Public-Key Infrastructure (PKI)

PKI (public key infrastructure)

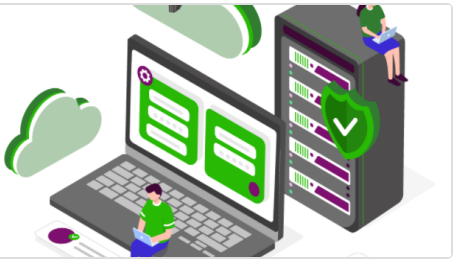
Precisamos ter certeza de que a chave pública pertence a pessoa que achamos que pertence. Se não fazermos isso, ficamos vulneráveis ao man-in-the-middle ataque.

Uma forma de evitar isso é usar ssh e fornecer a chave manualmente (github).

What is PKI? A Public Key Infrastructure Definitive Guide

Symmetric encryption is a simple cryptographic algorithm by today's standards, however, it was once considered state of the art. In fact, the German army used it to send private communications during

https://www.keyfactor.com/resources/what-is-pki/



Um exemplo de man-in-the-middle é explicado neste artigo (sec. **The Emergency of PKI to Govern Encryption Keys).** Imagine que Alice quer enviar uma mensagem ao Bob. Bob tem de enviar a sua public a Alice, no entanto, se Carol interceptar esse envio e enviar para Alice a sua public key, Alice vai falar com Carol pensando que está a falar com Bob e Bob irá falar com Carol pensando que é Alice. Neste sentido, há a necessidade de se comprovar quem é o dono da chave.

Certificados de Chave Pública

Alice envia a Bob uma chave pública, mas **Bob tem de ter certeza de que essa chave pertence a Alice**.

Solução trivial

- Bob tem um canal autenticado com Trusted-Third-Party (TTP)
- Alice mostrou anteriormente a TTP que é dona do pk
- Bob pergunta ao TTP se aquela é realmente a chave da Alice.

> *É um procedimento parecido ao que temos no cartório. Assinamos um documento, autenticamos no cartório e depois a pessoa que detém o documento pode verificar no cartório se aquela é realmente a nossa assinatura.*

O problema é que não é realista termos apenas uma TTP.

Problemas da TTP

- Como ter um canal seguro com a TTP?
- E se a TTP estiver offline?
- Como garantimos que Bob e a Alice confiam em TTP?
- O que é confiança?

TTP

A TTP é a Autoridade de Certificação/Certification Authority (CA).

A pessoa que é dona da chave pública precisa provar a uma autoridade qualquer que é dona da chave pública. Uma das formas é assinar um documento a autoridade ou quem gera a chave é a própria autoridade de certificação e fornece a pessoa.

Depois a **CA** vai gerar um documento com uma série de informações:

- Identidade da Alice + chave pública
- Informação específica da CA: identidade e novo número de série
- Validade

CA assina o documento eletrónico com esta informação.

Pagamos a autoridade para garantir este tipo de serviço.

Esta informação é guardada numa estrutura chamada **ASN.1**

TTP canal seguro e sempre online

Os certificados acabam por resolver este tipo de problema.

A própria Alice envia o certificado ao Bob e ele consegue verificar que o certificado não foi deturbado, já que foi assinado pela entidade. No entanto, chegamos ao mesmo problema, como podemos saber se a assinatura da entidade é válida?

Ponto de partida

O que foi gerado pela entidade foi um certificado que contém:

- Identidade da Alice + chave pública
- Validade (data de ínicio/fim)
- Metadados
- Tudo assinado pela autoridade de certificação (CA)

O que o Bob (browser) deve fazer?

- Primeiramente o Bob tem de verificar a identidade da Alice (do site). Se ele não corresponder ao que está no certificado digital, então o browser dá um alerta.
- Confirma-se a data de validade
- Confirma-se os metadados
- **Verificar que o CA é de confiança**
- **Obter chave pública da CA para verificar assinatura no certificado**

S/MIME

Muitos clientes de emails permitem-nos enviar um certificado digital ou cifrar nossas mensagens. No entanto, o que se faz muito é utilizar a própria chave de autenticação para cifrar os emails, o que não é correto. Precisaríamos de dois certificados: um que é utilizado para aprovar a chave pública de verificação (que é usado nas assinaturas) e um certificado correspondente a chave pública para cifras que é usado para decifrar emails com cifra.

