Seguridad de Redes de Computadores

Redes de Computadores

FIEC04705

Sesión 25

Agenda

- Terminología
- Seguridad en capas de aplicación y de transporte:
  - SSL
  - PGP

Terminología

Terminología

- **Message Authentication**: una medida de seguridad en la cual el remitente del mensaje es verificado por cada mensaje enviado.
- **Función Hash**: un algoritmo que crea un digest de tamaño fijo a partir de un mensaje de longitud variable. Ejemplos: MD5, SHA-1, SHA-2.
- **Message Authentication Code (MAC)**: una función hash con llave.
- **Internet Engineering Task Force (IETF)**: desarrolla y promueva estándares para el Internet en colaboración con la W3C e ISO/IEC.

Secure Sockets Layer - SSL

SSL

- SSL es un protocolo de capa de transporte, diseñado para proveer seguridad y servicios de compresión a los datos generados desde la capa de aplicación.
- SSL puede recibir datos desde cualquier protocolo de capa de aplicación, pero usualmente es el protocolo HTTP.

SSL

- SSL provee varios servicios para los datos recibidos desde la capa de aplicación:
  - **Fragmentación**: SSL divide los datos en bloques de hasta 2^{14} bytes
  - **Compresión**: cada fragmento de datos es compreso utilizando un mecanismo de compresión negociado entre el cliente y el servidor. Este servicio es opcional.
  - **Integridad del mensaje**: SSL utiliza una función hash con llave para crear un MAC.
  - **Confidencialidad**: el dato original y el MAC son encriptados utilizando criptografía simétrica.
  - **Framing**: Se agrega una cabecera al mensaje encriptado.

Protocolos definidos por SSL

Figure 32.16 *Four SSL protocols*

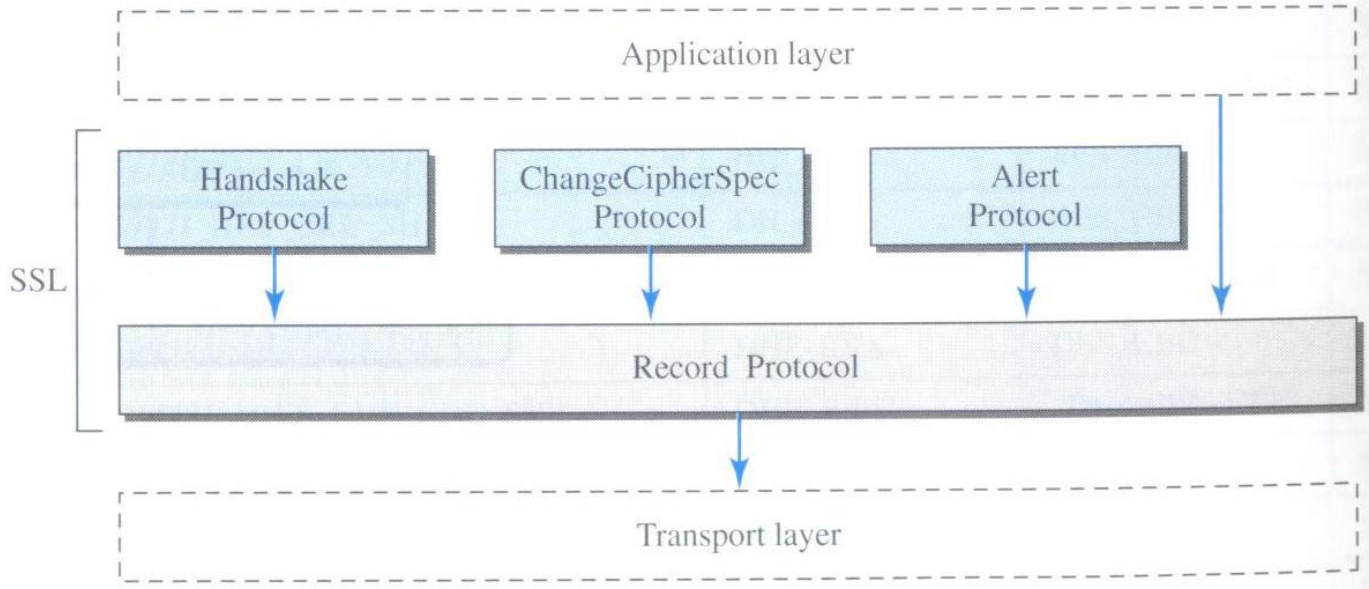
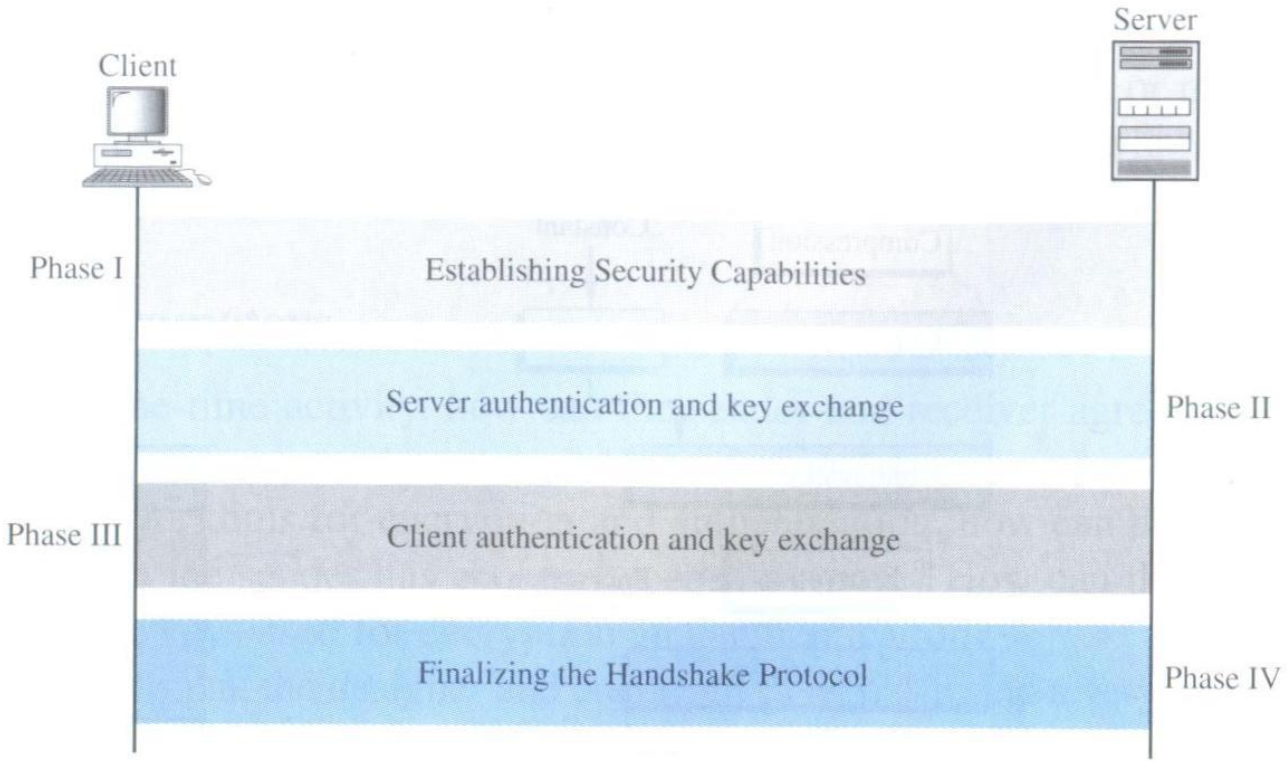


