Segurança+

Domínio 1: Conceitos Gerais de Segurança

SY0-701

Brian Olliff

Instrutor de Engenharia Defensiva

Tópicos

Visão geral do Security+

Conceitos fundamentais

Controles de segurança

Gestão de mudanças

Criptografia

Objetivos de aprendizagem

- Ser capaz de resumir e comparar vários controles de segurança
- Compreender a diferença entre as categorias de controles de segurança
- Compreender os conceitos fundamentais de segurança
  - + CIA, AAA
  - + Não repúdio
  - + Confiança zero
- Explicar a importância dos processos de gestão de mudanças
- Compreender os fundamentos da criptografia
  - + Assimétrico vs. simétrico
  - + PKI
  - + Métodos, ferramentas e práticas de criptografia

CompTIA Security+

- Conceitos Gerais de Segurança
  - Controles de segurança, conceitos fundamentais de segurança, gestão de mudanças, criptografia soluções
- Ameaças, Vulnerabilidades e Mitigações • Atores e motivações de ameaças, vetores e superfícies de ataque • Tipos de vulnerabilidades e técnicas de mitigação • Arquitetura de Segurança • Modelos e tipos de arquitetura, princípios de arquitetura de segurança • Proteção de dados, resiliência e recuperação da arquitetura • Operações de Segurança • Reforço da segurança, gestão de ativos, alertas e monitoramento • Gestão de vulnerabilidades, IAM, IR e investigações
- Gestão e Supervisão de Programas de Segurança
  - Governança de segurança, gestão de riscos, conformidade • Avaliações, auditorias e análises de terceiros

Estudar e fazer o exame

• Utilize diversos recursos para estudar •

Dedique tempo suficiente e revise os tópicos, se

necessário • Tire

suas dúvidas • Agende sua prova e defina

uma meta • Máximo de

90 questões ÿ Combinação de questões de múltipla escolha e questões práticas

• Limite de tempo de 90 minutos

• É necessário obter 750 pontos para ser aprovado (em

uma escala de 100 a 900) • O custo do exame varia dependendo do local/moeda

Controles de segurança

Controle de segurança

- Procedimentos, atividades e ferramentas concebidos para proteger a confidencialidade, Integridade, disponibilidade do sistema e dos dados •

Exemplos

- Software e dispositivos de segurança
- Políticas de segurança escritas (para usuários e equipe de segurança) •

Portas e portões trancados •

Câmeras de segurança

- Programas de gerenciamento de riscos • Quatro categorias principais
  - Técnico
  - Gerencial •

Operacional •

Físico

Controles técnicos

- Controle implementado como algum tipo de sistema
  - Hardware, software, firmware, etc.

Exemplos

- Firewall de rede
- Software antivírus (AV) ou de detecção e resposta de endpoints (EDR)
- Configurações de segurança do sistema operacional
- Software de criptografia
- Sistema de prevenção de intrusões (IPS)
- Listas de controle de acesso (ACL)

Controles operacionais

- Controle implementado principalmente por pessoas em vez de sistemas
- Os *controles gerenciais* podem ser coletivamente denominados como **Controles Administrativos**
- Distinção importante:
  - Todos os controles são implementados por pessoas, o que não os define como operacionais.
- Exemplos •
  - Guardas de segurança •
  - Programas de treinamento
    - ÿ Equipe de TI e segurança ÿ
    - Treinamento de conscientização de segurança para usuários

Controles gerenciais

- Controles que fornecem supervisão e gerenciamento de programas de segurança
- Frequentemente descrevem requisitos para outras categorias de controles
- Exemplos
  - • Programas de avaliação e gestão de riscos • Ferramentas utilizadas para auxiliar na identificação de riscos • Sistemas para avaliar e selecionar outros controles de segurança • Políticas
    - de segurança ÿ Políticas de Uso Aceitável (PUA) para usuários ÿ Políticas que estabelecem requisitos para controles operacionais e técnicos

Controles físicos

- Controles que proporcionam segurança a estruturas ou áreas definidas • Utilizados para controlar e monitorar o acesso a diversos locais
- Exemplos •
  - Alarmes de segurança •
  - Portas trancadas
  - Câmeras de vigilância de circuito fechado
  - Iluminação de segurança •
  - Crachás de identificação de segurança • Fechaduras biométricas de segurança

Tipos de controle

- Preventivo
  - Eliminar ou reduzir a probabilidade de um ataque bem-sucedido
  - Opera antes que o ataque possa ocorrer • ACLs, AV/EDR
- Deter
  - Projetado para desencorajar tentativas de ataque • Pode não impedir qualquer tipo de acesso • Placas de “Proibida a entrada”, avisos legais nos sistemas
- Detetive
  - Identifica e registra (logs) tentativas (ou ataques bem-sucedidos)/intrusões • Semelhante a um mecanismo de dissuasão, não foi projetado para impedir ataques • Sistemas de registro

Tipos de controle

- Corretivo
  - Auxilia na redução ou eliminação do efeito/impacto do ataque • Usado após o término do ataque
  - Backup de dados/sistemas, correção de vulnerabilidades exploradas •
  - Compensação • Controle secundário (ou substituto) ao controle primário • Oferece o mesmo nível de proteção ou um nível superior • Utiliza tecnologia ou metodologia diferente (defesa em profundidade
- Diretiva
  - Implementado para monitorar a conformidade regulatória •
  - Fornecer orientações alinhadas especificamente aos requisitos da organização

Conceitos Fundamentais de Segurança

Tríade da CIA

- Confidencialidade •

  Privacidade e segurança de dados e ativos • Impedir o acesso de pessoas não autorizadas às informações • Criptografia, controle de acesso, treinamento

- Integridade •

  Garantir que os dados/ativos estejam livres de alterações não autorizadas
  • Intencionais ou acidentais
  • Malware no sistema / Usuário inserindo informações incorretas

- Disponibilidade •

  Manter o acesso aos sistemas de forma oportuna e confiável • Os sistemas permanecem online o máximo possível • Recuperação rápida e segura em caso de interrupções