Infelizmente o RSA utiliza isto: mesmas chaves pra cifrar e autenticar.

Attachments

Alguns certificados possuem algumas extensões que possui o que chamamos de identificador de objecto (OI object identifier) e uma flag que diz se aquela extensão é crítica ou não. Se o computador não conseguir interpretar a secção marcado como crítica, então não pode-se aceitar o certificado.

Alguns attachments importantes

- Subject/authority key identifier: hash da chave pública
- Basic constraints: flag que assina certificado como pertencente a CA
- **Key usage:** CA pode restringir utilização do certificado.

Public Key Infrastructure

Assegura que quando utilizamos um certificado assinado por uma autoridade de certificação, de que a chave pertence a uma pessoa e pode ser utilizada para um fim. Essas responsabilidades/obrigações são bem definidas para todos.

```
certificado -> assinado por autoridade -> pertence a uma pessoa -> para um fim
```

Armazenamento/transmissão de certificados

Estes certificados podem ser simplesmente armazenados em repositórios ou em aplicações. A sua transmissão baseia-se em diversos protocolos como HTTP, MIME, FTP.

Como funciona PKI

Todas as chaves públicas são codificadas em certificados X.509.

Se Bob recebeu um certificado de Alice. Bob pode verificar que o certificado que contém a chave da Alice é válido ao verificar a assinatura da CA. Como Bob possui o certificado da CA de antemão, ele consegue verificar a assinatura da CA e, portanto, validar a pk da Alice.

Esses certificados das CA são instalados nos nossos computadores pelo sistema operativo. O interessante é que a cadeia de confiança não é baseada em princípios sólidos: há entidades poderosas em que se confia (e.g google, governo, microsoft), os sistemas operativos confiam nessas entidades e nós, por simplesmente instalarmos o sistema operativo, confiamos neste.

Podemos verificar nossas entidades de certificado rodando o seguinte comando no arch linux:

```
trust list
```

Estes certificados que são pré-instalados no computador são auto assinados.

Cadeia de certificação

Qualquer pessoa pode gerar um certificado auto-assinado. Confiar num certificado auto-assinado é um salto de fé.

Há uma certa hierarquia entre CAs, porque algumas assinam o certificado de outras.

A verificação de um certificado é feita por um bottom up. Realiza-se essa verificação até se chegar num certificado que o utilizador já conhece por default.

Registo

Autoridades de Registo/Registration Authorities (RA)

Front-end: há contacto direto com os utilizadores/titulares

Reponsáveis por verificar os dados colocados nos certificados

Certificate Revogation List (CRL)

Volta e meia as CAs publicam a lista de certificados revogados. Os consumidores de certificados devem publicar as CRL mais recente. Os próprios certificados levam consigo um URL para a CRL, mas o problema desta abordagem é que há pouco suporte para isto por parte das aplicações.

Certificação

Back-end: infra-estrutura que produz chaves e certificados

- No mundo real há três soluções para este problema
  - Trusted Service Provider Lists (TSL):
    - white-list actualizada de certificados
    - usada em comunidades pequenas/fechadas (e.g., banking) e high-security
  - On-line Certificate Status Protocol (OCSP)):
    - servidor seguro (geralmente gerido pela própria CA) verifica estado de revogação
    - usado típicamente em contextos organizacionais (e.g., eGov)
  - Certificate pinning:
    - web servers/browsers/aplicações gerem white-lists próprias
    - permitem identificar certificados mais importantes para entidades críticas (e.g., Google)

Certificate pinning

HTTP Public Key Pinning - Wikipedia

HTTP Public Key Pinning (HPKP) is an obsolete Internet security mechanism delivered via an HTTP header which allows HTTPS websites to resist impersonation by attackers using misissued or otherwise fraudulent digital certificates. A server uses it to deliver to the client (e.g.

https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

What is certificate pinning?

SSL/TLS certificates are signed by other certificates. Browsers normally recognize a certificate as valid when in some point of this signature chain a trusted entity is found. The signatures of the

https://security.stackexchange.com/questions/29988/what-is-certificate-pinning

Segundo o wikipedia certificate pinning é uma técnica **considerada obsoleta** 😱, onde eram enviados no header to protocolo HTTP, onde eram enviados uma série de hashes de chaves públicas que devem aparecer na corrente de certificados para futuras conexões do mesmo domínio.

