NEaD
Núcleo de Educação a Distância

CYBER SECURITY

Faculdade IMPACTA

9

Noções básicas de defesa

Alex Sandro da Silva Feitosa

Resumo

Nessa aula iniciaremos com a explicação de como a estratégia de Defesa em profundidade é usada para proteger as redes, abordaremos conceitos sobre políticas, regulamentos e padrões de segurança, finalizando com controle de acesso, fontes de inteligência e criptografia.

1.1. Compreendendo a Defesa

1.1.1 Defesa em profundidade

Analistas de segurança cibernética devem se preparar para qualquer tipo de ataque. É seu trabalho proteger os ativos da rede da organização.

Para fazer isso, os analistas de segurança cibernética devem primeiro identificar:

- Ativos - qualquer coisa de valor para uma organização que deve ser protegida, incluindo servidores, dispositivos de infraestrutura, dispositivos finais e o maior ativo, dados.
- Vulnerabilidades - Uma fraqueza em um sistema ou em seu design que pode ser explorada por um ator de ameaça.
- Ameaças- Qualquer perigo potencial para um ativo.

A coleta de todos os dispositivos e informações de propriedade ou gerenciadas pela organização são os ativos.

Estes ativos devem ser inventariados e avaliados quanto ao nível de proteção necessário para impedir potenciais ataques.

O gerenciamento de ativos consiste em inventários de todos os ativos e, em seguida, desenvolver e implementar políticas e procedimentos para protegê-los.

Essa tarefa pode ser assustadora, considerando que muitas organizações precisam proteger usuários e recursos internos, trabalhadores móveis e serviços virtuais e baseados em nuvem.

Além disso, as organizações precisam identificar onde os ativos de informações essenciais estão armazenados e como o acesso é obtido a essas informações.

Os ativos de informação variam, assim como as ameaças contra eles. Cada um desses ativos pode atrair diferentes atores de ameaças que têm diferentes níveis de habilidade e motivações.

Identificando Vulnerabilidades

A identificação de ameaças fornece a uma organização uma lista de prováveis ameaças para um ambiente específico.

Ao identificar ameaças, é importante fazer várias perguntas:

- Quais são as possíveis vulnerabilidades de um sistema?
- Quem pode querer explorar essas vulnerabilidades para acessar ativos de informações específicas?
- Quais são as consequências se as vulnerabilidades do sistema forem exploradas e os ativos forem perdidos?

A identificação de ameaças para um sistema de e-banking incluiria:

- Compromisso interno do sistema: O atacante usa os servidores de e-banking expostos para invadir um sistema bancário interno.
- Dados roubados do cliente: Um atacante rouba os dados pessoais e financeiros dos clientes bancários do banco de dados do cliente.
- Transações falsas de um servidor externo: Um invasor altera o código do aplicativo de e-banking e faz transações falsas usando um PIN de cliente roubado ou cartão inteligente: Um invasor rouba a identidade de um cliente e conclui transações mal-intencionadas da conta comprometida.
- Erros de entrada de dados: Um usuário insere dados incorretos ou faz solicitações de transação incorretas.
- Destruição do data center: Um evento cataclísmico danifica gravemente ou destrói o data center.

Identificar vulnerabilidades em uma rede requer uma compreensão dos aplicativos importantes usados, bem como das diferentes vulnerabilidades desse aplicativo e hardware. Isso requer uma quantidade significativa de pesquisa por parte do administrador de rede.

Identificando Ameaças

As empresas devem usar uma abordagem de defesa profunda para identificar ameaças e proteger ativos vulneráveis.

Essa abordagem usa várias camadas de segurança na borda da rede, na rede e nos pontos de extremidade da rede.

Nessa abordagem, um roteador primeiro faz a triagem do tráfego, antes de encaminhá-lo para um appliance de firewall dedicado, por exemplo, o Cisco ASA.

Os roteadores e firewalls não são os únicos dispositivos que são usados em uma abordagem de defesa em profundidade.

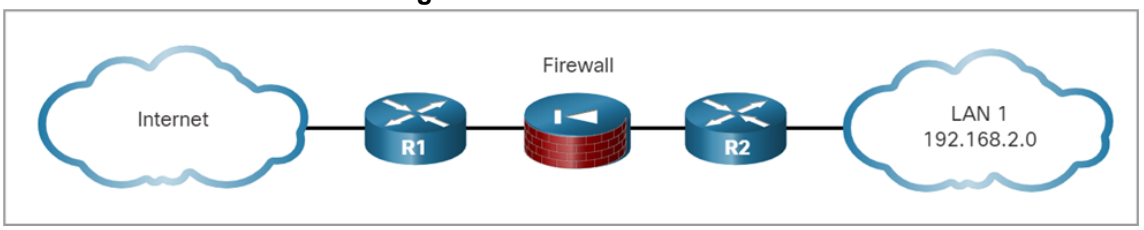
Outros dispositivos de segurança incluem IPS (Intrusion Prevention Systems), proteção avançada contra malware (AMP), sistemas de segurança de conteúdo da Web e de e-mail, serviços de identidade, controles de acesso à rede e muito mais.

Na abordagem de segurança em camadas de defesa em profundidade, as diferentes camadas trabalham juntas para criar uma arquitetura de segurança na qual a falha de uma salvaguarda não afeta a eficácia das outras salvaguardas.

