Secreto hacia atrás
Secreto hacia adelante

Pino Caballero-Gil

Grupo CryptULL de investigación en Criptología

Universidad de La Laguna

Forward secrecy
Backward secrecy

Pino Caballero-Gil

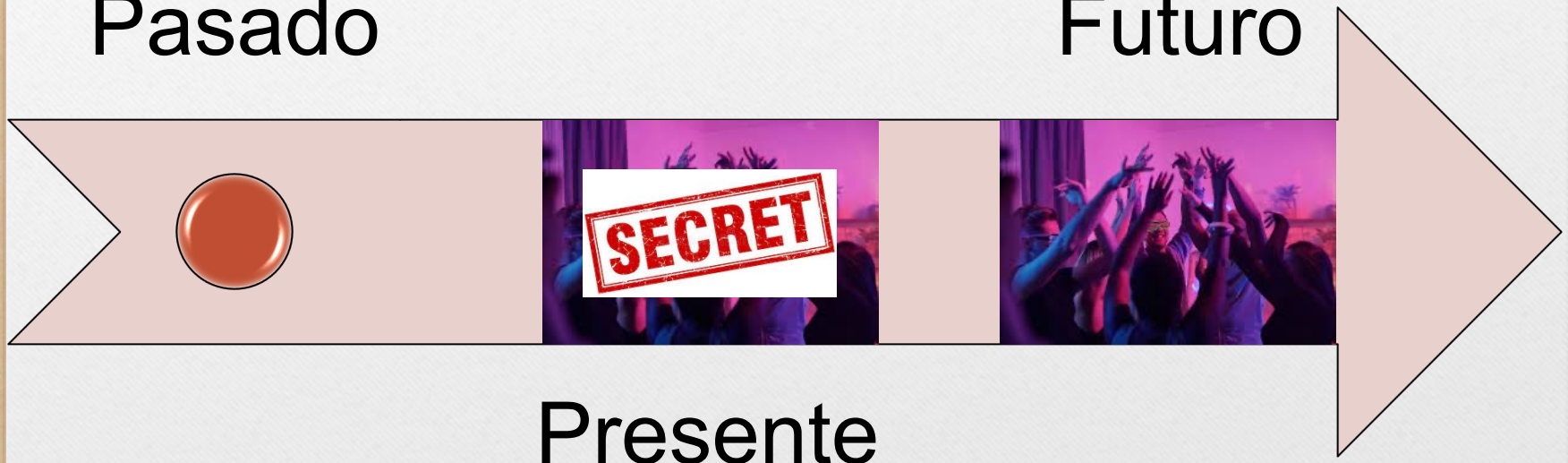
Grupo CryptULL de investigación en Criptología

Universidad de La Laguna

El Tiempo

Pasado

Futuro



Presente

Forward Secrecy

Ningún nodo de una **red** debe poder leer ningún mensaje transmitido por la red después de haberla **abandonado**.

Pasado

Futuro

miembro de la red

Presente

Backward Secrecy

Ningún nodo de una **red** debe poder leer ningún mensaje transmitido por la red antes de que se **uniera**.

Pasado

Futuro

miembro de la red

Presente

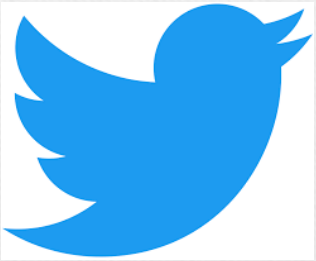
Forward/Backward Secrecy

Kim, Y., Perrig, A., Tsudik, G. Simple and fault-tolerant key agreement for dynamic collaborative groups. ACM Conference on Computer and Communications Security. 2000.

2. Forward Secrecy – (not to be confused with Perfect Forward Secrecy or PFS) guarantees that a passive adversary who knows a contiguous subset of old group keys cannot discover subsequent group keys.

3. Backward Secrecy – guarantees that a passive adversary who knows a contiguous subset group keys cannot discover preceding group keys.

Forward/Backward Secrecy en Redes Sociales



Perfect Forward Secrecy

- *Günther, C.G. An identity-based key-exchange protocol. Eurocrypt '89.*

> This modification restores a property of the Diffie-Hellman scheme, which we could call *perfect forward secrecy:* If Alice and Bob are not impersonated, when the protocol is run, finding the key ζ is as difficult as breaking the Diffie-Hellman scheme for *every* third party. We note that even the KAC could be the third party. This has the important consequence that if by accident the KAC's secret key becomes known, the confidentiality of past message would not be compromised. Only the authenticity in the future would be lost.

Perfect Forward Secrecy

- El PFS implica la garantía de que, incluso aunque se comprometa alguna clave privada a largo plazo, las **claves de sesión** no quedan comprometidas.

Perfect Forward Secrecy

La misma clave privada no se debe usar para autenticación y cifrado porque:

- la **autenticación** solo importa mientras se establece la comunicación
- el **cifrado** debe durar mucho más tiempo

PFS en Tecnologías

NBC News

Twitter joins Google, Facebook with 'forward secrecy' security

Twitter is the latest to implement "forward secrecy," a cryptographic technique that should stymie even the NSA.

