INSTITUTO FEDERAL
Pará

Sistemas de Informação Gerencial

Segurança dos sistemas de informação

Prof. Dr. Tiago Araújo

Eleições Presidenciais Americanas

Os Hackers têm como alvo as eleições presidenciais americanas: O que aconteceu? (1 de 2)

- **Problemas**
  - Segurança da Rede fraca
  - Recursos Financeiros Limitados
- **Soluções**
  - Tecnologia de detecção de malwares
  - Isolar sistemas e redes
  - Impedir o acesso não autorizado

Os Hackers têm como alvo as eleições presidenciais americanas: O que aconteceu? (2 de 2)

- Os hackers tiraram vantagem da segurança e controles desiguais e da estrutura de gerenciamento fracos para atacar a campanha de Clinton
- Demonstra vulnerabilidades nos sistemas de tecnologia da informação
- Ilustra algumas das razões pelas quais as organizações precisam prestar atenção especial à segurança do sistema de informação

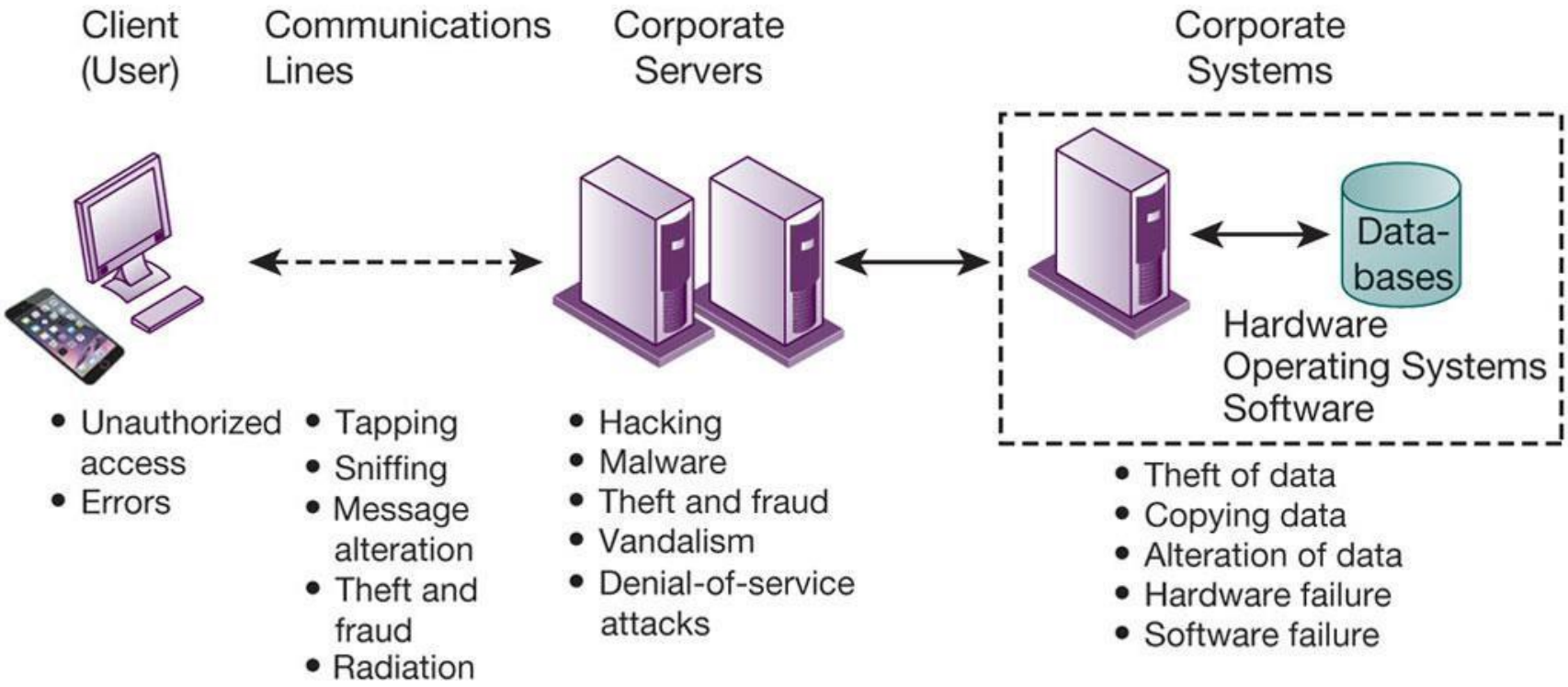
Por que os sistemas são vulneráveis (1 de 2)

- **Segurança**
  - Políticas, procedimentos e medidas técnicas utilizadas para evitar acesso não autorizado, alteração, roubo ou dano físico aos sistemas de informação
- **Controles**
  - Métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização; precisão e confiabilidade de seus registros contábeis; e aderência operacional aos padrões de gestão.