A figura exibe uma topologia simples de uma abordagem de defesa em profundidade:

- Roteador de borda - A primeira linha de defesa é conhecida como um roteador de borda (R1 na figura). O roteador de borda tem um conjunto de regras especificando qual tráfego ele permite ou nega. Ele passa todas as conexões que se destinam à LAN interna para o firewall.
- Firewall - Uma segunda linha de defesa é o firewall. O firewall é um dispositivo de ponto de verificação que executa filtragem adicional e rastreia o estado das conexões. Ele nega o início de conexões das redes não confiáveis para a rede confiável, ao mesmo tempo em que permite que os usuários internos estabeleçam conexões bidirecionais com as redes não confiáveis.
- Roteador interno - Outra linha de defesa é o roteador interno (R2 na figura). Ele pode aplicar regras de filtragem finais no tráfego antes de ser encaminhado para seu destino.

Figura 1.1 Firewal de Borda



Fonte: CCNA Cyber OPS Associate v1, 2020.

Entendendo a Defesa, a Security Onion e Security Artichoke

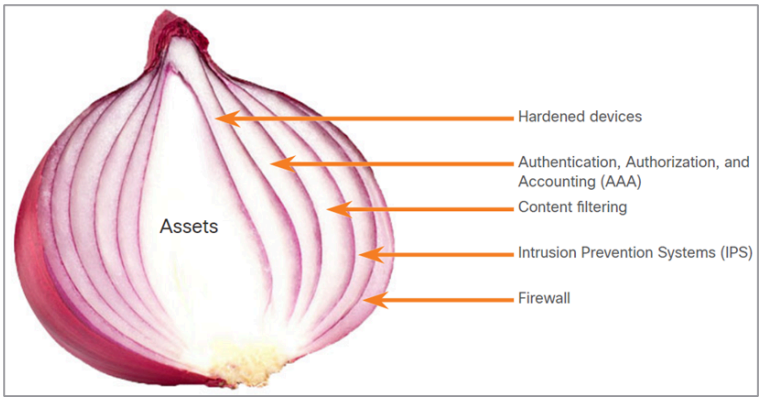
Existem duas analogias comuns que são usadas para descrever uma abordagem de Security Onion.

Uma analogia comumente usada para descrever uma abordagem de defesa em profundidade é chamada de “The Security Onion”.

Como ilustrado na figura, um ator de ameaça teria que descascar as defesas de uma rede camada por camada de uma maneira semelhante a descascar uma cebola.

Somente depois de penetrar cada camada, o ator da ameaça alcançaria os dados ou o sistema de destino. Defesa em profundidade.

Figura 1.2 Onion



Fonte: CCNA Cyber OPS Associate v1, 2020.

Observação: A Security Onion descrita nesta página é uma forma de visualizar a defesa em profundidade. Isso não deve ser confundido com o conjunto Security Onion de ferramentas de segurança de rede.

Security Artichoke

A evolução das redes sem fronteiras mudou a analogia com a "Security Artichoke", que beneficia o ator de ameaça.

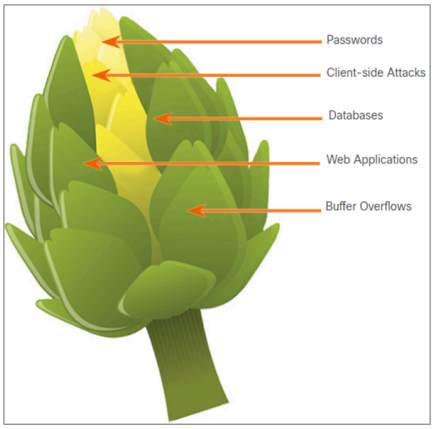
Conforme ilustrado na figura, os atores da ameaça não precisam mais descascar cada camada. Eles só precisam remover certas "artichoke leaves" (folhas de alcachofra).

O bônus é que cada "folha" da rede pode revelar dados confidenciais que não estão bem protegidos.

Para chegar ao coração da alcachofra, o hacker arranca a armadura de segurança ao longo do perímetro.

Embora os sistemas voltados para a Internet estejam muito bem protegidos, os hackers persistentes encontram uma lacuna nesse exterior hard-core através do qual eles podem entrar.

Figura 1.3 Alcachofra



Fonte: CCNA Cyber OPS Associate v1, 2020.

Políticas de segurança, regulamentos e padrões

Políticas de negócios são as diretrizes que são desenvolvidas por uma organização para governar suas ações.

As políticas definem padrões de comportamento correto para a empresa e seus funcionários.

Na rede, as políticas definem as atividades permitidas na rede.

Isso define uma linha de base de uso aceitável. Se um comportamento que viola a política de negócios for detectado na rede, é possível que tenha ocorrido uma violação de segurança.

Tabela 1.1. Uma organização pode ter várias diretivas orientadoras, conforme listado na tabela

Política	Descrição
Políticas da empresa	•Estabelece as regras de conduta e as responsabilidades dos trabalhadores e dos empregadores. •Protege os direitos dos trabalhadores, bem como os interesses comerciais dos empregadores. •Dependendo das necessidades da organização, várias políticas e procedimentos estabelecem regras relativas à conduta dos funcionários, assiduidade, código de vestimenta, privacidade e outras áreas relacionadas com os termos e condições de emprego.
Políticas de funcionários	•Essas políticas são criadas e mantidas pela equipe de recursos humanos para identificar o salário dos funcionários, o cronograma de pagamento, os benefícios dos funcionários, o horário de trabalho, as férias e muito mais. •Muitas vezes, eles são fornecidos a novos funcionários para revisar e assinar.
Políticas de Segurança	•Essas políticas identificam um conjunto de objetivos de segurança para uma empresa, definem as regras de comportamento para usuários e administradores e especificam os requisitos do sistema. •Esses objetivos, regras e requisitos garantem coletivamente a segurança de uma rede e dos sistemas de computador em uma organização. •É um documento em constante evolução com base nas mudanças no cenário de ameaças, vulnerabilidades e requisitos de negócios e funcionários.

