Sistemas Telemáticos para Medios Audiovisuales
Práctica 6: Claves

Departamento de Teoría de la Señal y Comunicaciones
y Sistemas Telemáticos y Computación
(GSyC)

Noviembre de 2018

1. Ejercicio 1

Se ha diseñado un sistema de comunicación que pretende que los usuarios puedan intercambiar información de manera anónima. El objetivo es dificultar que alguien que intercepte uno de los mensajes pueda conocer qué nodo envió originalmente el mensaje, ni cuál es el destinatario final del mismo, ni cuál es el contenido del mensaje.

Para conseguir este objetivo el mensaje se va enviando a través de una serie de nodos, elegidos por el nodo origen de la comunicación.

El nodo origen de una comunicación tiene que indicar en el mensaje que envía dos tipos de información:

- La secuencia de nodos que tiene que seguir el mensaje que envía
- El Contenido del Mensaje, que incluye la dirección del nodo que envía originalmente el mensaje, y el texto del mensaje.

Cuando un nodo recibe un mensaje, tiene que enviárselo al primero de los nodos especificados en la secuencia de nodos que viene en el mensaje, eliminando la primera entrada de la secuencia de nodos antes de enviar el mensaje.

Ejemplo con 5 ordenadores, X, B, C, D, Z, con direcciones IP $IP_X, IP_B, IP_C, IP_D, IP_Z$ respectivamente:

Supongamos que X quiere enviar el texto $mensajeParaZ$ a Z a través de la ruta $X \Rightarrow B \Rightarrow C \Rightarrow D \Rightarrow Z$, y que X conoce $K_B^+, K_C^+, K_D^+, K_Z^+$.

1º) X le envía a B un datagrama IP en cuyo campo de datos va la siguiente información:
- Secuencia de nodos: $\boxed{K_B^+(IP_C) \mid K_C^+(IP_D) \mid K_D^+(IP_Z) \mid K_Z^+(IP_Z)}$
- Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

2º) B descifra el primer componente de la secuencia de nodos recibida, y aprende que el siguiente salto es C. B le envía entonces a C un datagrama IP con la siguiente información en su campo de datos:
- Secuencia de nodos: $\boxed{K_C^+(IP_D) \mid K_D^+(IP_Z) \mid K_Z^+(IP_Z)}$
- Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

3º) C descifra el primer componente de la secuencia de nodos recibida, y aprende que el siguiente salto es D. C le envía a D:
- Secuencia de nodos: $\boxed{K_D^+(IP_Z) \mid K_Z^+(IP_Z)}$
- Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

4º) D descifra el primer componente de la secuencia de nodos recibida, y aprende que el siguiente salto es Z. D le envía a Z:
- Secuencia de nodos: $\boxed{K_Z^+(IP_Z)}$
- Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

5º) Z descifra el primer y único componente de la secuencia de nodos recibida, y aprende que él es el nodo destinatario. Entonces Z descifra el Contenido del Mensaje, sabiendo así que el mensaje lo ha enviado originalmente IP_X, y que el mensaje que le quería transmitir a Z era $mensajeParaZ$.

Preguntas

1. Explica si el nodo receptor del mensaje Z puede o no descifrar el mensaje para acceder a su contenido.
2. Explica si el nodo receptor del mensaje Z estar seguro de la confidencialidad del mensaje, es decir, de que ningún otro nodo ha podido descifrarlo.
3. Explica si el nodo receptor del mensaje Z puede autenticar al nodo emisor del mensaje X.
4. Explica si el nodo receptor del mensaje Z puede estar seguro de la integridad del mensaje, es decir, que ningún otro nodo ha podido alterar el contenido del mensaje.
5. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el texto del $mensajeParaZ$.
6. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el destino final del mensaje.
7. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el nodo que creó el mensaje.

2. Ejercicio 2

En una sistema existen las siguientes autoridades de certificación CA1 y CA2, ambas autoridades de certificación han incluido sus propios certificados autofirmados en las aplicaciones de comunicaciones que se usan dentro de este sistema.

Alicia tiene un certificado de su clave pública firmado por CA1 y Roberto tiene un certificado de su clave pública firmado por CA2.

Cuando Alicia se quiere comunicar con Roberto elige una clave simétrica de sesión para la comunicación que quiere establecer, K_s. Ésta es la clave que usará para convertir sus mensajes en confidenciales.

Preguntas

1. Indica cómo crees que debería enviarle la clave K_s de Alicia a Roberto.
2. Alicia no tiene la clave pública de Roberto ni Roberto la de Alicia. Indica cómo podría conseguir Alicia la K_R^+, sin quedar físicamente para intercambiarse las claves, y como puede Alicia estar segura de que esta clave se corresponde con la de Roberto.
3. Con este sistema, ¿puede estar Alicia segura de que los mensajes que envía a Roberto son confidenciales y de que en realidad se está comunicando con Roberto? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.
4. Con este sistema, ¿puede estar Roberto seguro de que los mensajes son confidenciales y provienen de Alicia? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.
5. El certificado de la clave públicad de Roberto ha caducado y ya no es válido. Roberto decide cambiar de autoridad de certificación y consigue un certificado de su clave pública emitido por la autoridad de certificación CA3. Esta autoridad de certificación CA3 no ha incluido su certificado autofirmado en las aplicaciones de comunicaciones del sistema, pero CA3 tiene un certificado de la clave pública de CA3 firmado por CA2. Indica si ahora Alicia podría enviar a Roberto mensajes confidenciales y auténticos y explica cómo lo haría.

3. Ejercicio 3

Abre el navegador Firefox y a través del menú selecciona la opción: Editar → Preferencias → Privacidad y Seguridad → Seguridad → Certificados → Ver Certificados.

En la pestaña “Autoridades” verás los certificados de las autoridades de certificación de primer nivel. Cualquier certificado que venga firmado por las autoridades de certificación que se encuentran en esta pestaña podrá ser verificado ya que se poseen de forma fiable las claves públicas de estas autoridades de certificación que permiten comprobar las firmas.

1. Escribe en la URL del navegador la siguiente dirección: `www.amazon.es`, una vez que se haya cargado la página verás junto a la URL un candado verde, pulsa sobre él y luego sobre la flecha derecha al lado de "Conexión segura" ("Mostrar detalles de la conexión"). Indica cuál es la autoridad de certificación que ha verificado esta conexión segura.

2. En esa ventana de detalles de la conexión, pulsa sobre el botón "Más información" y luego en "Ver Certificado" y en la pestaña "Detalles". Indica cuál es la jerarquía de certificados que se está utilizando para verificar a Amazon. Selecciona empezando por www.amazon.es el campo "Emisor" y ve comprobando quiénes han sido las entidades que han generado los certificados que aparecen en la jerarquía. Comprueba la cadena de todos los certificados. Señala qué certificados de la jerarquía están autofirmados.

3. Vuelve a visitar la información de certificados de las Preferencias (Editar → Preferencias → Privacidad y Seguridad → ... → Ver Certificados). Observarás que las dos entidades que aparecen en la jerarquía de certificados de Amazon tienen instalado su certificado. Una de ellas muestra su certificado como `Builtin object token`, es decir, se trata de un certificado autofirmado de una autoridad de certificación raíz que venía instalado con la aplicación Firefox. El otro certificado se muestra como `Disp. software de seguridad`, por lo que no es un certificado autofirmado y la entidad que lo ha firmado es una autoridad de certificación raíz. Indica cuál de ellos es `Builtin object token` y cuál es `Disp. software de seguridad`.