Funções e responsabilidades

- Diretor de Informação (CIO) • Responsável geral pelos sistemas e funções de TI • Diretor de Tecnologia (CTO)
  - Pode ser semelhante a um CIO (Diretor de Informática)
- Diretor de Segurança (CSO)/Diretor de Segurança da Informação (CISO)
  - Responsável direto pela segurança da informação/ cibersegurança • Pode se reportar ao CIO em algumas organizações • Oficial de Segurança de Sistemas de Informação (ISSO)
  - Funcionários com responsabilidades administrativas técnicas/especializadas em segurança

Outros conceitos

- Não repúdio • Prova de que um indivíduo/sistema realizou uma ação, não podendo ser negada ÿ Criação/modificação de arquivos, envio de e-mails, etc. • Frequentemente implementada com assinaturas digitais e certificados.
- Análise de lacunas • Revisão detalhada de todos os controles de segurança, políticas, procedimentos, etc. • Projetada para identificar áreas que podem precisar de melhorias • Comparada a padrões e estruturas de segurança cibernética ÿ Frequentemente específica do setor (financeiro, saúde, etc.) • Auxilia na compreensão dos riscos e vulnerabilidades na organização.

Autenticação, Autorização e Contabilização

AAA

- Autenticação, Autorização e Contabilização (Auditoria/Responsabilidade)
- Autenticação
  - Comprovante de identidade
  - Senha, PIN, MFA
- Autorização
  - Verificação de que o usuário pode acessar o recurso
  - Listas de controle de acesso, vários modelos de autorização
- Contabilidade
  - Garante que os usuários sejam *responsabilizados* por suas ações
  - Registro e auditoria

Autenticação

- Método para verificar e comprovar uma identidade declarada
- Múltiplos tipos (fatores) de autenticação
    - Baseado em conhecimento
    - Baseado em propriedade
    - Biométrico
    - Localização
    - Comportamental
- Autenticação forte
    - MFA - Autenticação multifator
- Os métodos de autenticação devem ser protegidos

Autorização

- Garantir que usuários devidamente autenticados tenham acesso aos seus recursos • Mas **NÃO** aos recursos aos quais não deveriam ter acesso •

Processo contínuo • Ocorre sempre que o acesso ao recurso é tentado • Múltiplos mecanismos/modelos

- Controle de acesso discricionário (DAC) •
- Controle de acesso obrigatório (MAC) • Controle de acesso baseado em funções (RBAC)
  - ÿ Controle de acesso baseado em regras (RB-RBAC) •
- Controle de acesso baseado em atributos
- Controle de acesso baseado em risco

Responsabilidade

• Usuários identificados, autenticados e autorizados a acessar o sistema. • Garantir que todos os acessos estejam corretos e não sejam utilizados indevidamente.

• Registro, monitoramento e auditoria

- Detectar intrusões
- Monitorar atividades suspeitas • Auxiliar em atividades de resposta a incidentes • Rastrear ações até os indivíduos responsáveis
- Apoio jurídico • Impedir possíveis ações maliciosas • Requer revisão periódica - manual ou automatizada

Modelos de autorização

- DAC - Controle de Acesso Discricionário
  - Proprietário atribuído ao recurso, que atribui permissões diretamente. • Utilizado pela maioria dos sistemas operacionais.
- MAC - Controle de Acesso Obrigatório
  - Rótulos de sensibilidade de dados atribuídos a recursos e usuários • Os usuários podem acessar recursos que correspondam ao seu “nível de acesso”
- RBAC - Controle de Acesso Baseado em Funções
  - Permissões concedidas com base na função • Usuários atribuídos a funções, funções atribuídas a recursos • ABAC

- Controle de Acesso Baseado em Atributos
  - Acesso baseado na combinação de atributos do sujeito/objeto • Sistema operacional utilizado, endereço IP da solicitação, patches instalados, localização geográfica, etc.

Confiança Zero

O que

• A confiança em uma rede deve ser avaliada continuamente • Arquitetura para proteger recursos de rede internos • Perímetro menos facilmente identificável em redes modernas • Uma vez que o invasor ultrapassa os controles de perímetro, o movimento lateral é irrestrito • Todos os recursos e comunicações são protegidos, independentemente da localização • Redes internas não são mais “zonas de confiança implícitas” • Nenhum recurso é inerentemente confiável • Nem todos os recursos pertencem à empresa • A arquitetura Zero Trust é comumente dividida em dois componentes • Plano de Controle - comunicação de back-end (políticas, administração, etc.) • Plano de Dados - comunicação de aplicativos (usuários, servidores, etc.)

Por que

- Despermetrização •
  Afastamento dos limites da rede para proteger recursos/dados individuais • Os ataques podem vir de qualquer lugar na rede • Alguns atacantes levam seu tempo
  • Pode ficar inativo na rede por dias, semanas ou meses •

Usuários internos maliciosos (ou descuidados)

- Presume-se que tudo na rede seja malicioso, a menos que se prove o contrário • Múltiplos pontos de entrada e saída na maioria das redes •
  Integração com produtos de terceiros, provedores de nuvem, dispositivos móveis, etc.
- Projetado para reduzir o escopo de possíveis ameaças •
  Superfície de ataque menor e mais controlada

Adaptação constante

- A arquitetura de confiança zero deve ser flexível
- Utiliza controles de identidade adaptativos •
  Contas de usuário internas não são inerentemente
  confiáveis • Identidades e autenticação/autorização são constantemente
verificadas • Múltiplos métodos para verificar identidades
  - Credenciais
  - Autenticação baseada em risco
  - Certificados digitais •
  Localização da rede
- Nenhum atributo único usado para autenticação

Plano de controle

- Componente principal - **ponto de decisão de política** (PDP) • O

PDP geralmente consiste em **um mecanismo de política** (PE) e **um administrador de política** (PA) • Mecanismo de

política • Utiliza políticas definidas e entradas externas (inteligência de ameaças, registros, informações de identidade, etc.)

