Universidad
Carlos III de Madrid

COSEC Lab · *Dpto. Informática*

TEMA 2. CRIPTOGRAFÍA
T 2.7 AUTENTICACIÓN DE USUARIOS

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

Curso 2012-2013

Introducción

- Autenticación
  - Procedimiento de comprobación de la identidad de un usuario

- Factores de autenticación
  - Basadas en algo que el usuario conoce (secretos) Contraseña
  - Basadas en algo que el usuario tiene (tokens) Dispositivo físico, automático que sustituya a la contraseña
  - Basadas en algo que el usuario es (biometría) Retina, iris
  - Combinaciones de lo anterior (varios factores)

Autenticación mediante secretos

- El usuario dispone de determinada información secreta que sólo él y el sistema conocen
- Incluye métodos basados en contraseñas, PIN, desafío-respuesta, etc.
- Método de autenticación simple y extendido
- Necesaria una gestión de las contraseñas

Autenticación mediante secretos – Gestión de contraseñas

- Criterios de calidad
  - Fácil de recordar (débil) versus aleatoria (menos débil)
  - Longitud, complejidad
- Custodia de la contraseña por el usuario
  - No divulgación (ingeniería social, phishing, etc.)
- Almacenamiento de contraseñas en el sistema
  - Almacenamiento del resumen de cada contraseña
  - Cifrado de las contraseñas
- Caducidad de contraseñas
  - Cuanto mayor sea la criticidad del sistema, menor debe ser el periodo de validez de las contraseñas

Ante cualquier sospecha cambiar la clave.

Autenticación mediante secretos – Gestión de contraseñas

- Recuerdo de contraseñas
  - Establecer un número mínimo de contraseñas diferentes consecutivas
- Bloqueo de contraseñas / baja de cuentas de usuario
  - En caso de sospecha de uso fraudulento
- Problemática en la reutilización de contraseñas para acceso a diferentes sistemas
- Amenazas
  - Ataques de fuerza bruta y de diccionario
  - Intercepción de contraseñas
  - Ataque a la base de datos del sistema (talón de Aquiles)
  - Ingeniería social

Autenticación mediante secretos – Gestión de contraseñas

- Programas de ruptura de contraseñas
  - L0phtcrack , John the Ripper, Pwdump
  - Diccionarios y listados (teléfonos, matrículas…)

- Programas de gestión de las contraseñas
  - Password Safe (http://www.schneier.com/passsafe.html)
  - SplashID (http://splashdata.com/splashid/)

Autenticación mediante Token

- Dispositivos criptográficos
  - Tarjetas inteligentes, tokens USB
  - Autenticación mediante firma digital

- Tokens OTP
  One Time Password ⇒ Difícil recordarlas todas.

Autenticación mediante Token – OTP

- OTP (*One-Time Password*)
- Contraseñas desechables de un solo uso (sesión, transacción)
- Se generan mediante un token que posee el usuario o software específico