Por que os sistemas são vulneráveis (2 de 2)

- Acessibilidade das redes
- Problemas de hardware (avarias, erros de configuração, danos por uso indevido ou crime)
- Problemas de software (erros de programação, erros de instalação, alterações não autorizadas)
- Catástrofes
- Uso de redes/computadores fora do controle da empresa
- Perda e roubo de dispositivos portáteis

Desafios e Vulnerabilidades de Segurança Contemporânea



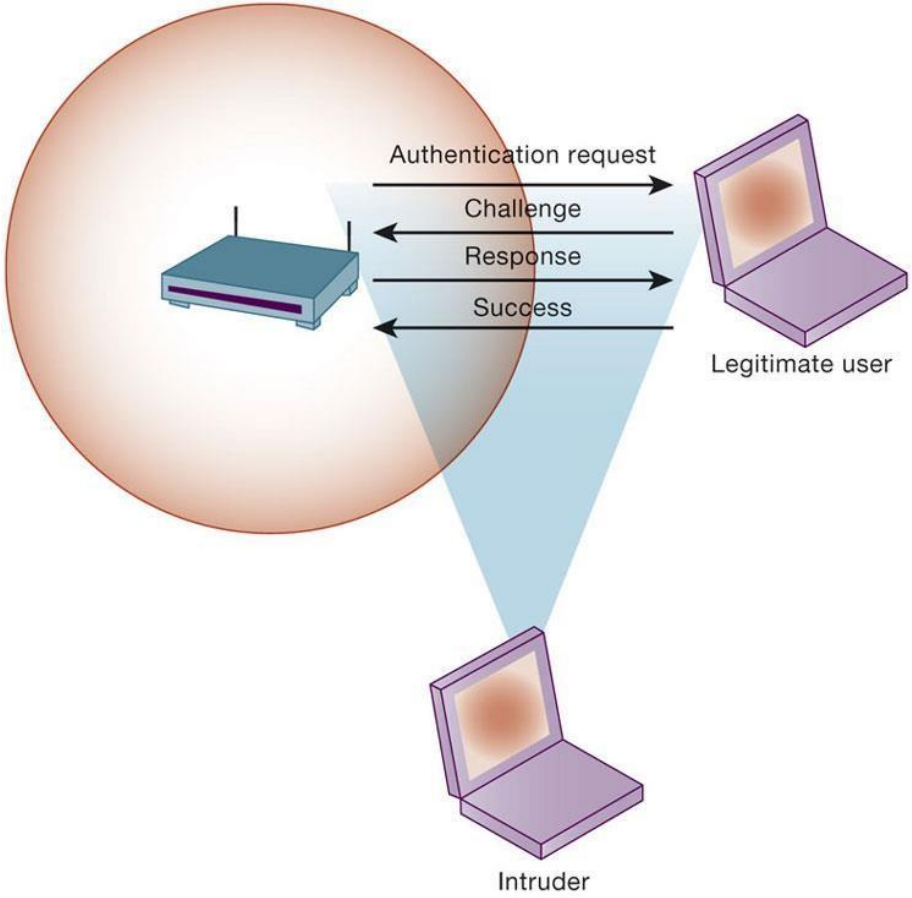
Vulnerabilidades da Internet

- Rede aberta a qualquer pessoa
- O tamanho da Internet significa que os abusos podem ter amplo impacto
- O uso de endereços fixos na Internet com modems a cabo / DSL cria alvos fixos para hackers
- VOIP não criptografado
- E-mail, P2P, IM
- Intercepção
- Anexos com software malicioso
- Transmissão de segredos comerciais

