1.Introdução ao Hashing

Hashes são usados para verificar e garantir a integridade dos dados. Eles também são usados para verificar a autenticação. O hash é baseado em uma função matemática unilateral que é relativamente fácil de calcular, mas significativamente mais difícil de reverter.

Com funções hash, é computacionalmente inviável que dois conjuntos diferentes de dados apresentem a mesma saída hash. Além disso, o valor do hash muda toda vez que o é mudado ou alterado. Por causa disso, os valores de hash criptográficos são freqüentemente 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.

Existem quatro funções hash bem conhecidas:

- **MD5:** Desenvolvido por Ron Rivest e usado em uma variedade de aplicações de internet, MD5 é uma função unidirecional que produz uma mensagem hash de 128 bits. MD5 é considerado um algoritmo legado e deve ser evitado e usado apenas quando não houver alternativas melhores disponíveis. Recomenda- se que SHA-2 ou SHA-3 sejam usados em vez disso.
- **SHA-1:** Desenvolvido pela U.S. National Security Agency (NSA) em 1995. É muito semelhante às funções hash MD5. Existem várias versões. O SHA-1 cria uma mensagem de 160 bits e é um pouco mais lento que o MD5. O SHA-1 possui falhas e é um algoritmo antigo.
- **SHA-2:** Desenvolvido pela NSA. Inclui SHA-224 (224 bits), SHA-256 (256 bits), SHA-384 (384 bits) e SHA-512 (512 bits). Se você estiver usando SHA-2, então os algoritmos SHA-256, SHA-384 e SHA-512 devem ser usados sempre que possível.
- **SHA-3:** SHA-3 é o algoritmo de hashing mais recente e foi apresentado pelo Instituto Nacional de Padrões e Tecnologia (NIST) como uma alternativa e substituição eventual para a família SHA-2 de algoritmos de hash. SHA-3 inclui SHA3-224 (224 bits), SHA3-256 (256 bits), SHA3-384 (384 bits) e SHA3-512 (512 bits). A família SHA-3 são algoritmos de última geração e devem ser usados sempre que possível.

2.Assinatura digital

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.

- **Autenticidade:** A assinatura não pode ser falsificada e fornece prova de que o signatário, e ninguém mais, assinou o documento.

- **Inalterável:** Após assinar um documento, 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 em a**ssinaturas de códigos e certificados digitais**.

Assinar digitalmente o código fornece várias garantias sobre o código como garantir que o código é autêntico e é realmente originado pela editora; O código não foi modificado desde que saiu do editor do software e a editora publicou inegavelmente o código. Isso fornece não repúdio do ato de publicação.

Um **certificado digital** é equivalente a um passaporte eletrônico. Ele permite que usuários, hosts e organizações troquem informações com segurança pela Internet. Especificamente, um certificado digital é usado para autenticar e verificar se um usuário que está enviando uma mensagem é quem afirma ser. Os certificados digitais também podem ser usados para fornecer confidencialidade ao receptor com os meios de criptografar uma resposta.

O certificado digital verifica de forma independente uma identidade. Assinaturas digitais são usadas para verificar se um artefato, como um arquivo ou mensagem, é enviado pelo indivíduo verificado. Em outras palavras, um certificado verifica a identidade, uma assinatura verifica se algo vem dessa identidade.

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

- **Digital Signature Algorithm (DSA):** DSA é o padrão original para gerar pares de chaves públicas e privadas e para gerar e verificar assinaturas digitais.
- **Rivest Shamir Adleman (RSA):** RSA é um algoritmo assimétrico que é comumente usado para gerar e verificar assinaturas digitais
- **Algoritmo de assinatura baseado em curva elíptica (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

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 do site. Para implementar SSL em seu site, você compra um certificado SSL para seu domínio de um provedor de Certificado SSL.

A empresa terceirizada de confiança faz uma investigação aprofundada antes da emissão das credenciais. Após essa investigação aprofundada, o terceiro emite credenciais (ou seja, certificado digital) que são difíceis de falsificar. Desse ponto em diante, todos os indivíduos que confiam no terceiro simplesmente aceitam as credenciais que o terceiro emite.

Quando os computadores tentam se conectar a um site sobre HTTPS, o navegador da Web verifica o certificado de segurança do site e verifica que é válido e originado de uma **autoridade de certificação confiável (CA)**. Isso valida que a identificação do site é verdadeira. O certificado digital é salvo localmente pelo navegador da Web e é usado em transações subseqüentes. A chave pública do site está incluída no certificado e é usada para verificar futuras comunicações entre o site e o cliente.

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.

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.

Os certificados PKI contêm a chave pública de uma entidade ou de um indivíduo, a sua finalidade, a autoridade de certificação (AC) que validou e emitiu o certificado, o intervalo de datas durante o qual o certificado é válido e o algoritmo usado para criar a assinatura.

O armazenamento de certificados reside em um computador local e armazena certificados emitidos e chaves privadas

O Certificado de Autoridade PKI (CA) é um terceiro confiável que emite certificados PKI para entidades e indivíduos após verificar sua identidade. Ele assina esses certificados usando sua chave privada

O banco de dados de certificados armazena todos os certificados aprovados pela autoridade de certificação

As autoridades de certificação, especialmente aquelas que são terceirizadas, emitem certificados baseados em classes que determinam a confiabilidade de um certificado. A tabela fornece uma descrição das classes.

Classe	Descrição

0	Usado para testes em situações em que não foram realizadas verificações
1	Usado por indivíduos que exigem verificação de e-mail
2	Usado por organizações para as quais a prova de identidade é necessária
3	Usado para servidores e assinatura de software. A autoridade certificadora procede à verificação e verificação independentes da identidade e da autoridade
4	Usado para transações comerciais on-line entre empresas
5	Usado para organizações privadas ou segurança do governo

PKIs podem formar diferentes topologias de confiança. O mais simples é a topologia PKI de raiz única. Uma única autoridade de certificação, chamada de CA raiz, emite todos os certificados para os usuários finais, que geralmente estão dentro da mesma organização.

2.1 Topologias de AC certificadas cruzadas

Este é um modelo ponto a ponto no qual as ACs individuais estabelecem relações de confiança com outras ACs através da certificação cruzada de certificados de AC. Os usuários em ambos os domínios da CA também têm a certeza de que podem confiar uns nos outros. Isso fornece redundância e elimina o ponto único de falha.

2.2 Topologias de CA hierárquicas

A CA de nível mais alto é chamada de CA raiz. Ele pode emitir certificados para usuários finais e para uma autoridade de certificação subordinada. As subCAs podem ser criadas para suportar várias unidades de negócios, domínios ou comunidades de confiança. A autoridade de certificação raiz mantém a "comunidade de confiança" estabelecida garantindo que cada entidade na hierarquia esteja em conformidade com um conjunto mínimo de práticas. Os benefícios dessa topologia incluem maior escalabilidade e capacidade de gerenciamento. Esta topologia funciona bem na maioria das grandes organizações. No entanto, pode ser difícil determinar a cadeia do processo de assinatura.

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 auto-assinado. Somente uma autoridade de certificação raiz pode emitir um certificado auto-assinado reconhecido ou verificado por outras autoridades de certificação dentro 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. As organizações e seus domínios do site enviam seus certificados públicos para os visitantes do site.

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

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.

3.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.

4.Protocolo de Status de Certificado Online (OSCP)

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.