Fonte: CCNA Cyber OPS Associate v1, 2020.

As políticas de segurança são usadas para informar os usuários, funcionários e gerentes sobre os requisitos de uma organização para proteger os ativos de tecnologia e informação.

Uma política de segurança abrangente tem uma série de benefícios, incluindo os seguintes:

- Demonstra o compromisso de uma organização com a segurança;
- Define as regras para o comportamento esperado;
- Garante a consistência nas operações do sistema, aquisição e uso de software e hardware e manutenção;
- Define as consequências legais das violações;
- Dá ao pessoal de segurança o apoio da gestão.

Uma política de segurança também especifica os mecanismos necessários para atender aos requisitos de segurança e fornece uma linha de base a partir da qual adquirir, configurar e auditar sistemas e redes de computadores para conformidade.

Tabela 1.2 A tabela a seguir lista as diretivas que podem ser incluídas em uma diretiva de segurança:

Política	Descrição
Política de identificação e autenticação	Ele especifica pessoas autorizadas que podem ter acesso a recursos de rede e procedimentos de verificação de identidade.
Políticas de senha	Isso garante que as senhas atendam aos requisitos mínimos e sejam alteradas regularmente.
Política de uso aceitável (AUP)	Ele identifica os aplicativos de rede e os usos aceitáveis para a organização. Também podem identificar as ramificações, se esta política for violada.
Política de acesso remoto	Ele identifica como os usuários remotos podem acessar uma rede e o que é acessível por meio de conectividade remota.
Políticas de Manutenção de Rede	Ele especifica os sistemas operacionais do dispositivo de rede e os procedimentos de atualização do aplicativo do usuário final.
Procedimentos de tratamento de incidentes	Descrevem como os incidentes de segurança são tratados.

Fonte:CCNA Cyber OPS Associate v1

Há também regulamentos externos em relação à segurança da rede.

Os profissionais de segurança de rede devem estar familiarizados com as leis e códigos de ética que são vinculativos para os profissionais de Segurança de Sistemas de Informação (INFOSEC).

Muitas organizações são obrigadas a desenvolver e implementar políticas de segurança.

Os regulamentos de conformidade definem o que as organizações são responsáveis pelo fornecimento e a responsabilidade caso não cumpram.

Os regulamentos de conformidade que uma organização é obrigada a seguir dependem do tipo de organização e dos dados que a organização manipula.

1.2. Controle de Acesso

1.2.1 Conceitos de controle de acesso

A segurança da informação trata da proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição.

Tríade CIA

A tríade da CIA consiste em três componentes da segurança da informação:

- Confidencialidade - Apenas indivíduos, entidades ou processos autorizados podem acessar informações confidenciais.
- Integridade - Refere-se à proteção de dados contra alterações não autorizadas.
- Disponibilidade - Os usuários autorizados devem ter acesso ininterrupto aos recursos e dados da rede de que necessitam.

Figura 1.4 Triade CIA

Fonte: CCNA Cyber OPS Associate v1, 2020.

Segurança Zero Trust

Zero Trust é uma abordagem abrangente para proteger todo o acesso em redes, aplicações e ambientes.

Essa abordagem ajuda a proteger o acesso de usuários, dispositivos de usuário final, APIs, IoT, microsserviços, contêineres e muito mais.

O princípio de uma abordagem de confiança zero é “nunca confiar, sempre verificar”.

Uma estrutura de segurança de confiança zero ajuda a impedir acesso não autorizado, conter violações e reduzir o risco de movimento lateral de um invasor através de uma rede.

Em uma abordagem de confiança Zero, qualquer lugar em que uma decisão de controle de acesso seja necessária deve ser considerado um perímetro.

Os três pilares da confiança zero são força de trabalho, cargas de trabalho e local de trabalho.

Confiança zero para a Força de Trabalho - Este pilar consiste em pessoas que acessam aplicativos de trabalho usando seus dispositivos pessoais ou gerenciados por empresas. Ele garante que apenas os usuários certos e dispositivos seguros possam acessar aplicativos, independentemente da localização.

Confiança zero para cargas de trabalho - Esse pilar está preocupado com aplicativos que estão sendo executados na nuvem, em data centers e outros ambientes virtualizados que interagem entre si. Ele se concentra no acesso seguro quando uma

API, um microsserviço ou um contêiner está acessando um banco de dados dentro de um aplicativo.

Confiança zero para o local de trabalho - Este pilar se concentra no acesso seguro para todos os dispositivos, inclusive na Internet das Coisas (IoT), que se conectam a redes empresariais, como terminais de usuário, servidores físicos e virtuais, impressoras, câmeras e muito mais.

Modelos de Controle de Acesso

Uma organização deve implementar controles de acesso adequados para proteger seus recursos de rede, recursos do sistema de informações e informações.

Um analista de segurança deve entender os diferentes modelos básicos de controle de acesso para ter uma melhor compreensão de como os invasores podem quebrar os controles de acesso.

A tabela a seguir lista vários tipos de modelos de controle de acesso:

- Uma organização deve implementar controles de acesso adequados para proteger seus recursos de rede, recursos do sistema de informações e informações.
- Um analista de segurança deve entender os diferentes modelos básicos de controle de acesso para ter uma melhor compreensão de como os invasores podem quebrar os controles de acesso.

