Universidad de Costa Rica
Seguridad de Sistemas Computacionales
CI0143 - I Semestre 2022

Laboratorio de Infraestructura de Llave Pública - PKI
Fecha entrega: 14 de junio

Prof. Ricardo Villalón Fonseca

1. Objetivo General

Aplicar los conceptos básicos de seguridad en infraestructura de llave pública (PKI) en la creación de una autoridad certificadora para generar certificados digitales que permitan proveer servicios seguros en una red privada.

2. Objetivos Específicos

1. Crear una autoridad certificadora raíz.
2. Crear certificados digitales firmados por la autoridad certificadora.
3. Instalar un certificado digital para proveer un servicio web seguro.
4. Realizar una breve investigación acerca de revocación de certificados digitales.

3. Descripción General

La encripción y los servicios de infraestructura de llave pública son instrumentos de seguridad cada vez más relevantes para proteger la operación de actividades comerciales, financieras o de cualquier otra índole que se realizan en la red Internet. En este laboratorio se pretende que usted se familiarice con los conceptos y procesos de estas tecnologías y sea capaz de involucrarse en procesos de infraestructura tecnológica que involucren encripción de llave pública, firmas digitales, generación de certificados, procesos de autenticación, etc. y tenga un conocimiento básico de las herramientas requeridas para ponerlos en ejecución.

4. Etapas del laboratorio

4.1. Creación de una Autoridad Certificadora (CA) (50 pts)

Una Autoridad Certificadora (CA) es una entidad de confianza que emite certificados digitales. El certificado digital certifica la posesión de una llave pública a nombre del sujeto del certificado.

Existen varias CA comerciales que son consideradas como entidades raíz de certificación, por ejemplo, VeriSign es una importante CA reconocida a nivel mundial. Las CA normalmente cobran por emitir certificados digitales a los usuarios para certificar la autenticidad de sus sistemas.

En nuestro caso vamos a crear certificados digitales, pero no vamos a pagarle a una CA comercial. Lo que haremos es crear nuestra propia CA raíz y luego usar esta CA para generar certificados para otros (por ejemplo para servidores). En esta parte del laboratorio haremos la CA raíz y generaremos un certificado para dicha CA. A diferencia de un certificado normal, que es usualmente firmado por un tercero confiable, el certificado de la CA es firmado por ella misma. Los certificados raíz de las CAs suelen ser precargados en la mayoría de sistemas operativos, navegadores y otros programas que dependen de la infraestructura PKI y se confía en ellos de forma incondicional.

Para crear la CA, todos los estudiantes del curso desarrollarán, como un solo grupo, un pequeño documento de instrucciones para crear una CA en un computador con sistema operativo CentOS 7. La CA tendrá como *objetivo principal la emisión de certificados para sitios web y servicios de red seguros, solamente*. El documento debe contener al menos lo siguiente:

1. Portada.
2. Página de aprobación: nombres de quienes participaron, hicieron y aprobaron el contenido del documento.
3. Tabla de contenido.
4. Breve introducción al documento, de uno a dos párrafos.
5. Instrucciones para instalación de una CA, incluyendo:
   - consideraciones de configuración a nivel del sistema operativo si las hubiera;
   - el perfil y parámetros de configuración de los certificados;
   - instrucciones para instalar y/o configurar el software de la CA;
   - instrucciones para crear las llaves, las solicitudes, los certificados, y otros archivos que sean parte de la CA;
6. Descripción de alto nivel del proceso completo para crear un certificado digital, es decir, considerando todos los usuarios involucrados en el proceso.
7. Para el operador de la CA (encargado o el docente del curso): instrucciones para emitir o revocar un certificado digital para un servicio de un host.
8. Para los usuarios de la CA (los estudiantes del curso): instrucciones que permitan generar una solicitud de certificado digital para un servicio de host.

Esta sección se evaluará de forma grupal general (la misma evaluación para todos los estudiantes del curso), por lo cual tod@s l@s estudiantes deben participar y aprobar el documento. Considerando que el documento tiene la posibilidad de ser revisado por múltiples personas antes de ser entregado, se considerarán tres tipos de errores: a) errores menores con un valor negativo de 10 puntos, como por ejemplo documentación de instrucciones ambigüa o incorrecta o pasos que producen errores; b) errores medios con un valor negativo de 20 puntos, como por ejemplo consideraciones técnicas no incluídas en las instrucciones y que dejan por fuera casos especiales, más allá de los casos por defecto; c) errores principales con un valor negativo de 30 puntos, como por ejemplo errores de concepto en los procesos documentados. El mecanismo de coordinación para aceptar el documento por parte de todo el grupo se definirá en horario de clase.

4.2. Creación e instalación del certificado para un servicio web (25 pts)

Utilice el nombre de host del servicio web donde instaló la aplicación desarrollada previamente durante el curso, genere una solicitud de certificado para dicho sitio web y solicite la firma del certificado a la autoridad certificadora. Luego, instale el certificado digital para asegurar las comunicaciones de su aplicación web con el protocolo https.

Como complemento a la instalación del certificado en el servidor, realice una investigación e implementación de los parámetros de configuración del módulo ssl en el servidor que sirven para mejorar la seguridad de su servicio web. Debe incluir el análisis y mejora en los valores de los algoritmos criptográficos permitidos por el servidor.

Para evaluar la seguridad de las comunicaciones desde el cliente, utilice el sistema operativo de su preferencia para establecer una comunicación segura con su servidor web. Investigue, documente y configure los navegadores Firefox y Chrome para que logren establecer una comunicación segura válida, en cuanto al reconocimiento apropiado de los certificados emitidos con la autoridad certificadora creada previamente.

La evaluación de esta sección se hará por grupos pequeños, definidos por los mismos grupos de trabajo definidos para la creación de la tarea de la aplicación web.

4.3. Esquemas de revocación de certificados (25 pts)

En la actualidad existen dos esquemas de revocación de certificados para los casos en que un certificado digital expira o su seguridad se ve comprometida de forma alguna. Estos esquemas se conocen con los nombres de Certificate Revocation List (CRL) y Online Certificate Status Protocol (OCSP). Las listas de revocación CRL son el mecanismo tradicional para validar la vigencia de un certificado, pero lamentablemente tienen una cantidad importante de debilidades que pueden poner en peligro la seguridad de transacciones en Internet. Por otra parte, el protocolo OCSP busca solventar algunas de las debilidades de CRL habilitando la validación de certificados en línea.

Entonces, haga una breve investigación y resumen de cada una de estas técnicas de revocacion de certificados, en donde explique sus principales características y cómo funcionan al acceder a un sitio web seguro con un navegador.

La evaluación de esta sección se hará por grupos pequeños, definidos por los mismos grupos de trabajo definidos para la creación de la tarea de la aplicación web. Posterior a la entrega de la tarea, se hará una evaluación oral al azar, a cualquiera de los miembros de algún(os) grupo(s) para validar el entendimiento de los esquemas de revocación. Esta evaluación podría afectar la nota obtenida por el correspondiente grupo de trabajo.

5. Reporte del laboratorio

Debe entregarse un único documento con todos los componentes para la creación de la CA.

Para las tareas en grupos pequeños debe generar, por cada grupo, un reporte de laboratorio que contenga los archivos de configuración de los servicios configurados, scripts resultados, pantallas mostrando los resultados así como un detalle de los puntos más relevantes identificados durante el proceso de instalación, configuración y pruebas.

Recuerde incluir referencias a los recursos y la bibliografía utilizados en el trabajo.