Desafios da segurança sem fio

- **Faixas de radiofrequência fáceis de escanear**
- **SSIDs (identificadores do conjunto de serviços)**
  - Identificar pontos de acesso, transmitidos várias vezes, podem ser identificados por programas sniffer
- **Condução de guerra**
  - Os espiões passam pelos edifícios e tentam detectar o SSID e obter acesso à rede e aos recursos
  - Uma vez que o ponto de acesso é violado, o intruso pode ganhar acesso a unidades e arquivos em rede
- **Pontos de acesso indevidos**

Desafios da segurança Wi-Fi



Software malicioso: Vírus, Worms, cavalos de Tróia e Spyware (1 de 2)

- Malware (software malicioso)
- Vírus
- Worms (minhocas)
- Worms e vírus espalhados por:
  - Downloads e dirigidos- por download
  - E-mail, anexos de IM
- Malwares de dispositivos móveis
- Malwares de redes sociais

Software malicioso: Vírus, Worms, cavalos de Tróia e Spyware (2 de 2)

- Cavalo de Tróia
- Ataques de injeção SQL
- Ransomware
- Spyware
  - Registradores chave
  - Outros tipos
    - Reiniciar a página inicial do navegador
    - Pedidos de busca redirecionada
    - Lentidão no desempenho do computador, ocupação da memória

Hackers e crimes informáticos (1 de 3)

- Hackers vs. crackers
- As atividades incluem:
  - Intrusão do sistema
  - Danos ao sistema
  - Cibervandalismo
    - Ruptura intencional, desfiguração, destruição de website ou sistema de informação corporativa
- **Falsificar e sniffing (farejar)**

Hackers e crimes informáticos (2 de 3)

- Ataques de negação de serviço (DoS)
- Ataques de negação de serviço distribuídos (DDoS)
- Botnets
- Spam
- Crimes cibernéticos
  - Computador pode ser alvo de crime
  - O computador pode ser um instrumento do crime

Hackers e crimes informáticos (3 de 3)

- Roubo de identidade
  - Phishing
  - Evil twins
  - Pharming
- Fraude por clique
- Ciberterrorismo
- Guerra cibernética

Ameaças Internas: Funcionários

- As ameaças à segurança muitas vezes se originam dentro de uma organização
- Conhecimento Interno
- Procedimentos de segurança descuidados
  - Falta de conhecimento do usuário
- Engenharia social
- Tanto os usuários finais quanto os especialistas em sistemas de informação são fontes de risco

Vulnerabilidades de Software

- **O software comercial contém falhas que criam vulnerabilidades de segurança**
  - Bugs (defeitos no código do programa)
  - Zero defeitos não pode ser alcançado
  - As falhas podem abrir redes para intrusos
- **Vulnerabilidades de dia zero**
- **Patches**
  - Pequenas peças de software para reparar falhas
  - Gerenciamento de patches

Qual é o valor comercial da segurança e do controle?

- Falhas nos sistemas de computador podem levar a uma perda significativa ou total da função comercial
- As empresas estão agora mais vulneráveis do que nunca
  - Dados pessoais e financeiros confidenciais
  - Segredos comerciais, novos produtos, estratégias
- Uma quebra de segurança pode cortar o valor de mercado de uma empresa quase imediatamente
- A segurança e os controles inadequados também trazem problemas de responsabilidade

Evidência Eletrônica e Computação Forense

- **Evidência Eletrônica**
  - Provas de crimes de colarinho branco muitas vezes em formato digital
  - O controle adequado dos dados pode economizar tempo e dinheiro ao responder ao pedido de descoberta legal
- **Computação Forense**
  - Coleta científica, exame, autenticação, preservação e análise de dados de mídia de armazenamento de dados de computador para uso como prova em tribunal
  - Recuperação de dados ambientais

Controles de Sistemas de Informação

- **Pode ser automático ou manual**
- **Controles gerais**
  - Projeto, segurança e uso de programas de computador e segurança dos arquivos de dados em geral em toda a organização
  - Controles de software, controles de hardware, controles de operações de computador, controles de segurança de dados, controles de desenvolvimento de sistemas, controles administrativos,
- **Controles de Aplicação**
  - Controles exclusivos para cada aplicação computadorizada
  - Controles de entrada, controles de processamento, controles de saída

Avaliação de risco

- **Determina o nível de risco para a empresa se uma atividade ou processo específico não for adequadamente controlado**
  - Tipos de ameaça
  - Probabilidade de ocorrência durante o ano
  - Potenciais perdas, valor da ameaça
  - Previsão de perda anual