Table 32.3 *SSL cipher suite list*

Cipher Suite	*Key Exchange Algorithm*	*Encryption Algorithm*	*Hash Algorithm*
SSL_NULL_*WITH*_NULL_NULL	NULL	NULL	NULL
SSL_RSA_*WITH*_NULL_MD5	RSA	NULL	MD5
SSL_RSA_*WITH*_NULL_SHA	RSA	NULL	SHA
SSL_RSA_*WITH*_RC4_128_MD5	RSA	RC4_128	MD5
SSL_RSA_*WITH*_RC4_128_SHA	RSA	RC4_128	SHA
SSL_RSA_*WITH*_IDEA_CBC_SHA	RSA	IDEA_CBC	SHA
SSL_RSA_*WITH*_DES_CBC_SHA	RSA	DES_CBC	SHA
SSL_RSA_*WITH*_3DES_EDE_CBC_SHA	RSA	3DES_EDE_CBC	SHA
SSL_DH_anon_*WITH*_RC4_128_MD5	DH_anon	RC4_128	MD5
SSL_DH_anon_*WITH*_DES_CBC_SHA	DH_anon	DES_CBC	SHA
SSL_DH_anon_*WITH*_3DES_EDE_CBC_SHA	DH_anon	3DES_EDE_CBC	SHA
SSL_DHE_RSA_*WITH*_DES_CBC_SHA	DHE_RSA	DES_CBC	SHA
SSL_DHE_RSA_*WITH*_3DES_EDE_CBC_SHA	DHE_RSA	3DES_EDE_CBC	SHA
SSL_DHE_DSS_*WITH*_DES_CBC_SHA	DHE_DSS	DES_CBC	SHA
SSL_DHE_DSS_*WITH*_3DES_EDE_CBC_SHA	DHE_DSS	3DES_EDE_CBC	SHA
SSL_DH_RSA_*WITH*_DES_CBC_SHA	DH_RSA	DES_CBC	SHA
SSL_DH_RSA_*WITH*_3DES_EDE_CBC_SHA	DH_RSA	3DES_EDE_CBC	SHA
SSL_DH_DSS_ *WITH*_DES_CBC_SHA	DH_DSS	DES_CBC	SHA
SSL_DH_DSS_ *WITH*_3DES_EDE_CBC_SHA	DH_DSS	3DES_EDE_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_NULL_SHA	FORTEZZA_DMS	NULL	SHA
SSL_FORTEZZA_DMS_*WITH*_FORTEZZA_CBC_SHA	FORTEZZA_DMS	FORTEZZA_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_RC4_128_SHA	FORTEZZA_DMS	RC4_128	SHA

