“Problemas con la seguridad”

Rogelio Ferreira Escutia

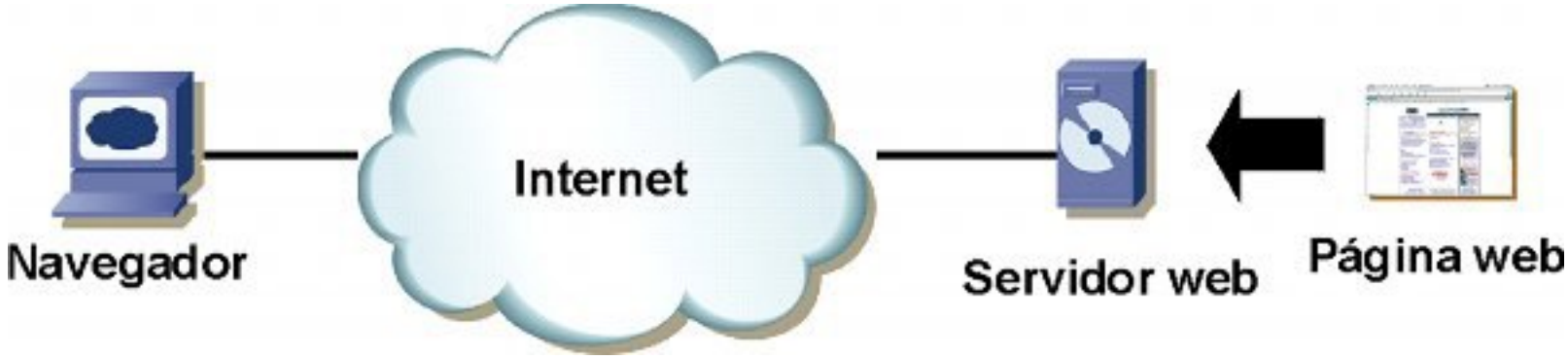
Tecnologías Web

Tecnologías Web

- **Existen básicamente 2 tipos de Tecnologías Web:**
  - **Páginas Web.**
  - **Servicios Web**

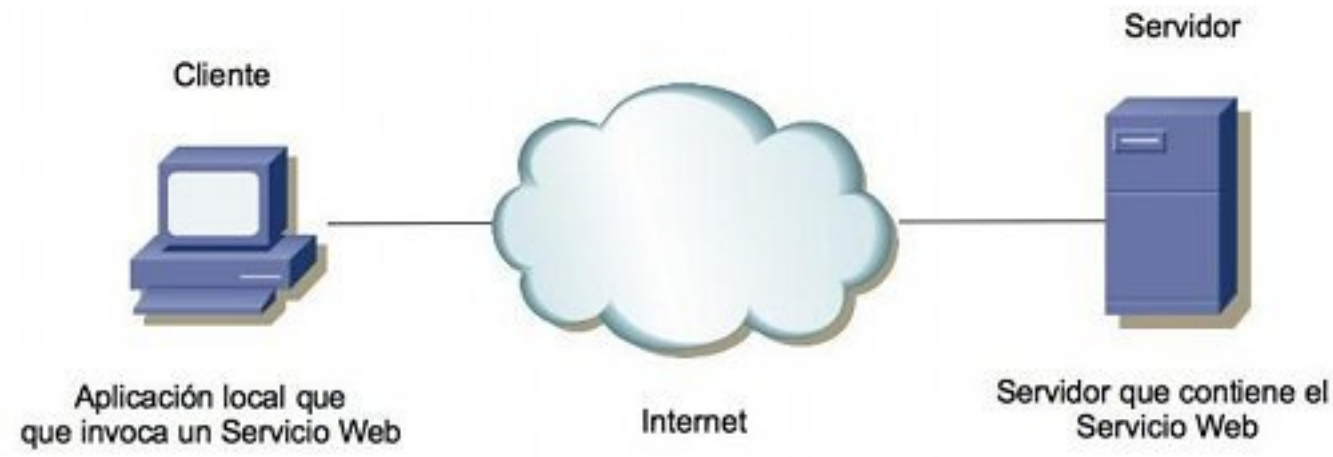
Páginas Web

- **Un cliente con con una computadora con navegador, se comunica por medio de Internet con un Servidor Web para solicitar una página Web.**



Servicios Web

- **Un cliente con con una aplicación local, se comunica por medio de internet, con un servidor que contiene el servicio Web**