Políticas de certificação

É um conjunto de regras que definem:

- Direitos e responsabilidades para titulares e utilizadores
- Direitos e responsabilidades da CA

Estas regras podem decretadas em lei e uma vez decretadas possuem um object identifier (OID)

Perguntas

1) Por que foi criada a PKI?

▼ Resposta

Devido a necessidade de sabermos se a chave de uma pessoa pertence a quem achamos que pertence.

2) O que é uma TTP? Explique uma solução trivial para o problema da autenticidade de chaves. Qual o problema da solução trivial?

▼ Resposta

A TTP (trusted thirdy party) é uma thirdy party que garante que a chave pública de um sujeito realmente pertence a ele. Uma solução trivial para o problema da autenticidade de chaves é termos uma thirdy party (TTP) em que, quando (A) envia uma mensagem assinada para (B) junto a sua key, podemos contactar a TTP e verificar com esta se a chave recebida realmente pertence a (B). O **problema** desta abordagem é que isto forçaria a TTP sempre estar online e a existencia de uma TTP singular não é factível. Além disso outro problema surge: como sabemos que podemos confiar na TTP?

3) Como CA's amenizam os problemas da questão anterior? Justifique explicando como CAs funcionam.

▼ Resposta

Na questão anterior 3 problemas foram citados: a TTP precisa sempre estar online, não sabemos se podemos confiar na TTP e uma thirdy party singular não é factível. As CAs (certificate authority) são certificados de autoridades responsáveis por

verificar se um um certificado digital é válido (estas assinam estes). Quando a CA assina um certificado ela afirma que este é verdadeiro e portanto, a chave que veio junto pertence a quem se espera falar. Isto resolve dois problemas citados anteriormente: a thirdy party não precisa estar sempre online e também podem haver vários CAs.
A resolução do problema de confiança é “solucionado” por meio da confiança implicitas em entidades poderosas como a microsoft ou a google. Alguns certificados (os de raíz) são instalados no nosso sistema operacional. Estes certificados de raíz podem assinar outros CAs que assinam outros e assim em diante criando uma cadeia de confiança. É necessário verificar a autenticidade desta cadeia de segurança até que cheguemos num ponto em que conhecemos o certificado que assinou um prévio.

4) O que é TSL?

▼ Resposta

É uma trusted service provider list. É uma white list de certificados atualizadas.

5) O que é Online Certificate Status Protocol (OCSP). Qual o problema do seu uso?

▼ Resposta

Pode acontecer ainda de uma CA ser revogada ou um certificado digital ser revogado. Para verificarmos a condição de um certificado, podemos utilizar o Certifica Status Protocol. No entanto, com isto voltamos ao nosso problema inicial de precisarmos ter uma TTP sempre online. O OCSP verifica o estado de revogação de um certificado.

6) O que é certificate pinning?

▼ Resposta

É uma técnica obsoleta para restringir certificados permitidos num website. Era enviado para o cliente uma lista de hashed public keys no header do protocolo HTTP. Estas hashed public keys deveriam estar presentes na chain de certificados digitais em conexões futuras.

(slide 25)

7) Como é que um utilizador contacta/toma conhecimento de uma CA?

8) Como é que o Bob verifica a assinatura produzida por uma CA num certificado?

9) Como é que o Bob sabe se pode confiar na CA?

10) Como é que os certificados de chave pública circulam/são distribuídos e armazenados?

▼ Resposta

Certificados são armazenados em repositórios e são distribuídos por meio de protocolos seguros como HTTP, MIME, FTP.

11) Qual a diferença entre RA e CA?

▼ Resposta

Uma RA (registration authority) é uma entidade responsável por validar registos e possui contacto direto com o cliente. A Certificate Authority valida um certificado, mas por sua vez não possui contacto direto com o cliente.

12) O que é uma CRL? Como é que sabemos onde está a CRL mais recente? Qual o problema desta abordagem?

▼ Resposta

O CRL é a certificate revogation list. Os próprios certificados geralmente vem com um URL que contém a lista. O problema desta abordagem é que muitas aplicações não suportam esta abordagem.

13) O que são políticas de certificação?

▼ Resposta

É quando uma PKI passa a ter um valor legal. Quando isto acontece, esta recebe uma Object Identifier (OID). A política de certificação geralmente promove direitos e responsabilidaes tanto por parte do consumidor tanto para a CAs. O uso da PKI que fujam do que foi descrito são consideradas ilegalidades, crime.