Seguridad de red privada virtual de Microsoft

Documento estratégico

Resumen

Este documento estratégico proporciona una descripción general de los temas de seguridad acerca de la implementación de redes privadas virtuales (VPNs) utilizando la familia de sistemas operativos Microsoft® Windows®. En Windows 95, Windows 98, y los sistemas operativos Windows NT 4.0, Microsoft proporciona soporte de red privada virtual (VPN) a través del protocolo de túnel de punto a punto (PPTP). Para responder a los problemas reportados y mejorar la seguridad PPTP, Microsoft recientemente ha realizado mejoras a PPTP. Con el lanzamiento del sistema operativo de Windows 2000, Microsoft ampliará su soporte de protocolo VPN para incluir soporte para Protocolo de túnel nivel 2 (L2TP), así como para Seguridad de protocolo Internet (IPSEC) y el Protocolo de autenticación ampliable (EAP). Este documento describe estas tecnologías, además de abordar las medidas preventivas y amenazas de seguridad.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0399

TABLA DE CONTENIDOS

INTRODUCCION

Los sistemas operativos Microsoft® Windows® 95, Windows 98 y Windows NT® proporcionan comunicaciones económicas, seguras y fáciles que habilitan los negocios sin límites. Una de las funciones de una plataforma de comunicaciones basada en Windows es el soporte de Red privada virtual (VPN).

Las VPNs se han hecho populares debido a que ofrecen ahorros operacionales, al tiempo que mantienen la seguridad relacionada con la infraestructura de red privada. Al utilizar una VPN, un trabajador que se traslada de un lado al otro o una sucursal, puede conectarse a la red corporativa con una llamada local, proporcionando ahorros importantes en el uso de larga distancia, número 800 ó líneas contratadas. La seguridad se mantiene debido a que VPN utiliza un túnel seguro, con lo que permite que sólo los usuarios autentificados accedan a la Intranet corporativa. Las soluciones VPN de Microsoft ofrecen encriptación de 128 bits dentro de los Estados Unidos, con encriptación de 40 bits soportada en el extranjero donde la ley lo permita. Una Red privada virtual se puede describir como la capacidad de conectarse por túnel a través de Internet u otra red pública de manera que proporcione la misma seguridad y otras funciones que antes estaban disponibles únicamente en las redes privadas. Con el túnel, se encapsula un paquete de mensajes dentro de un paquete IP para su transmisión a través de la red pública y la encapsulación de información se abre al llegar a la red objetivo, como puede ser la red de área local corporativa (LAN).

Las VPNs son tan importantes para las organizaciones que soportan teleconmutadores, sucursales y socios fuera de sitio, que se están convirtiendo en una parte crítica de la estrategia de tecnología de información corporativa.

Microsoft ha sido pionero en la integración de soluciones VPN, y sigue trabajando con los socios industriales y con la Fuerza de ingeniería de tareas (IETF) de Internet para impulsar la tecnología y seguridad de redes privadas virtuales. Este documento ve en la seguridad VPN, la continuidad de retos de seguridad, y las diferentes maneras en las que las soluciones VPNs de Microsoft proporcionan seguridad.

Las soluciones VPN de Microsoft cubren un espectro de necesidades de seguridad. El protocolo de túnel de punto a punto (PPTP), el cual está disponible para los sistemas operativos de Microsoft Windows 95, Windows 98 y Windows NT 4.0, así como en Windows 3.1 y Macintosh de terceros, fue diseñado para proporcionar los costos totales de propiedad más bajos. PPTP se ejecuta bien en una amplia variedad de hardware, soporta la autenticación de contraseña, y no requiere la implementación de una infraestructura certificada, aunque el soporte certificado estará disponible en la configuración de tiempo de Windows 2000.

Las implementaciones de Protocolo de túnel de nivel 2 (L2TP) y Seguridad protocolo Internet (IPSEC) de Microsoft, las cuales estarán disponibles en la plataforma Windows 2000, están diseñadas para proporcionar la mayor seguridad posible. En consecuencia, estas soluciones VPN requieren la implementación de una Infraestructura de clave pública, y requieren un procesador de clase Pentium.

Se pretende que este documento ayude a los administradores de red y a otros encargados de tomar decisiones para evaluar las necesidades de seguridad VPN de su organización y elegir la solución que mejor se ajuste a sus necesidades. El documento también analizará el papel que la política de seguridad y la educación de empleado juegan al proteger una red sin importar la tecnología implementada.

Asegurar una red es un reto dinámico y no estático. Toda la seguridad representa un balance que actúa entre la protección contra amenazas de seguridad potenciales y el no saturar la red o el desempeño organizacional.

Microsoft está comprometido en impulsar su tecnología para proporcionar las soluciones de seguridad más avanzadas, al tiempo que permite que la tecnología sea fácil de administrar e implementar.

La solidez de la seguridad de las soluciones VPN Microsoft permite que las organizaciones aprovechen al máximo la conveniencia y ahorros en los costos de conexión por túnel a través de redes públicas, sin permitir el acceso no autorizado.

