UNIVERSIDAD DE GRANADA

Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

– 3er curso del Grado en Ingeniería Informática (y dobles grados) –

Convocatoria ordinaria (1 de febrero de 2021)

Apellidos y nombre:

Titulación / grupo:

ENTREGA:

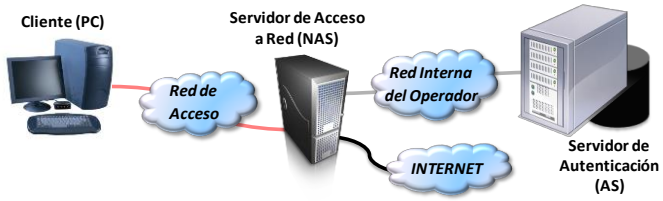
Haga la resolución de cada ejercicio en papel, escrito con bolígrafo de su puño y letra.

Después escanee o fotografíe los folios que desee que se evalúen, **INCLUYENDO SU DNI FÍSICO EN TODAS LAS PÁGINAS**. Preferiblemente todos juntos en un documento PDF.

Súbalo a la entrega en PRADO que se habrá habilitado durante la duración del examen, en los 10 minutos habilitados para la entrega.

PROBLEMA 1-A (3 puntos sobre 10)

La figura y mensajes siguientes describen un protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



PC → NAS: peticion_acceso + usuario
NAS → PC: desafio
PC → NAS: usuario + K_{PC-AS}(desafio)
NAS → AS: peticion_autenticacion + usuario + K_{PC-AS}(desafio)
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
NAS → PC: peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar) + MD5($Ksesion_{PC-NAS}$ (datos_a_enviar))
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta) + MD5($Ksesion_{PC-NAS}$ (datos_de_respuesta))

Siendo:

- $Kpub_X$ (P) → cifrado de P con la clave pública de X
- $Kpriv_X$ (P) → cifrado de P con la clave privada de X
- K_{X-Y} (P) → cifrado de P con la clave secreta entre X e Y
- K_{X-Y} → clave secreta entre X e Y
- MD5 → función *hash*

a) Indique qué servicios de seguridad se proporcionan (confidencialidad, autenticación, integridad y no repudio) y entre qué elementos (PC, NAS, AS). Explique detalladamente su respuesta.
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

NOTA: Responda razonadamente a las cuestiones.

UNIVERSIDAD DE GRANADA

Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

– 3er curso del Grado en Ingeniería Informática (y dobles grados) –

Convocatoria ordinaria (1 de febrero de 2021)

Apellidos y nombre:

Titulación / grupo:

ENTREGA:

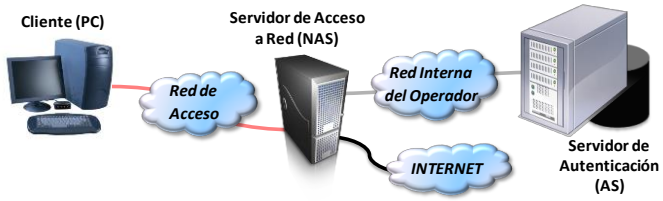
Haga la resolución de cada ejercicio en papel, escrito con bolígrafo de su puño y letra.

Después escanee o fotografíe los folios que desee que se evalúen, **INCLUYENDO SU DNI FÍSICO EN TODAS LAS PÁGINAS**. Preferiblemente todos juntos en un documento PDF.

Súbalo a la entrega en PRADO que se habrá habilitado durante la duración del examen, en los 10 minutos habilitados para la entrega.

