Publicación quincenal editada por el Departamento de Telecomunicaciones y Telemática del Instituto Superior Politécnico José Antonio Echeverría
Auspiciada por el Ministerio de la Informática y las Comunicaciones

Año VII No. 19

ISSN: 1729-3804

Telem@tica

Enero 13, 2009
"Año del 50 aniversario del triunfo de la Revolución"

REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

FRASE DE LA SEMANA

"La debilidad de actitud se vuelve debilidad de carácter."
Albert Einstein

SUMARIO

Colectivo

Contáctenos

REVISTA TELEM@TICA
Departamento de Telemática
Facultad de Ingeniería Eléctrica

Instituto Superior Politécnico
José Antonio Echeverría

Calle 114, No. 11901, entre 119 y 127, Municipio Marianao, Habana,Cuba

Teléfono:
+53 (7) 2606279 / 2679880

Fax:
+53 (7) 2671576

Telematica@revistas.cujae.edu.cu

Sitio Web:
http://www.cujae.edu.cu/revistas/telematica

IR al SUMARIO

NOTA DEL EDITOR

Estimado lector:

El presente artículo aborda la implementación de la Public Key Infrastructure en redes institucionales, y en particular su aplicación como solución integral de seguridad en la Intranet de la UCLV. Aunque el proceso de investigación incluyó el estudio del estado del arte, los estándares, los productos de software y de hardware; se concentra en efectuar de forma práctica la instalación y puesta en marcha de la PKI dentro de un entorno académico en el MES. Se muestran la metodología diseñada y un análisis de esta que hace énfasis en los servicios y configuración. Son mencionados los escenarios típicos de empleo de certificados, aunque en el desarrollo de las actividades investigativas se probaron la mayoría de las aplicaciones de los certificados digitales. El estado actual del desarrollo de las redes, así como los requerimientos en materia de seguridad justifican este proyecto, cuya perspectiva va más allá de las redes universitarias.

Nos encontraremos nuevamente en el próximo número.

Los Editores.

TÉCNICAMENTE HABLANDO

Implementación: Poner en funcionamiento, aplicar métodos, medidas, etc., para llevar algo a cabo.

Metodología: Conjunto de métodos que siguen en una investigación.

PKI: (Public Key Infraestructura) Infraestructura de Clave Pública

Solución integral de seguridad: Se refiere a la protección de los recursos e información implicados con los servicios típicos en las redes de computadoras a través de la implementación de una infraestructura de seguridad que, como su nombre indica, sirva como sustrato de seguridad a todos los sistemas.

ARTÍCULO

Metodología para la Implementación de una infraestructura de llave pública en intranets

INTRODUCCIÓN

La Intranet de la Universidad Central “Marta Abreu” de Las Villas, como parte de la creciente red del Ministerio de Educación Superior, se ha desarrollado palpablemente a medida que adopta las nuevas tecnologías. Mucho se ha trabajado en materia de seguridad, más no existe un estudio sobre el tema de una infraestructura de seguridad aplicada a dicho entorno [1].

Un sustrato dominante constituye el soporte de base para una empresa; una infraestructura puede ser vista como tal [2]. El siguiente principio es fundamental: la infraestructura existe de forma que diversas entidades puedan conectarse y servirse de ella según sus necesidades y los puntos de acceso deben ser convenientemente uniformes.

Una infraestructura con propósitos de seguridad, debe sostener este mismo principio para proveer a la organización de un sustrato de seguridad que ha de ser accesible por todos los objetos y aplicaciones que necesiten ser protegidos; este es su objetivo principal. Su extensa definición abarca muchos puntos que incluyen consistencia de nombres, políticas de seguridad y su cumplimiento, monitoreo, auditoría, administración de los recursos, control de acceso a los dispositivos, etc. Su interfaz tiene que ser de fácil manipulación; el resultado de los servicios entregados debe ser predecible. La manera en que la infraestructura obtiene este resultado no necesita ser comprendida por el dispositivo que la usa [3].

En muchos entornos, constituye una buena parte de su arquitectura. Favorece la interoperabilidad, la manejabilidad y la consistencia a través de múltiples aplicaciones y plataformas de computación. Muchas facetas de la sociedad moderna demuestran que el esfuerzo empleado en su diseño e implementación vale la pena.

Una PKI es la base de una infraestructura de seguridad masivamente extendida cuyos servicios son implementados y se entregan con el empleo de los principios y técnicas de llaves públicas. Provee los componentes y servicios que permiten el despliegue y operación prácticos de un sistema que usa certificados. Debe lidiar con asuntos como la creación segura de pares de llaves y certificados, distribución de certificados con la información asociada, validación de identidades, validación, renovación y revocación de certificados, almacenamiento y recuperación seguros de las llaves, generación de firmas y estampillas de tiempo y realización y manejo de las relaciones de confianza. De la manera más precisa que puede ser definida es explorando lo anterior en términos de las consecuencias prácticas [2].

Necesidad de una Metodología General

Al generar la propuesta para la implementación de una infraestructura aplicada a un entorno, es muy importante trazar una estrategia que permita obtener resultados exitosos. Esto implica vencer los retos que se presentan en el diseño: estar a la altura de los requerimientos de la institución, lograr la completa interoperatividad e integración del diseño generado con las aplicaciones y servicios ya existentes, realizar un correcto planeamiento para su despliegue y una ejecución consecuente de las tareas, producir documentación para generar confianza, efectuar una correcta administración que afirme la fiabilidad del sistema y contemplar la posibilidad de una migración, o sea, la solución tiene que ser escalable [4]-[6].