PRINCIPIOS BASICOS DE SEGURIDAD VPN

Un túnel VPN funciona mediante la encapsulación de datos dentro de paquetes IP para transportar información que no cumple de ninguna forma con los estándares de direccionamiento en Internet. Posteriormente, estos paquetes encapsulados se transportan entre una red, o cliente único, y otra red sobre una red intermedia. A todo este proceso de encapsulación y transmisión de paquetes se le conoce como conexión por túnel, y a la conexión lógica por la que los paquetes viajan se le llama túnel. Un túnel es una conexión a través del Internet u otra red intermediaria. El resultado es que los usuarios remotos se convierten en nodos virtuales en la red a la que han sido conectados por túnel.

Desde la perspectiva del usuario, la naturaleza de la red física que ha sido conectada por túnel es irrelevante ya que aparece como si la información haya sido enviada sobre una red privada dedicada.

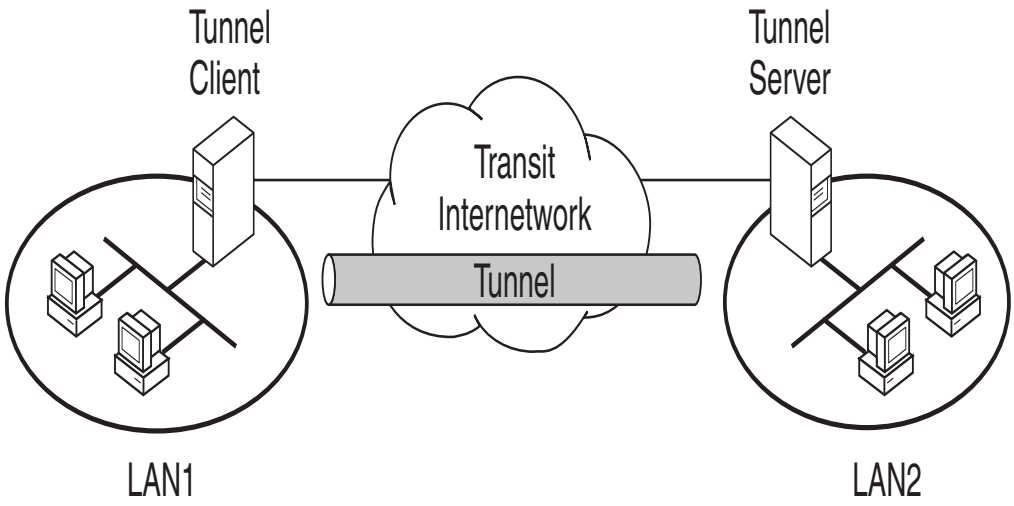

Figura 1. Un modelo conceptual de una VPN.

La comunicación a través de Internet requiere que, tanto la encapsulación como la encriptación de flujo de datos, sea viable. PPTP y L2TP proporcionan servicios de encapsulación, a fin de facilitar las comunicaciones de protocolos múltiples mediante Internet. La encapsulación permite que los paquetes de datos no basados en IP se comuniquen a través de Internet basada en IP desde un cliente remoto a una LAN corporativa privada, la cual permite que las redes no basadas en IP aprovechen al máximo el Internet.

Dando soporte a procesadores de componente frontral

Las VPNs de Microsoft están diseñadas para permitir que los procesadores de componente frontal (FEPs) se conecten con servidores que ejecutan Windows NT Server, de manera que los clientes que llaman a FEP tengan acceso transparente a la red del servidor. Esto significa que incluso los clientes que no están habilitados por una VPN puedan realizar conexiones por túnel, aún sin darse cuenta si van

directamente al servidor, o a un FEP por túnel a través del servidor. Debido a que la VPN de Microsoft proporciona acceso transparente a un cliente PPP, puede trabajar con UNIX, Win 16, el sistema operativo MS-DOS®, Macintosh y con otros clientes.

Un proveedor de servicios de Internet puede operar un FEP ya que los FEPs no permiten acceso al intercambio de datos entre el cliente y servidor. El FEP es solo un conducto que carece de inteligencia para evaluar la información que pasa a través de él. Desde un punto de vista de seguridad, esto significa que una compañía no perderá control de quien acceda a su red. Se mantiene la privacidad de datos. Es muy importante para las compañías, que se pueda acceder a la marcación externa ya que necesitan que sus datos estén seguros.

Otro punto importante es mantener control de quien tiene acceso al servidor en lugar de que tener acceso a un FEP. El servidor autentifica los clientes que llaman, el FEP únicamente ve la identidad del que llama y establece el túnel al servidor. Puesto que tiene un papel pasivo, la seguridad es absoluta.

Túneles obligatorios y voluntarios

Hay dos tipos de túneles VPN—obligatorio y voluntario. Los túneles voluntarios requieren que el cliente esté habilitado por una VPN mientras que los túneles obligatorios se utilizan cuando el cliente confía en un FEP habilitado por una VPN.