- Determina se o acesso deve ser concedido, negado ou revogado

- Administrador de políticas
  - As decisões da PE são repassadas à PA •

    Responsável por estabelecer/encerrar a comunicação entre o aluno e recurso
  - Executa essas ações por meio de comandos para **o ponto de aplicação de políticas** (PEP)
    - ÿ localizado no plano de dados

Plano de dados

- Ponto de aplicação da política
  - Habilitar, monitorar e encerrar conexões entre o sujeito e o recurso/sistema •
    Comunicar-se com o PA
    ÿ Encaminha solicitações de comunicação ÿ
    Recebe atualizações de políticas
- Zonas de confiança
  - Ausência de confiança implícita universal na rede
  - Múltiplas divisões lógicas da rede contendo recursos relacionados ÿ Denominadas "zonas de confiança implícita"
  - O PEP controla o acesso a essas zonas
    ÿ Abordagem microsegmentada granular

Segurança física

Segurança física

- Projetado para restringir/monitorar o acesso a locais e ativos físicos • Edifícios seguros
  - Data centers e salas de cabeamento
- Utiliza os mesmos conceitos de AAA que outros controles de segurança • Frequentemente dividido em zonas
  - Separadas por diversas barreiras • Entrada/saída controlada por diversos mecanismos • Zonas mais seguras = controle de segurança mais rigoroso • Ex: zona pública, zona de segurança média, zona de alta segurança, etc.

Recomendações gerais

- As zonas seguras devem estar localizadas longe das áreas públicas.
  - Telas e monitores não devem ficar voltados para portas, janelas ou corredores.
  - Minimize o uso de janelas ou utilize vidro unidirecional.
- Utilize placas e outros avisos como medidas dissuasivas.
- Os pontos de entrada para zonas seguras devem ser discretos.
  - Os mecanismos de segurança específicos não devem ser óbvios.
- O tráfego entre zonas deve ser minimizado.
- As áreas públicas devem ser altamente visíveis
  - Projetadas para impedir que invasores usem portas de rede, scanners, etc., de forma oculta

Controles físicos

- Estratégia de defesa em profundidade
  - Defesa em camadas
- Pontos de entrada
  - Balizadores para bloquear o tráfego de veículos e proteger a estrutura física •
  - Cercas ao redor de locais seguros (não públicos) ÿ Transparentes
    - ÿ Robustas
    - ÿ Segurança contra escalada •
  - Portas trancadas (físicas, eletrônicas, biométricas) •
- Iluminação de segurança •
  - Segurança noturna
  - Auxilia na vigilância por vídeo

Pontos de entrada/saída

- Vestíbulo de controle de acesso
  - Tipo mais comum - dois conjuntos de portas, apenas um conjunto pode ser aberto/destrancado de cada vez (“armadilha para homens”)
  - Projetado para impedir a entrada não autorizada, aumentando a dificuldade de acesso • Catraca utilizada em implementações menos seguras
- Cartões/crachás de acesso
  - Utilizado para conceder acesso a áreas seguras e para identificar pessoal.
    - ÿ RFID, NFC, tarja magnética ÿ Identificação com foto
    - ÿ Também pode indicar o nível de acesso (número, código de cores, etc.)
  - Obrigatoriedade de tê-lo sempre visível ÿ Qualquer pessoa sem um deve ser questionada/denunciada

Prevenir e dissuadir

- Guardas de segurança •
  - Armados ou desarmados (dependendo da necessidade)
  - Utilizados para monitorar e controlar o acesso a pontos de controle críticos ÿ
    - Verificação de identidade, confirmação de acesso adequado, etc. • Presença visível é um forte fator de dissuasão e também pode prevenir agressões • Requer seleção e treinamento adequados • Videovigilância
  - Menos dispendioso que seguranças privados
    - ÿ O tempo de resposta a potenciais incidentes pode ser maior ÿ Requer monitorização constante
  - Possibilidade de registar eventos para efeitos de prova ou investigação • Forte efeito dissuasor, mas não preventivo

Sensores de segurança física

- Infravermelho
  - Detecta calor e movimento em áreas escuras
  - Normalmente, detectam apenas movimento de criaturas vivas.
- Micro-ondas
  - Sensor muito sensível, usado em locais mais críticos • Pode detectar qualquer movimento, especialmente através de objetos não metálicos • Funcionamento semelhante ao de um sonar
- Ultrassônico
  - Emite ondas sonoras em frequências acima da faixa de audição humana. • Frequentemente usado em sistemas de iluminação automatizados.
- Pressão
  - Detecta mudanças de pressão em uma área específica • Peso de pessoa, veículo, etc.

Engano e Perturbação Técnicas

Defesa Ativa

- Engajamento defensivo com o adversário
- O mais comum é o uso de recursos de isca
- Atuam como chamariz ou isca para os atacantes
  - Não armazenar recursos sensíveis
  - Isolado do restante da infraestrutura
- Projetado especificamente para ser vulnerável e acessível
  - Pode ser uma vulnerabilidade ou fraqueza específica, ou algo mais abrangente
- Os ativos de isca são monitorados de perto
- Permite a detecção de ameaças e intrusões ativas sem comprometer a segurança
- Pode ser usado para fins de pesquisa ou para detectar ameaças internas.