Ing. Erisbel Orozco Crespo

Ingeniero en Telecomunicaciones y Electrónica, egresado de la Facultad de Ingeniería Eléctrica de la Universidad Central “Marta Abreu” de Las Villas. Actualmente profesor en dicha facultad y trabaja en el Departamento de Informatización y Comunicaciones, específicamente en el Grupo de Redes.

Erisbel@uclv.edu.cu

MSc. Ramón Torres Rojas

Ingeniero en Telecomunicaciones y Electrónica, egresado de la Facultad de Ingeniería Eléctrica de la Universidad Central “Marta Abreu” de Las Villas. Cursó estudios de Master en Telemática

Actualmente se desempeña como profesor e investigador en dicha facultad.

Rtorres@uclv.edu.cu

Para ello hay que asumir el siguiente punto de vista: la solución se entrega mediante métodos de ingeniería y la metodología general es fundamental para su correcto despliegue y operación.
El procedimiento que se empleará en el diseño de esta propuesta consta de los pasos siguientes: análisis de los requerimientos, diseño de la arquitectura, diseño de las operaciones, verificación, integración, despliegue y postdespliegue [1], [7].
En el análisis de los requerimientos se estudian los problemas actuales de la universidad y cuáles solucionar con la puesta en marcha de la infraestructura. Esto implica determinar las vulnerabilidades de los sistemas, el nivel apropiado de seguridad a alcanzar y qué legislaciones deben ser cumplidas. En el diseño de la arquitectura serán definidos los modelos de operación y de confianza, los componentes, su organización y su distribución en la Intranet. En el siguiente paso, se diseñan las operaciones y políticas para efectuar la instalación. Luego, esta se verifica para comprobar el correcto funcionamiento del sistema y más tarde se toman las últimas medidas de seguridad. En la integración se preparan los servicios, aplicaciones y componentes administrativas de la arquitectura. Finalmente, el despliegue, donde se pone en funcionamiento la PKI y el postdespliegue para las tareas de gestión y futuros estudios.

Análisis de los requerimientos de la Intranet UCLV

La Intranet UCLV cuenta con más de 2600 computadoras repartidas en 14 áreas entre las que se encuentran facultades, centros de investigación y administrativos. En general, está compuesta por dominios físicos Ethernet 100BASET interconectados en una Gigabit Ehternet por medio de un backbone de fibra óptica con topología estrella [1], [8].
El espacio de nombres de dominio asignado al bosque del Directorio Activo es UCLV.EDU.CU, del cual se derivan diferentes dominios de Windows 2003. Las aplicaciones más importantes como el correo electrónico, acceso a Internet y sistema de control docente, están ubicadas en dos nodos principales: en el Grupo de Redes y en La Puerta. Así se logra homogeneizar y centralizar la gestión de los sistemas y servicios más importantes, establecer relaciones de confianza entre los dominios y suministrar condiciones óptimas de respaldo eléctrico y hardware. Las cuentas de los usuarios también son administradas centralmente para mayor estabilidad. En el resto de los dominios se gestionan las cuentas locales de algunos usuarios y de los dispositivos particulares de cada dependencia; esto permite que cada uno aplique bajo ciertos términos su propia política de seguridad [1], [8].
Los dominios de la Intranet están todos construidos sobre Windows Server 2003 y la mayoría de los servicios fundamentales están totalmente implementados sobre estos sistemas operativos o bien, relacionados a ellos de alguna forma lo suficientemente importante. La inmensa mayoría de las computadoras personales también emplean los sistemas operativos de Microsoft.
Otros sistemas operativos presentes son los de la familia Linux como Debian, Ubuntu y Gentoo. Estos aparecen en su mayoría en servidores y dependencias investigativas.

Vulnerabilidades

La autentificación de los usuarios está basada en contraseñas. Aunque el mecanismo es práctico y la mayoría de los clientes negocian los protocolos de autentificación para elegir, de los que soportan, el más fuerte (casi siempre Kerberos), su seguridad puede cuestionarse debido a razones bien conocidas y a otras relacionadas con la presencia de clientes inferiores a Windows 2000 que emplean autentificación LM o NTLM. No existen otras formas de autentificación, de hecho, la presencia de certificados es casi nula [8].
Los dispositivos capa 3 son administrados en su mayoría mediante Telnet o una interfaz web. Esto resulta aún más riesgoso si se tiene en cuenta que la autentificación con ellos es básica y toda la comunicación viaja en texto plano.
No existen mecanismos por parte de la institución que usen las prestaciones de la criptografía relacionadas con el cifrado y la firma digital para proteger los sistemas de archivos, el correo electrónico y las relaciones de confianza entre los usuarios de la Intranet; tampoco una infraestructura propiamente dicha que brinde múltiples servicios de seguridad, actúe como móvil para soluciones más fiables y sirva para sostener un modelo de confianza mucho más robusto.