Conexión por túnel voluntario

La conexión por túnel voluntario es una metodología en la cual la estación de trabajo de cliente se ofrece como voluntario para crear el túnel en la red objetiva. Para que ocurra esta conexión por túnel, el cliente debe estar habilitado por VPN con los protocolos PPTP o L2TP y software de soporte. (El servidor de túnel siempre viene con este soporte de protocolo). El cliente y el servidor deben utilizar el mismo protocolo de túnel.

Con la conexión por túnel voluntario el cliente puede tener una conexión de red que puede proporcionar transporte entre la estación de trabajo y servidor de túnel seleccionado. Frecuentemente, la estación de trabajo puede haber establecido una conexión de marcación a la red de transporte antes de que el cliente pueda configurar un túnel.

Conexión por túnel obligatorio

Si un cliente desea conectarse a través de Internet, pero no está habilitado por una VPN, puede conectarse a un FEP habilitado por una VPN en un proveedor de software independiente. En el caso de conexión por túnel obligatorio, el cliente puede operar sin el software de soporte L2TP o PPTP (estos protocolos se implementan en el FEP). Es evidente, que el FEP y el servidor de túnel deben soportar y utilizar el mismo protocolo VPN (PPTP o L2TP]) para cualquier conexión específica.

Comúnmente, el usuario que se encuentra en una máquina de cliente recibe un número telefónico especial para marcar al FEP. Por ejemplo, una corporación que

tiene su propia red privada puede tener un contrato con un proveedor de software independiente para ensamblar un conjunto de FEPs en todo el país. Estos FEPS pueden establecer VPNs a través de Internet para un servidor de túnel en la red privada de corporación. Esta configuración es conocida como conexión por túnel *obligatorio* debido a que el cliente está obligado a utilizar la VPN. Una vez que se ha realizado la conexión inicial, automáticamente se enruta al cliente a través del túnel.

UTILIZACIÓN DE VPNS PPTP

Microsoft utiliza el Protocolo de túnel de punto a punto para proporcionar una solución de operación de red privada virtual muy sólida y segura. La facilidad de implementación y seguridad absoluta de la tecnología VPN habilitada por PPTP de Microsoft lo ha convertido en el método de conexión por túnel más solicitado en la industria, de acuerdo con el estudio de mercado VPN 1998 realizado por Infonetics Research.

PPTP es un estándar abierto en la industria. La especificación para PPTP es el resultado de la reunión de esfuerzos con un *host* de proveedores de operaciones de red reconocidos entre los que se incluyen Ascend Communications, 3Com/Primary Access, ECI Telematics, US Robotics, y Microsoft. Estas compañías constituyeron el foro PPTP, cuyos esfuerzos unidos se dieron a conocer públicamente y fueron presentados ante la organización de estándares y IETF en 1996.

PPTP está integrado con el servidor de Servicios de acceso remoto, que viene incluido en Windows NT Server, y Windows 98, y es un componente de la actualización Dial-Up Networking 1.2 para Windows 95.

Cómo proporcionar seguridad en el mundo real

Todos los especialistas de comunicación de operación de red y seguridad se dan cuenta que en los escenarios del mundo real, la seguridad de una computadora es una función de diversos elementos dinámicos que incluyen la tecnología, la política y la seguridad física. Es dentro de este grupo estructurado, y después de una evaluación cuidadosa de sus recursos, que cada organización define su nivel de riesgo aceptable y las soluciones que implementa. PPTP participa en todo el plan operacional para comunicaciones seguras, se basa en un enfoque de mundo real pragmático para problemas de seguridad, y es utilizado por Microsoft para conexiones VPN a sus propias redes corporativas.

En el contexto del mundo real, Microsoft nunca ha sido contactado por ninguno de sus clientes sobre un caso en el que no se haya podido realizar la comunicación VPN basada en Windows. Sin embargo, a pesar de este registro Microsoft sigue mejorando su tecnología de operación de red y comunicaciones Windows con el reciente lanzamiento de la Actualización de rendimiento y seguridad PPTP para clientes y servidores basados en Windows. Esto se puede obtener sin costo en el sitio Microsoft Communications Web en http://www.microsoft.com/communications.

La solución VPN habilitada por PPTP de Microsoft combina los siguientes beneficios: una plataforma ampliamente disponible, una operación de red con todas las funciones, la integración activa de Windows y la facilidad de uso para entregar una plataforma de comunicaciones altamente programable y flexible. Un sistema basado en Windows configurado adecuadamente, que utilice herramientas Windows y PPTP para reforzar la política de seguridad de contraseña responsable, proporciona una solución VPN económica, confiable y segura que permite ahorros en los costos relacionados con las comunicaciones basadas en Internet.

Avance de tecnología

Para Microsoft la seguridad es muy importante. Como resultado de una continua revisión experimentada y de los rápidos avances tecnológicos, la vanguardia de la encriptación y seguridad de red cambia constantemente. Por esta razón, Microsoft proporciona periódicamente actualizaciones oportunas para sus servicios de seguridad y productos. Los clientes que pagan la política de seguridad siempre deberán estar al tanto sobre los más recientes avances de seguridad disponibles en Microsoft, y deberán monitorear regularmente el sitio Web de seguridad de Microsoft en http://www.microsoft.com/security y el sitio Web de comunicaciones en http://www.microsoft.com/communications.

