

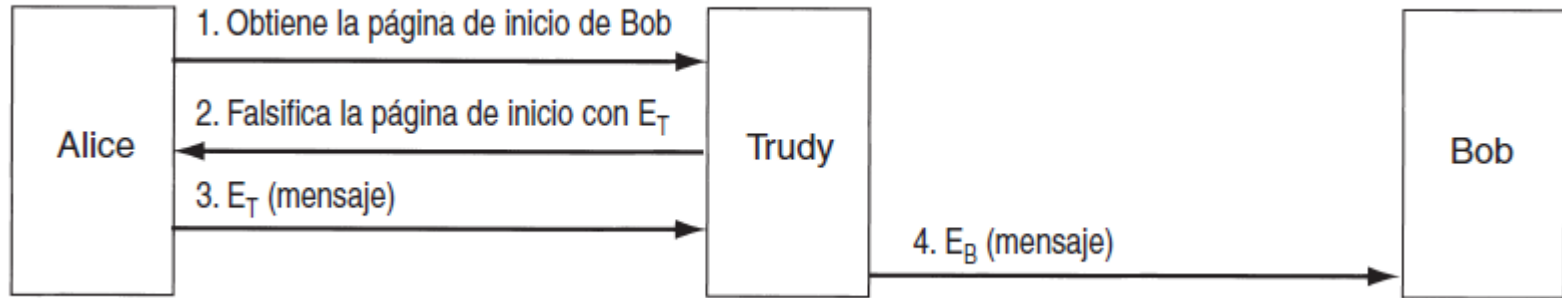
Administración de Claves Públicas

Claudio Acuña, Cristian Garrido, Guillermo Rojas, José Acuña, Leonardo Jofré.

Introducción

La criptografía de clave pública hace posible que las personas que no comparten una clave común se comuniquen con seguridad. También posibilita firmar mensajes sin la presencia de un tercero confiable. Por último, los compendios de mensajes firmados hacen que verificar fácilmente la integridad de mensajes recibidos sea una realidad.

Introducción



Certificados

Ejemplo para distribuir clave Pública

Como un primer intento para distribuir claves públicas de manera segura, podemos imaginar un centro de distribución de claves disponible en línea las 24 horas del día que proporciona claves públicas a petición.

Problemas

- Solución No Escalable.
- El centro de distribución a la larga genera cuellos de botella.
- Si el sistema falla. No Habría seguridad.

Una mejor Solución

Es certificar las claves públicas que pertenecen a las personas, empresas y otras organizaciones.

las organizaciones que certifican claves públicas se conocen como CA (autoridad de certificación)

¿Que es un certificado?

Es un mecanismo para asegurar que las claves públicas puedan intercambiarse de manera segura.

Como trabaja un certificado

El trabajo fundamental de un certificado es enlazar una clave pública con el nombre de un personaje principal (individual, empresa, etcétera).

Otra forma de trabajo

también un certificado se puede utilizar para enlazar una clave pública a un atributo.

Enlazar una clave pública a un atributo permite que no sea necesario conocer la identidad del dueño.

Lo cual es útil en las situaciones en que la privacidad es importante.

X.509

X.509

Si todas las personas que desean algo firmado fueran a la CA con un tipo diferente de certificado, administrar todos los formatos diferentes pronto se volvería un problema. Para resolverlo se ha diseñado un estándar para certificados, el cual ha sido aprobado por la ITU. Dicho estándar se conoce como X.509 y se utiliza ampliamente en Internet.

La IETF estaba de acuerdo con el X.509, aunque en casi todas las demás áreas, desde direcciones de máquinas, protocolos de transporte hasta formatos de correo electrónico, la IETF por lo general ignoró a la OSI y trató de hacerlo bien. La versión IETF del X.509 se describe en el RFC 3280.

X.509

En esencia, el X.509 es una forma de describir certificados.

Las descripciones dadas en la siguiente tabla deben proporcionar una idea general de lo que hacen los campos en un certificado.

X.509

Campo	Significado
Versión	Cuál versión del X.509
Número de serie	Este número junto con el nombre de la CA identifican de manera única el certificado
Algoritmo de firma	El algoritmo que se utilizó para firmar el certificado
Emisor	El nombre X.500 de la CA
Validez	Las fechas de inicio y final del periodo de validez
Nombre del sujeto	La entidad cuya clave se está certificando
Clave pública	La clave pública del sujeto y el ID del algoritmo usado para generarla
ID del emisor	Un ID opcional que identifica de manera única al emisor del certificado
ID del sujeto	Un ID opcional que identifica de manera única al sujeto del certificado
Extensiones	Se han definido muchas extensiones
Firma	La firma del certificado (firmada por la clave privada de la CA)

X.509

Por ejemplo, si Bob trabaja en el departamento de préstamos del Banco Monetario, su dirección X.500 podría ser:

`/C=MX/O=BancoMonetario/OU=Prestamo/CN=Bob/`

donde C corresponde al país, O a la organización, OU a la unidad organizacional y CN a un nombre común. Las CAs y otras entidades se nombran de forma similar. Un problema considerable con los nombres X.500 es que si Alice está tratando de contactar a `bob@bancomonetario.com` y se le da un certificado con un nombre X.500, tal vez no sea obvio para ella que el certificado se refiera al Bob que ella busca.