IR al SUMARIO

Legislaciones

Para la ejecución de la propuesta, habrá que cumplir con lo estipulado legalmente en cuanto a la autorización por parte del Ministerio de Interior como órgano regulador de este tipo de actividades. Según el Decreto-Ley Nº 199 Sobre la Seguridad y Protección de la Información Oficial en el Artículo 39, Capítulo VI, corresponde al Ministerio del Interior autorizar el diseño, producción y comercialización de sistemas de protección criptográfica y prestación de estos servicios a órganos, organismos y entidades estatales [9].

Diseño de la Arquitectura

El modelo de confianza de una jerarquía de autoridades de certificación se ajusta muy bien al esquema de la Intranet [10]-[12]. Una jerarquía de un solo nivel es recomendada para organizaciones pequeñas que solo requieren de los servicios fundamentales de la PKI. Típicamente, estas organizaciones manejan menos de 300 cuentas de usuarios. En lugar de múltiples CAs, una sola autoridad raíz es instalada como miembro del dominio. Si se tienen en cuenta las características de la Intranet UCLV, no es el diseño más apropiado.
Una jerarquía de dos niveles está compuesta por una CA raíz y una o más CAs que combinan roles de autoridades de políticas y emisoras de certificados. Para mejorar la seguridad la CA raíz es autónoma, es decir, está fuera del dominio, lo cual permite que permanezca sin conexión y retirada de la red para otorgarle protección física adicional. Este diseño se acerca más a los requerimientos, pero aún no es el más apropiado porque no delimita un nivel para políticas globales.
La jerarquía de tres niveles provee la mayor flexibilidad. Está compuesta por una CA raíz autónoma y sin conexión; una o más autoridades intermedias de políticas, autónomas y sin conexión y por una o más CAs emisoras de certificados subordinadas que deben pertenecer al dominio. Es recomendada para los siguientes escenarios: las políticas de seguridad estipulan fuerte protección física de la jerarquía, son requeridas dos o más políticas para la emisión de certificados y la gestión de la jerarquía de CAs es dividida entre equipos diferentes de administradores de red [13].
Analizados estos escenarios, se concluye que el diseño de una jerarquía de tres niveles es el que más se ajusta a las características y necesidades de la Intranet UCLV.
La organización y el número de CAs en la jerarquía dependen de la cantidad de certificados a emitir, el modelo administrativo, la estructura de la universidad y el número de categorías diferentes de usuarios y servicios de la Intranet. No tiene mucho sentido tener una autoridad de certificación por dependencia; en su lugar, se ajusta mejor el esquema de una o más autoridades de certificación por servicio. De esta manera, se puede dividir la administración entre equipos y centralizar todos los servicios de certificados al igual que los demás de la universidad [1]. El diseño de arquitectura de esta propuesta se refleja en la figura 1.

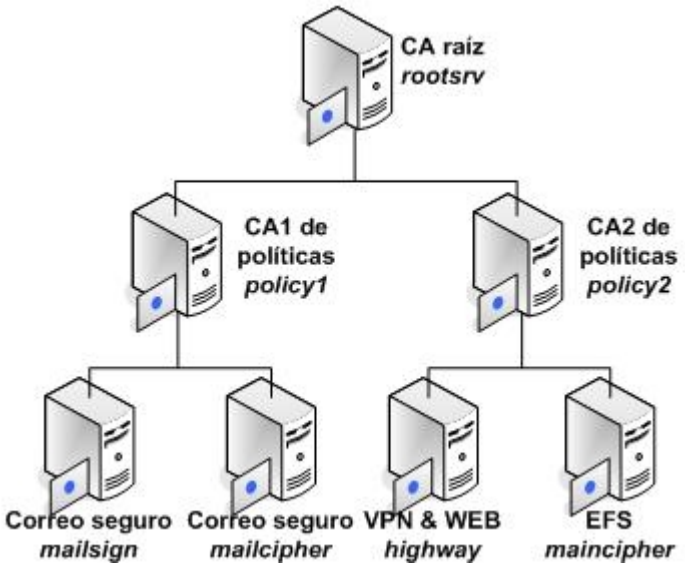

Fig. 1. Arquitectura de tres niveles seleccionada para la Intranet UCLV.

IR al SUMARIO

Solución con Windows Server 2003

Uno de los enfoques que mejor permiten lograr interoperatividad y máxima integración, consiste en centrarse en la familia de productos de un solo fabricante, en nuestro caso, Microsoft. A pesar de la existencia de múltiples soluciones de software para PKI, los servicios de certificados de Microsoft permiten desplegar soluciones integrales con grandes prestaciones para entornos organizacionales, si se realizan el diseño y la implementación de forma adecuada [7], [13].

Preparación del Directorio Activo

La PKI con Windows Server 2003, no requiere que todos los controladores de dominio de la Intranet sean escalados hacia esta versión del sistema operativo. Además, no necesita niveles de funcionamiento en específico de los bosques de dominio. Por tanto, la infraestructura puede ser creada de un modo mixto con entornos de Directorio Activo Windows 2000, para lo cual habrá que efectuar preparaciones iniciales. Como ya no existen estos tipos de dominio en la Intranet, la propuesta solo abarca la preparación del Directorio Activo del 2003.
La única modificación a efectuar concierne a los grupos de publicadores de certificados. Para que una CA emisora expida certificados a cualquier objeto del bosque de dominio, su cuenta debe ser añadida a este grupo en cada dominio de la Intranet [13].