Los desarrollos recientes con la tecnología VPN PPTP de Microsoft incluyen:

- Mejora de autenticación con MS-CHAP versión 2
- Opción para solicitar autenticación de contraseña más sólida
- Mejora de encriptación con la Encriptación de punto a punto de Microsoft (MPPE)

Mejora de autenticación con MS-CHAP versión 2

El Protocolo de autenticación *Handshake* de Microsoft (MS-CHAP) es un mecanismo de autenticación que se utiliza para validar las credenciales del usuario contra los dominios Windows NT, mientras que las claves de sesión resultantes se utilizan para encriptar los datos del usuario, como se describe a continuación en Análisis de MPPE.

La Encriptación es el proceso de codificación de datos que sirve para prevenir el acceso no autorizado, especialmente durante la transmisión. La Encriptación se lleva acabo utilizando un algoritmo especial junto con uno confidencial (también conocido como *clave*) para transformar datos, como puede ser una contraseña, de manera tal que los datos no puedan ser entendidos por ninguna persona que no conozca la clave correcta. La contraseña *hashed* sólo puede ser decriptada por una computadora que tenga la misma clave como si dos niños tuvieran los anillos decodificadores, pero utilizando algoritmos que harían casi imposible romper la encriptación, especialmente en claves de más de 128 bits.

La versión 2 MS-CHAP incluye una función de una salida de la contraseña del usuario, un reto generado por el servidor y el cliente, además de datos adicionales en el mensaje *Satisfactorio* de la versión 2 MS-CHAP. El cliente de la versión 2 MS-CHAP se desconecta si no puede autentificar el servidor.

Cuando el servidor de acceso de red recibe una solicitud de autenticación MS-CHAP versión 2, por parte de un cliente remoto, éste envía un reto, el cual consiste en una ID de sesión y una cadena de retos arbitrarios, para el cliente remoto. El cliente remoto debe confirmar el nombre del usuario, el *hash* de la cadena de retos, la ID de sesión y la contraseña *hashed* . Este diseño, el cual manipula un *hash* del *hash* de contraseña, proporciona un nivel adicional de seguridad ya que permite que el servidor almacene contraseñas *hashed* en lugar de contraseñas de texto.

La versión 2 MS-CHAP también proporciona códigos de error adicionales incluyendo un código expirado de contraseña, mensajes encriptados adicionales de cliente-servidor permiten a los usuarios cambiar sus contraseñas. En la implementación de la versión 2 de MS-CHAP de Microsoft, tanto el cliente como el servidor generan una clave inicial de manera independiente para la encriptación de datos subsecuentes por MPPE.

Anteriormente, las VPNs PPTP de Microsoft podían ser configuradas para aceptar protocolos de autenticación menos demandantes. Para mejorar la seguridad durante la autenticación, Microsoft PPTP ahora utiliza únicamente MS-CHAP.

Opción para requerir autenticación de una contraseña más sólida

Como se indicó anteriormente, cuando los clientes basados en Windows se conectan a un servidor PPTP basado en Windows NT, realizan una autenticación de respuesta a retos mediante el uso de una técnica denominada MS-CHAP. Esta técnica utiliza una función *hashing* para obscurecer la contraseña Windows NT en la respuesta. (Una contraseña Windows NT debe ir en minúsculas y puede tener hasta 14 caracteres de longitud y utiliza el conjunto de caracteres Unicode de 16 bits).

Debido a que la autenticación se basa, en parte en el *hashing* de la contraseña del usuario para generar claves de encriptación inicial, los administradores de red deben reforzar el uso de una estructura de contraseña Windows NT más compleja. Teóricamente, el conocimiento de la contraseña del usuario podría dar pie a intromisiones de mala fe en la red entre el cliente y el servidor para desencriptar los datos en la sesión PPTP encriptada. (Esto se vuelve aún más difícil con un algoritmo de encriptación de 128 claves ya que la contraseña es la única parte de la información *hashed* para crear la clave).

Aunque se pueden utilizar las contraseñas anteriores del Administrador LAN (LM), las contraseñas LM no son tan complejas como las contraseñas Widows NT, y por lo tanto son más susceptibles a la fuerza bruta o ataques de diccionario, en la que un intruso trata de adivinar la contraseña del usuario.