Avaliação de risco do processamento de pedidos on-line

Exposure	Probability of Occurrence	Loss Range (Average) ($)	Expected Annual Loss ($)
Power failure	30%	$5,000 – $200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000 – $50,000 ($25,500)	$1,275
User error	98%	$200 – $40,000 ($20,100)	$19,698

Política de Segurança

- **Classifica os riscos da informação, identifica objetivos de segurança e mecanismos para atingir esses objetivos**
- **Conduz outras políticas**
- **Política de uso aceitável (AUP)**
  - Define os usos aceitáveis dos recursos de informação e equipamentos de informática da empresa
- **Gestão da identidade**
  - Identificação de usuários válidos
  - Controle de acesso

Regras de acesso para um sistema de pessoal

SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

Planejamento de Recuperação de Desastres e Planejamento de Continuidade de Negócios

- **Planejamento de recuperação em caso de desastre**
  - Desenvolve planos para a restauração de serviços interrompidos
- **Planejamento da continuidade dos negócios**
  - Foca no restabelecimento das operações comerciais após o desastre
- **Ambos os tipos de planos necessários para identificar os sistemas mais críticos da empresa**
  - Análise de impacto comercial para determinar o impacto de uma interrupção
  - A administração deve determinar quais sistemas restaurados primeiro

O papel da auditoria

- **Auditoria de sistemas de informação**
  - Examina o ambiente geral de segurança da empresa, bem como os controles que regem os sistemas de informação individuais
- **Auditorias de segurança**
  - Revisar tecnologias, procedimentos, documentação, treinamento, e pessoal
  - Pode até simular um desastre para testar respostas
- **Listar e classificar os pontos fracos do controle e a probabilidade de ocorrência**
- **Avaliar o impacto financeiro e organizacional de cada ameaça**

Lista de Fraquezas de Controle do Auditor Amostra

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2018**		**Received by: T. Benson** **Review date: June 28, 2018**	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/18	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/18	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

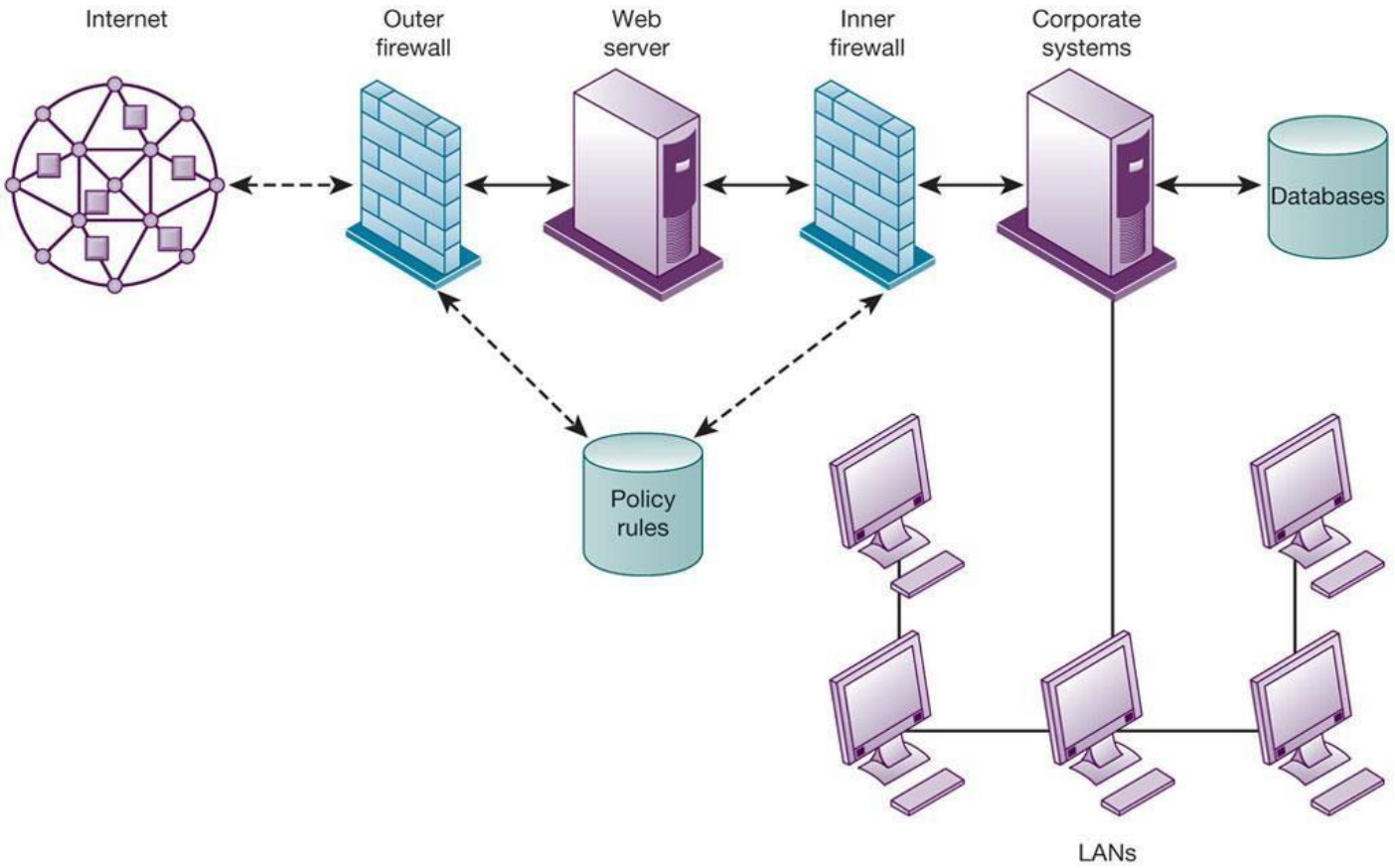
Ferramentas e Tecnologias para Salvaguarda dos Sistemas de Informação (1 de 3)