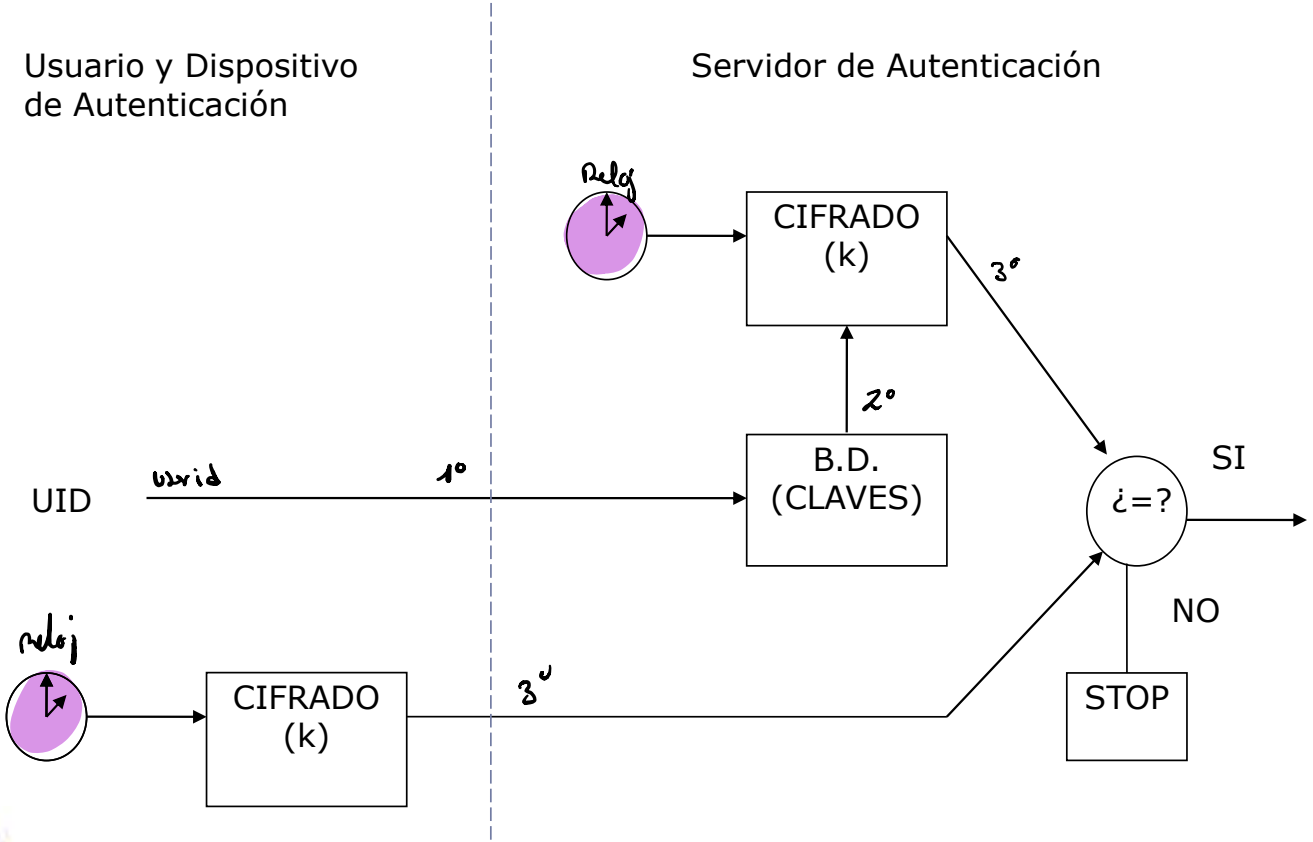
- Evitan los inconvenientes derivados de la gestión de contraseñas clásicas
- Custodia segura del token

Autenticación mediante Token – OTP

- Se basan en aleatoriedad, evitando ataques por predicción

- Tipos
  - **Síncronos**: existe sincronía entre los relojes del token y el servidor de autenticación
  - **Encadenados**: La generación de un OTP depende del OTP anterior
  - Basados en **desafíos**: La generación de un OTP depende del desafío enviado por el servidor de autenticación y un contador interno

Autenticación mediante Token – OTP síncrono



Autenticación mediante Token – OTP encadenado

- Aplicación de una función *f* irreversible de forma encadenada

- Generación de una serie de OTPs basadas en el valor anterior

  f(s), f(f(s)), f(f(f(s))) … f(…(f(f(f(s)))…)

- Uso de las OTPs de forma inversa

  f(…(f(f(f(s)))…)… f(f(f(s))) , f(f(s)), f(s)