Tabela 1.3 A tabela a seguir lista vários tipos de modelos de controle de acesso:

Modelos de controle de acesso	**Descrição**
Discretionary access control (DAC)	•Este é o modelo menos restritivo e permite que os usuários controlem o acesso aos seus dados como proprietários desses dados. •Ele pode usar ACLs ou outros métodos para especificar quais usuários ou grupos de usuários têm acesso às informações.
Controle de acesso obrigatório (MAC)	•Isso se aplica ao controle de acesso mais rigoroso e é usado em aplicações militares ou de missão crítica. •Ele atribui rótulos de nível de segurança às informações e permite que os usuários tenham acesso com base em sua autorização de nível de segurança.
Role-based access control (RBAC)	•As decisões de acesso são baseadas nas funções e responsabilidades de um indivíduo dentro da organização. •Diferentes funções recebem privilégios de segurança e indivíduos são atribuídos ao perfil RBAC para a função. •Também conhecido como um tipo de controle de acesso não discricionário.
Controle de acesso baseado em atributos (ABAC)	Permite o acesso com base em atributos do objeto a ser acessado, o sujeito acessando o recurso e fatores ambientais sobre como o objeto deve ser acessado.
Rule-based access control (RBAC)	•A equipe de segurança de rede específica conjuntos de regras ou condições associadas ao acesso a dados ou sistemas.

	•Essas regras podem especificar endereços IP permitidos ou negados, ou determinados protocolos e outras condições. •Também conhecido como RBAC Baseado em Regras.
Controle de acesso baseado em tempo (TAC)	Permite o acesso a recursos de rede com base na hora e no dia.

Fonte: CCNA Cyber OPS Associate v1, 2020.

1.3. Inteligência de Ameaças

1.3.1 Fontes de Informações

Para proteger eficazmente uma rede, os profissionais de segurança devem manter-se informados sobre as ameaças e vulnerabilidades.

Há muitas organizações de segurança que fornecem inteligência de rede, recursos, workshops e conferências para ajudar os profissionais de segurança.

Para permanecer eficaz, um profissional de segurança de rede deve:

- Mantenha-se a par das ameaças mais recentes — Inclui a subscrição de feeds em tempo real relativos a ameaças, a análise rotineira de Web sites relacionados à segurança, o seguimento de blogues e podcasts de segurança e muito mais.
- Continuar a atualizar habilidades — Inclui participar de treinamento relacionado à segurança, workshops e conferências.
  - Nota: A segurança de rede tem uma curva de aprendizagem muito acentuada e requer um compromisso com o desenvolvimento profissional contínuo.

Tabela 1.4 A tabela lista a organização de segurança de rede importante

Empresa	**Descrição**
SysAdmin, Auditoria, Rede, Segurança (SANS)	Os recursos do Instituto SANS são amplamente gratuitos mediante solicitação e incluem: •O Internet Storm Center - o popular sistema de alerta antecipado da internet •NewsBites - O resumo semanal de artigos de notícias sobre segurança informática. •@RISK - O resumo semanal de vetores de ataque recém-descobertos, vulnerabilidades com explorações ativas e explicações de como os ataques recentes funcionaram. •Alertas de segurança rápidos •Sala de Leitura - Mais de 1.200 trabalhos de pesquisa originais premiados. •O SANS também desenvolve cursos de segurança.
Mitre	A Mitre Corporation mantém uma lista de Vulnerabilidades e Exposições Comuns (CVE) usada por organizações de segurança proeminentes.
Fórum de equipes de resposta a incidentes e segurança (FIRST)	É uma organização de segurança que reúne uma variedade de equipes de resposta a incidentes de segurança de computador de organizações governamentais, comerciais e educacionais para promover a cooperação e

	coordenação no compartilhamento de informações, prevenção de incidentes e reação rápida.
SecurityNewsWire	Um portal de notícias de segurança que agrega as últimas notícias relativas a alertas, explorações e vulnerabilidades.
International Information Systems Security Certification Consortium (ISC)2	Fornece produtos educacionais neutros e serviços de carreira a mais de 75 mil profissionais do setor em mais de 135 países.
Center for Internet Security (CIS)	É um ponto focal para prevenção, proteção, resposta e recuperação de ameaças cibernéticas para governos estaduais, locais, tribais e territoriais (SLTT) por meio do Centro de Análise e Compartilhamento de Informações Multiestaduais (MS-ISAC). O MS-ISAC oferece alertas e alertas de ameaças cibernéticas 24 horas por dia, 7 dias por semana, identificação de vulnerabilidades e mitigação e resposta a incidentes.

Fonte: CCNA Cyber OPS Associate v1, 2020.

Os recursos para ajudar os profissionais de segurança a manter-se a par das ameaças mais recentes são o Relatório Anual de Segurança Cibernética da Cisco e o Relatório de Segurança Cibernética do Meio Ano.

Esses relatórios fornecem uma atualização sobre o estado de preparação para a segurança, análise especializada das principais vulnerabilidades, fatores por trás da explosão de ataques usando adware, spam e assim por diante.

Os analistas de segurança cibernética devem se inscrever e ler esses relatórios para saber como os atores de ameaças estão direcionando suas redes e quais ações podem ser tomadas para mitigar esses ataques.

Blogs e podcasts também fornecem conselhos, pesquisas e técnicas de mitigação recomendadas.

A Cisco fornece blogs sobre tópicos relacionados à segurança de vários especialistas do setor e do Cisco Talos Group.

Cisco Talos oferece uma série de mais de 80 podcasts que podem ser reproduzidos a partir da internet ou baixados para o seu dispositivo de escolha.