Seguridad en Páginas Web

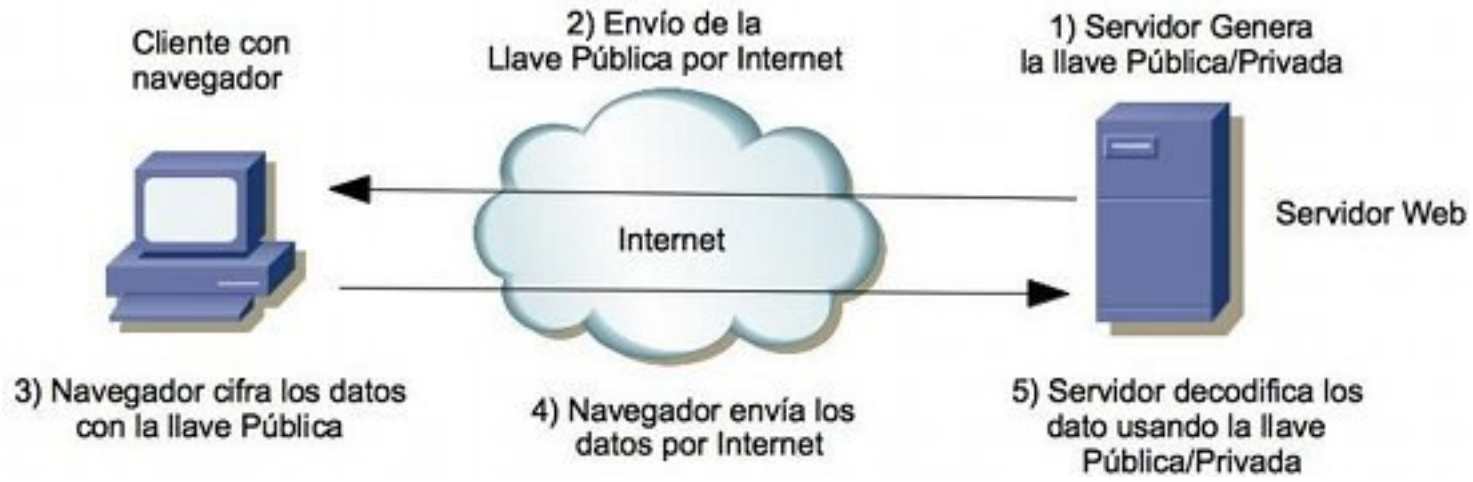
Puntos que requieren seguridad

- **1) Transferencia segura de datos (cifrado de las páginas Web que se envían o reciben.**
- **2) Integridad de los datos (que los archivos o documentos que se enviaron lleguen sin cambio).**
- **3) Autentificar al usuario (verificar que el usuario adecuado es el que envió la información).**

1) Transferencia segura de Datos

- **Se utilizan algoritmos basados en llave Pública/Privada (básicamente RSA). Los pasos son los siguientes:**
  - **1) El servidor genera una llave Pública en base a una llave Privada.**
  - **2) El servidor envía la llave pública por internet al cliente Web.**
  - **3) El cliente (por medio del navegador) cifra los datos a enviar por medio de la llave pública y 4) los envía al servidor.**
  - **5) El Servidor decodifica la página por medio de la llave Pública/Privada.**
- **El posible interceptor en internet tiene acceso a la llave pública pero no a la privada y no puede decodificar.**

1) Transferencia segura de Datos



2) Integridad de los Datos

- **Se requiere utilizar una “huella digital” del documento a enviar para verificar su integridad.**
- **Para crear su “huella” se utilizan algoritmos Hash (generalmente MD5), que al aplicarlos sobre el archivo, generan una cadena de caracteres que se convierte en la “huella”. Los pasos son los siguientes:**