- **Software de gerenciamento de identidade**
  - Automatiza o controle de todos os usuários e privilégios
  - Autentica os usuários, protegendo identidades, controlando o acesso
- **Autenticação**
  - Sistemas de senhas
  - Tokens
  - Cartões inteligentes
  - Autenticação biométrica
  - Autenticação de dois fatores

Ferramentas e Tecnologias para Salvaguarda dos Sistemas de Informação (2 de 3)

- **Firewall**
  - Combinação de hardware e software que impede usuários não autorizados de acessar redes privadas
  - Filtragem de pacotes
  - Inspeção estatal
  - Tradução de endereços de rede (NAT)
  - Filtragem por procuração de aplicação

Um Firewall Coorporativo



Ferramentas e Tecnologias para Salvaguarda dos Sistemas de Informação (3 de 3)

- **Sistema de detecção de intrusão**
  - Monitora pontos de risco em redes corporativas para detectar e dissuadir intrusos
- **Antivírus e software antispyware**
  - Verifica computadores quanto à presença de malware e pode muitas vezes também o eliminar
  - Requer atualização contínua
- **Sistemas de gestão unificada de ameaças (UTM)**

Segurança de redes sem fio

- **Segurança WEP**
  - As chaves de criptografia estática são relativamente fáceis de quebrar
  - Melhorado se usado em conjunto com VPN
- **Especificação WPA2**
  - Substitui o WEP por padrões mais fortes
  - Chaves de criptografia em constante mudança, mais longas

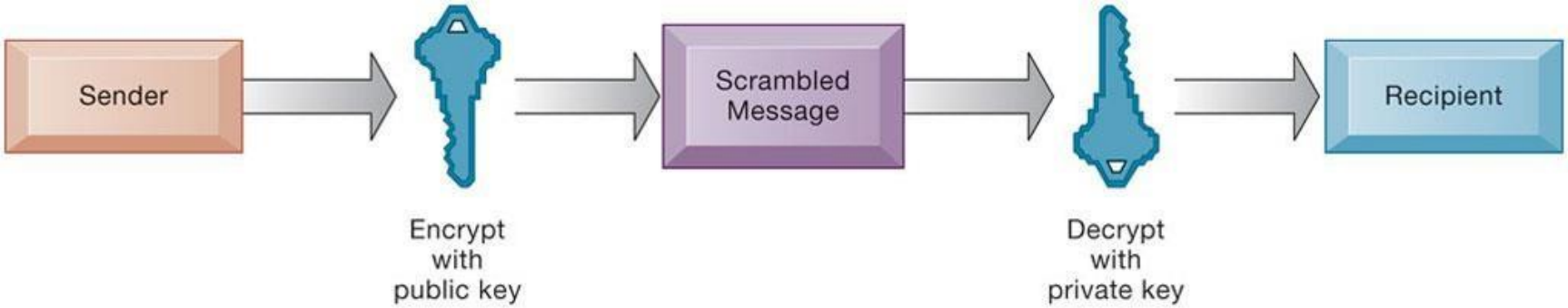
Sistemas Criptografia e infraestrutura de chave pública (1 de 3)