Pote de mel

- Sistema configurado especificamente para atrair atacantes •
  Semelhante ao mel que atrai moscas
- Registro extensivo ativado
  - Permite a análise de estratégias, táticas e ferramentas
- Projetado para fornecer um “alerta antecipado” de possíveis ataques
- Pode desviar a atenção de ativos sensíveis reais • Fundamental para isolar do restante do ambiente
  - Protege o restante da rede
  - Impede que o atacante obtenha informações sobre a infraestrutura • Rede completamente separada ou localizada na DMZ

Rede de Mel

- Semelhante a um honeypot, mas com uma rede de isca completa
- Consiste em múltiplos recursos (servidores, estações de trabalho, dispositivos de rede)
- Depende das necessidades e do cenário
- Pode usar recursos de rede reais ou emuladores
  - Emuladores podem ser mais baratos, mas podem não ser tão convincentes.
- Mais frequentemente usado para monitoramento e campanhas mais abrangentes
- Ameaças mais avançadas que exigem múltiplos recursos
- Comparado a vulnerabilidades ou ameaças de recurso único

Arquivos Enganosos

- Honeyfile e honeytoken
- Dados falsos sem significado para a organização
- Projetados para parecerem convincentes para o atacante
- Os arquivos contêm dados específicos e exclusivos que podem ser usados para rastrear
  - Endereços de e-mail, dados de banco de dados, arquivos executáveis
  - Beacons - objetos dentro do arquivo que contatam o servidor assim que o arquivo é aberto
  - Chaves AWS (ou de outra nuvem) únicas, porém inúteis
- Uma vez que os dados são roubados e/ou vazados, podem ser rastreados até um agente de ameaça específico
- Geralmente integrados a honeypots e honeynets

Estratégias de ruptura

• Adaptado de técnicas de ofuscação comumente usadas por atacantes • O objetivo é tornar os ataques mais difíceis e “caros” para os atacantes

• Requer mais recursos e tempo para os adversários • Comumente usado em ambientes de produção, em vez de honeynet • Exemplos • Registros DNS falsos que não existem

• Servidores web com diretórios falsos • Retornos falsificados em varreduras de portas (portas abertas que não são acessíveis) • Sumidouros de DNS

ÿ Pode ser encaminhado para honeypot ou honeynet para análise.

Gestão de Mudanças
Operações

Gestão de Mudanças

• Organizações e sistemas estão em constante evolução • Mudanças nos sistemas de informação são sempre necessárias • Abordagem sistemática para gerenciar todas as mudanças na infraestrutura de TI • Objetivo: minimizar interrupções e tempo de inatividade • Maximizar a eficiência e o valor das mudanças • Requer planejamento, testes, aprovações, supervisão, etc. • O processo trabalha em conjunto com a organização • Determinar impactos e dependências potenciais • Planos de contingência e planos de reversão • Documentação necessária

Operações comerciais

- O CM impacta mais do que apenas as operações de segurança •

As mudanças podem ser simples ou complexas

  - Atualizações ou implantações de software de rotina
  - Implantações de novos produtos
  - Modificações importantes na arquitetura de rede

- Processo de aprovação estruturado necessário para garantir o mínimo de interrupções • Novas vulnerabilidades introduzidas
  - Tempo de inatividade

  inesperado • Introdução de problemas

de conformidade • Após a conclusão das alterações, revisões e auditorias garantem os resultados

Partes interessadas

- Qualquer pessoa com interesse direto na mudança ou no projeto •
  - Trabalhar com e implementar mudanças (servidor, rede, segurança, desenvolvimento, etc.) •
  - Liderança supervisionando as operações •
  - Equipes de conformidade •

O envolvimento das partes interessadas garante:

- As alterações propostas recebem contribuições de múltiplas perspectivas •
- Ajuda a evitar riscos e problemas não óbvios • Minimiza
- interrupções não planejadas • Auxilia na

aceitação e adoção das mudanças

- Envolvimento e contribuições de diversas áreas da organização

Propriedade

- Indivíduos/grupos responsáveis pela implementação da mudança
  - Gerentes de projeto, líderes de equipe, etc.
- Responsáveis por garantir que a mudança seja concluída conforme planejado.
  - Prazos com
  - Se forem necessárias modificações, certifique-se de que sejam apropriadas

e aprovadas • Gerencie os riscos relacionados à

mudança • Qualquer tempo de

inatividade potencial • Necessidades adicionais de pessoal

- Planejar e implementar comunicação e treinamento conforme necessário •

Garantir que as partes interessadas sejam informadas e tenham aprovado

Conceitos de Gestão de Mudanças

- Análise de impacto •
  - Processo de identificação/avaliação das implicações da mudança •
  - Como afeta usuários, processos, sistemas, etc. •

Resultados dos testes

- As alterações são testadas primeiro em ambiente de teste antes de serem implementadas nos sistemas de produção. • Permitem identificar problemas ou impactos inesperados. •
- Planos de reversão • Planejam a reversão das alterações, retornando os sistemas às configurações anteriores. • Minimizam o risco de tempo de inatividade caso a alteração não ocorra conforme o planejado. • Janelas de manutenção
- Prazo predefinido para implementação de alterações

- POPs (Procedimentos Operacionais Padrão)
  - Instruções escritas e detalhadas para operações ou alterações de rotina

Gestão de Mudanças

Considerações técnicas

Listas de permissão e bloqueio

- Listas podem ser usadas em múltiplos contextos
  - Aplicativos permitidos/bloqueados
  - Regras de firewall
  - Relacionado a mudanças
- Contexto de gestão de mudanças
  - Tipos de alteração de software e hardware que não precisam passar por todo o processo
  - Alterações de software e hardware não permitidas/que sempre devem passar pelo processo
  - Indivíduos autorizados a aprovar alterações
  - Restrições/permissões existentes nos sistemas que podem afetar as alterações
  - Software permitido com base no valor de hash - valor diferente após a alteração

- As alterações geralmente envolvem reinicializações •
  - Reinicializações do servidor
  - Reinicialização de serviços/processos durante atualizações e patches
  - Aplicativos atualizados param de funcionar durante atualizações
- Reinicializações geralmente resultam em algum tempo de inatividade • Devem ser minimizadas sempre que possível • Agendadas e comunicadas aos usuários com antecedência adequada • Objetivo - reduzir o impacto nos usuários e nos processos de negócios • Os sistemas podem ter dependências de outros softwares/sistemas
  - A reinicialização do servidor/serviço de banco de dados afeta todos os aplicativos que utilizam esse servidor. • Alterações simples podem ter impactos maiores se não forem cuidadosamente planejadas. • Pode afetar o tempo necessário para a implementação da alteração e o tempo de inatividade resultante.