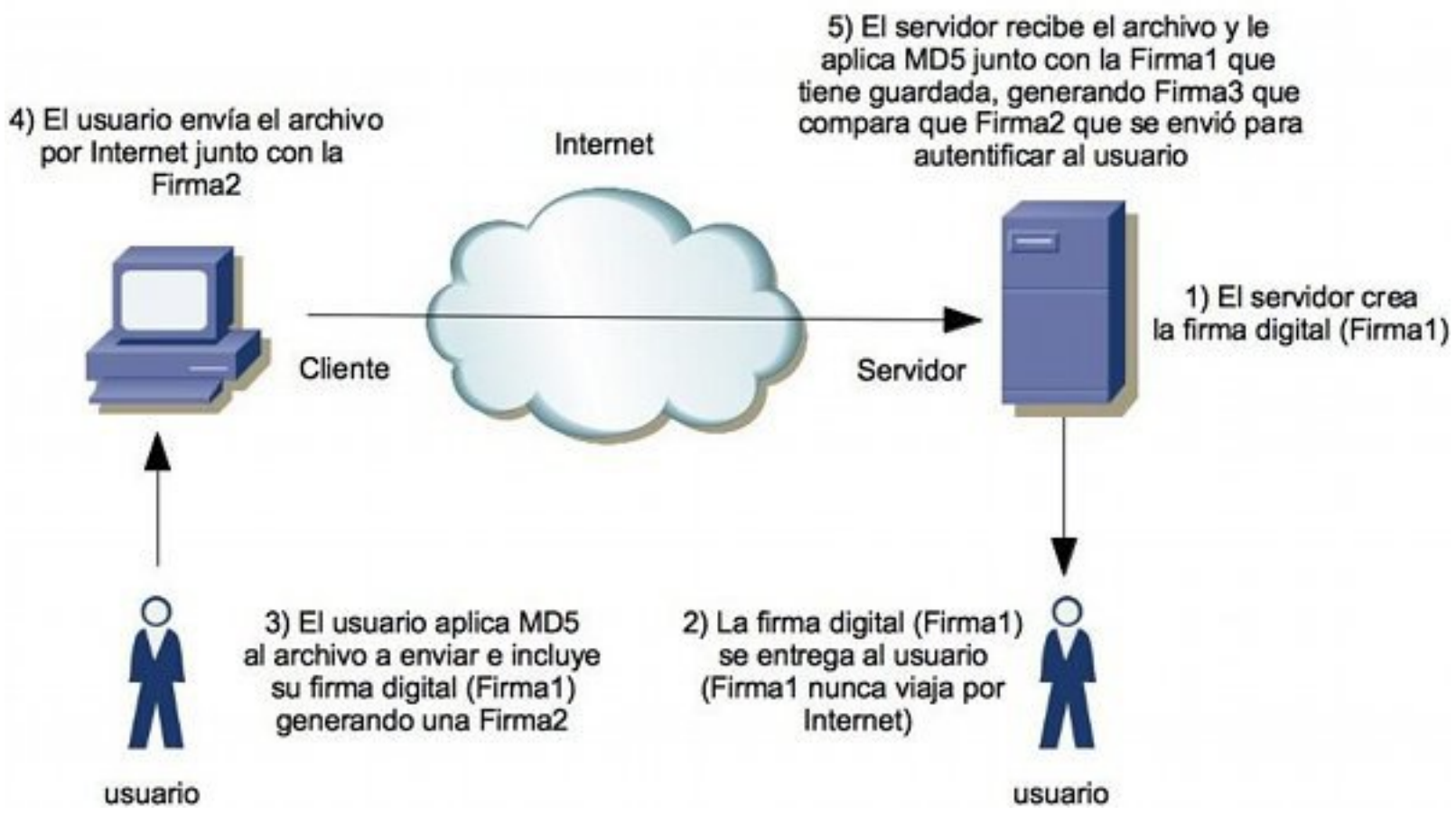
  - **1) Cliente aplica el algoritmo MD5 sobre el archivo para crear una cadena de caracteres(“huella digital”).**
  - **2) Se envía el archivo junto con su huella digital.**
  - **3) El servidor recibe el archivo y vuelve a aplicar el MD5, y 4) compara la huella nueva con la que se envió para determinar la integridad.**

2) Integridad de los Datos

3) Autentificar al usuario

- **Se requiere crear una “firma digital” única del usuario, para que el servidor lo pueda autentificar. La firma digital es un conjunto de caracteres. Los pasos son los siguientes:**
  - **1) El servidor crea la “firma digital única” del cliente (Firma1).**
  - **2) Esta firma digital se le entrega al cliente (de manera personal, no por Internet).**
  - **3) El cliente que va enviar algún documento le aplica MD5 al archivo a enviar junto con la firma que se le asignó (Firma1) y se crea una “Firma2”.**
  - **4) Se envía el archivo por internet junto con la Firma2.**
  - **5) El servidor le aplica MD5 al archivo que llegó junto con la Firma1 del cliente que tiene almacenada y genera una Firma3.**
  - **6) El servidor compara Firma3 con la Firma2 que envió el cliente para determinar la Autenticidad del emisor.**

3) Autentificar al usuario



Metodologías

Metodologías para Seguridad

- **Actualmente no existe alguna metodología especial para modelar la parte de seguridad de un sistema.**

- **La parte de seguridad se incorpora sólamente como un conjunto de requerimientos en la parte inicial del proyecto.**

Rogelio Ferreira Escutia

Instituto Tecnológico de Morelia
Departamento de Sistemas y Computación

Correo:	***rogeplus@gmail.com***
	rogelio@itmorelia.edu.mx
Página Web:	***http://antares.itmorelia.edu.mx/~kaos/***
	http://www.xumarhu.net/
Twitter:	***http://twitter.com/rogeplus***
Facebook:	***http://www.facebook.com/groups/xumarhu.net/***