IFCT0109. SEGURIDAD INFORMÁTICA

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

RESUMEN FINAL

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA
3. TEORÍA DE LA INFORMACIÓN
4. PROPIEDADES DE LA SEGURIDAD QUE SE PUEDEN CONTROLAR MEDIANTE LA APLICACIÓN DE LA CRIPTOGRAFÍA: CONFIDENCIALIDAD, INTEGRIDAD, AUTENTICIDAD, NO REPUDIO, IMPUTABILIDAD Y SELLADO DE TIEMPOS
5. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA Y DE CLAVE PÚBLICA
6. CARACTERÍSTICAS Y ATRIBUTOS DE LOS CERTIFICADOS DIGITALES
7. IDENTIFICACIÓN Y DESCRIPCIÓN DEL FUNCIONAMIENTO DE LOS PROTOCOLOS DE INTERCAMBIO DE CLAVES USADOS MÁS FRECUENTEMENTE
8. ALGORITMOS CRIPTOGRÁFICOS MÁS FRECUENTEMENTE UTILIZADOS
9. ELEMENTOS DE LOS CERTIFICADOS DIGITALES, LOS FORMATOS COMÚNMENTE ACEPTADOS Y SU UTILIZACIÓN
10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN Y LOS CRITERIOS PARA SU UTILIZACIÓN
11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 6/2020, DE 11 DE NOVIEMBRE, REGULADORA DE DETERMINADOS ASPECTOS DE LOS SERVICIOS ELECTRÓNICOS DE CONFIANZA
12. ELEMENTOS FUNDAMENTALES DE LA FIRMA DIGITAL, LOS DISTINTOS TIPOS DE FIRMA Y LOS CRITERIOS PARA SU UTILIZACIÓN
13. CRITERIOS PARA LA UTILIZACIÓN DE TÉCNICAS DE CIFRADO DE FLUJO Y DE BLOQUE
14. PROTOCOLOS DE INTERCAMBIO DE CLAVES

RESUMEN

LA CRIPTOGRAFÍA ES UNA DISCIPLINA TÉCNICA FUERTEMENTE RELACIONADA CON LA PROTECCIÓN DE LA INFORMACIÓN. A LO LARGO DE LA HISTORIA HA SUFRIDO UNA EXTRAORDINARIA EVOLUCIÓN.

LOS SISTEMAS DE CRIPTOGRAFÍA CLÁSICOS SE PUEDEN DIVIDIR EN **SISTEMAS MONOALFABÉTICOS**, COMO EL DE CÉSAR, O LOS **POLIALFABÉTICOS**, COMO EL DE VIGÈNERE.

TODOS ELLOS COMPARTÍAN LA MISMA PROPIEDAD: **LA CLAVE DE CIFRADO ERA LA MISMA QUE LA DE DESCIFRADO**. POR ELLO, SE CONOCÍAN COMO **SISTEMAS DE CLAVE SECRETA O SIMÉTRICA.**

RESUMEN

FUE EN 1976 CUANDO SURGIÓ LA **CRIPTOGRAFÍA DE CLAVE PÚBLICA O ASIMÉTRICA**, PASANDO **A UTILIZARSE UN PAR DE CLAVES: UNA PÚBLICA Y UNA PRIVADA.**

LA CRIPTOGRAFÍA PERMITE SATISFACER UNAS PROPIEDADES DE SEGURIDAD U OTRAS.

LA ELECCIÓN SE REALIZA EN BASE A LOS USUARIOS QUE ESTÁN IMPLICADOS EN LA COMUNICACIÓN (**AUTENTICIDAD**), LA PREVENCIÓN DE ACCESOS NO AUTORIZADOS (**CONFIDENCIALIDAD**), LA PREVENCIÓN DE MODIFICACIONES DEL MENSAJE (**INTEGRIDAD**), LA PREVENCIÓN DE ENVÍOS NO DESEADOS (**NO REPUDIO**), EL SEGUIMIENTO DE LAS ACCIONES REALIZADAS (**IMPUTABILIDAD**) Y EL CONOCIMIENTO DE LA FECHA EN LA QUE SE PRODUCE LA COMUNICACIÓN (**SELLADO DE TIEMPO**).

RESUMEN

LA SATISFACCIÓN DE LAS PROPIEDADES DE SEGURIDAD DEPENDE DE LA APLICACIÓN DE NUMEROSOS MECANISMOS, COMO SON **EL CIFRADO, LA FIRMA O LA CREACIÓN DE RESÚMENES**.