Solicitud del uso de contraseña Windows NT

Microsoft ha lanzado una actualización para los componentes de cliente y servidor PPTP para Windows NT que le da a los administradores la habilidad de configurar el servidor PPTP de manera tal que sólo puedan aceptar la autenticación de una contraseña más sólida de Windows NT. Esta actualización también permite que el administrador configure clientes PPTP basados en Windows NT para que nunca puedan utilizar la autenticación LM. En breve, Microsoft planea liberar una actualización para el cliente PPTP basado en Windows 95 que le permitirá ser configurado de manera tal que nunca tenga que utilizar la autenticación LM al conectarse a los servidores PPTP. Windows 98 ya incluye esta funcionalidad actualizada. La información específica con respecto a la actualización y a la manera de configurar Windows para controlar el uso de Windows NT Hash se incluye en las notas de la versión del software de actualización. Por favor consulte http://www.microsoft.com/communications/ para obtener información sobre la

versión actualizada para Windows 95, Windows NT y sobre los servicios de acceso remoto y encaminamiento integrado de Windows NT Server para la VPN de servidor a servidor.

Reforzamiento de la política de contraseña

Microsoft recomienda que los clientes refuercen el uso de contraseñas sólidas (complejas) en sus redes mediante el uso de las herramientas de Windows que le permiten al administrador hacerlo. Las contraseñas podrían mezclar letras minúsculas y mayúsculas, números y puntuación. Una política de contraseñas adecuada que especifique la longitud mínima de contraseña, la diversidad de caracteres y la actualización regular es una parte importante en el mantenimiento de la seguridad de la red. Windows NT puede reforzar fácilmente esta política de contraseñas. Service Pack 2 para Windows NT 4.0 y versiones Service Pack subsecuentes proporcionan herramientas para que los administradores de Windows NT refuercen aún más la política de seguridad a través de la administración de contraseña mejorada.

Principios básicos de la política de contraseñas adecuadas

Como se indicó anteriormente las contraseñas sólidas solicitan por lo menos un número mínimo de caracteres y una diversidad de tipos de caracteres. Las buenas contraseñas deberán ser indescifrables por otros. Esto es importante ya que las contraseñas mal elegidas atentan contra la seguridad.

Las contraseñas mal elegidas incluyen aquellas que:

- Se forman únicamente de palabras de diccionario.
- Son de un solo tipo (mayúsculas o minúsculas).
- Se crean de nombres de personas o cosas que podrían descifrarse por otros, tal como el nombre de un hijo de usuario, mascota, o incluso el nombre de soltera de la madre.

Las claves bien elegidas incluyen aquellas que:

- Contiene por lo menos un número y un símbolo (tales como un ?) en medio.
- Aparecen ser “gobbledygook” al observador casual.
- No contiene palabras del diccionario o nombres propios.

Microsoft Knowledge Base article Q161990 proporciona información sobre la habilitación de la política de contraseña sólida dentro de una organización. La administración adecuada de la política de contraseñas hace que cualquier solución basada en una contraseña sea más difícil de comprometer. Las contraseñas complejas, la tecnología adecuada, y las restricciones físicas, todas en conjunto hacen que Windows sea una solución muy segura de VPN en el mundo real.

Observe que en el algoritmo de encriptación de 128 bits de Microsoft, la clave de encriptación no sólo es una función de una contraseña compleja si no también incluye una función en el reto. Este algoritmo hace que un ataque sea mucho más difícil. Microsoft recomienda para Norteamérica el uso de las claves de encriptación de 128 bits como una política no solo para la protección en contra de un ataque, si no también porque se ha visto que las claves de 40 bits son

susceptibles a ataques de fuerza bruta bajo condiciones controladas.

Mejora de encriptación con MPPE

El uso de encriptación proporciona un nivel adicional de seguridad para redes privadas virtuales basadas en PPTP. Aunque esto es poco común, si alguna vez se ve en el mundo real es posible que una persona intercepte paquetes VPN. Si un agresor pudiera colocar una máquina entre el cliente y su servidor de destino, la máquina en el medio podría intentar suplantar el servidor PPTP sujeto y aceptar el tráfico del cliente. La vulnerabilidad a intromisiones de un intruso existe con cualquier protocolo de autenticación de respuestas de reto no mutuo y por lo tanto no es específico para productos de Microsoft. Además, la versión 2 MS-CHAP proporciona autenticación mutua y se diseñó específicamente para vencer dicho ataque.

Al utilizar la encriptación basada en software de 128/40 bits, todo usuario comunicado con datos entre el cliente y el servidor está totalmente protegido y no puede ser leído por la máquina intrusa, la cual no cuenta con la clave necesaria para desencriptar la información transmitida.

PPTP utiliza el algoritmo de encriptación RSA RC4, que opera en el nivel de encriptación más sólido permitido por el gobierno de los Estados Unidos–utilizando claves de 128 bits en Norteamérica y claves de 40 bits en otras partes. Cuando se utiliza la versión 2 MS-CHAP, las claves separadas de encriptación de RC4 se derivan para cada dirección, y por predeterminación, las claves de encriptación se cambian en cada paquete. Estos hechos hacen que las intromisiones sean extremadamente difíciles.