1.4. Criptografia

1.4.1 Integridade e autenticidade

Estes são os quatro elementos das comunicações seguras:

- Integridade dos dados - Garante que a mensagem não foi alterada. Quaisquer alterações nos dados em trânsito serão detectadas. A integridade é garantida pela implementação de um dos algoritmos Secure Hash (SHA-2 ou SHA-3). O algoritmo MD5 message digest ainda está em uso, mas deve ser evitado, pois é inseguro e cria vulnerabilidades em uma rede.
- Autenticação de origem - garante que a mensagem não é uma falsificação e realmente vem de quem é declarada. Muitas redes modernas

garantem autenticação com algoritmos como código de autenticação de mensagem baseado em hash (HMAC).

- Confidencialidade dos dados - Garante que apenas usuários autorizados possam ler a mensagem. Se a mensagem for interceptada, ela não poderá ser decifrada dentro de um razoável período de tempo. A confidencialidade dos dados é implementada usando algoritmos de criptografia simétrica e assimétrica.
- Dados não repudiáveis - Garante que o remetente não possa repudiar ou refutar a validade de uma mensagem enviada. O não repúdio depende do fato de que apenas o remetente possui as características ou a assinatura exclusivas de como essa mensagem é tratada (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

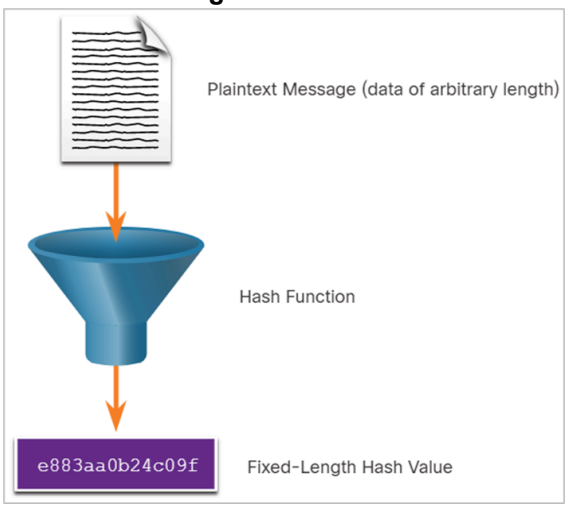
Hashes são usados para verificar e garantir a integridade dos dados.

O hash é baseado em uma função matemática unilateral que é relativamente fácil de calcular, mas significativamente mais difícil de reverter.

Como mostrado na figura abaixo, uma função hash leva um bloco variável de dados binários, chamado de mensagem, e produz uma representação condensada de comprimento fixo, chamado hash.

O hash resultante também é às vezes chamado de mensagem digest, digest ou impressão digital.

Figura 1.5 Hash



Fonte: CCNA Cyber OPS Associate v1, 2020.

Com funções hash, é computacionalmente inviável que dois conjuntos diferentes de dados apresentem a mesma saída hash.

Cada vez que os dados são modificados ou alterados, o valor de hash também muda. Por isso, muitas vezes os valores criptográficos de hash são chamados de impressões digitais.

Eles podem ser usados para detectar arquivos de dados duplicados, alterações de versão de arquivos e aplicativos semelhantes.

Esses valores são usados para proteger contra uma alteração acidental ou intencional dos dados ou corrupção acidental dos dados.

A função hash criptográfico é aplicada em muitas situações diferentes para autenticação de entidade, integridade de dados e fins de autenticidade de dados.

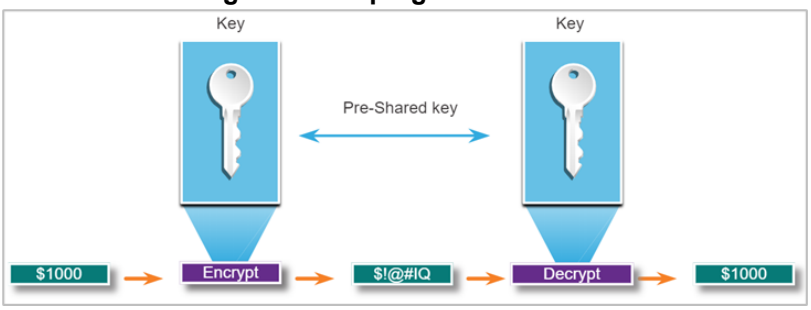
Existem quatro funções hash bem conhecidas:
MD5 com resumo de 128 bits- Desenvolvido por Ron Rivest e usado em muitos aplicativos da Internet, MD5 é uma função unilateral que produz uma mensagem hash de 128 bits. MD5 é um algoritmo legado e usado somente quando nenhuma alternativa melhor está disponível. Recomenda- se que SHA-2 ou SHA-3 sejam usados em vez disso.
SHA-1 - Desenvolvido pela Agência de Segurança Nacional dos EUA (NSA) em 1995. É muito semelhante às funções hash MD5. O SHA-1 cria uma mensagem de 160 bits e é um pouco mais lento que o MD5. O SHA-1 possui falhas conhecidas e é um algoritmo antigo.
SHA-2 - Desenvolvido pela NSA. Ele inclui SHA-224, SHA-256, SHA-384 e SHA-512. Se estiver usando SHA-2, os algoritmos SHA-256, SHA-384 e SHA-512 devem ser usados.
SHA-3 - SHA-3 é o mais novo algoritmo de hash e foi introduzido pelo NIST como uma alternativa para a família SHA-2 de algoritmos de hash. O SHA-3 inclui SHA3-224, SHA3-256, SHA3-384 e SHA3-512. A família SHA-3 são algoritmos de última geração e devem ser usados sempre que possível.
Embora o hashing possa ser usado para detectar alterações acidentais, ele não pode ser usado para proteger contra alterações deliberadas feitas por um agente de ameaça.
Não há informações de identificação única do remetente no procedimento de hash.
Isso significa que qualquer pessoa pode processar um hash para quaisquer dados, desde que tenha a função hash correta.
Portanto, hash é vulnerável a ataques man in the middle e não oferece segurança aos dados transmitidos. Para fornecer autenticação de integridade e origem, é necessário algo mais.
Observação:Os algoritmos de hash protegem somente contra alterações acidentais e não protegem os dados contra alterações feitas deliberadamente por um ator de ameaça (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