Instalación de la jerarquía de CAs

La instalación de la jerarquía se realiza desde la autoridad raíz hacia abajo. Se propone el diseño de operaciones siguiente: preparación de los scripts de configuración antes de la instalación, instalación de la CA raíz autónoma, instalación de las CAs de políticas sin conexión, instalación de las CAs emisoras en línea y verificación de la instalación.
El archivo más importante para efectuar la instalación es el CAPolicy.inf. No aparece por defecto con la instalación del Windows Server 2003 y es la única manera de definir configuraciones específicas como la implementación vacía de extensiones Certificate Distribution Point y Authority Information Access en el certificado de la CA raíz [14], [15].
Después que este archivo se coloca en el directorio %windir% del sistema operativo se procede a la instalación de los servicios de certificados. Las computadoras a instalar deben tener al menos dos particiones, una para el sistema operativo y otra para la base de datos y de eventos de la CA. Además, sus credenciales; o sea, el nombre y el grupo de trabajo o dominio no pueden ser cambiados después de la instalación, por lo que deben ser chequeados previamente [1], [13].

Verificación

La verificación es fundamental pues garantiza que los URLs de AIA y CDP estén operativos antes de emitir los certificados. Si existen errores, los mecanismos en cadena fallarán cuando intenten descargarlos desde estas locaciones; lo mismo sucede con las Certificate Revocation Lists. No se puede regresar atrás y editar los certificados emitidos [16], [17].
La herramienta PKI Health Tool (pkiwiew.msc) incluida en Windows Server 2003 Resource Kit evalúa cada URL incluido en las extensiones de AIA y CDP de los certificados en la jerarquía. Su principio es conectarse a cada uno de ellos para reportar si los certificados y CRLs son alcanzables y si están cerca de la fecha de expiración. Tiene que ser ejecutada en un servidor miembro del dominio [13].

Medidas de seguridad

La jerarquía de certificación será tan segura como las medidas de configuración y protección física que se tomen. El plan de seguridad debe incluirlas para no permitir el comprometimiento de las llaves privadas [8].
Las medidas para proteger las llaves privadas dependen de la forma en que estas son almacenadas [18]. En el caso de Windows Server 2003 existen 3 posibilidades: en el sistema de archivos local de la máquina, en un dispositivo bifactor como Smart Cards o en un Hardware Security Module [13].
La única manera de proteger la llave almacenada localmente es restringir los usuarios de los grupos de administradores en la CA, pues tienen acceso completo a ella. Para facilitar la administración segura de los servicios de certificación, Microsoft Windows 2003 soporta la separación de roles por criterio común o Comon Criteria Roles. Esto implica que ninguna persona tenga el control completo de la PKI. Los roles implementados en estos sistemas son: Administrador de CA, Manejador de Certificados, Auditor y Operador de Salvas.

IR al SUMARIO

Es muy importante definir plantillas de seguridad para las CAs. Estas plantillas se construyen por medio de la consola Microsoft Management Console Security Templates que aporta el paquete de herramientas Windows Server 2003 Resource Kit.
En el marco de las configuraciones de las plantillas hay que definir los servicios innecesarios. Una CA solo debe funcionar como CA; no es seguro permitir en la misma computadora otros roles.
Se deben especificar los miembros de los grupos de administradores de la CA. Los permisos de administración de auditorías tienen que ser asignados al Auditor y los relacionados con las salvas, recuperación de archivos y directorios tienen que asignarse al Operador de Salvas. Solo se debe permitir el inicio de sesiones locales y remotas a los portadores de los roles por criterio común. Habilitar la separación de roles se logra mediante el comando:
certutil setreg CA\RoleSeparationEnabled 1
La configuración de auditorías abordada en el diseño de las operaciones con la especificación del filtro 172 en el comando certutil -setreg CA\AuditFilter 172 asegura que el log contenga todos los eventos relacionados con la operación de los servicios de certificados.
Es recomendable no permitir la administración a través de los Terminal Services, por lo que la opción de conectarse por escritorio remoto o Remote Desktop Protocol tiene que estar desmarcada. Otras variantes son deshabilitar este servicio y añadir al grupo Everyone el permiso de Deny Logon Through Terminal Services en las políticas de seguridad local o en una plantilla para las Políticas de Grupo aplicada a la cuenta de la CA en el Directorio Activo.
Las medidas de seguridad física que se proponen son: ubicar las autoridades de certificación sin conexión en un local con seguridad razonable, deshabilitar el hardware de las CAs a través de las utilidades de configuración de sus BIOS y establecer contraseñas para acceder a estas.

Recuperación ante desastres

Es preciso diseñar algún mecanismo para salvas de seguridad, automáticas o manuales. Las automáticas se prefieren para facilitar el trabajo de los administradores y garantizar que son aplicadas uniformemente en todas las autoridades de certificación.
A través de la utilidad System State Backups que forma parte de las herramientas del sistema se puede realizar esta operación de forma manual, al igual que con la MMC de los servicios de certificados. La forma automática se da mediante la configuración de una tarea programada con el script:
net start certsvc
certutil backup D:\CABackup
El script presupone la existencia del camino D:\CABackup. Con la ejecución del comando de certutil se pide una contraseña para proteger el archivo con formato PKCS #12 [19] que se forma para almacenar el par de llaves. Si solo se quiere hacer salva de la base de datos o de la llave se puede ejecutar certutil backupdb D:\CABackup o certutil backupkey D:\CABackup indistintamente.