Protección de canal de control

Un error que se encontró y reportó a Microsoft hace varios meses habría permitido que un agresor mal intencionado enviara información defectuosa al servido PPTP sobre lo que se llama canal de control. Este código, si se construye apropiadamente, pudo haber causado que el servidor PPTP se dañara. Microsoft ha lanzado un programa disponible para corregir este fallo. Dicho programa proporciona una más amplia verificación de parámetros en los datos que se transfieren al canal de control para asegurarse de que los datos en el canal de control no puedan bloquear el servidor PPTP. Este programa de reparación también se incluye en las actualizaciones de PPTP recientemente lanzadas para Windows NT. Microsoft Knowledge Base article Q179107 proporciona mayor información sobre este fallo resuelto.

Después de esta reparación, el peor resultado de un ataque de este tipo sería abandonar la sesión activo de PPTP. Para eliminar tales ataques, Microsoft planea mejorar el canal de control PPTP en una actualización futura para autenticar completamente cada paquete de canal de control que se envía al servidor PPTP

Lo que los clientes deberán hacer

Los clientes norteamericanos deberán continuar usando la sólida versión de 128 bits de PPTP en sus redes. Asimismo, los clientes deberán actualizarse al Service Pack más reciente para Windows NT 4.0 e instalar los programas de reparación PPTP más actuales.

En general, los clientes deberán revisar con frecuencia el sitio Microsoft Security Web en http://www.microsoft.com/security, y el sitio Windows Communications Web en http://www.microsoft.com/communications. Posteriormente, los clientes deberán cargar y usar la información más reciente de seguridad, las consultas y las actualizaciones para los servicios de acceso remoto y encaminamiento que habiliten de servidor a servidor y las actualizaciones más recientes de operación de red para las VPNs de servidor a cliente. Los usuarios deberán asegurarse de que la organización utilice las herramientas proporcionadas para reforzar una política de seguridad responsable. Los sistemas basados en Windows propiamente configurados combinados con una política de seguridad adecuada, aseguran que pueda obtener todos los beneficios de una solución segura VPN.

TUNEL CON L2TP

El protocolo para conexión por túnel nivel 2 es una tecnología que combina lo mejor de PPTP y direccionamiento nivel 2 (L2F). L2F es un protocolo de transmisión propuesto que permite que los servidores de acceso conmutado estructuren el tráfico conmutado en PPP y transmitirlo sobre vínculos WAN a un servidor L2F, el cual abre los paquetes y los inyecta a la red.

L2TP proporciona conexión por túnel sobre cualquiera de los medios que proporcionen conectividad punto a punto orientada al paquete, que incluye tecnologías WAN tales como X.25, Frame Relay y ATM. L2TP también proporciona la capacidad de establecer múltiples túneles entre los dos puntos extremos del túnel. (L2TP se documenta en "protocolo de conexión por túnel nivel 2 - L2TP", publicado como draft-ietf-pppext-l2tp-12.txt. la versión más reciente de este documento puede encontrarse en el sitio Web IETF, http://www.ietf.org/).

Cuando se utiliza entre redes IP, L2TP es muy similar a PPTP. Se crea un túnel L2TP entre un cliente L2TP y un servidor L2TP. El cliente puede incluirse a una red IP (tales como LAN) que puede alcanzar al servidor del túnel, o un cliente puede marcar a un servidor de acceso de red (NAS) para establecer la conectividad IP (para usuarios de Internet de marcación).

Tanto PPTP como L2TP usan PPP para proporcionar un sobre inicial para datos y anexar iniciadores adicionales para transportar entre-redes de tránsito. Algunas diferencias entre PPP y L2TP son las siguientes:

- PPTP requiere que el tránsito entre-redes sea una *Internetwork* IP. L2TP únicamente requiere que los medios de túnel proporcionen conectividad de punto a punto orientada al paquete. L2TP puede ejecutarse sobre IP (usando UDP), Frame Relay PVCs, X.25 VCs, o ATM VCs.
- PPTP sólo puede soportar un solo túnel entre dos puntos extremos. L2TP permite el uso de túneles múltiples entre puntos extremos.
- L2TP sostiene la compresión del iniciador, documentada en <<insert here>>. Cuando se habilita la compresión del iniciador, L2TP opera con 4 bytes de carga general, comparado con 6 bytes para PPTP.
- L2TP proporciona autenticación de túnel, mientras que PPTP no lo hace, sin embargo, cuando ya sea que PPTP o L2TP se ejecute sobre IPSec, la autenticación de túnel es proporcionada por IPSec para que no sea necesaria la autenticación de túnel nivel 2.

La creación de túneles L2TP debe autenticarse usando los mismos mecanismos de autenticación como conexiones PPP. L2TP hereda la encriptación y/o la compresión de cargas de pago PPP de PPP, y se puede agregar seguridad adicional de encriptación implementando seguridad IP (IPSec), que se describe en la siguiente sección.

Conexión por túnel con IPSec

La seguridad de protocolo de Internet (IPSec) fue diseñada por IETF como un mecanismo de extremo a extremo para reforzar la seguridad de datos en comunicaciones basadas en IP. IPSec ha sido desarrollada y analizada por

algunos expertos en seguridad de red durante varios años. Es un esquema que autentifica y encripta individualmente paquetes IP, se cree que es sumamente segura. Sin embargo, IPSec fue diseñada en un principio para brindar protección a cada máquina (en particular, para proteger el tráfico entre los encaminadores de Internet). Actualmente, IPSec más o menos asume que cada Host tiene una dirección estática IP.