- **Criptografia**
  - Transformação de texto ou dados em texto cifrado que não pode ser lido por destinatários não intencionais
  - Dois métodos de criptografia em redes
    - Camada de soquetes seguros (SSL) e sucessor Segurança na camada de transporte (TLS)
    - Protocolo de Transferência de Hipertexto Seguro (S-HTTP)

Sistemas Criptografia e infraestrutura de chave pública (2 de 3)

- **Dois métodos de criptografia de mensagens**
  - Criptografia de chave simétrica
    - Criptografia de chave simétrica
  - Criptografia de chave pública
    - Utiliza duas chaves, matematicamente relacionadas: chave pública e chave privada
    - O remetente criptografa a mensagem com a chave pública do destinatário
    - Descriptografados com chave privada

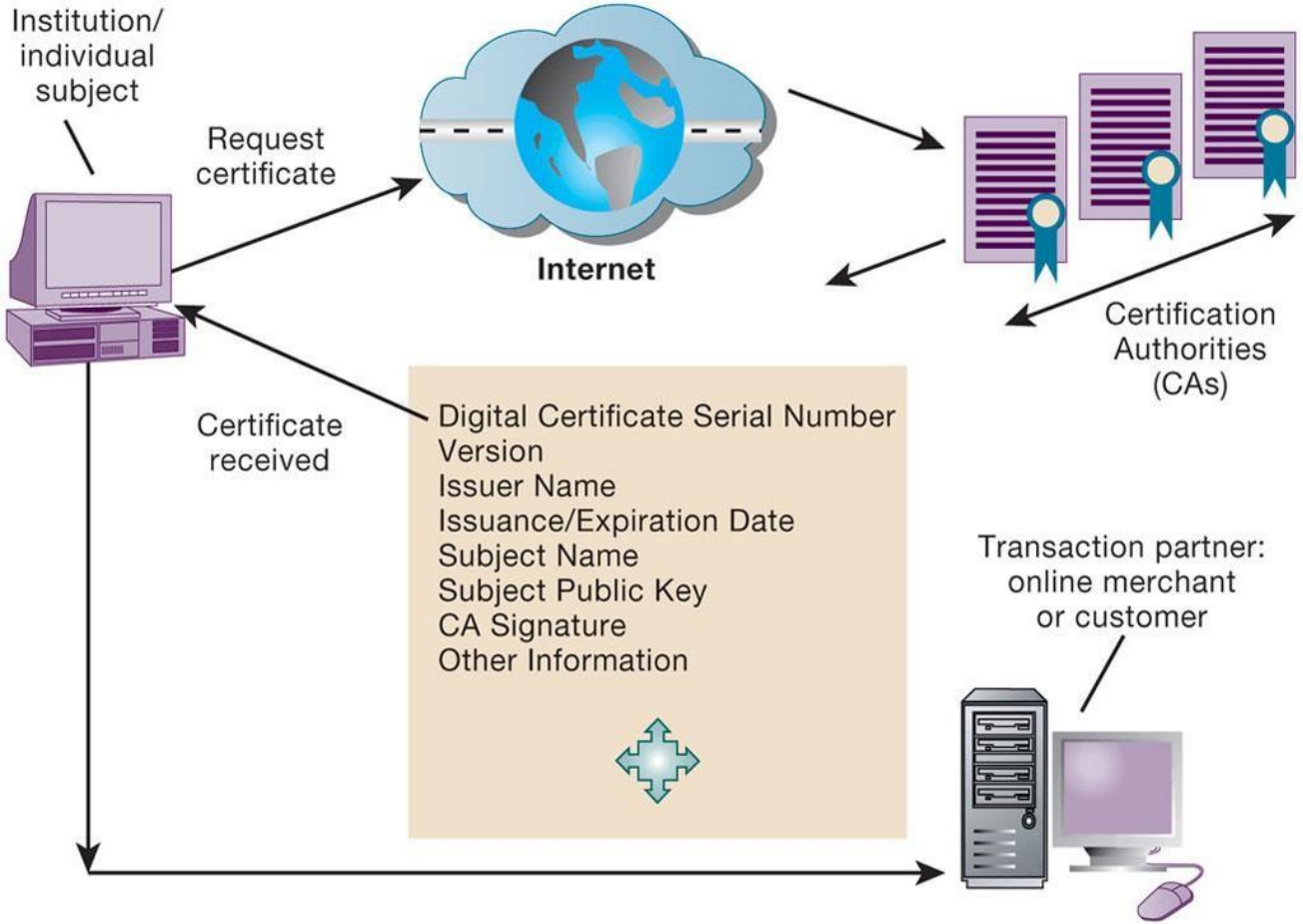
Criptografia de chave pública



A Criptografia e infraestrutura de chave pública (3 de 3)

- **Certificado digital**
  - Arquivo de dados utilizado para estabelecer a identidade dos usuários e eletrônico ativos para proteção de transações on-line
  - Utiliza um terceiro de confiança, autoridade de certificação (AC), para validar a identidade de um usuário
  - CA verifica a identidade do usuário, armazena informações no servidor da CA, o que gera um certificado digital criptografado contendo informações de identificação do proprietário e cópia da chave pública do proprietário
- **Infraestrutura de chave pública (PKI)**
  - Uso de criptografia de chave pública trabalhando com autoridade certificadora
  - Amplamente utilizado no comércio eletrônico

Certificados digitais



Garantindo a disponibilidade do sistema

- **O processamento de transações on-line requer 100% de disponibilidade**
- **Sistemas de computador tolerantes a falhas**
  - Contêm componentes redundantes de hardware, software e fornecimento de energia que criam um ambiente que fornece serviço contínuo e ininterrupto
- **Inspeção profunda de pacotes**
- **Terceirização de segurança**
  - Fornecedores de serviços de segurança gerenciados (MSSPs)