Aplicações Legadas

- Muitas organizações ainda utilizam sistemas/softwares "legados".
  - Pode não receber mais atualizações •
  - Pode conter problemas/vulnerabilidades de segurança
- Aplicativos legados podem ser incompatíveis com softwares mais recentes . •

Podem criar complicações com outras alterações. • Aplicativo

antigo com banco de dados no servidor que precisa de atualizações. •

Atualizações do servidor de banco de dados criam problemas com

o aplicativo legado . • Podem exigir soluções

especializadas . • Virtualização, emulação, software personalizado, sistemas extras, etc.

- Frequentemente carecem de documentação e suporte suficientes por parte do fornecedor.

Documentando as alterações

Documentação

- Todas as alterações precisam de documentação cuidadosa e intencional.
  - Solicitação, anotações, aprovação, discussão, implementação, etc. •

Alterações frequentemente exigem a atualização de outros documentos.

- Políticas e procedimentos •
- Diagramas de rede/estrutura •
- Instruções de usuário específicas do software

- A frequência de atualização da documentação depende da organização e das alterações.
  - Normalmente atualizado sempre que ocorrem mudanças ou atualizações importantes ÿ Aplicativos, sistemas, processos,

etc. • A documentação atualizada deve ser indicada com as novas informações de versão. • Arquive as versões antigas, mas mantenha-as acessíveis para consulta, se necessário.

Tipos de Documentação

- Solicitações de alteração
  - Informações sobre a alteração necessária
  - Atualizações para refletir mudanças de status, modificações, aprovações, etc.
- Políticas e procedimentos
  - Revisar e atualizar conforme necessário após/durante as alterações
- Sistemas e processos • Atualizado para refletir as mudanças do sistema • Alterações na arquitetura, diagramas, manuais do usuário, etc.
- Gerenciamento de configuração
  - Informações de configuração atualizadas, atualizadas após cada alteração
- Material de treinamento
- Planos de resposta/recuperação de incidentes

Controle de versão

- Rastreamento e gerenciamento de alterações em documentos, código, etc.
- Mantém um histórico de todas as alterações
- Solicitações, aprovações, etc.
- Permite a reversão oportuna de alterações, se necessário
- Em vez de consultar a documentação e reverter manualmente
- Documentação atualizada
  - Diagramas, processos, procedimentos, políticas, instruções, etc.
  - Oferece um método fácil para visualizar atualizações.
  - Ajuda a evitar confusão e o uso potencial de documentos desatualizados.

Tipos de criptografia

Terminologia de Criptografia

• Texto plano - dados originais e legíveis •
Algoritmo/Cifra - método de criptografia e descriptografia do texto plano • Texto cifrado -
dados criptografados, que aparentam ser aleatórios e ilegíveis • Chave - dados que
passam pelo algoritmo usado para codificar e decodificar • Espaço de chaves - intervalo
de valores que podem ser usados para construir a chave • Comprimento da chave
- número de bits usados na chave • Criptografia
de chave simétrica - usa a mesma chave para criptografar e descriptografar • Criptografia de chave
assimétrica - chaves separadas para criptografar e descriptografar
descriptografia
• Chave pública e chave privada

Criptografia e Hashing para Fins

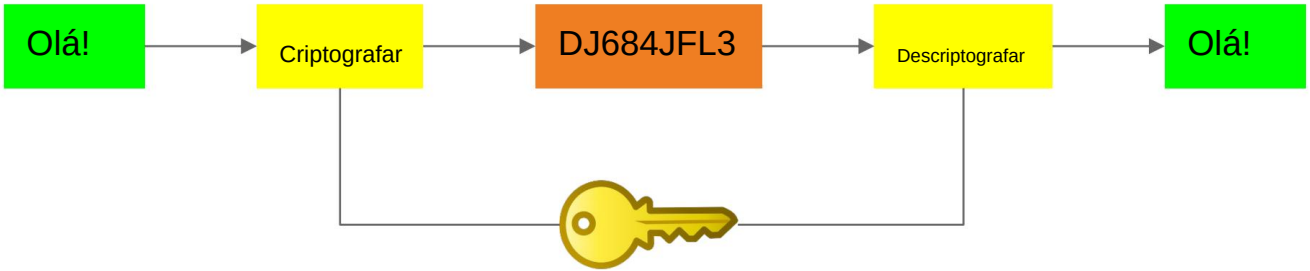
- Confidencialidade •
  Texto criptografado ilegível sem descriptografia
- Integridade
  • A verificação por hash garante que os dados não foram alterados.
- Autenticidade •
  Pares de chaves pública/privada e certificados verificam a origem dos dados • Não repúdio •
  Certificados e chaves/assinaturas exclusivas comprovam a atividade • Autorização
  • Certificados utilizados para comprovar identidade e conceder acesso

Força da criptografia

- Dificuldade em descobrir o algoritmo e/ou a chave • Qualquer
  um que não seja de conhecimento
público • Tempo necessário para quebrar a
criptografia • Quantidade de poder de processamento e recursos
necessários •
  Determinado por • Algoritmo de
  criptografia usado • Comprimento e
  complexidade da
chave • Sigilo da chave • Quanto mais forte a criptografia, mais tempo deve levar para quebrá-la (se for p

Criptografia Simétrica

- A criptografia simétrica usa a mesma chave/cifra para criptografar e descriptografar.



