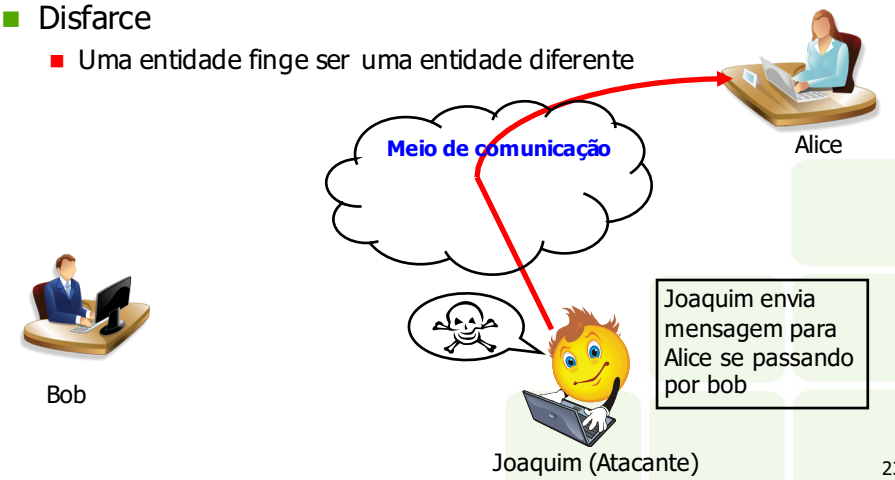
Ataque à Segurança - Passivo

- Análise de tráfego

22

Ataque à Segurança - Ativo

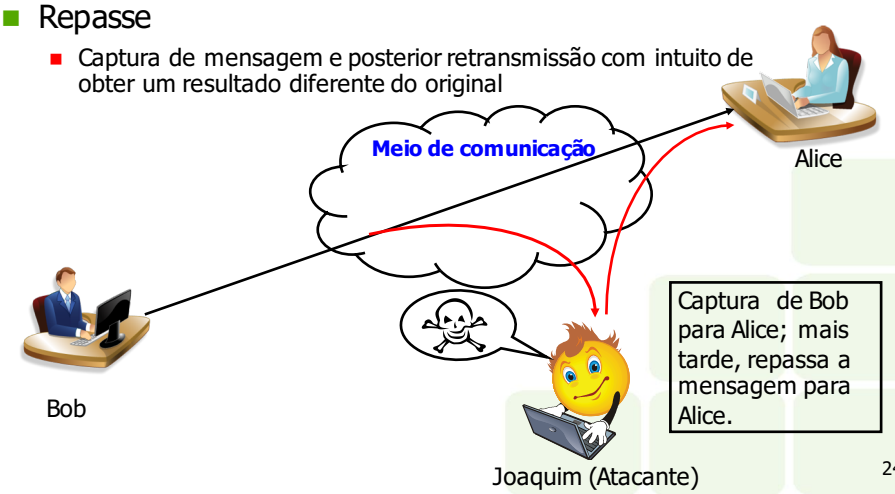
- Disfarce
  - Uma entidade finge ser uma entidade diferente



23

Ataque à Segurança - Ativo

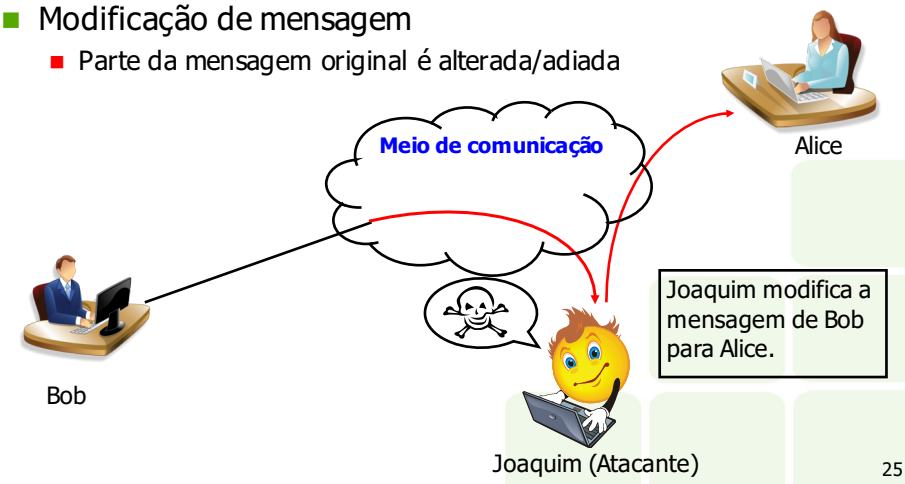
- Repasse
  - Captura de mensagem e posterior retransmissão com intuito de obter um resultado diferente do original