LA **CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA** PROPORCIONAN LAS HERRAMIENTAS FUNDAMENTALES PARA APLICAR LOS MECANISMOS ANTERIORES, SIENDO IMPRESCINDIBLE ESCOGER LA MÁS APROPIADA EN CADA CASO.

LA **CRIPTOGRAFÍA SIMÉTRICA** SE CARACTERIZA POR SU **RAPIDEZ**, MIENTRAS QUE LA **ASIMÉTRICA** PRESENTA LA VENTAJA DE **NO NECESITAR UN CANAL SEGURO** PARA INTERCAMBIAR LAS CLAVES DE CIFRADO.

RESUMEN

ADEMÁS, DADO QUE EN AMBOS TIPOS DE CRIPTOGRAFÍA LOS USUARIOS TIENEN QUE INTERCAMBIAR CLAVES, EL PROTOCOLO A UTILIZAR HA DE CONSIDERARSE. HAY QUE ANALIZAR, ENTRE OTRAS COSAS, SI EL INTERCAMBIO SE REALIZA ENTRE EMISOR Y RECEPTOR O SI ES NECESARIA UNA ENTIDAD INTERMEDIA.

UNA CUESTIÓN ESPECIALMENTE RELACIONADA CON LOS SISTEMAS DE CLAVE PÚBLICA ES **ASEGURAR LA IDENTIDAD DE SU PROPIETARIO**. EN ESTE SENTIDO SURGEN LOS **CERTIFICADOS DE CLAVE PÚBLICA.**

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

RESUMEN

LAS **INFRAESTRUCTURAS DE CLAVE PÚBLICA** (**PKI**) CONSTITUYEN EL ELEMENTO FUNDAMENTAL QUE PERMITE QUE LOS CERTIFICADOS DIGITALES DE CLAVE PÚBLICA PUEDAN UTILIZARSE DE FORMA MASIVA EN INTERNET.

EN UNA **PKI** PARTICIPAN UNA O VARIAS AUTORIDADES DE CERTIFICACIÓN, RELACIONADAS EN FORMA DE JERARQUÍA O DE RED. PARA QUE LOS USUARIOS PUEDAN DISPONER Y UTILIZAR SUS CERTIFICADOS, ES NECESARIO SOLICITARLOS A TRAVÉS DE PETICIONES **CSR**.

RESUMEN

DOS ASPECTOS CLAVE EN LA GESTIÓN DE CERTIFICADOS SON:

- **LA VERIFICACIÓN** DEL MISMO (COMPROBANDO, ENTRE OTRAS CUESTIONES, LA VALIDEZ DE LA CADENA DE CERTIFICACIÓN)
- **LA REVOCACIÓN** (BIEN A TRAVÉS DE LISTAS **CRL** O UTILIZANDO EL PROTOCOLO **OCSP**).

ASOCIADAS A LAS **PKI** SURGEN LAS **PMI**, O **INFRAESTRUCTURAS DE GESTIÓN DE PRIVILEGIOS**. GRACIAS A ELLAS ES POSIBLE GESTIONAR LOS CERTIFICADOS DE ATRIBUTOS QUE PERMITEN ATESTIGUAR QUE EL PROPIETARIO PUEDE DISFRUTAR DE UN DETERMINADO DERECHO.

LOS CERTIFICADOS DE ATRIBUTOS SON A LOS PRIVILEGIOS LO QUE LOS CERTIFICADOS DE CLAVE PÚBLICA SON A LA IDENTIDAD.

CONTENIDOS

1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

7. RESUMEN

EL ESTABLECIMIENTO DE CANALES SEGUROS DE COMUNICACIÓN ES FUNDAMENTAL PARA EL INTERCAMBIO DE DATOS.

LAS **REDES PRIVADAS VIRTUALES** (**VPN**) Y **LOS TÚNELES DE CIFRADO** SON ELEMENTOS ESENCIALES.

GRACIAS A ELLOS ES POSIBLE ESTABLECER COMUNICACIONES SEGURAS ENTRE DOS ENTIDADES O USUARIOS, ELIMINANDO LA NECESIDAD DE TENER QUE ESTAR FÍSICAMENTE EN LA MISMA RED. Y NO SOLO ESO: PERMITEN CREAR UNA COMUNICACIÓN SEGURA UTILIZANDO UN CANAL INSEGURO, COMO PUEDE SER INTERNET.

7. RESUMEN

HAY MÚLTIPLES PROTOCOLOS QUE PERMITEN SU ESTABLECIMIENTO. ENTRE ELLOS CABE DESTACAR **IPSEC, SSL Y SSH.**

IPSEC ES UN PROTOCOLO QUE ACTÚA EN LA CAPA DE RED Y ESTÁ COMPUESTO ESENCIALMENTE DE LOS PROTOCOLOS DE **INTERNET KEY EXCHANGE** (**IKE**) Y **ENCAPSULATING SECURITY PAYLOAD** (**ESP**).