Alice

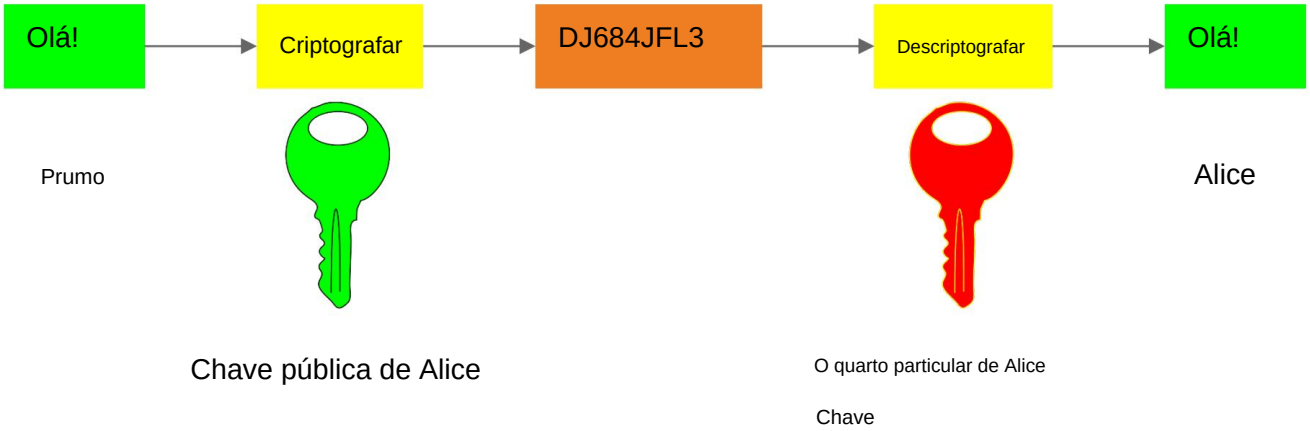
Prumo

Criptografia Simétrica

- Os algoritmos tendem a ser mais seguros do que os algoritmos assimétricos
- Mais rápidos do que os algoritmos assimétricos
- Oferecem confidencialidade, mas não autenticidade ou integridade
- Centenas de algoritmos diferentes disponíveis
  - DES - Data Encryption Standard
  - 3DES - Triple DES
  - AES - Advanced Encryption Standard
  - RC4 - Rivest Cipher 4
  - RC5 - Rivest Cipher 5
- Requer chave compartilhada entre os pontos de comunicação
  - Como essa chave pode ser compartilhada facilmente sem ser comprometida?

Criptografia Assimétrica

- A criptografia assimétrica usa chaves diferentes para criptografar e descriptografar.



Criptografia Assimétrica

- A criptografia assimétrica é a “chave” da PKI
- Chave pública - disponível publicamente, qualquer pessoa pode ter e usar
  - Bob pode usar a chave pública de Alice para criptografar dados secretos e enviá-los para Alice.
- Chave privada - conhecida apenas pela pessoa/entidade que a cria.
  - NÃO DEVE SER COMPARTILHADO
  - Bob pode usar sua chave pública para descriptografar dados privados enviados a ele.
  - Alice pode usar sua chave privada para assinar digitalmente os dados enviados a Bob.
    - ÿ Bob descriptografa (e verifica a assinatura) usando a chave pública de Alice .
- Cada chave só pode criptografar OU descriptografar.
  - Os dados criptografados com uma chave pública **NÃO** podem ser descriptografados com essa mesma chave.
- **O serviço de custódia de chaves** pode ser usado para garantir que as chaves não sejam perdidas.
  - Chave(s) arquivada(s) com um terceiro *CONFIÁVEL*

Algoritmos de criptografia assimétrica

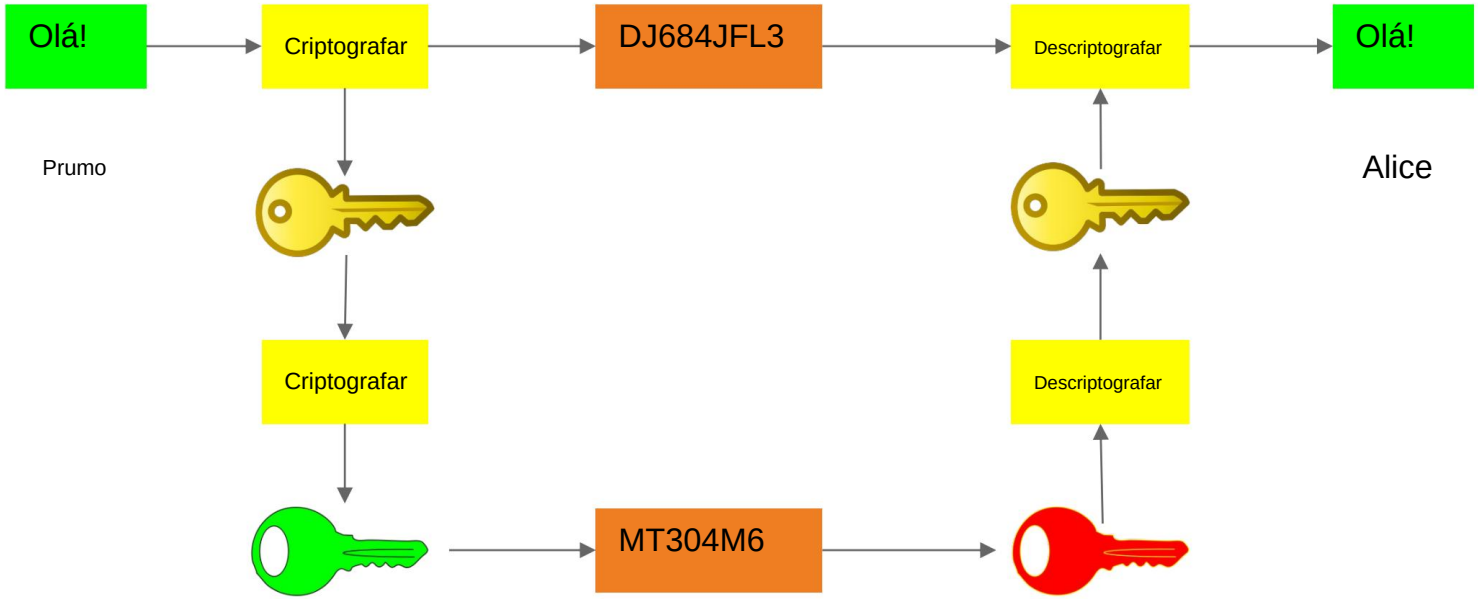
• Algoritmos mais complexos que os simétricos • Muito mais lentos que os algoritmos simétricos • Oferecem confidencialidade, autenticidade e não repúdio • Requerem duas chaves - privada e pública • Dois algoritmos principais em uso • Diffie-Hellman - usado principalmente para troca de chaves • RSA - Rivest Shamir Adleman

