Resumen

8.9.3: SSL – La Capa de Sockets Seguros

ANtes habían páginas estáticas pero se comenzaron a necesitar transacciones como compras en linea. Netscape entonces fabricante líder de navegadores, respondió con un paquete de seguridad llamado SSL (Capa de Sockets Seguros). Ssl contruye conexión segura incluyendo:

- Negociación de parámetros entre el cliente y el servidor.
- Autenticación tanto del cliente como del servidor.
- Comunicación secreta.
- Protección de la integridad de los datos.

Es una capa colocada entre la capa de aplicación y la de transporte,que acepta solicitudes tcp, establecida la conexión SSL maneja la compresión y encriptación. Http + ssl = Https, usa puerto 443 y no está restringido solo a navegadores. SSL consiste en dos subprotocolos, uno para establecer una conexión segura y otro para utilizarla. SSL soporta múltiples algoritmos criptográficos. El más robusto utiliza triple DES con tres claves separadas para encriptación y SHA-1 para la integridad de mensajes. Son lentas por lo que se usan en operaciones bancarias.

Para un transporte real se utiliza un segundo subprotocolo, mensajes del navegador se dividen en unidades de 16kb y se agrega un hash a cada uno y se tiene un hash de todo comprimido. SSL mediante RC4 no es muy confiable. Otro problema con SSL es que tal vez los personajes principales no tienen certificados e incluso si los tienen, no siempre verifican que coincidan las claves que se utilizan.

8.5: Administración

Criptografía hace que personas sin clave común se comunique seguramente.

8.5.1 Certificados

Centro de distribución de claves disponible en línea las 24 horas del día proporcionando claves públicas no escalable y con futuros cuellos de botella. Por lo que se creó un centro que no necesita estar en línea solo certifica claves publicas. La función estándar de un certificado es enlazar una clave pública a un personaje principal, pero también se puede utilizar para enlazar una clave pública a un atributo. Un ejemplo en el que un certificado podría contener un atributo es un sistema distribuido orientado a objetos.

8.5.2 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 usa X.509 un estándar para certificados. X.509 es una forma de describir certificados. Los certificados están codificados mediante la ASN.1 (Notación de Sintaxis Abstracta 1) de la OSI, que puede considerarse como si fuera una estructura de C, pero con una notación peculiar y poco concisa.

8.5.3 Infraestructuras de clave pública

El hecho de que una sola CA emita todos los certificados del mundo obviamente no funciona. Tampoco sirve tener múltiples CAs y tampoco una organización va a estar operando CA. Por tal razon, se ha desarrolla una forma diferente para certificar claves públicas. Tiene el nombre general PKI (Infraestructura de Clave Pública).

PKI tiene múltiples componentes, entre ellos usuarios, CAs, certificados y directorios, proporciona una forma para estructurar estos componentes y definir estándares para los diversos documentos y protocolos. Puede verse como una jerarquía de CAs. Debido a que todos los certificados están firmados, se puede detectar con facilidad cualquier intento de alterar el contenido. Navegadores modernos vienen precargados con claves públicas para aproximadamente 100 raíces, algunas veces llamadas anclas de confianza.

Directorios

Otro problema de cualquier PKI es en dónde están almacenados los certificados (y sus cadenas hacia un ancla de confianza conocida). Hacer que los usuarios la guarden no sirve por lo que se propone utilizar DNS como un directorio de certificados. También es mejor dedicar servidores de directorio cuyo único trabajo sea manejar los certificados X.509.

Revocación

Algunas veces estos certificados pueden revocarse, por ejemplo, las licencias de conducir pueden revocarse por conducir en estado de ebriedad, otorgante de un certificado podría decidir revocarlo porque la persona u organización que lo posee ha abusado de alguna manera o si la clave se ha expuesto.

PKI necesita tratar el problema de la revocación. Un primer paso en esta dirección es hacer que cada CA emita periódicamente una CRL que proporcione los números seriales de todos los certificados que ha revocado, pero esto no funciona. La única forma es preguntar a la CA. Otra complicación es que un certificado revocado puede reinstalarse nuevamente. ¿Dónde deben almacenarse las CRLs? normalmente es donde se almacenan los certificados.

Si los certificados tienen tiempos de vida largos, las CRLs también los tendrán. Por ejemplo, si las tarjetas de crédito son válidas durante cinco años, el número de revocaciones pendientes será mucho más grande que si se emitieran nuevas tarjetas cada tres meses.