Se ha definido IPSec en una serie de petición de comentarios (RFCs) notablemente RFCs 1825, 1826, y 1827, los cuales definen la arquitectura general, un iniciador de autenticación para verificar la integridad de datos y una carga de pago de seguridad de encapsulamiento para encriptación e integridad de datos.

El enfoque principal de IPSec connota en proporcionar seguridad a nivel de red para IP. IPSec se integra con la seguridad inherente del sistema operativo Windows NT Server para proporcionar una plataforma ideal que proteja las comunicaciones de Internet e Intranet.

IPSec habilita la conexión por túnel de servidor a servidor, tales como la que existe entre los encaminadores, en lugar de que se usen para la conexión por túnel de servidor de cliente. Por lo tanto, lo complementa en lugar de superponer la funcionalidad proporcionada por PPTP y L2TP. Por lo tanto la flexibilidad de los protocolos VPN nivel 2 (PPT/L2TP) pueden combinarse de manera avanzada con la seguridad proporcionada por IPSec. Microsoft planea dar soporte a dicha plataforma fusionada V*PN* (PPTP o L2TP que se ejecutan sobre IPSec) en Windows 2000.

Además de su definición de los mecanismos de encriptación para tráfico IP, IPSec define el formato de paquete IP sobre un modo de túnel IP, generalmente llamado modo túnel IPSec. Un túnel IPSec consiste en un servidor de túnel y en un cliente de túnel, los cuales se configuran para usar la conexión por túnel IPSec y un mecanismo de encriptación negociado.

El modo de túnel IPSec utiliza el método de seguridad negociada (si hay alguno) con el propósito de encapsular y encriptar paquetes completos de IP para transferencia segura a través de Internet IP público o privado. La carga de pago encriptada se encapsula otra vez con un iniciador IP de texto sencillo, y se envía entre-redes para entregarse al servidor de túnel. Cuando el datagrama lo recibe, el servidor de túnel procesa y descarta el iniciador IP de texto sencillo, y decripta sus contenidos para retirar el paquete original IP de carga de pago. El paquete IP de carga de pago se procesa normalmente y se encamina a su red objetiva.

El modo de túnel de IPSec soporta sólo el tráfico IP, y funciona desde el inicio de la pila IP. Por lo tanto las aplicaciones y protocolo de más alto nivel heredan su comportamiento. Se controla por medio de una política de seguridad o una serie de reglas de adaptación de filtro, el cual establece los mecanismos de encriptación y conexión por túnel disponibles en orden de preferencia al igual que los métodos de autenticación. Tan pronto como hay tráfico, las dos máquinas desempeñan la autenticación mutua, y después negocian los métodos de encriptación que se

utilizarán. Después, se encripta todo el tráfico usando el mecanismo negociado de encriptación y luego se envuelve en un iniciador de túnel.

Autenticación IPSec

IPSec utiliza un encabezado de autenticación y un número de secuencia para proporcionar autenticación de fuente e integridad sin encriptación. IPSec utiliza la Carga de pago de seguridad encapsulada (ESP) para proporcionar integridad y autenticación además de la encriptación. Con la seguridad IP, sólo el emisor y el receptor conocen la clave de seguridad. Si los datos de autenticación son validos, el receptor sabe que la comunicación vino del emisor y que no fue cambiada en tránsito.

PROTOCOLO DE AUTENTICACION EXTENDIBLE

El protocolo de autenticación ampliable (EAP) es una extensión de PPP, que proporciona un mecanismo de soporte estándar para los esquemas de autenticación como las tarjetas *token*, Kerberos, Clave pública y clave/S, y está totalmente soportado tanto en Windows NT Dial-Up Server como en Dial-Up Networking Client. EAP es un componente de tecnología crítica para las VPNs seguras, protegiéndolas de la fuerza bruta de un ataque de diccionario o de que las contraseñas sean adivinadas.

EAP permite que los módulos de autenticación de terceros interactúen con la implementación de una VPN de Servicio de acceso remoto (RAS) Microsoft Windows NT. La disponibilidad de EAP en Windows NT es una respuesta a la creciente demanda para aumentar la autenticación RAS con dispositivos de seguridad de terceros.

EAP es una extensión propuesta por IETF para PPP que permite que los mecanismos arbitrarios de autenticación se empleen para la validación de una conexión PPP. EAP se diseñó para permitir la adición dinámica de módulos de conexión de autenticación tanto del lado del cliente como del servidor en una conexión. Esto permite que los proveedores suministren un nuevo esquema de autenticación en cualquier momento. EAP proporciona la máxima flexibilidad en variedad y singularidad de autenticación. Se planea que EAP se pondrá en marcha en Microsoft Windows 2000.