PKI

Simétrico e assimétrico

- O método simétrico é rápido, mas a troca de chaves é complexa.
- O método assimétrico resolve o problema da troca de chaves, mas os algoritmos são lentos.
  - Possível problema com a confiabilidade da fonte da chave pública.
- Criptografia assimétrica usada para proteger a(s) chave(s) da criptografia simétrica
  - Os dados a serem protegidos são criptografados com uma chave.
  - O remetente encontra a chave pública do destinatário e criptografa a primeira chave, enviando-a ao destinatário.
  - O destinatário usa a chave privada para descriptografar a mensagem e recebe a primeira chave.
  - Descriptografa a mensagem original usando essa chave.
- Base da maioria das comunicações seguras usadas atualmente.
  - Sites HTTPS

Criptografia e troca de chaves



Criptografia de chave pública

- Compartilhamento de chaves necessário para fluxos de trabalho de criptografia • É necessário compartilhar uma chave secreta OU • Utilizar pares de chaves pública/privada

- Compartilhar chaves públicas universalmente é problemático
  - Como compartilhar essas chaves de forma confiável? • Como ter certeza de que a chave é legítima? ÿ Qualquer pessoa pode criar pares de chaves ÿ Qualquer pessoa pode reivindicar a propriedade de uma chave pública

Infraestrutura de chave pública

- Sistemas projetados para tornar a comunicação segura fácil e acessível
  - Padrões
  - Protocolos de comunicação •
  - Políticas de segurança •
  - Sistemas de criptografia
- O objetivo é estabelecer e manter um alto nível de confiança nas chaves. •

Funciona com base em um modelo de criptografia híbrida.

  - Criptografia simétrica e assimétrica
- PKI não é criptografia de chave pública
  - Infraestrutura que possibilita confiança e facilidade de uso
  - Construído parcialmente com base em criptografia de chave pública

Infraestrutura de chave pública

- Fornece a confiança necessária para chaves públicas
  - Rede de confiança
- Computadores e navegadores confiam em determinadas Autoridades Certificadoras Raiz (Autoridades Certificadoras Raiz Confiáveis) • Autoridades Certificadoras Confiáveis emitem certificados digitais • Servidores web (e outros) instalam esses certificados • Criptografam a comunicação • Verificam a identidade do servidor
- Certificados assinados por Autoridades Certificadoras confiáveis • Chave pública verificada e identificada nos certificados
- O computador/navegador confia implicitamente no site

Autoridades de Certificação (AC)

- Entidade confiável (organização ou servidor) • Todos os dispositivos confiam nas ACs da organização • Os certificados emitidos têm o mesmo nível de confiança
- Mantém e emite certificados
- CA raiz
  - Autoridade Certificadora principal da organização • Verifica as Autoridades Certificadoras subordinadas
  - Altamente seguro • Normalmente mantido offline •

Autoridade Certificadora intermediária (ou Autoridade Certificadora subordinada) • Confiável e certificado pela Autoridade Certificadora raiz • Processa solicitações e emite certificados

Certificados digitais

- Conceito central de PKI

Associa uma chave pública a um proprietário declarado • O padrão mais comum é o X.509

  - Exige o uso de determinados campos no certificado • Algoritmo, datas de validade, assinatura do emissor

Especifica o “sujeito” - quem é o proprietário do certificado

Também o “emissor” - qual entidade gerou e emitiu o certificado

  - O emissor certifica a identidade do titular do documento

- Certificados autoassinados

  Criados pelo proprietário (titular) e não emitidos por terceiros

Tipos de Certificados

- Autoassinado •
  - Não emitido por uma CA confiável
  - • Criado pelo sistema/aplicativo que está usando o certificado • Comum em certificados padrão em novos dispositivos
- Terceiros •
  - Certificados (geralmente) adquiridos de um fornecedor especializado
    - ÿ Autoridade Certificadora (AC)

publicamente confiável • Coringa

- • Certificados válidos para vários subdomínios •
  - Exemplo: *.example.com - válido para domain1.example.com e domain2.example.com

Revogação de Certificado

- Os certificados emitidos precisam ser revogados ocasionalmente.
  - Chaves comprometidas •
    Substituições por diversos motivos
- Lista de Revogação de Certificados (CRL)
  - Cada Autoridade Certificadora mantém a sua própria
  - Lista de todos os certificados que foram revogados
- Protocolo de Status de Certificado Online (OCSP)
  - Retorna o status de um único certificado em vez da CRL completa • Não depende do navegador ou de outros sistemas • O OCSP verifica automaticamente a CRL das ACs

Solicitação de Assinatura de Certificado (CSR)

- Usado ao solicitar um certificado de uma Autoridade Certificadora (CA)
  - Servidores web - administradores de sistema
  - E-mail - usuário final
- PKCS #10 - Padrão de Criptografia de Chave Pública #10
  - Define o formato para todas as solicitações de certificado
- O sistema/indivíduo solicitante gera o par de chaves e mantém a chave privada.
- A chave pública é passada para a Autoridade Certificadora (CA) na solicitação.
- Informações adicionais incluídas.
  - Nome comum
  - Nome da organização
  - Localidade (cidade), Estado, Condado
  - Endereço de e-mail

Ferramentas de criptografia

Módulo de plataforma confiável (TPM)

• Padrão para armazenamento baseado em hardware para dados criptografados •

Normalmente um chip integrado à placa-mãe ou CPU • Cada um é codificado

com uma chave privada estática - não pode ser alterada • As subchaves podem ser

redefinidas por meio da “propriedade” do TPM

• Finalidades: •

Armazenamento seguro para chaves de

criptografia • Autenticação de dispositivos de plataforma de

hardware • Verificação criptográfica da configuração de hardware ÿ Útil durante o

processo de inicialização para verificar a integridade do sistema •

Comumente usado com o BitLocker do Windows

Módulo de segurança de hardware (HSM)

• Dispositivo de hardware físico separado para gerenciamento de chaves • Diferente do TPM (não integrado a outros hardwares) • Finalidade dedicada com menor superfície de ataque • Geralmente um dispositivo reforçado, com recursos de segurança dedicados • Hardware certificado, sistema operacional focado em segurança, etc. • Recursos de detecção de adulteração • Executa operações de criptografia

• Assinaturas digitais, autenticação, etc. • Podem ser parte integrante de um ambiente de Infraestrutura de Chaves Públicas (PKI).