Autenticación mediante Token – OTP encadenado

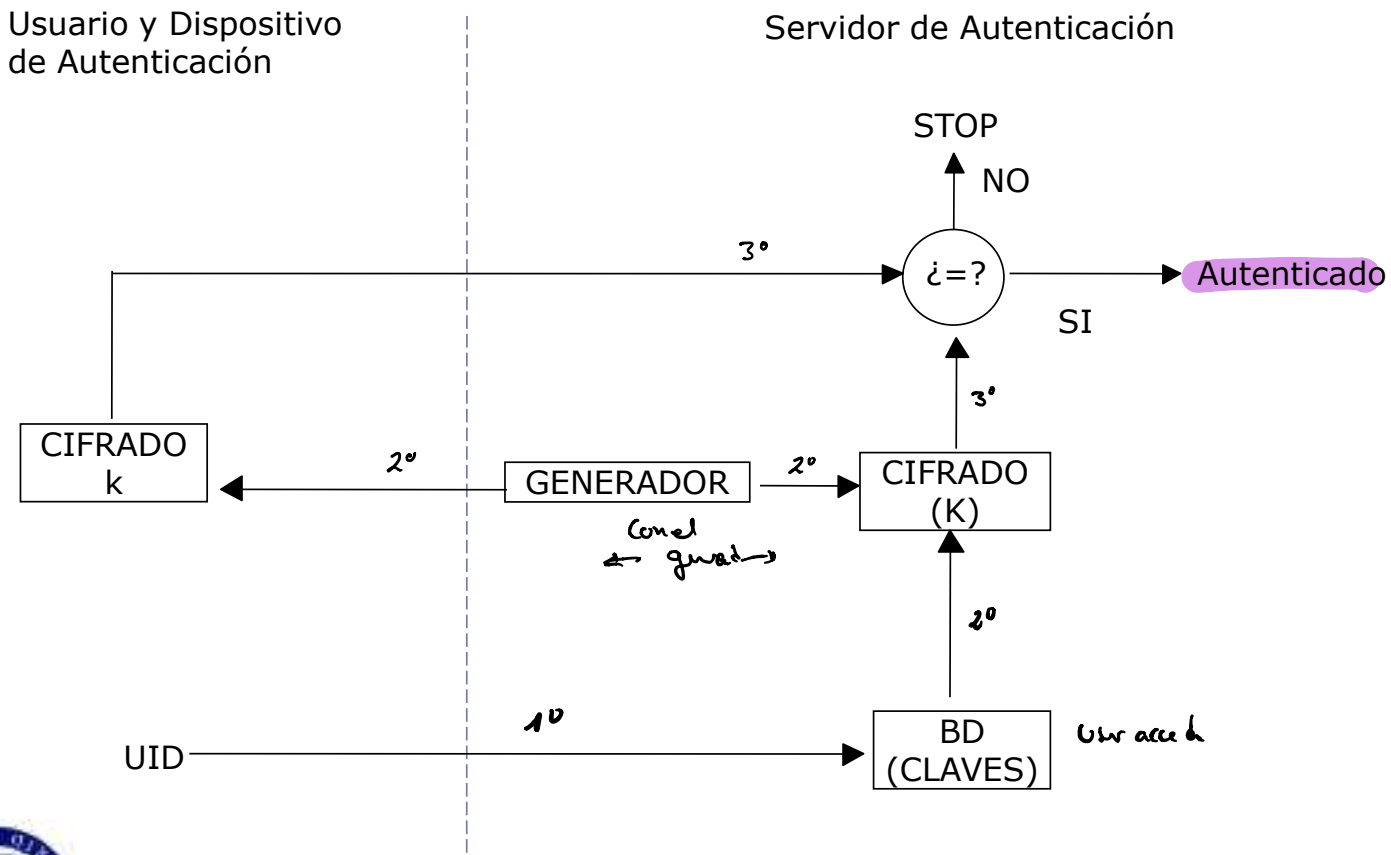
- Inicialización
  1. El servidor de autenticación elige la función *f*
  2. El usuario elije el máximo nº de autenticaciones (n)
  3. El token inicializa la semilla s y calcula $f^n(s)$
  4. El usuario envía n y $f^n(s)$ al servidor de autenticación por un canal seguro
  5. El servidor de autenticación registra $f^n(s)$ junto con el ID del usuario
- Uso
  6. El token envía el ID y $f^{n-1}(s)$ al servidor de autenticación
  7. El servidor de autenticación recupera $f^n(s)$ mediante el ID

Autenticación mediante Token – OTP encadenado

8. El servidor de autenticación calcula $f(f^{n-1}(s))$ y comprueba si coincide con $f^n(s)$ almacenado
9. El servidor de autenticación borra $f^n(s)$ del registro y almacena en su lugar $f^{n-1}(s)$
10. El servidor de autenticación resta 1 a n
11. Se repite el proceso hasta que n=0

- Un atacante que intercepte un OTP deberá ser capaz de invertir la función *f* para conocer el siguiente valor OTP
  - Normalmente se emplean funciones resumen

Autenticación mediante Token – OTP basado en desafío



Autenticación biométrica

- El sistema autentica al usuario basándose en rasgos biométricos (característica física única e irrepetible)
- Existe un proceso de registro en el sistema (extracción del patrón biométrico y almacenamiento)
- El proceso de autenticación implica la obtención del patrón biométrico del usuario, y su comparación con el patrón almacenado
- Múltiples técnicas biométricas (huella dactilar, iris, vascular, geometría de la mano, escritura y firma manuscrita, voz, …)
  - Diferentes tasas de eficacia (falsos positivos / falsos positivos)

Iris y voz poco confiables.