22 nov 2013

ComputerHoy.com

WhatsApp añade mensajes cifrados y más seguridad en Android

El nuevo sistema de encriptación de WhatsApp también emplea una tecnología Forward Secrecy, que evita que un hacker pueda acceder a la...

18 nov 2014

Redes Zone

El estándar WPA3 para Wi-Fi es lanzado oficialmente: estas son las características que tienes que conocer

WPA3 Forward Secrecy. Ahora utiliza el protocolo de enlace SAE. Se trata de una característica de seguridad que evita que los atacantes...

26 jun 2018

ADSLZone

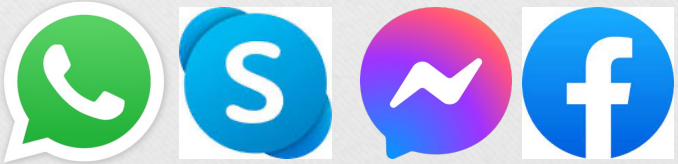
Netflix será más rápido y seguro gracias a TLS 1.3

Netflix será más rápido y seguro gracias a TLS 1.3 ... Ofrecer la mejor experiencia de visionado es una de las principales obsesiones de las plataformas de...

21 abr 2020

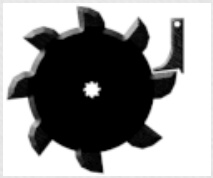
PFS en Signal

- En el protocolo Signal de llamadas y mensajería, si la clave privada del servidor queda vulnerable, las claves de sesiones futuras no se ven comprometidas.
- Para ello se usa el algoritmo **Double Ratchet** que permite al protocolo autocurarse tras un compromiso.



Algoritmo Double Ratchet

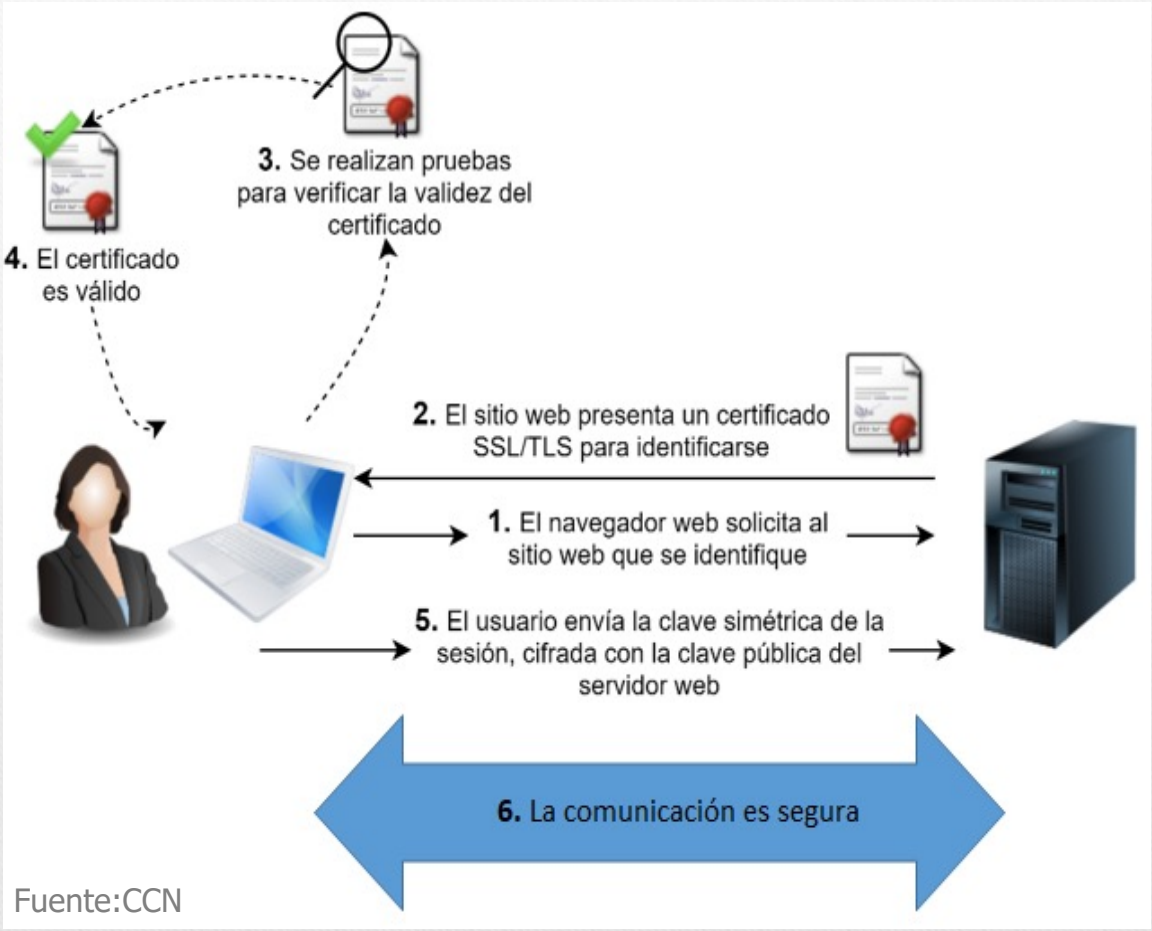
- Para la gestión de claves en cifrados extremo a extremo, tras un intercambio de claves inicial, este algoritmo gestiona la **renovación continua de las claves de sesión**, combinando un intercambio de claves Diffie-Hellman (DH) con una función hash para la derivación de claves (KDF).
- Se garantiza PFS ya que cada clave de sesión se establece tras varias rondas de comunicación, de forma que un atacante tendría que interceptar todas esas rondas para acceder a la clave de sesión.