PROBLEMA 1-B (3 puntos sobre 10)

La figura y mensajes siguientes describen un protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



PC → NAS: $Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC: desafio
PC → NAS: $Kpub_{NAS}$(usuario + K_{PC-AS}(desafio))
NAS → AS: $Kpriv_{NAS}$(peticion_autenticacion + usuario + K_{PC-AS}(desafio))
AS → NAS: $Kpriv_{AS}$(peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$))
(o $Kpriv_{AS}$(peticion_rechazada))
NAS → PC: peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: datos_de_respuesta

Siendo:

- $Kpub_X$ (P) → cifrado de P con la clave pública de X
- $Kpriv_X$ (P) → cifrado de P con la clave privada de X
- K_{X-Y} (P) → cifrado de P con la clave secreta entre X e Y
- K_{X-Y} → clave secreta entre X e Y

a) Indique qué servicios de seguridad se proporcionan (confidencialidad, autenticación, integridad y no repudio) y entre qué elementos (PC, NAS, AS). Explique detalladamente su respuesta.
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

NOTA: Responda razonadamente a las cuestiones.

UNIVERSIDAD DE GRANADA

Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

– 3er curso del Grado en Ingeniería Informática (y dobles grados) –

Convocatoria ordinaria (1 de febrero de 2021)

Apellidos y nombre:

Titulación / grupo:

ENTREGA:

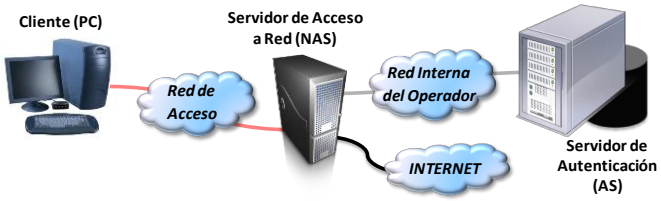
Haga la resolución de cada ejercicio en papel, escrito con bolígrafo de su puño y letra.

Después escanee o fotografíe los folios que desee que se evalúen, **INCLUYENDO SU DNI FÍSICO EN TODAS LAS PÁGINAS**. Preferiblemente todos juntos en un documento PDF.

Súbalo a la entrega en PRADO que se habrá habilitado durante la duración del examen, en los 10 minutos habilitados para la entrega.

PROBLEMA 1-C (3 puntos sobre 10)

La figura y mensajes siguientes describen un protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



PC → NAS: $Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC: $Kpriv_{NAS}$(desafio)
PC → NAS: $Kpub_{NAS}$(usuario + $K_{PC\text{-}AS}$(desafio))
NAS → AS: $Kpriv_{NAS}$(peticion_autenticacion + usuario + $K_{PC\text{-}AS}$(desafio))
AS → NAS: $Kpriv_{AS}$(peticion_aceptada + $Ksesion_{PC\text{-}NAS}$ + $K_{PC\text{-}AS}$($Ksesion_{PC\text{-}NAS}$))
(o $Kpriv_{AS}$(peticion_rechazada))
NAS → PC: $Kpriv_{NAS}$(peticion_aceptada + $K_{PC\text{-}AS}$($Ksesion_{PC\text{-}NAS}$))
(o $Kpriv_{NAS}$(peticion_rechazada))
PC → NAS: datos_a_enviar + MD5(datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC\text{-}NAS}$ (datos_de_respuesta) + MD5($Ksesion_{PC\text{-}NAS}$ (datos_de_respuesta))

Siendo:

- $Kpub_X$ (P) → cifrado de P con la clave pública de X
- $Kpriv_X$ (P) → cifrado de P con la clave privada de X
- $K_{X\text{-}Y}$ (P) → cifrado de P con la clave secreta entre X e Y
- $K_{X\text{-}Y}$ → clave secreta entre X e Y

a) Indique qué servicios de seguridad se proporcionan (confidencialidad, autenticación, integridad y no repudio) y entre qué elementos (PC, NAS, AS). Explique detalladamente su respuesta.
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

NOTA: Responda razonadamente a las cuestiones.

Seguridad A

Los aspectos de seguridad son 5: confidencialidad, autenticación, integridad, no repudio y disponibilidad. Respecto a este último punto, disponibilidad, no se puede dar información porque no se conocen aspectos como la infraestructura física, elementos redundantes, etc.

