CST0211-Arte de garantir a integridade: Parte 3 - Certificados

Data do Post	@September 2, 2022 9:00 AM
Status	Not started
Palavras-chave	Arte de garantir a integridade
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☐

Post- Linkedin

No artigo passado, trouxe as assinaturas digitais como assunto principal. Nesse artigo, apresento, mais um assunto associado a digitalização. Dessa vez, explico alguns conceitos básicos sobre certificados digitais. Leia o artigo na integra

Siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.

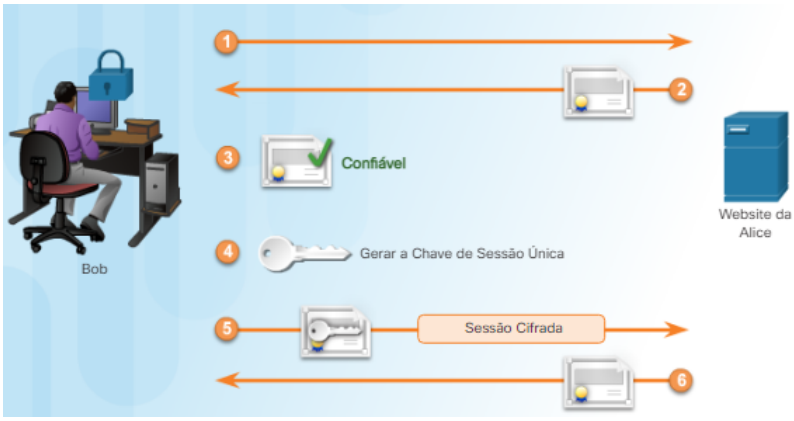
#cybersecurity #technology #linux #programming #hacking #maliciouscode #malwares #protection

Introdução

Um certificado digital é equivalente a um passaporte electrónico. Eles permitem que os utilizadores, dispositivos e organizações troquem informações com segurança pela Internet. Mais especificamente, um certificado digital autentica e verifica se os utilizadores que enviam uma mensagem são quem eles afirmam ser. Os certificados digitais também podem fornecer confidencialidade ao destinatário, providenciando os meios para cifrar uma resposta.

Utilização de certificados digitais

Para compreender como usar um certificado digital, consulte a Figura 1. Neste cenário, o Bob confirma uma encomenda à Alice. O servidor web da Alice usa um certificado digital para assegurar a realização de uma transação segura.

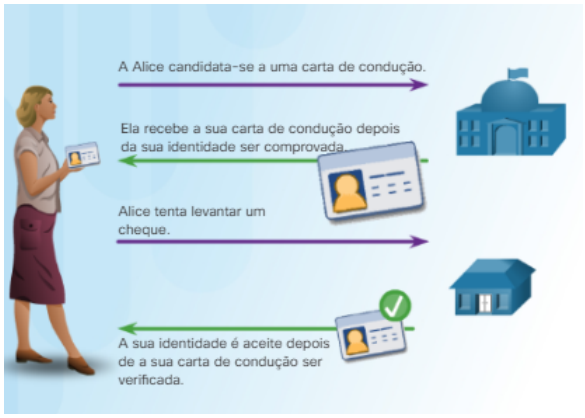


1. Passo: Bob acede ao site da Alice. Um navegador requer uma ligação segura mostrando um ícone com um cadeado na barra de estado de segurança.
2. Passo: O servidor web da Alice envia um certificado digital para o navegador do Bob.
3. Passo: O navegador do Bob verifica o certificado armazenado nas configurações do navegador. Somente certificados confiáveis permitem que a transacção siga.
4. Passo: O Bob ainda precisa de se autenticar e fornecer uma palavra-passe. Isto cria uma sessão segura em segundo plano entre o computador do Bob e o servidor web da Alice.
5. Passo: O navegador Web do Bob cria uma única chave de sessão única.
6. Passo: O navegador do Bob usa a chave pública do servidor web, constante no certificado recebido, para cifrar a sessão. O resultado é que somente o servidor web da Alice pode ler as transacções enviadas pelo navegador de Bob

Autoridade de certificação

Na Internet, a troca contínua da identificação entre todas as partes seriam impraticáveis. Por conseguinte, os indivíduos concordam em aceitar a palavra de uma terceira parte, considerada neutra.