Integración de los servicios y aplicaciones

La petición de un certificado está dada por un conjunto de acciones donde se genera la petición y en la autoridad de certificación que emite el certificado [1]. El diagrama de la figura 2 muestra el proceso genérico que ocurre con los servicios de certificados y sistemas operativos de Microsoft.
Pueden implementarse varios métodos para el despliegue de certificados manuales o automáticos. A través de las páginas web de los servicios de certificados, los usuarios pueden efectuar de forma manual las peticiones de certificados aplicados a ellos o a computadoras. Para que los navegadores tengan acceso a dichas páginas, el servidor web Internet Information Server tiene que estar en el mismo bosque que la CA (casi siempre en la propia CA) y la computadora debe ser confiable para la delegación de roles. Desde la MMC, a través del Certificate Request Wizard, se puede efectuar también la petición manual mediante los pasos apropiados [13]. La tabla I muestra los métodos disponibles con las plantillas de certificados versiones 1 y 2 [14], [15] para los sistemas operativos más comunes de la Intranet.

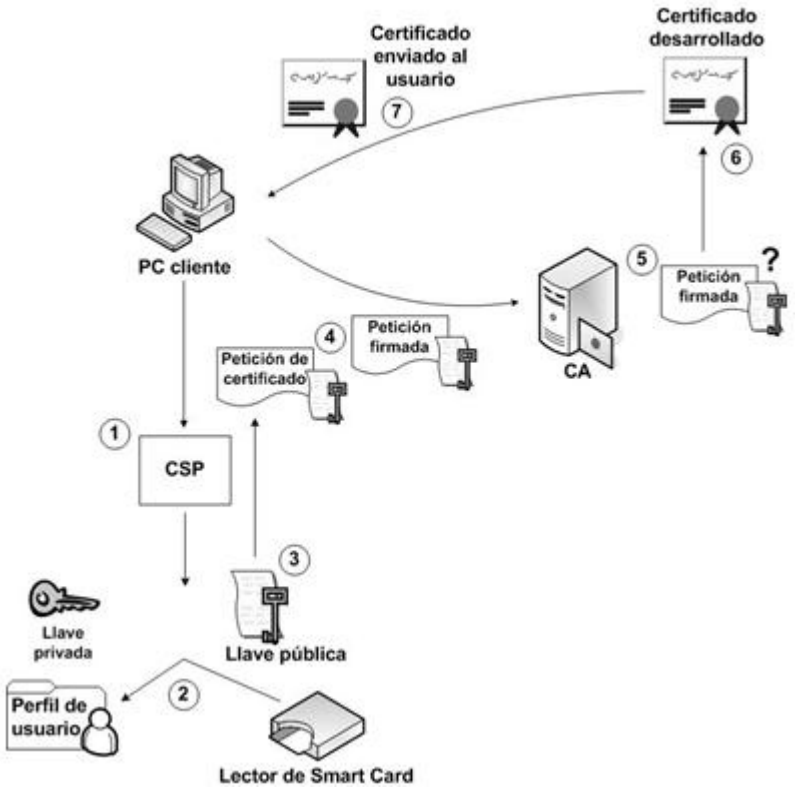

Fig. 2. Proceso de despliegue de certificados.

TABLA I
Métodos de despliegue manual

Despliegue manual	MMC	Despliegue web
Windows 2000	V1: Sí V2: No	V1: Sí V2: Sí
Windows XP o 2003	V1: Sí V2: Sí	V1: Sí V2: Sí

Como se muestra en la tabla II, los métodos automáticos mediante las políticas de grupo Automatic Certificate Request Settings y Autoenrollment Settings, son empleados para el despliegue de certificados de las plantillas versión 1 y 2 respectivamente. En ambos casos, las cuentas de las computadoras y de usuarios tienen que pertenecer a la Organizational Unit para la cual fueron definidas estas políticas de grupo. En el primero, las cuentas deben tener habilitados los permisos Read y Enroll y en el segundo el de Autoenrollment con los dos anteriores. Otro método alternativo utiliza scripts, sobre todo cuando se trata de automatizar el despliegue de certificados para usuarios de Windows 2000. El Simple Certificate Enrollment Protocol permite que los dispositivos como los de Cisco con sistema operativo IOS (Cisco Internetwork Operating System) obtengan automáticamente certificados de las Cas.

IR al SUMARIO

TABLA II
Métodos de despliegue automático

Despliegue automático	ACRS	*Autoenrollment Settings*	*Scripts*
Certificados a computadoras	V1: Sí V2: No	V1: No V2: Sí	V1: Sí V2: Sí
Certificados a usuarios	V1: No V2: No	V1: No V2: Sí	V1: Sí V2: Sí
Renovación automática de certificados	V1: Sí V2: No	V1: No V2: Sí	V1: Sí V2: Sí

Correo seguro

Dos métodos diferentes pueden ser implementados para asegurar el correo electrónico. El primero es proteger el contenido de los mensajes con Secure / Multipurpose Internet Mail Extensions [20] y el segundo, dar seguridad a los datos mientras son transmitidos entre el cliente y el servidor de correo mediante la implementación de Secure Socket Layer/Transport Layer Security [21]. S/MIME provee servicios de cifrado y firmas digitales para la entrega de correos. SSL puede aplicarse a cualquiera de los protocolos POP3, IMAP4, SMTP y NNTP soportados por Microsoft Exchange Server 2003 para lo cual dicho servidor usará los puertos SSL en lugar de los estándares [13].

