

UNPSJB

LICENCIATURA EN SISTEMAS OPGCPI

ADMINISTRACIÓN DE REDES Y SEGURIDAD

Trabajo Práctico 3

Criptografía

Cátedra

Lic. Bruno Damián Zappellini

Integrantes:

Luciano Serruya Aloisi

8 de noviembre de 2018



Índice

1. Conceptos básicos	2
1.1. Verdadero o falso	2
2. PKI	3
2.1. Instalando un certificado en Firefox	3
2.2. Certificado personal	4
2.3. Correos electrónicos firmados y encriptados	5
2.4. Análisis sobre una clave privada robada	6
2.4.1. Cómo actuar	6
2.4.2. Consecuencias con la información encriptada	7
2.4.3. Consecuencias con la información firmada	7

1. Conceptos básicos

Juan quiere mandarle un mensaje a Julio. A Julio no le importa asegurarse que el mensaje fue enviado por Juan, sin embargo Juan quiere estar seguro de que el mensaje no podrá ser leído ni alterado por un tercero. Juan trabaja en una empresa en Argentina y Julio es empleado de una empresa ubicada en España

Para esta situación, un sistema de cifrado simétrico no cumpliría los requisitos solicitados; en el caso de que la clave compartida sea interceptada, la comunicación puede ser espiada por un tercero. Sin embargo, si se garantiza un canal seguro para transmitir la clave privada al inicio de la comunicación, sí se podría utilizar un cifrado simétrico. En caso de que esto último no sea posible, la alternativa sería usar un sistema de cifrado asimétrico, donde el emisor encripta el mensaje con la clave pública del receptor, y el receptor descifra el mensaje recibido con su clave privada.

Adriana y Leandro quieren comunicarse en forma segura. Para ellos resulta fácil conseguir un medio seguro para intercambiar información que luego necesiten para realizar esta comunicación segura. En este caso lo que importa es que nadie pueda espiar los datos involucrados en dicha comunicación

Debido a que se cuenta con un canal seguro, se lo podría utilizar para compartir una clave, la cual se utilizará para cifrar los mensajes intercambiados de forma simétrica.

Analía usará el correo electrónico para enviar la aceptación de un contrato al estudio en el cual trabaja. Para la persona que lo reciba es importante tener la garantía de que el mismo fue enviado efectivamente por Analía

Lo adecuado para esta situación sería que el correo enviado por Analía sea firmado utilizando la clave privada de Analía.

1.1. Verdadero o falso

En los criptosistemas simétricos no puede garantizarse el no repudio porque ambas partes de la transacción conocen la clave utilizada

Falso. Si la clave compartida no fue transmitida por un canal seguro puede haber sido

interceptada, logrando que un tercero envíe un mensaje encriptado.

Si únicamente me importara la eficiencia del método que uso para encriptar, debería optar por un algoritmo de cifrado asimétrico

Falso. Si se busca eficiencia, la encriptación asimétrica se debería evitar. La encriptación simétrica es mucho más rápida y no incrementa el tamaño del mensaje.

Con ambos tipos de criptosistemas necesito contar con un mecanismo seguro para transmitir la clave

Falso. Con los criptosistemas asimétricos, no es necesario que las claves públicas sean compartidas de forma segura (se pueden alojar en un servidor o un repositorio para que distintos usuarios la consigan).

2. PKI

Para poder verificar la firma de un correo electrónico, el receptor necesita la **clave pública** del emisor.

Al enviar un mensaje firmado, el emisor genera un *resumen* del mensaje (con alguna función de *hashing*), y luego lo encripta con su **clave privada**, generando así la **firma digital**.

El receptor también genera el resumen del mensaje (con el mismo algoritmo), y desencripta la firma con la **clave pública** del emisor (el receptor debía contar con la clave pública del emisor o la debe poder conseguir ya sea a través de un *certificado* o de un repositorio). Luego compara el resumen que él generó, y el que recibió del emisor. Si son iguales, entonces la firma es considerada válida; si no son iguales, entonces significa que se utilizó una clave distinta para firmar el mensaje, o fue alterado.

Ahora bien, si el mensaje está encriptado, para poder abrirlo el receptor necesita su **clave privada**, ya que el mensaje debió ser cifrado con la **clave pública** del receptor. En caso de que el mensaje hubiese sido cifrado con la **clave privada** del emisor, cualquier tercero que tenga la **clave pública** del emisor podrá desencriptarlo.

2.1. Instalando un certificado en Firefox

- Algoritmo de firma utilizado: PKCS #1 MD5 With RSA Encryption
- Cantidad de bits de cifrado: 4096 bits

- Periodo de validez: desde el 30/03/2003 hasta el 29/03/2033
- Emisor:
 - E = support@cacert.org
 - CN = CA Cert Signing Authority
 - OU = http://www.cacert.org
 - O = Root CA

▼ Root CA	
CAcert Class 3 Root	Software Security Device
CA Cert Signing Authority	Software Security Device