Protocolo Handshake

Figure 32.17 *Handshake Protocol*



TLS

- Transport Layer Security (TLS) es la versión SSL standard de la IETF.
- Es muy similar a SSL, pero con unas pequeñas diferencias.

Pretty Good Privacy - PGP

PGP

- Aplicación para encriptación y desencriptación de datos creada por Phil Zimmermann.
- El formato de mensaje utilizado por PGP es estandarizado (RFC 4880), de tal manera que se posibilita la interoperabilidad entre diferentes programas.
- Nosotros usaremos GnuPG

Generando una clave

- gpg --gen-key
- Cada usuario tiene un (o más) par de llaves, que consisten en una una llave privada y una pública.
  - La llave privada puede ser encriptada usando una ***passphrase***
  - Todas las llaves son almacenadas en un ***keyring***
- Este comando genera un nuevo par de llaves y los almacena en el *keyring*

Publicando la llave pública

- gpg -- export -a c.mera

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (Darwin)
mQGiBE00488RBAC3hea3pPqaJ9RL4vwJgE1cF2v4OKNbNXkAuvGg+tjEzv2NvyiN
g2gmhQDnxCxxTy0h7o26Lu0fYcKtuj+Wif4KpbsV/Aeh6nGRC/JWhWczfAKWt5N7
Hn4fNpiAgqjgsJzWNLUPzmOkPPi1oZoeGicSjqGMU1vLSG6Ce4Xg/Y83qwCggGoQ
U/b8mCswq9lrXegjasvwHWkEAJY/EGb5zpRG4/mwy3BJDtEHEf4eI9aJB1wOLVxq
oZgR1tKwba7eoQCPAZ+oTvo+/H78DKPZBS8dITEqMWSsyhyPHgV9QPV1kbepHhkg
8zcQoBA3JRrOSqL5EnGbguU/XpGhrPTgkH4q5AzNRiRDCCp3SyzrSul30IwdB5fj
oKadA/9Lxr6+EkkIyP7SnIOT3Sa/DPIb/EEe6khhrscskHI8MuHUQwYM+n01foP6
. . .
ZtmDLsvb5uxs3sFxVEneJ7xMm0NOOQn00euWPDCBIG7xDzo/HmkHDff3GxZKSvws
epcEZyHqOtiDA34fbVyw1quuuL60AMdiCgSISQQYEQIACQUCTTTjzwIbDAAKCRD6
9q1BZidnIXwlAJ4zsnLMlSyqxhCnifkTvbwtLxwlNACfR0/jt4ZTIWAdVwwQMghc
Uv6Fbc0=
=jAEI
-----END PGP PUBLIC KEY BLOCK-----
```

- La llave pública puede ser subida a su website o a un keyserver, tal como pgp.mit.edu

Encriptando un mensaje

- gpg -e secreto.txt c.mera
- Encripta el archivo secreto.txt de tal manera que el receptor c.mera puede recuperar el contenido plano del texto.
- En la práctica, una llave de sesión es generada de forma aleatoria y es utilizada para encriptar simétricamente el archivo.
- La llave de sesión es encriptada con la llave pública del receptor(es) y se adjunta al archivo

Desencriptando un mensaje

- gpg -d secreto.gpg

Firmando un mensaje

- gpg -s -a secreto.txt
- Genera una firma para el archivo dado (en formato ASCII) usando la llave privada del usuario
- La firma puede ser verificada utilizando la llave pública del firmante:
  - gpg --verify secreto.asc

```
gpg: Signature made Tue Jan 18 01:07:10 2011 GMT using
DSA key ID 66276721
gpg: Good signature from "Carlos Mera
<c.mera@cs.bham.ac.uk"
```

Otras operaciones comunes

- Generando una firma separada
- Firmando y encriptando un mensaje
- Web of Trust: firmar una llave pública
- Revocar una llave

Puntos para recordar

- Comando de PGP
- Conceptos de SSL

Próxima Sesión

- Seguridad operativa:
  - firewalls,
  - IDSs y
  - DMZs