Para habilitar SSL en el servidor de correo tiene que instalarse un certificado que incluya el Object ID de Server Authentication Enhanced Key Usage en la extensión Enhanced Key Usage, muy similar a un certificado web. Después de instalado, se debe habilitar la función en el servidor Exchange dentro del cuadro de diálogo de Virtual Server Properties correspondiente al protocolo en cuestión [1], [13].

Con Outlook Web Access la conexión al servidor Exchange se realiza por medio de Active Server Pages, lo que brinda a los usuarios la capacidad de acceder completamente a su perfil de correo y la habilidad de usar S/MIME. Debido a los riegos asociados a archivar llaves de certificados S/MIME que pueden utilizarse en firmas digitales, es recomendable separar estas de las que se emplean para el cifrado. Así se garantiza que solo la llave privada asociada al cifrado sea almacenada. Es recomendable crear los certificados por medio de plantillas; los de firmas digitales a partir de la plantilla Exchange Signature Only y los de cifrado de Exchange User [1], [13].

Acceso seguro a sitios web

Dos tipos de certificados SSL aparecen en la comunicación entre el navegador y el sitio web: el del servidor web y el del cliente. El primero es obligatorio para la implementación de SSL en el servidor, no así el segundo; sin embargo, con su empleo, aumenta la seguridad de las credenciales de los usuarios a través de autentificación basada en certificados [22]. La plantilla Web Server se ajusta bien a las necesidades, aunque puede considerarse la creación de otra de versión 2 para explotar otras capacidades [13].

Los certificados para IIS pueden emitirse por CAs del dominio y fuera del dominio. En principio la petición ocurre de igual manera pero la instalación de los certificados es diferente.

Además del cifrado con SSL, los servidores web podrán implementar autentificación basada en certificados. En lugar de conectarse anónimamente a los sitios, los usuarios emplearán certificados con el OID de Server Authentication Enhanced Key Usage en la extensión Enhanced Key Usage. Para efectuar este proceso los certificados realizan mapeos. Sin importar el tipo de mapeo que se utilice, los usuarios deben tener acceso a sus llaves privadas para probar su identidad [1], [13].

IR al SUMARIO

CONCLUSIONES

EA pesar de que quedó reflejado el empleo de los servicios de certificados de Microsoft, se probaron satisfactoriamente las mismas funciones con productos de software libre y otros de RSA Laboratories.
No fue posible exponer en este artículo todas las posibilidades de la PKI en cuanto a los servicios debido a su extensión, en su lugar solo se mencionaron las más comunes y más interesantes. Resulta inoperante implementar una PKI que no emplee sus soluciones para Virtual Private Network, almacenamiento de llaves de cifrado, cifrado en los sistemas de archivo, etcétera.
La puesta en práctica de la metodología es válida de forma general para cualquier entorno. Es muy importante introducir los niveles de seguridad que se logran con el empleo de estos sistemas en la medida que se introducen las nuevas tecnologías y se informatiza nuestra sociedad [8], [23].

Agradecimientos

Nos complace agradecer a nuestros amigos Ana Laura Suárez Rivero, Erik Orozco Crespo y a los colegas del "Laboratorio de Redes 224" de la Facultas de Ingeniería Eléctrica de la UCLV.

Referencias

[1] E. O. Crespo, "Propuesta para la implementación de una infraestructura de Llave Pública en la Intranet UCLV," Departamento de Telecomunicaciones y Electrónica, UCLV, Sta. Clara, 2008.
[2] C. Adams, and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition*. Boston: Addison Wesley, 2002.
[3] H. Myrvang, "An Infrastructure for Authentication, Authorization and Delegation," Department of Computer Science, University of Tromsø, 2000.
[4] T. Straub, "Usability Challenges of PKI," Ph.D. dissertation, Fachbereich Informatik, Technischen Universität, Darmstadt, 2005.
[5] A. J. Slagell, and R. Bonilla, "PKI Scalability Issues," 2005.
[6] A. J. Slagell, R. Bonilla, and W. Yurcik, "A Survey of PKI Components and Scalability Issues," in *IEEE International Performance, Computing, and Communications Conference (IPCCC'06)*, Phoenix, 2006, pp. 10.
[7] R. Housley, and T. Polk, *Planning for PKI: best practices guide for deploying public key infrastructure*. New York: Wiley, 2001.
[8] R. T. Rojas, "Seguridad en Redes de Mediana y Pequeña Empresa," Departamento de Telecomunicaciones y Electrónica, UCLV, Sta. Clara, 2004.
[9] F. C. Ruz. (2008, Septiembre, 10) **Decreto-Ley Nº 199 Sobre la Seguridad y Protección de la Información Oficial. *Gaceta Oficial de la República de Cuba* [En línea]. Disponible en: http://www.informatica-juridica.com/anexos/anexo432.asp**
[10] R. Perlman, "An overview of PKI trust models," *Network, IEEE*, vol. 13, pp. 38-43, 1999.
[11] G. Kambourakis, D. P. N. Kontoni, A. Rouskas, and S. Gritzalis, "A PKI approach for deploying modern secure distributed e-learning and m-learning environments," *Computers & Education*, vol. 48, pp. 1-16, 2007.
[12] C. Satizábal, R. Páez, and J. Forné, "PKI Trust Relationships: from a Hybrid Architecture to a Hierarchical Model," in *The First International Conference on Availability, Reliability and Security (ARES 2006)*, **Fukuoka**, 2006, pp. 563-570.
[13] B. Komar, and M. Team, *Microsoft Windows Server 2003 PKI and Certificate Security*. Redmond, Washington: Microsoft Press, 2004.
[14] *El directorio: Marcos para certificados de claves públicas y atributos*. Estándar ITU X.509. 2008.