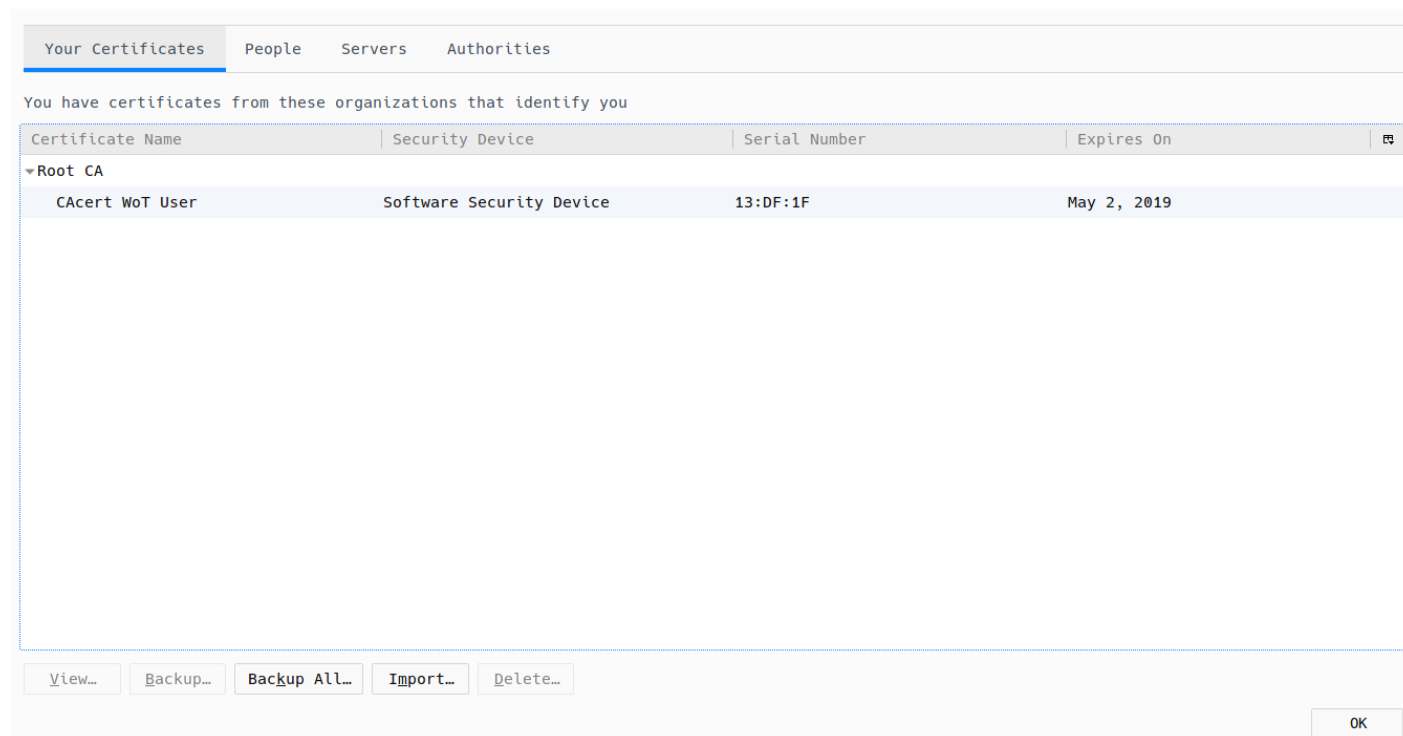
Certificado de CACert instalado en Firefox



Ingresando a CACert con HTTPS

2.2. Certificado personal

Después de generar el certificado personal para la dirección de correo electrónico *lucianoserruya@gmail.com* e instalarlo en Firefox, se puede ver el siguiente certificado instalado



Certificado personal instalado en Firefox

2.3. Correos electrónicos firmados y encriptados

Para los siguientes experimentos que se muestran a continuación, se utilizaron dos cuentas personales: lucianoserruya@gmail.com y lucianoserruya@hotmail.com. Para ambas cuentas se generaron los respectivos certificados en CAcert y se instalaron correctamente en Thunderbird

Una vez instalados los certificados de ambas cuentas en Thunderbird, se realizaron los siguientes experimentos:

- Enviar un correo firmado - el emisor necesita su clave privada para encriptar la firma, y el receptor necesita la clave pública del emisor para poder verificarla
- Enviar un correo encriptado - el emisor necesita la clave pública del receptor para encriptar el mensaje, y el receptor necesita su clave privada para poder desencriptarlo
- Enviar un correo firmado y encriptado - se tienen que cumplir las dos condiciones anteriores

A continuación se incluyen capturas de pantalla de los correos electrónicos enviados. Como el mismo cliente tiene tanto las claves privadas como las públicas de ambas cuentas, se pudieron realizar los experimentos sin inconvenientes.

Thunderbird indica con un logo de un candado a los correos que hayan sido encriptados, y con un sobre a aquellos que fueron firmados (y que se pudo validar la firma).



Correo firmado



Correo encriptado



Correo firmado y encriptado

2.4. Análisis sobre una clave privada robada

La infraestructura de PKI brinda un elemento esencial una situación de este tipo. Este se llama **Certificate Revocation List (CRL)**, es un repositorio que mantiene la CA (**Certificate Authority**, ente encargado de emitir los certificados) con los certificados que dejaron de ser válido (que fueron revocados, los certificados expirados no entran en esta lista).

2.4.1. Cómo actuar

Tanto si la clave privada fue robada como si fue robada y además eliminada de la máquina del dueño, lo primero que se debe hacer es **revocar los certificados** que corresponden a esa clave privada. Para ello se debe agregar el número de identificación del certificado a la CRL de la CA correspondiente.

Cuando un cliente pida el certificado del servidor cuya clave privada fue comprometida, lo rechazará y pedirá uno nuevo al verificar que ese certificado se encuentra en la CRL.

2.4.2. Consecuencias con la información encriptada

Como la clave privada es la que se utiliza para descryptar mensajes, estando comprometida un tercero podría descryptar los mensajes que vayan hacia el dueño original de la clave.

2.4.3. Consecuencias con la información firmada

Para firmar se utiliza la clave privada, por lo tanto alguien más podría firmar documentos haciéndose pasar por el dueño de la clave.