• Armazenamento de chaves, arquivamento, custódia

Sistema de gerenciamento de chaves

- Sistema responsável pelo ciclo de vida completo das chaves criptográficas
  - Geração, distribuição, revogação, expiração e renovação
- Geralmente integrado a ambientes de PKI
  - Disponível de forma independente
- Pode incluir funcionalidade de garantia fiduciária essencial
  - Armazenar chaves de “backup” de forma segura • Depende de onde as chaves foram geradas e da finalidade das chaves ÿ TPM e HSM também podem ser usados

Enclave Seguro

• Local de memória isolado • Permite a

execução de código em um ambiente de execução confiável (TEE)

• Protege código sensível e seguro •

Protegido e seguro por hardware dedicado • Não pode ser alterado ou

gravado por processos externos • Exemplos: • Intel SGX (Software Guard

Extensions) ÿ

integrado em CPUs Intel modernas

• Zona de confiança do Arm

Criptografia

Soluções

Criptografia de dados

- Os dados podem estar em um de três estados.
  - Dados em repouso - em mídias de armazenamento
  - Dados em trânsito (movimento) - sendo transferidos pela rede
  - Dados em uso (processamento) - dados presentes na RAM (ou outra memória volátil)

Criptografia de arquivos

- Arquivos individuais (ou múltiplos) no disco são criptografados
- Também pode ser em nível de pasta

- Criptografia de banco de dados
  - Todo o banco de dados (ou parte dele) é criptografado
  - A unidade e/ou o volume podem ou não ser criptografados
  - Também é possível criptografar tabelas, colunas e registros específicos

Criptografia em nível de disco

- Criptografia de disco completo (FDE) •

  Todo o conteúdo da unidade é criptografado • Para a unidade do sistema operacional, a descriptografia ocorre na inicialização • As chaves normalmente são armazenadas no TPM • Criptografia de partição e volume

  • Uma partição é um "pedaço" bruto de um disco.

  • Volume é uma partição formatada com uma letra de unidade atribuída (no Windows) • Partição ou volume único em disco criptografado

Hashing

- Função unidirecional • O hashing não pode ser revertido • Pode ser alvo de força bruta
- Os algoritmos são informações públicas •

Usados para verificar a integridade de arquivos, mensagens, etc.

  - Assinatura digital
- Algoritmos de hash robustos evitam “colisões”
  - Duas entradas diferentes resultam na mesma saída de hash
- MD5 (Message Digest 5) - hash de 128 bits • SHA (Secure Hash Algorithm) - hash de 160 bits • SHA-1, SHA-256, SHA-384, SHA-512
  - Hashes de 160 bits a 512 bits

Assinaturas digitais

- Utiliza criptografia assimétrica • Chaves públicas e privadas
- O autor gera um hash do item criado • Arquivo, documento, imagem, e-mail, aplicativo, etc.
- O autor usa sua própria chave privada para “assinar” digitalmente • Criptografa o hash com a chave privada
- O destinatário usa a chave pública do autor para descriptografar o hash e verificar • Fornece autenticidade, verificação de integridade e não repúdio • Somente a chave pública do autor pode descriptografar o hash • Um hash verificado indica que o documento não foi modificado

Salga

- Normalmente usado para ajudar a proteger hashes de senhas armazenadas
  - O hash não pode ser revertido, mas pode ser alvo de força bruta para determinar o valor original.
- O “salt” é adicionado ao valor original da senha antes do hash.
  - Personagens aleatórios
- Impede que atacantes usem tabelas hash como força bruta • Tabelas não calculadas com o salt específico usado • Não podem ser usadas para força bruta
- Salt diferente para cada senha -> senhas idênticas, valores diferentes • Alongamento de chave • Chave gerada a partir da senha/salt, convertida repetidamente em chaves mais longas • Não necessariamente uma chave mais forte, mas pode retardar ataques

Ofuscação

- Esteganografia •
  Incorporação de informações em outra fonte • Normalmente,
  os dados são ocultos em um arquivo de imagem
  • A mensagem pode ser criptografada antes da incorporação
- Mascaramento de
  dados • Redação de dados (substituição por um caractere diferente, “x”)
  • Frequentemente realizada em campos de banco de dados
- Tokenização
  • Todos ou parte dos dados substituídos por um token gerado aleatoriamente •
  O token é armazenado com o valor original em um local separado •
  Serviços/aplicativos autorizados podem consultar o cofre de tokens para obter os dados originais

Blockchain

- Lista de registros transacionais armazenados usando criptografia
- Cada registro é um “bloco” e é processado por uma função hash
  - O hash do bloco anterior é adicionado ao cálculo do hash do próximo bloco na cadeia.
  - Garante que cada bloco subsequente esteja criptograficamente vinculado.
- Um bloco valida o hash do bloco anterior, e assim por diante.
  - Garante que os registros de transações não foram adulterados
- Registrado em **livro-razão público aberto**
  - Registro descentralizado - mitiga o risco de ponto único de falha/comprometimento
- Pode ser usado para garantir a integridade e a transparência de
  - Transações financeiras, contratos legais
  - Proteção de direitos autorais e propriedade intelectual
  - Votação online, gerenciamento de identidade

ESPECIALISTAS EM TORNÁ-LO UM ESPECIALISTA