Questões de segurança para Cloud Computing e a Plataforma Móvel Digital (1 de 2)

- **Segurança na nuvem**
  - A responsabilidade pela segurança reside na posse dos dados da empresa
  - As empresas devem garantir que os fornecedores forneçam proteção:
    - Onde os dados são armazenados
    - Atendimento aos requisitos corporativos, leis de privacidade legais
    - Segregação de dados de outros clientes
    - Auditorias e certificações de segurança
  - Acordos de nível de serviço (SLAs)

Questões de segurança para Cloud Computing e a Plataforma Móvel Digital (2 de 2)

- **Segurança de Plataformas Moveis**
  - As políticas de segurança devem incluir e cobrir quaisquer requisitos especiais para dispositivos móveis
    - Diretrizes para o uso de plataformas e aplicações
  - Ferramentas de gerenciamento de dispositivos móveis
    - Autorização
    - Registros de inventário
    - Atualizações de controle
    - Bloquear/formatar dispositivos perdidos
    - Criptografia
  - Software para segregação de dados corporativos em dispositivos

Garantindo a qualidade do software

- Métricas de software: Avaliações objetivas do sistema na forma de medidas quantificadas
  - Número de transações
  - Tempo de resposta on-line
  - Cheques de folha de pagamento impressos por hora
  - Bugs conhecidos por cem linhas de código
- Testes antecipados e regulares
- Caminhada: Revisão da especificação ou documento de projeto por um pequeno grupo de pessoas qualificadas
- Depuração: Processo pelo qual os erros são eliminados

Organizações: Quão segura é a nuvem?

- **Discussão em classe**
  - Que tipos de problemas de segurança a computação em nuvem representa? Quão sérios eles são? Explique sua resposta.
  - Quais fatores de gerenciamento, organização e tecnologia são responsáveis pelos problemas de segurança na nuvem? Até que ponto a segurança na nuvem é um problema de gerenciamento?
  - Que medidas as organizações podem tomar para tornar seus sistemas baseados em nuvem mais seguros?
  - As empresas devem usar a nuvem pública para executar seus sistemas de missão crítica? Por que ou por que não?