IR al SUMARIO

[15] R. Housley, W. Polk, W. Ford, and D. Solo. (2008, Septiembre, 10) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280) [En línea]. Disponible en: http://www.ietf.org/rfc/rfc3280.txt
[16] M. Zhao, and S. W. Smith, “Modeling and Evaluation of Certification Path Discovery in the Emerging Global PKI,” Lecture Notes in Computer Science, vol. 4043, pp. 16-30, 2006.
[17] E. Ball, D. Chadwick, and A. Basden, “The Implementation of a System for Evaluating Trust in a PKI Environment,” Trust in the Network Economy, vol. 2, pp. 263-269, 2003.
[18] Y. Lee, J. Ahn, S. Kim, and D. Won, “A PKI System for Detecting the Exposure of a User's Secret Key,” Lecture Notes in Computer Science, vol. 4043, pp. 248-250, 2006.
[19]PKCS #12: Personal Information Exchange Syntax Standard. RSA Laboratories Public-Key Cryptography Standards. 1999.
[20] S. Santesson. (2008, Septiembre, 10) X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities (RFC 4262) [En línea]. Disponible en: http://www.ietf.org/rfc/rfc4262.txt
[21] T. Dierks, and E. Rescorla. (2008, Septiembre, 10) The Transport Layer Security (TLS) Protocol Version 1.1(RFC 4346) [En línea]. Disponible en: http://www.ietf.org/rfc/rfc4346.txt
[22] M. A. Piñón, and M. R. Camacho, “Implantación de Servicios de PKI en el Canal Web de Internet del Banco de España,” Datamation: la revista española de Tecnología de la Información para Empresa, pp.56-60, 2007.
[23] A. Lioy, M. Marian, N. Moltchanova, and M. Pala, “PKI past, present and future,” International Journal of Information Security, vol. 5, pp. 18-29, 2006.

IR al SUMARIO

EVENTOS

Informática 2009

XIII CONVENCIÓN Y FERIA INTERNACIONAL

Estimados colegas:

Del 9 al 13 de febrero de 2009, La Habana acogerá la XIII edición de la Convención y Feria Internacional Informática 2009, que sesionará en el Palacio de Convenciones de La Habana y en el recinto ferial PABEXPO. ¨Las Tecnologías de la Información y las Comunicaciones como soporte para el desarrollo endógeno y la soberanía tecnológica de los pueblos¨, es el tema central que promoverá el evento, y es la fuente de la invitación a la discusión científico tecnológica, a la exposición de proyectos e iniciativas que promuevan los propósitos y acciones que emprenden los países para impulsar el uso de las TIC en el desarrollo de la sociedad.
Informática 2009 estimulará el intercambio entre profesionales, científicos, técnicos, empresarios, representantes gubernamentales, organismos internacionales y público en general, interesados en investigar, promover, analizar y conocer sobre el avance de las tecnologías de la información, las telecomunicaciones, la electrónica y la automática, así como sus aplicaciones actuales en los diversos sectores de la sociedad.
El Comité Organizador de INFORMÁTICA 2009 les reitera la invitación a presentar sus contribuciones profesionales y muestras comerciales con la garantía de que alcanzaremos los objetivos comunes en un clima de amistad y solidaridad.

Dr. Jorge Luis Perdomo Di-Lella
Presidente Ejecutivo del Comité Organizador
Viceministro de la Informática y las Comunicaciones

GDiVX Player VERSION Zenith 1.1

Por:

Ing. Julio Cesar Camps

Email: camps@tesla.cujae.edu.cu

Ficha Técnica	
Fecha:	Septiembre 21/2004
Nombre:	**GDiVX Player**
Propiedad:	Copyright (C) 1999-2003 Michael Saunders.
Versiones:	**GDiVX Player VERSION Zenith 1.1**
Tamaño:	873 KB
Plataformas	Windows 2000/XP/2003
Idiomas	Inglés
Clasificación	Downloads/windows/audio&video/media player
URL	http://www.divxity.com/
Descripción	Global Divx Player es basicamente un visualizador de ficheros de video, usado principalmente para ver archivos comprimidos con el codec DIVX, pero posee capacidades técnicas para visualizar casi cualquier formato de video.
Observaciones	Global Divx Player soporta los siguientes formatos de ficheros de video: • .asf • .wmv • .mpeg • .mpg • .dat • .avi • .rm
Calificación	Bueno, según opiniones y análisis @ @ @ @ (el ejecutable contiene anuncios)

Características

GDivX Zenith Player 1.1 incluye una interface simple de fullscreen, control mediante atajos de teclado, un wizard para la elección y activación de codecs, soporte para video en formato Real (.rm).

