Cómo mejoras la seguridad en FTP

Cómo mejoras la seguridad en FTP

El principal problema es que el protocolo FTP usa para comunicarse texto plano. La solución pasa por **encriptar**.

Tenemos dos posibles soluciones actualmente al alcance:

- FTPS
- SFTP

FTPS

Es una extensión de FTP que añade soporte para TLS (Transport Layer Security), es decir, añade una capa por debajo para cifrar las transmisiones.

Publicado en 1997. Definido en el ***RFC4217 Securing FTP with TLS*** y que usa también las extensiones de seguridad añadidas en el RFC2228.

FTPS usa criptografía híbrida. También utiliza certificados X.509

Al ser una extensión de FTP permite usar todos sus comandos. Es más sencillo de implementar.

SFTP

SFTP (Secure File Transfer Protocol), a veces conocido como *SSH File Transfer Protocol* es un protocolo para la transferencia de ficheros de forma segura. Es una extensión de SSH para la transferencia de ficheros.

El protocolo asume que funciona sobre un canal seguro cómo es SSH. Actualmente van por la versión 6 (2006).

Sólo usa un canal de comunicación, y solo envía y recibe los mensajes en binario.

SFTP es más avanzado que FTPS aunque a veces la facilidad de implementación de FTPS y la compatibilidad hacia FTP hace que se use más FTPS.

Comparación

	FTP	FTPS	SFTP
Puerto	21	21	22
Método encriptación	No usa	Certificado	Infraestructura de clave pública (PKI)
Método transferencia	Transferencia directa	Transferencia directa	Túnel