1.4.2 Criptografia simétrica e assimétrica

Existem duas classes de criptografia usadas para fornecer confidencialidade de dados; assimétrico e simétrico. Essas duas classes diferem na maneira como usam as chaves.
Algoritmos de criptografia simétrica, como Data Encryption Standard (DES), 3DES e Advanced Encryption Standard (AES), baseiam-se na premissa de que cada parte que se comunica conhece a chave pré-compartilhada.
A confidencialidade dos dados também pode ser garantida usando algoritmos assimétricos, incluindo Rivest, Shamir e Adleman (RSA) e a infraestrutura de chave pública (PKI).
Os algoritmos simétricos usam a mesma chave pré-compartilhada para criptografar e descriptografar dados.
Uma chave pré-compartilhada, também chamada de chave secreta, é conhecida pelo remetente e pelo receptor antes que qualquer comunicação criptografada possa ocorrer.

Considere um exemplo de criptografia simétrica em que Alice e Bob desejam trocar mensagens secretas um com o outro por meio do sistema de correio.
Na figura, Alice e Bob têm chaves idênticas e pré-compartilhadas. Alice escreve uma mensagem secreta e a coloca em uma pequena caixa e a tranca usando sua chave. Ela manda a caixa para Bob. Quando Bob recebe a caixa, ele usa sua chave para desbloquear e recuperar a mensagem. Bob pode usar a mesma caixa e chave para enviar uma resposta secreta de volta para Alice (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

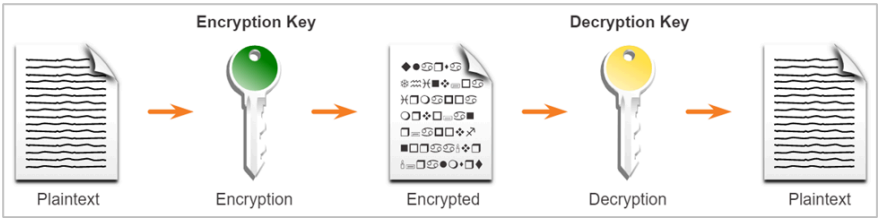
Figura 1.6 Criptografia Simétrica



Fonte: CCNA Cyber OPS Associate v1, 2020.

Os algoritmos de criptografia simétricos são comumente usados com tráfego VPN.
Isso ocorre porque os algoritmos simétricos usam menos recursos da CPU do que os algoritmos de criptografia assimétrica.
Isso permite que a criptografia e a descriptografia de dados sejam rápidas ao usar uma VPN.
Ao usar algoritmos de criptografia simétrica, quanto maior a chave, mais tempo levará para alguém descobrir a chave. A maioria das chaves de criptografia tem entre 112 e 256 bits.
Para garantir que a criptografia é segura, um comprimento mínimo de chave de 128 bits deve ser usado. Use uma chave mais longa para comunicações mais seguras.
Algoritmos de criptografia simétrica às vezes são classificados como uma cifra de bloco ou uma cifra de fluxo.
Os algoritmos assimétricos, também chamados de algoritmos de chave pública, são projetados de forma que a chave usada para criptografia seja diferente da chave usada para descriptografia, conforme mostrado na figura.
Algoritmos assimétricos usam uma chave pública e uma chave privada. Ambas as chaves são capazes do processo de criptografia, mas a chave emparelhada complementar é necessária para descriptografia.
O processo também é reversível. Os dados criptografados com a chave pública requerem a chave privada para descriptografar. Algoritmos assimétricos alcançam confidencialidade e autenticidade usando este processo (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Figura 1.7 Criptografia Assimétrica



Fonte: CCNA Cyber OPS Associate v1, 2020.

A criptografia assimétrica pode usar comprimentos de chave entre 512 e 4.096 bits.
Comprimentos de chave maiores ou iguais a 2.048 bits podem ser confiáveis, enquanto comprimentos de chave de 1.024 ou menores são considerados insuficientes.
Exemplos de protocolos que usam algoritmos de chave assimétrica incluem:
Internet Key Exchange (IKE) - é um componente fundamental das redes virtuais privadas IPsec (VPNs).
Secure Socket Layer (SSL) - Agora isso é implementado como TLS (Transport Layer Security) padrão da IETF.
Secure Shell (SSH) - Este protocolo fornece uma conexão segura de acesso remoto a dispositivos de rede.
Pretty Good Privacy (PGP) - Este programa de computador fornece privacidade e autenticação criptográficas. É frequentemente usado para aumentar a segurança das comunicações por email.
Os algoritmos assimétricos são substancialmente mais lentos que os algoritmos simétricos (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

1.4.3 Assinaturas digitais

As assinaturas digitais são uma técnica matemática usada para fornecer autenticidade, integridade e não repúdio.

As assinaturas digitais têm propriedades específicas que permitem autenticação de entidade e integridade de dados. Além disso, as assinaturas digitais fornecem não repúdio da transação.

Em outras palavras, a assinatura digital serve como prova legal de que o intercâmbio de dados ocorreu. As assinaturas digitais usam criptografia assimétrica.

As propriedades das assinaturas digitais são as seguintes:

Autêntico: A assinatura não pode ser forjada e fornece prova de que o signatário, e ninguém mais, assinou o documento.

Imutável: Depois que um documento é assinado, ele não pode ser alterado.