Este procedimiento persigue que un usuario (cliente) se autentique frente a un servidor de autenticación (AS) para ver si tiene derecho a acceder a Internet a través de un servidor de acceso a red (NAS). Es un esquema típico que utilizan los ISPs. Básicamente el cliente le manda una petición al NAS, que le responde con un desafío. El cliente manda dicho desafío cifrado con la clave secreta entre el PC y el AS, que es reenviado por el NAS al AS. Si este desafío cifrado coincide con lo que calcula el AS, le devuelve que la petición ha sido aceptada. Si no, se rechaza. En el mensaje de sesión aceptada, AS manda a NAS la clave de sesión entre el PC y el NAS (sin cifrar y cifrada con la clave secreta entre PC y AS). NAS se la reenvía a PC (cifrada con la clave secreta entre PC y AS). Así, tanto PC como NAS conocen dicha clave de sesión que usarán después para enviar entre ellos los datos que van/vienen de Internet.

Respecto a confidencialidad:

- La petición inicial entre PC y NAS va sin cifrar, por lo que cualquiera puede ver esos datos (petición y usuario).
- La respuesta al desafío (K_{PC-AS}(desafio)) no incluye ningún *nonce* o elemento que no se repita, por lo que es susceptible de ataques por repetición.
- La información entre NAS y AS va sin cifrar, por lo que un trabajador del ISP podría ver todos esos mensajes y la información enviada.
- La clave de sesión sí se envía cifrada entre NAS y PC, por lo que no podría ser vista por alguien externo en ese enlace (sí entre AS y NAS, donde se envía sin ir cifrada).
- Los datos desde el PC al NAS y viceversa (respuestas) sí van cifradas con una clave de sesión. Hacia Internet estos datos van sin cifrar.

Respecto a la autenticación:

- El procedimiento persigue que el PC se autentique frente al AS enviando una prueba de ello (el desafío cifrado con la clave secreta compartida entre el PC y el AS).
- El NAS se fía de la respuesta (peticion_aceptada o peticion_rechazada) enviada por el AS. Esto puede ser problemático porque el AS no se autentica frente al NAS (no hay ningún procedimiento para ello, ni cifra los mensajes con su clave privada para que el otro descifre con la pública, ni nada similar).
- NAS no se autentica con el PC. Tampoco se autentican NAS y AS entre ellos.

Respecto a la integridad: solo se incluye un resumen (a través de la función *hash* MD5) de los datos enviados y sus respuestas entre PC y NAS. Eso significa que esos mensajes no pueden ser modificados sin que nos demos cuenta. El resto de mensajes no tienen ningún resumen por lo que podrían ser modificados sin que nos diésemos cuenta.

Respecto al no repudio: no hay ninguna prueba (e.g. por haber cifrado algo con mi clave pública y que pueda ser descifrado por cualquiera con mi clave privada) de que hemos participado en esta transacción. Incluso los mensajes cifrados con la clave secreta o de sesión no servirían, ya que puede haberlos cifrado cualquiera de los dos extremos (no serviría de prueba frente a un juez).

Las debilidades se han explicado en los párrafos anteriores. Las posibles soluciones serían conseguir confidencialidad en todos los mensajes (e.g. usando la clave pública del receptor),

autenticación (e.g. usando la clave privada del emisor), integridad (e.g. añadiendo resúmenes con MD5 de los mensajes enviados) y no repudio (se consigue también al usar, por ejemplo, la clave privada del emisor).

Seguridad B

El ejercicio es prácticamente igual que el de Seguridad A, con algunas pequeñas modificaciones. Resumidamente:

- Los datos mandados por el PC al NAS van cifrados con la clave pública del NAS, por lo que solo él los puede descifrar con su clave privada.
- Los datos entre NAS y AS van cifrados con sus respectivas claves privadas, consiguiendo así autenticación y no repudio (solo ellos han podido cifrarlos, y cualquiera puede descifrarlos con sus claves públicas).
- No se mandan resúmenes con MD5 en los mensajes entre PC y NAS (datos y respuestas), por lo que ahora no se consigue integridad en esa parte.

Seguridad C

El ejercicio es una mezcla entre los ejercicios de Seguridad A y B. Básicamente es el ejercicio B añadiendo los resúmenes MD5 en los últimos mensajes, consiguiendo así integridad en los mismos.