Assume-se que esta terceira parte faz uma profunda investigação antes da emissão das credenciais. Após esta profunda investigação, a terceira parte emite as credenciais que são difíceis de forjar. A partir deste ponto em diante, todos os indivíduos que confiam na terceira parte aceitam as credenciais emitidas por esta.



Por exemplo, na figura a Alice candidata-se a tirar a carta de condução. Nesse processo, ela envia as provas da sua identidade, como a certidão de nascimento, uma imagem de identificação entre outras para a Direcção Nacional de Viação e Trânsito. A Direcção Nacional de Viação e Trânsito, valida a identidade da Alice e permite que esta se submeta a um exame de condução. Após a conclusão bem-sucedida, a Direcção Nacional de Viação e Trânsito emite a carta de condução para a Alice. Mais tarde, a Alice precisa de levantar um cheque no banco. Ao apresentar o cheque ao funcionário do banco, este pede a identificação. O banco, porque confia na Direcção Nacional de Viação e Trânsito do governo, validade da identidade da Alice e aceita pagar o cheque.

Uma autoridade de certificação (CA) funciona da mesma forma queDirecção Nacional de Viação e Trânsito neste exemplo. Uma CA emite certificados digitais que autenticam a identidade de organizações, dispositivos e utilizadores. Estes certificados também permitem assinar mensagens para garantir que ninguém as adulterou.

Como criar um certificado digital

Como um certificado digital segue uma estrutura padrão, qualquer entidade pode lê-lo e compreendê-lo independentemente do emissor. A norma X.509 especifica uma infra-estrutura de chaves públicas (PKI), para gestão de certificados digitais. A PKI são as políticas, as funções e os procedimentos necessários para criar, gerir, distribuir, usar, armazenar e revogar certificados digitais.

A norma X.509 especifica que os certificados digitais contêm as informações padrão mostradas a seguir:

- **Numero de versão:** A versão da norma x.509
- **Número de série:** identifica de forma única o certificado
- **Identificador do Algoritmo do Certificado:** O nome do algoritmo de chave pública usado pela CA para assinar o certificado.
- **Nome do Emissor:** A identidade da CA
- **Período de validade: contém**uma data de início e a expiração para a qual o certificado digital é válido.
- **Nome do sujeito:** O proprietário do Certificado digital
- **Informação da Chave Pública do Sujeito:** A chave pública do proprietário e o algoritmo de chave pública
- **Identificador único do emissor:** Identifica de forma única o emissor do certificado digital
- **Identificador único do sujeito:** Identifica de forma única o proprietário do certificado digital
- **Extensões:** Informações adicionais relativas à actualização do certificado
- **Assinatura digital do CA: assinatura**digital criada com a chave privada da CA usando o algoritmo especificado no campo identificador do algoritmo de certificado.

O processo de validação

Os navegadores e aplicações validam os certificados antes de confiarem na informação que transmitem, para garantir que sejam válidos. Os três processos incluem:

- A Cadeia de Certificação valida o caminho de certificação, verificando cada certificado começando pelo certificado da CA raiz
- A Validação do Caminho selecciona um certificado da autoridade de certificação emissora para cada certificado na cadeia

O caminho do certificado

Um indivíduo recebe um certificado para uma chave pública de uma CA comercial. O certificado pertence a uma cadeia de certificados chamada cadeia de confiança. O número de certificados na cadeia depende da estrutura hierárquica da CA.

A figura mostra uma cadeia de certificados para uma CA de dois níveis. Existe uma CA raiz offline e uma CA subordinada online. A razão para a estrutura de dois níveis é que a assinatura X.509 permite uma recuperação mais fácil em caso de comprometimento Se há uma CA offline (modelo de 2 níveis) e a CA subordinada online fica comprometida, a CA raiz pode assinar um novo certificado para uma nova CA subordinada online. Caso não existisse um modelo de 2 níveis, o comprometimento da CA que emitiu os certificados implicariam que um utilizador teria que instalar um novo certificado de CA raiz em cada máquina cliente, telemóvel ou tablet.

Gostou do conteúdo? Acessa o perfil e leia outros artigos sobre tecnologia ou siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.

#cybersecurity #technology #linux #programming #hacking #maliciouscode #malwares #protection