24

Ataque à Segurança - Ativo

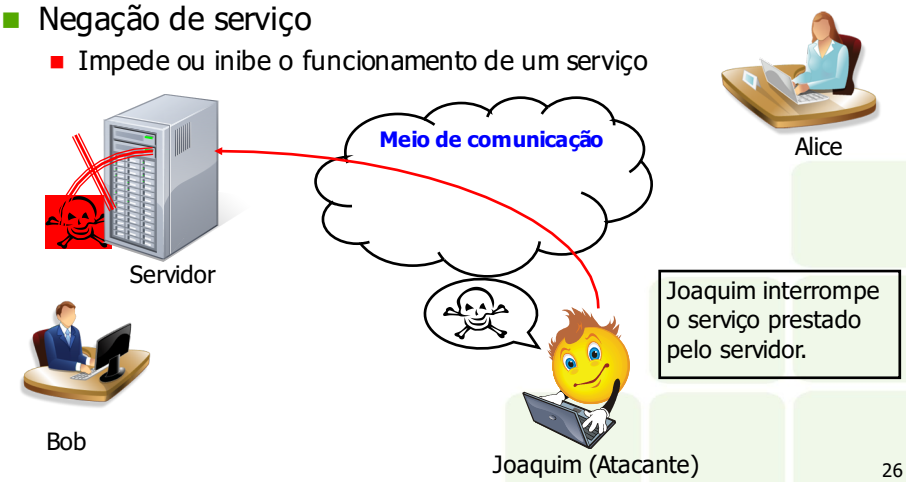
- Modificação de mensagem
  - Parte da mensagem original é alterada/adiada



25

Ataque à Segurança - Ativo

- Negação de serviço
  - Impede ou inibe o funcionamento de um serviço



26

Serviço de Segurança

- Um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e as transferências de informação de uma organização
- Servem para frustrar ataques à segurança e utilizam um ou mais mecanismos de segurança para prover o serviço
- A X.800 divide os serviços em 5 categorias e 14 serviços específicos

27

Serviço de Segurança

- Categorias
  - Autenticação : garantia de que a entidade se comunicando é aquela que afirma ser
  - Controle de acesso : impedimento de uso não autorizado de um recurso.
  - Confidencialidade : proteção dos dados contra divulgação não autorizada
  - Integridade : garantia de que os dados recebidos estão exatamente como foram enviados
  - Irretratabilidade : proteção contra negação de toda ou parte de uma comunicação
  - Disponibilidade : oferecer os serviços de acordo com o projeto do sistema sempre que os usuários os solicitarem (obs.: a X.800 trata como uma propriedade a ser associada a vários serviços)

28

Mecanismo de Segurança

- Processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou permitir a recuperação de um ataque à segurança
- São classificados na X.800 como:
  - Mecanismos específicos : podem ser incorporados a camada de protocolo apropriada a fim de oferecer algum serviço de segurança
  - Mecanismos pervasivos : não são específicos a qualquer serviço de segurança OSI ou uma camada de protocolo específica

29

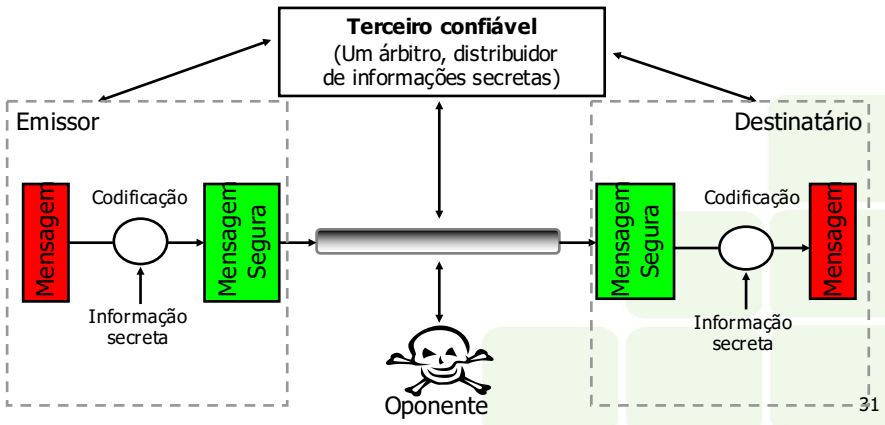
Mecanismo de Segurança

- Mecanismos específicos
  - Criptografia
  - Assinatura digital
  - Controle de acesso
  - Integridade
  - Autenticação
  - Preenchimento de tráfego
  - Controle de roteamento
  - Certificação (PKI)
- Mecanismos não específicos (Pervasivos)
  - Funcionalidade confiável (conforme política de segurança)
  - Detecção de eventos (relevantes a segurança)
  - Registro de auditoria
  - Recuperação de segurança (medidas de recuperação de falhas)

30

Modelo

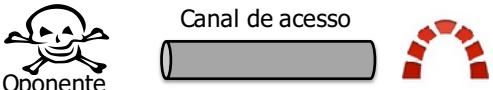
- Modelo para segurança de rede



31

Modelo

- Modelo de segurança de acesso à rede



- Humano (ex.: hacker)
- Software (ex.: vírus, worm)

Função de portaria

Sistema de informações
- Recursos computacionais (CPU, Memória, E/S) - Dados - Processos - Software
Controles de segurança internos

32

Referências

- KUROSE, J. F. e ROSS, K. - Redes de Computadores e a Internet - 5a Ed., Pearson, 2010.
- STALLINGS, W. – Criptografia e segurança de redes, 4. Ed., São Paulo: Pearson Prentice Hall, 2008.
- CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

105 ANOS
REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909-2014

Redes de Computadores

Segurança de Redes
Parte I

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>