Não reutilizável: A assinatura do documento não pode ser transferida para outro documento.

Não repudiado: O documento assinado é considerado o mesmo que um documento físico. A assinatura é a prova de que o documento foi assinado pela pessoa real.

As assinaturas digitais são comumente usadas nas duas situações a seguir:

Assinatura de código: Isso é usado para fins de integridade de dados e autenticação. A assinatura de código é usada para verificar a integridade dos arquivos executáveis baixados do site de um fornecedor. Ele também usa certificados digitais assinados para autenticar e verificar a identidade do site que é a origem dos arquivos.

Certificados digitais: são semelhantes a um cartão de identificação virtual e usados para autenticar a identidade do sistema com o site de um fornecedor e estabelecer uma conexão criptografada para trocar dados confidenciais.

Existem três algoritmos DSS (Digital Signature Standard) que são usados para gerar e verificar assinaturas digitais:

Algoritmo de Assinatura Digital (DSA): DSA é o padrão original para gerar pares de chaves públicas e privadas e para gerar e verificar assinaturas digitais.

Rivest-Shamir Adleman Algoritmo (RSA): RSA é um algoritmo assimétrico que é comumente usado para gerar e verificar assinaturas digitais.

Elliptic Curve Digital Signature Algorithm (ECDSA): O ECDSA é uma variante mais recente do DSA e fornece autenticação de assinatura digital e não repúdio com os benefícios adicionais da eficiência computacional, tamanhos de assinatura pequenos e largura de banda mínima.

Na década de 1990, a RSE Security Inc. começou a publicar padrões de criptografia de chave pública (PKCS). Havia 15 PKCS, embora 1 tenha sido retirado a partir do momento em que esta escrita foi escrita.

1.4.4 Autoridades e o sistema de confiança de PKI

O tráfego da Internet consiste no tráfego entre duas partes. Ao estabelecer uma conexão assimétrica entre dois hosts, os hosts trocarão suas informações de chave pública.

Um certificado SSL é um certificado digital que confirma a identidade de um domínio de site.

Para implementar SSL em um site, o usuário compra um certificado SSL para o domínio de um provedor de Certificado SSL.

O terceiro de confiança faz uma avaliação antes da emissão das credenciais.Após essa investigação aprofundada, o terceiro emite credenciais que são difíceis de falsificar.

Quando os computadores tentam se conectar a um site via HTTPS, o navegador verifica o certificado de segurança do site e verifica se ele é válido e originado com uma autoridade de certificação confiável.

Isso valida que a identificação do site é verdadeira. O certificado é salvo localmente pelo navegador da Web e, em seguida, é usado em transações subsequentes. A chave pública do site está incluída no certificado e é usada para verificar futuras comunicações entre o site e o cliente.

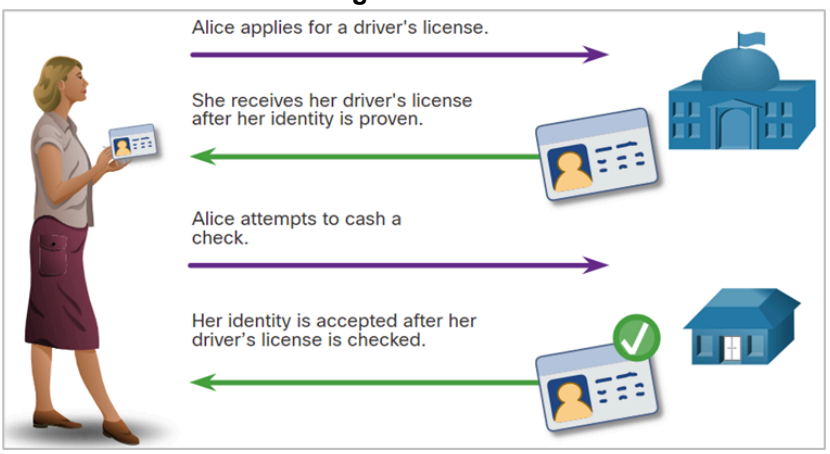
Esses terceiros confiáveis fornecem serviços semelhantes aos escritórios de licenciamento governamentais.

A figura ilustra como uma carteira de motorista é análoga a um certificado digital.

A Infraestrutura de Chave Pública (PKI) consiste em especificações, sistemas e ferramentas que são usados para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais.

A autoridade de certificação (CA) é uma organização que cria certificados digitais vinculando uma chave pública a uma identificação confirmada, como um site ou indivíduo.

Figura 1.8 CA



Fonte: CCNA Cyber OPS Associate v1, 2020.

O PKI é um sistema complexo projetado para proteger identidades digitais contra hacking por atores de ameaças ou estados-nação.

A PKI é necessária para oferecer suporte à distribuição em larga escala e à identificação de chaves de criptografia públicas.

A estrutura PKI facilita uma relação de confiança altamente escalável.

Consiste em hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais.

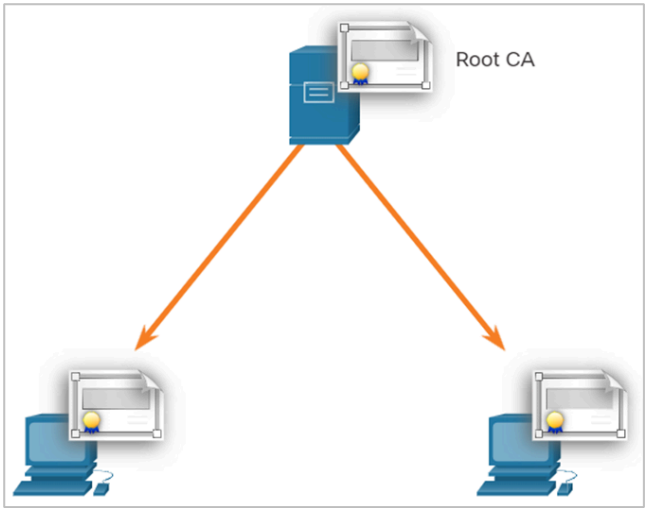
Topologia PKI de raiz única

Uma única AC, chamada de AC raiz, emite todos os certificados para os utilizadores finais dentro da mesma organização.