GDiVX Zenith surge a partir de una modificación total del GDIVX en un nuevo lenguaje, adquiriendo una mayor estabilidad y rapidez en la mayoría de las plataformas. Enunciamos a continuación alguna de sus características:

- posee un control de subtítulos avanzado.
- permite seleccionar los codecs desde el mismo player.
- usa MUCHO MENOS recursos del cpu que el Windows Media Player.
- soporta los estilos del Winamp.
- soporta las teclas de atajo del winamp (Z, X, C, V, B).
- control de saturación/hue.
- soporte para subtítulos (mpl2, sub).
- configuración se almacena en un fichero .ini en vez de en el registro de Windows.

Resumen

Global DiVX Player usa muchos menos recursos del CPU que el Media Player (y otros media y avi player), de forma que si los videos divx o avi se visualizan con saltos en tu computadora, o presentan problemas de sincronización, dale un vistazo al Global Divx. El no hará milagros, pero puede hacer la diferencia para aquellas cuyo hardware está en el borde del límite admisible (P2/K6/K6-2). Así que, por qué no?

IR al SUMARIO

SOFTWARE

Especulan que Google planea llevar Android al PC 07/01/2009

Entusiastas de la informática han logrado instalar en relativamente corto tiempo el sistema operativo Android en un aparato netbook. Esta situación ha desencadenado una serie de especulaciones en diversos foros especializados, sobre los planes del gigante de Internet, Google, para tal segmento. Hace pocas semanas se realizó una instalación similar en un aparato tablet Nokia N810.

Fuente: http://www.diarioti.com

SEGURIDAD

IBM lanza nuevos servicios de seguridad 05/01/2009

IBM anuncia un conjunto de iniciativas para ampliar sus soluciones de seguridad y ayudar a los clientes a ahorrar costes.Estos servicios ayudan a definir usuarios y gestionar quién tiene acceso a datos y aplicaciones sensibles. Según el informe trimestral del equipo de investigación de IBM ISS, publicado a principios de diciembre, más del 42 % de las vulnerabilidades están causadas por fallos en la gestión de accesos e identidades.

Fuente: http://www.diarioti.com

IR al SUMARIO

HARDWARE

Recomiendan no gritarle al disco duro 05/01/2009

Brendan Gregg, uno de los técnicos de parque de servidores de Fishworks, subsidiaria de Sun, sintió incredulidad al ver que un fuerte grito dirigido directamente al rack de servidores incidía inmediatamente en el comportamiento del disco duro."Se trata de las vibraciones. Y las vibraciones obviamente son algo negativo", comentó Gregg. Los gritos del técnico quedaban claramente reflejados en los gráficos que monitorizan en tiempo real cada uno de los discos duros del parque de servidores.

Fuente: **http://www.diarioti.com**

HARDWARE

Tandberg presenta gateway IP 3500 Codian 06/01/2009

Tandberg ha presentado la versión 2.0 del Gateway IP 3500 Codian, solución interoperable que permite acceso instantáneo y personalizado a los terminales de videoconferencia de todos los principales fabricantes.El Gateway IP 3500 de Tandberg Codian es un dispositivo de red que permite a los usuarios llamar a una empresa desde cualquier terminal de videoconferencia estándar y tener acceso de video a la información y usuarios deseados.

Fuente: **http://www.diarioti.com**

IR al SUMARIO

INTERNET

La industria discográfica considera crear competidor de YouTube 31/12/2008

YouTube alberga actualmente videos musicales de grandes artistas como Madonna og Red Hot Chili Peppers. Sin embargo, el sello discográfico Warner exige que todos los videos musicales de estos artistas, y de otros de sus representados, sean eliminados del sitio.Las intenciones de Warner Music son crear su propia videoteca, en competencia con YouTube de Google. La razón sería un desacuerdo en un contrato entre ambas empresas, informa The Times Online.

Fuente: **http://www.diarioti.com**

TELEM@TICA

PARA INSCRIBIRSE EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-subscribe@cujae.edu.cu

PARA ANULAR SU INSCRIPCIÓN EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-unsubscribe@cujae.edu.cu

PARA AUTORES QUE DESEEN PUBLICAR EN TELEM@TICA

Para la publicación en nuestra revista los interesados deberán enviar su propuesta escrita indicando claramente: Título del artículo, glosario de términos (No más de media cuartilla), imágenes referenciadas (No más de 200Kb), nombre de los autores, sus fotografías y la institución a la que pertenecen, así como alguna forma de comunicación (teléfono, Fax o correo electrónico). Para una guía más detallada descargue el formato de publicación de la dirección: http://www.cujae.edu.cu/revistas/telematica/Soporte_Tecnico/formato.doc
Su artículo se someterá a revisión por un comité de árbitros que decidirá sobre la publicación del mismo. Deberán acompañar igualmente (en no más de media cuartilla) un glosario, de los términos más importantes utilizados en el artículo. Puede contactarnos a través de nuestro email telematica@revistas.cujae.edu.cu