SSL ACTÚA EN UNA CAPA SUPERIOR, EN LA CAPA DE TRANSPORTE, Y SE COMPONE DE LOS PROTOCOLOS DE REGISTRO, SALUTACIÓN, CAMBIO DE ESPECIFICACIÓN DE CIFRADO Y AVISO.

TAMBIÉN EJECUTÁNDOSE EN LA CAPA DE TRANSPORTE, **SSH** ES UN PROTOCOLO DE AUTENTICACIÓN REMOTA COMPUESTO POR LOS PROTOCOLOS DE CAPA DE TRANSPORTE, AUTENTICACIÓN DE USUARIOS Y CONEXIÓN.

7. RESUMEN

FINALMENTE, CABE DESTACAR DOS DE LAS ALTERNATIVAS DE **VPN** MÁS EXTENDIDAS: **VPN SSL** Y **VPN IPSEC**.

LA ELECCIÓN ENTRE UNA U OTRA TECNOLOGÍA PARA IMPLEMENTAR UNA VPN DEBE PARTIR, NECESARIAMENTE, DEL ESTUDIO DETALLADO DEL CONTEXTO Y DE LAS NECESIDADES DE LOS USUARIOS.

LAS **VPN SSL** SON INTERESANTES PORQUE PASAN DESAPERCIBIDAS PARA LOS USUARIOS Y SE BASAN EN UTILIZAR EL NAVEGADOR WEB PARA ESTABLECER UNA COMUNICACIÓN ENTRE DOS EXTREMOS.

ACTIVIDADES

- ACTIVIDAD 01. CIFRADOS BÁSICOS
- ACTIVIDAD 02. CREACIÓN DE UN CONJUNTO DE RECOPILADORES DE DATOS
- ACTIVIDAD 03. INSTALACIÓN DE SISTEMA OPERATIVO WINDOWS SERVER 2019
- ACTIVIDAD 04. COMPRESIÓN DE ARCHIVOS
- ACTIVIDAD 05. DIRECTORIO ACTIVO, DHCP Y NAT EN WINDOWS SERVER
- ACTIVIDAD 06. CIFRADO CON AESCRYPT
- ACTIVIDAD 07. CIFRADO CON CRYPTOMATOR (E1)
- ACTIVIDAD 08. DIRECTIVAS DE GRUPO WINDOWS SERVER
- ACTIVIDAD 09. GENERAR CONTRASEÑAS SEGURAS

ACTIVIDADES

- ACTIVIDAD 10. CIFRADO CON BITLOCKER
- ACTIVIDAD 11. CIFRADO CON VERACRYPT
- ACTIVIDAD 12. CIFRADO CON GNUPG (E2)
- ACTIVIDAD 13. COMPARTIR CARPETAS EN WINDOWS SERVER
- ACTIVIDAD 14. USO DE FUNCIONES HASH
- ACTIVIDAD 15. USO DE CIFRADO Y HASH
- ACTIVIDAD 16. CIFRADO CON OPENSSL
- ACTIVIDAD 17. INFRAESTRUCTURA DE CLAVE PÚBLCA PKI
- ACTIVIDAD 18. FIRMA DIGITAL DE DOCUMENTOS
- ACTIVIDAD 19. INSTALAR SERVIDOR Y CLIENTE FTP
- ACTIVIDAD 20. INSTALAR SERVIDOR PROXY

ANEXOS

- CREACIÓN DE UN CONJUNTO DE RECOPILADORES DE DATOS EN WINDOWS
- PROTOCOLO DIFFIE-HELLMAN
- CONFIGURAR DIRECTORIO ACTIVO, DHCP Y NAT EN WINDOWS SERVER
- CIFRADO CON CRYPTOMATOR
- DIRECTIVAS DE GRUPO WINDOWS SERVER
- CIFRADO SIMÉTRICO CON GNUPG
- CIFRADO Y FIRMA CON PAR CLAVE PRIVADA-CLAVE PÚBLICA CON GNUPG
- CONEXIÓN REMOTA VÍA SSH
- USO DE CORREOS ELECTRÓNICOS CON CERTIFICADOS DIGITALES
- EL CIFRADO RSA

ANEXOS

- INSTALAR SERVIDOR PROXY
- INSTALAR SERVIDOR Y CLIENTE FTP
- USO DE VPN CON TUNNELBEAR Y PROTON VPN

ESTO ES TODO