O benefício da abordagem é a sua simplicidade.

É difícil dimensionar para um ambiente grande, pois requer uma administração estritamente centralizada, o que cria um único ponto de falha.

Figura 1.9 Hierarquia CA



Fonte: CCNA Cyber OPS Associate v1, 2020.

A interoperabilidade entre uma PKI e seus serviços de suporte, como o Lightweight Directory Access Protocol (LDAP) e diretórios X.500, é uma preocupação porque muitos fornecedores de CA propuseram e implementaram soluções proprietárias.

Para resolver esse problema de interoperabilidade, o IETF publicou o Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527).

O padrão X.509 versão 3 (X.509 v3) define o formato de um certificado digital.

Aplicações x.509v3

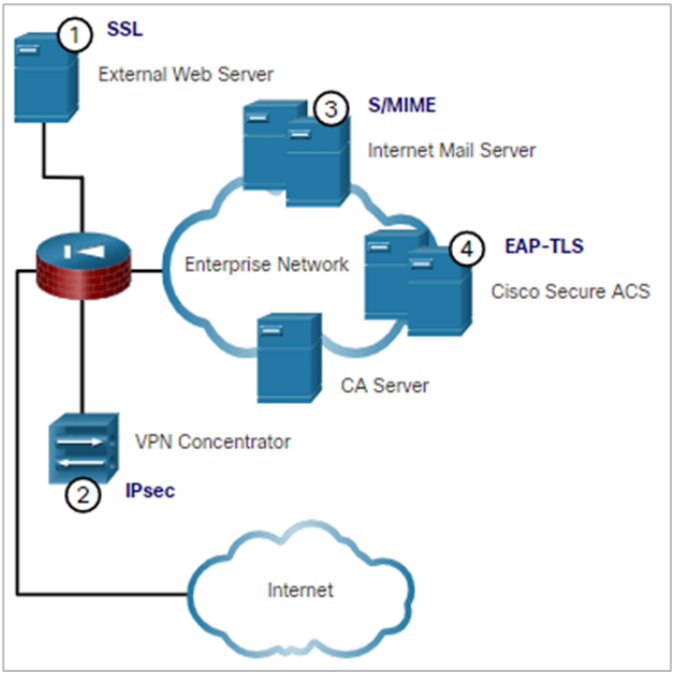
SSL: Servidores Web seguros usam X.509 v3 para autenticação de sites nos protocolos SSL e TLS, enquanto os navegadores da Web usam X.509 v3 para implementar certificados de cliente HTTPS.

IPsec: VPNs IPsec usam X.509 quando certificados podem ser usados como um mecanismo de distribuição de chave pública para autenticação baseada em RSA de troca de chaves de Internet (IKE).

S/MIME: agentes de correio do utilizador que suportam a proteção de correio com o protocolo S/MIME utilizam certificados X.509.

EAP-TLS: Os switches podem usar certificados para autenticar dispositivos finais que podem ser fornecidos a um ACS central por meio do protocolo de autenticação extensível com TLS (EAP-TLS).

Figura 1.10 Procedimento de autenticação com certificado



Fonte: CCNA Cyber OPS Associate v1, 2020.

A primeira etapa no procedimento de autenticação da autoridade de certificação é obter com segurança uma cópia da chave pública da autoridade de certificação.

Todos os sistemas que utilizam a PKI devem ter a chave pública da autoridade de certificação, que é chamada de certificado autoassinado.

A chave pública da autoridade de certificação verifica todos os certificados emitidos pela autoridade de certificação e é vital para o bom funcionamento da PKI.

Para muitos sistemas, como navegadores da Web, a distribuição de certificados de CA é processada automaticamente. O navegador da Web vem pré-instalado com um conjunto de certificados raiz de CA públicos.

O processo de registro de certificado é usado por um sistema host para se inscrever com uma PKI. Para fazer isso, os certificados de CA são recuperados em banda através de uma rede e a autenticação é feita fora de banda (OOB) usando o telefone.

O registro do sistema com a PKI entra em contato com uma autoridade de certificação para solicitar e obter um certificado de identidade digital para si mesmo e para obter o certificado autoassinado da autoridade de certificação.

O estágio final verifica se o certificado da autoridade de certificação foi autêntico e é executado usando um método fora de banda, como o POTS, para obter a impressão digital do certificado de identidade da autoridade de certificação válido.

A autenticação não requer mais a presença do servidor da autoridade de certificação e cada usuário troca seus certificados contendo chaves públicas.

Os certificados devem, por vezes, ser revogados. Aqui estão dois métodos mais comuns de revogação:

- **Lista de revogação de certificados (CRL):** Uma lista de números de série de certificados revogados que foram invalidados porque expiraram. As entidades PKI pesquisam regularmente o repositório CRL para receber a CRL atual.
- **Protocolo de Status de Certificado Online (OCSP):** Um protocolo de Internet usado para consultar um servidor OCSP para o status de revogação de um certificado digital X.509. As informações de revogação são imediatamente enviadas para um banco de dados on-line.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em: <https://www.netacad.com>.

SÊMOLA, Marcos. **Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes**: primeiros passos. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security**: applications and standards. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002** Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.