Infraestructura

Infraestructura

El hecho de que una sola CA emita todos los certificados del mundo obviamente no funciona. Podría derrumbarse por la carga y también podría ser un punto central de fallas. Una posible solución sería tener múltiples CAs que fueran ejecutadas por la misma organización y que utilizaran la misma clave privada para firmar los certificados. Si bien esto podría solucionar los problemas de carga y de fallas,

Infraestructura

Esto introduciría un nuevo problema: la fuga de claves. Si hubiera docenas de servidores esparcidos por todo el mundo, todos con la misma clave privada de la CA, la probabilidad de que la clave privada fuera robada o filtrada se incrementaría de manera considerable.

Además, ¿qué organización podría operar la CA? Es difícil imaginar cualquier autoridad que podría ser aceptada mundialmente como legítima y digna de confianza. En algunos países las personas insistirían en que fuera el gobierno, mientras que en otros lo rechazarían.

Infraestructura

Por estas razones, se ha desarrollado una forma diferente para certificar claves públicas. Tiene el nombre general PKI (Infraestructura de Clave Pública).

Infraestructura

Una PKI tiene múltiples componentes, entre ellos usuarios, CAs, certificados y directorios. Lo que una PKI hace es proporcionar una forma para estructurar estos componentes y definir estándares para los diversos documentos y protocolos. Una forma particularmente simple de PKI es una jerarquía de CAs. En este ejemplo mostramos tres niveles, pero en la práctica podrían ser menos o más.

Infraestructura

La CA de nivel superior, la raíz, certifica a CAs de segundo nivel, a las que llamaremos RAs (Autoridades Regionales) debido a que podrían cubrir alguna región geográfica, como un país o un continente.

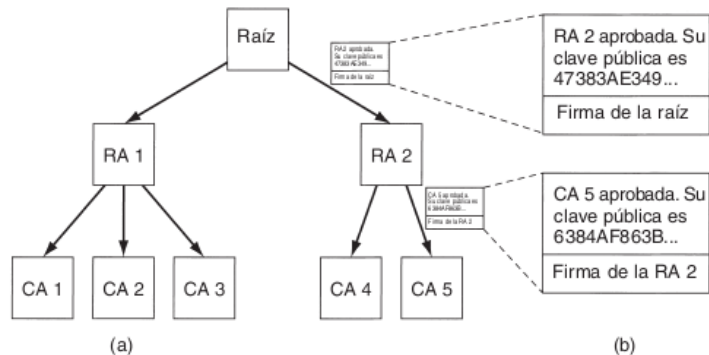


Figura 8-26. (a) Una PKI jerárquica. (b) Una cadena de certificados.

Infraestructura

Sin embargo, este término no es estándar; de hecho, ningún término es realmente estándar para los diversos niveles del árbol. Estas RAs, a su vez, certifican a los CAs reales, las cuales emiten los certificados X.509 a organizaciones e individuos. Cuando la raíz autoriza una nueva RA, genera un certificado X.509 donde indica que ha aprobado la RA, e incluye en él la nueva clave pública de la RA, la firma y se la proporciona a la RA. De manera similar, cuando una RA aprueba una CA, produce y firma un certificado que indica su aprobación y que contiene la clave pública de la CA.

Infraestructura

De esta manera, Alice no necesita contactar a nadie para realizar la verificación. Debido a que todos los certificados están firmados, Alice puede detectar con facilidad cualquier intento de alterar el contenido. Una cadena de certificados que va de esta forma a la raíz algunas veces se conoce como cadena de confianza o ruta de certificación. La técnica se utiliza ampliamente en la práctica.

Revocación

Revocación

El mundo real también está lleno de certificados, como los pasaportes y las licencias de conducir. Algunas veces estos certificados pueden revocarse, por ejemplo, las licencias de conducir pueden revocarse por conducir en estado de ebriedad y por otros delitos de manejo. En el mundo digital ocurre el mismo problema: el otorgante de un certificado podría decidir revocarlo porque la persona u organización que lo posee ha abusado de alguna manera. También puede revocarse si la clave privada del sujeto se ha expuesto o, peor aún, si la clave privada de la CA está en peligro. Por lo tanto, una PKI necesita tratar el problema de la revocación.

Revocación

- Un primer paso en esta dirección es hacer que cada CA emita periódicamente una CRL (lista de revocación de certificados) que proporcione los números seriales de todos los certificados que ha revocado.
- Desgraciadamente, introducir CRLs significa que un usuario que está próximo a utilizar un certificado debe adquirir la CRL para ver si su certificado ha sido revocado.

Revocación

- ¿Dónde deben almacenarse las CRLs? Un buen lugar sería el mismo en el que se almacenan los certificados.
- Si los certificados tienen tiempos de vida largos, las CRLs también los tendrán.

Directorios


Antes de contactar a X, Y probablemente tiene que buscar la dirección IP de Bob mediante DNS

Directorios

¿donde se almacenan los certificados?

si es seguro ¿por qué no cada usuario almacena sus propios certificados?


¿por qué no hacer que DNS retorne toda la cadena de certificados junto con la IP?



A pesar de que esto es posible hay personas que prefieren tener servidores de directorios para manejar los certificados X.509.



Tales directorios pueden usar propiedades de los nombres X.500 para hacer búsquedas.



“Dame una lista de todas las personas que tengan el nombre Alice y que trabajen en los departamentos de ventas en cualquier lugar de Estados Unidos o Canadá”

LDAP son las siglas de *Lightweight Directory Access Protocol*

Protocolo de acceso a directorios es un buen candidato para hacer estas consultas sobre directorios que almacenan los certificados.

ventajas de directorio

como **LDAP** se entiende como una base de datos ...