Autenticación biométrica

Autenticación biométrica

Universidad
Carlos III de Madrid

COSEC Lab · *Dpto. Informática*

ANEXO

Autenticación de entidades.

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

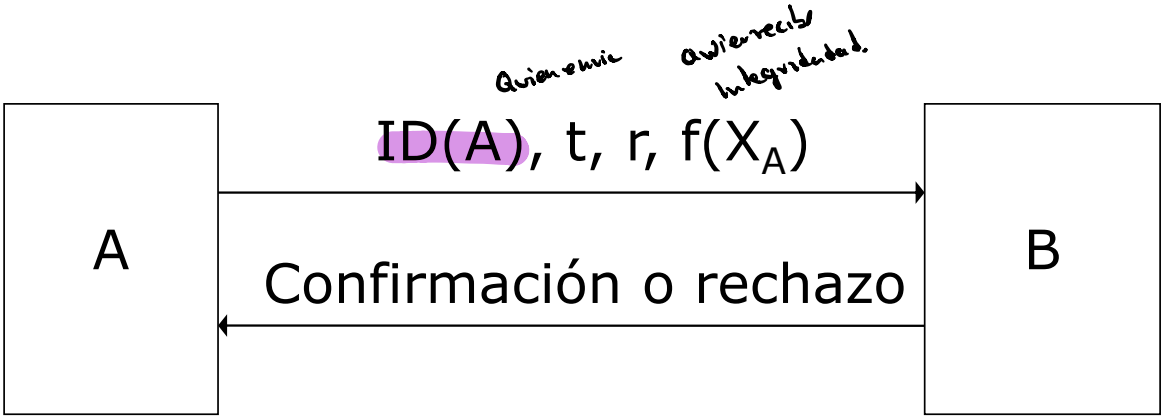
Curso 2012-2013

Tipos de autenticación de entidades

- Simple (basado en contraseña) Envía su nombre distintivos y una contraseña al servidor y este la verifica.
- Fuerte (basados en prueba de posesión de clave privada) Se basa en los criptosistemas de clave pública, comprobando con la pública que tiene la privada.
  - 1 sentido Unidireccional B autentica a A
  - 2 sentidos Bidireccional A autentica a B, B autentica a A
  - 3 sentidos De tres sentidos
    - Como bidireccional, A remite a B una nueva transmisión en la que el emisor devuelve el código generado por el receptor para que este compruebe su integridad. Sin control del tiempo.

