

Publicación de notas: lunes 27/1/2003 (D6 planta 0 y racó FIB).

Revisión examen: martes 28/1/2003, 12:00-13:00, D6-105.

Durante el examen puedes consultar los apuntes y transparencias.

Debes elaborar las respuestas con tus palabras, no con textos copiados de la documentación.

Cada pregunta puntúa un 20% (2 puntos de 10).

Resuelve los problemas en **hojas separadas**.

# Examen de AAD

17/1/2003. 18:30 – 20:00 (90")

Accept-Language: ca, es, fr, en

**Responde de forma concisa pero completa a las preguntas siguientes:**

1. Recientemente se han realizado ataques importantes al servicio DNS (En Octubre 2002 9 de los 13 servidores root de DNS tuvieron sobrecargas de tráfico durante unos 45 minutos debido a un ataque, lo que afectó a su capacidad de servicio). "DNS cache poisoning" es un mecanismo para introducir información falsa en un servidor DNS. También resulta posible que alguien capture y cambie el contenido de un paquete IP en tránsito con una respuesta DNS. A la vista de estos y otros problemas:

**¿Qué mecanismos de seguridad introducirías para proteger la integridad y verificar la autenticidad de la información de DNS que viaja por Internet (consultas, transferencias)? ¿Qué inconvenientes podrían acarrear?**

2. El protocolo http1.1 se utiliza también en las redes de PC (llamadas "Peer-to-peer" o P2P) de intercambio de archivos como Gnutella. En estas redes cuando desde un PC se busca un archivo con cierto nombre en otros PC de la red, puede encontrarse en decenas o cientos de PC desde donde se puede descargar, por trozos y en paralelo, usando la codificación "chunked" de http1.1.

Para identificar los archivos de forma inequívoca se les asigna un nombre URN calculando sha1(contenido del archivo). En el resultado de una búsqueda se recibe además del nombre de un archivo, el valor hash sha1 de su contenido.

Además cada PC que recibe un archivo recuerda de qué otros PC lo ha obtenido. Por ello la respuesta de un servidor Gnutella tiene entre otros los siguientes campos en la cabecera de la respuesta http:

X-URN: urn:sha1:JKAQMLAV...VMLRMLSA...

X-Alternate-Location: http://1.2.3.4/uri-res/N2R?url:sha1: JKAQMLAV...VMLRMLSA

Cualquier transacción tiene dos fases: 1) búsqueda (nombre→URN), en que se busca una frase y se selecciona un archivo y se conoce su sha1, 2) transferencia, en que se pide el URN y recibe de uno o varios servidores un archivo con cierto valor sha1.

**¿Qué consecuencias positivas y negativas podría tener para el Web la introducción de estas modificaciones?**

3. Para distribuir un archivo binario (por ejemplo una película o un programa) te piden que propongas un procedimiento (un CGI o un servlet) que permita que cada usuario sólo lo pueda descargar un máximo de tres veces con un margen de una semana y desde la misma ubicación. El usuario rellenaría un formulario web y a continuación podría acceder al archivo haciendo clic en un enlace de una página web en su navegador o tras recibir el enlace en un mensaje de correo recibido del proveedor.

**Indica qué procedimientos se te ocurren y qué información de cabeceras http1.1 podría ser útil recoger y/o poner en la cabecera y/o cuerpo de cada petición-respuesta http1.1 del archivo.**

4. **Explica qué inconvenientes pueden presentarse cuando alguien accede a un contenido servido por una red de distribución de contenidos (CDN) a través de una jerarquía de servidores proxy-caché.**

5. Una empresa multinacional quiere proporcionar un portal web para sus empleados. La empresa dispone de una red privada IP que interconecta en las sedes de 10 países. **Piden que les hagas 3 propuestas de cómo proporcionar el servicio** si quieren a la vez minimizar el tráfico entre sedes especialmente en horas punta (las conexiones internacionales son costosas y las conexiones dentro de la oficina prácticamente gratuitas) y dar un servicio fiable (alta disponibilidad y tiempos de respuesta aceptables).

Hay que considerar por separado los contenidos estáticos (documentos) y los contenidos dinámicos. (Se trata de un concurso entre varios proveedores y por tanto la respuesta ha de ser concreta y convincente para el ingeniero que conoce el tema y toma decisiones).