TLS 1.2

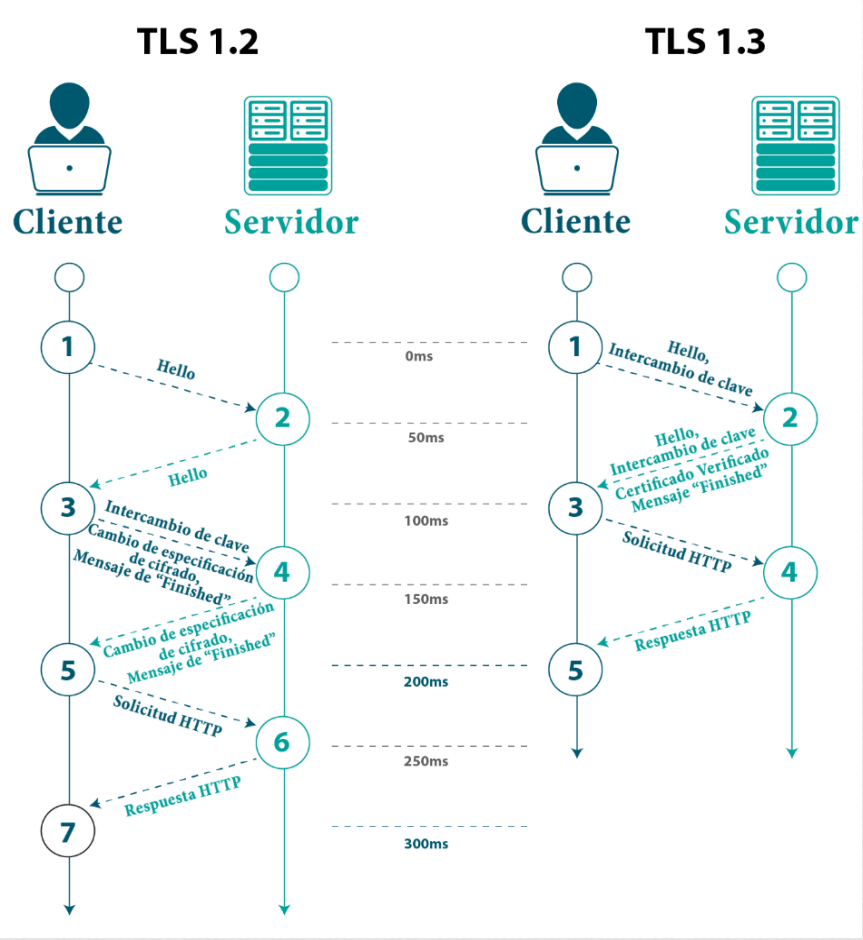
- En las suites de cifrado de versiones antiguas del TLS, el establecimiento de clave de sesión basado en RSA usaba la clave privada del servidor de forma que si esa clave quedaba comprometida, todas las claves de sesión en las que se hubiera usado quedaban comprometidas.

Handshake en TLS sin PFS



Fuente:CCN

Mejoras en TLS



Suites de Cifrado en TLS

Cipher Suites

 # TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS

Actualización de TLS

Intercambio de claves y Autenticación				
Algoritmo	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Sí	Sí	Sí	No
DH-RSA	Sí	Sí	Sí	No
DHE-RSA (PFS)	Sí	Sí	Sí	Sí
ECDH-RSA	Sí	Sí	Sí	No
ECDHE-RSA (PFS)	Sí	Sí	Sí	Sí
DH-DSS	Sí	Sí	Sí	No
DHE-DSS (PFS)	Sí	Sí	Sí	No
ECDH-ECDSA	Sí	Sí	Sí	No
ECDHE-ECDSA (PFS)	Sí	Sí	Sí	Sí
ECDH-EdDSA	Sí	Sí	Sí	No
ECDHE-EdDSA (PFS)	Sí	Sí	Sí	Sí
PSK	Sí	Sí	Sí	No
PSK-RSA	Sí	Sí	Sí	No
DHE-PSK (PFS)	Sí	Sí	Sí	Sí
ECDHE-PSK (PFS)	Sí	Sí	Sí	Sí
SRP	Sí	Sí	Sí	No
SRP-DSS	Sí	Sí	Sí	No
SRP-RSA	Sí	Sí	Sí	No
Kerberos	Sí	Sí	Sí	No