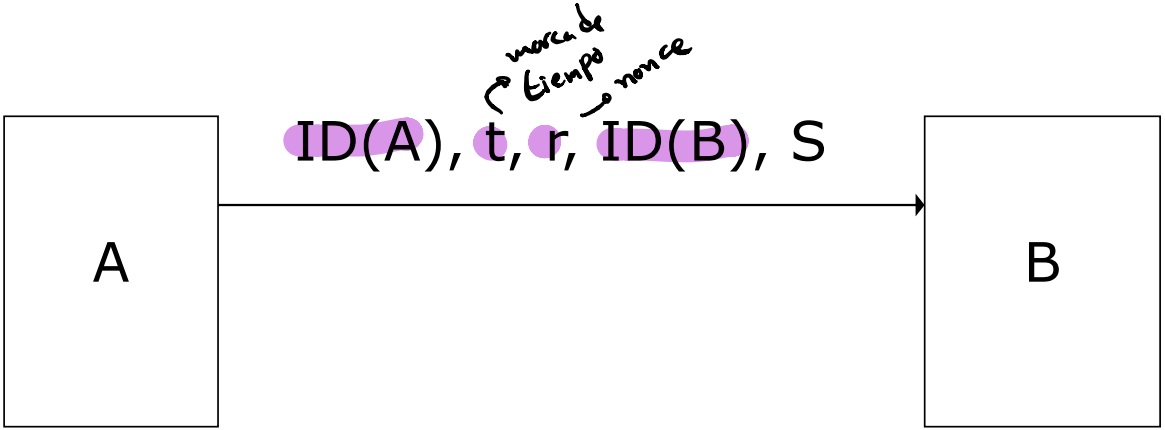
ITU-T X.509; ISO/IEC 9594-8

Autenticación de entidades simple



ITU-T X.509; ISO/IEC 9594-8

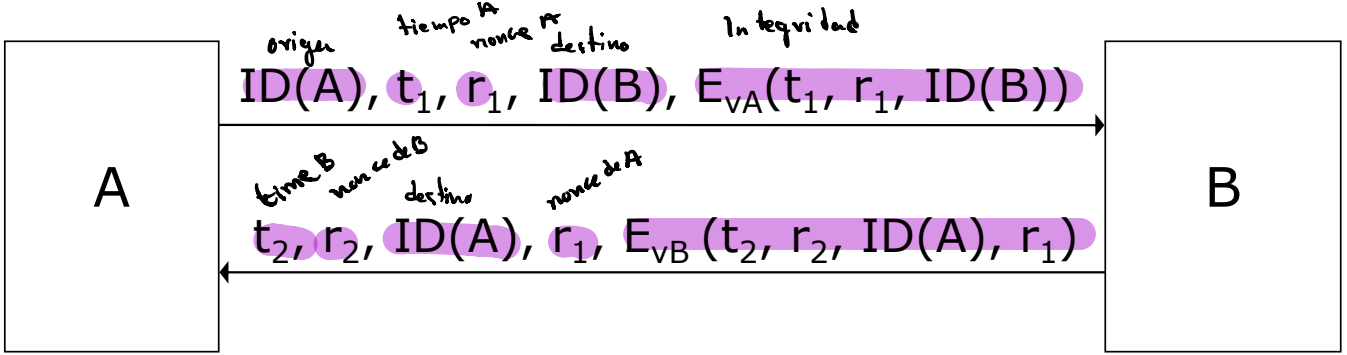
Autenticación de entidades fuerte: Unidireccional



$$S = E_{vA}(t, r, ID(B))$$

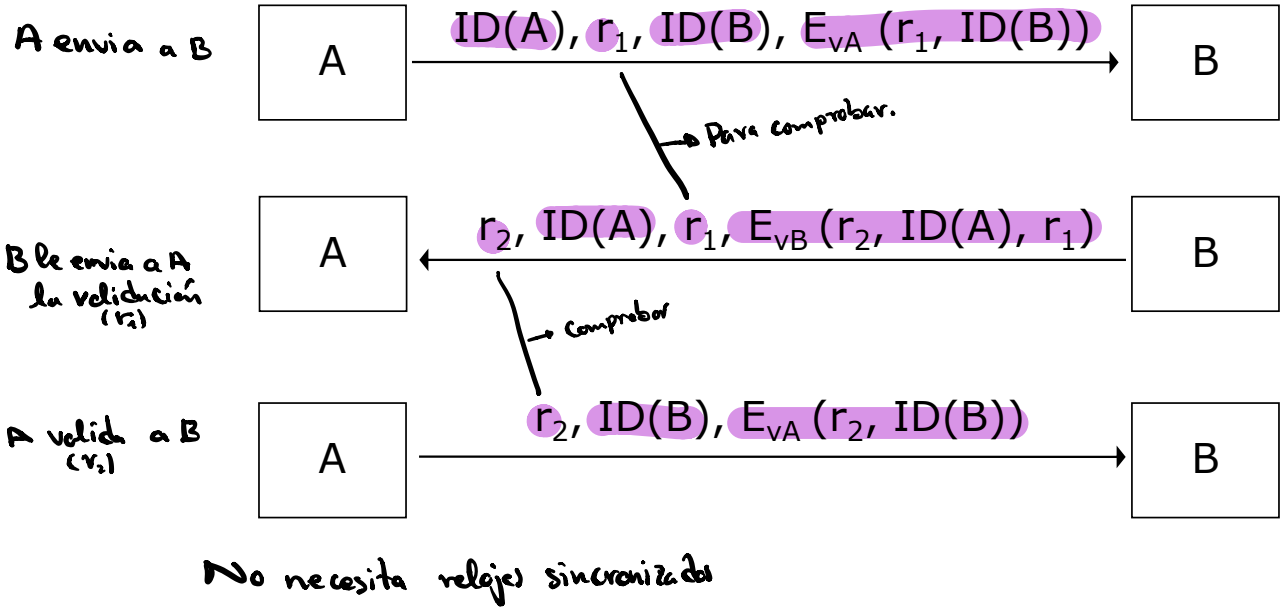
ITU-T X.509; ISO/IEC 9594-8

Autenticación de entidades fuerte: Bidireccional



ITU-T X.509; ISO/IEC 9594-8

Autenticación de entidades fuerte:
De tres sentidos



ITU-T X.509; ISO/IEC 9594-8