Seguridad de nivel de transacción (TLS)

Las tarjetas inteligentes y tarjetas *token* pueden ofrecer seguridad absoluta para las VPNs. Las tarjetas inteligentes son pequeños dispositivos casi del tamaño de una tarjeta de crédito, la cual contiene una CPU y una pequeña memoria. Se usan comúnmente para almacenar credenciales de autenticación (tales como certificados de clave pública) claves de encriptación, e información de una cuenta. Algunos también implementan algoritmos de encriptación en la tarjeta, para que las claves de encriptación nunca se borren de la tarjeta inteligente. En la actualidad, las tarjetas inteligentes no son comúnmente utilizadas para la seguridad de acceso remoto, ya que son pocos los paquetes de accesos remoto que las soportan. No obstante, Windows 2000 soportará el uso de tarjetas inteligentes en todas las variedades de autenticación, incluyendo RAS, L2TP, y PPTP.

Las tarjetas *token* de diferentes proveedores funcionan en diferentes formas, pero básicamente todas son generadoras de contraseñas de hardware. Por ejemplo, algunas tarjetas tienen una pequeña pantalla LCD y un teclado como el de una calculadora. El usuario introduce un PIN numérico y la tarjeta muestra un código de pase numérico, el cual a su vez se utiliza como contraseña. Normalmente, las tarjetas *token* están diseñadas de manera tal que sólo produzcan un código de pase determinado. Las tarjetas *token* funcionan muy bien para las aplicaciones de marcación (RAS) o autenticación del Host. Debido a que las aplicaciones de red de tarjetas *token* por lo regular se basan en cliente-servidor, las tarjetas inteligentes pueden ser vulnerables a ser descubiertas casualmente. (Y otras veces en esquemas de contraseña).

Estas tarjetas y certificados de usuario de clave pública recibirán soporte por medio del uso del Protocolo de autenticación ampliable – Seguridad de nivel de transacción (EAP-TLS), el cual se ha sometido a IETF como una propuesta preliminar para un método sólido de autenticación basado en certificados de clave pública. Con EAP-TLS, un cliente presenta un certificado de usuario al servidor de marcación, al mismo tiempo que el servidor presenta un certificado de servidor al cliente. El primero proporciona autenticación sólida de usuario al servidor; el segundo asegura al usuario que ha alcanzado el servidor que esperaba. Ambos sistemas llegan a la cadena de autoridades confiables para verificar la validez del certificado que se ofrece.

El certificado del usuario podría almacenarse en la PC de cliente de marcación, o almacenarse en una tarjeta inteligente externa. En cualquiera de los casos, el certificado no puede accederse sin alguna forma de identificación de usuario (número PIN o intercambio de contraseña/nombre) entre el usuario y la PC del cliente. Este enfoque cumple con “algo de lo que usted sabe más algo que usted tiene”, los cuales son criterios recomendados por la mayoría de los expertos en la seguridad.

EAP-TLS es el método especifico EAP que se implementará en Windows 2000. Como MA-CHAP, EAP-TLS regresará una clave de encriptación que permitirá que MPPE encripte los datos subsecuentes.

Autenticación RADIUS

El Servicio de usuario de marcación de autenticación remota es un servidor central de base de datos de autenticación, además del protocolo de solicitud de autenticación. El protocolo RADIUS es un protocolo basado en UDP que soporta PPP, PAP o CHAP, una función de conexión UNIX, así como otros mecanismos de autenticación. La autenticación RADIUS también proporciona capacidades de contabilidad.

El servidor de RADIUS recibe una solicitud de conexión de usuario desde el NAS y autentifica al cliente contra su base de datos de autenticación. Asimismo, un servidor RADIUS mantiene una base de datos de almacenamiento central de otras propiedades relevantes de usuario. Además de la simple respuesta de sí/no a una solicitud de autenticación, RADIUS puede informar al NAS sobre otros parámetros de conexión aplicables para el usuario, tales como el tiempo máximo de sesión, asignación de dirección IP estática, e información de llamada de respuesta.

RADIUS puede responder a las solicitudes de autenticación basado en su propia base de datos, o puede ser un componente frontal para otro servidor de base de datos, como lo son el servidor genérico de conectividad de base de datos abierta o el controlador de dominio primario. Este último servidor puede ubicarse en la misma máquina del servidor RADIUS, o puede centralizarse en otra parte. Además, un servidor RADIUS puede actuar como un cliente proxy para un servidor RADIUS remoto.

Contabilidad RADIUS

RADIUS permite la administración y contabilidad centralizada de varios servidores túnel. La mayoría de los servidores RADIUS se pueden configurar para colocar registros de solicitud de autenticación en un archivo de contabilidad. También existe un conjunto de mensajes que van del NAS al RADIUS, los cuales solicitan registros de contabilidad al principio de una llamada, al final y en intervalos predeterminados durante la misma. Algunos terceros han escrito paquetes de facturación y auditoría que leen los registros de contabilidad RADIUS y producen varios reportes útiles.

EAP y RADIUS

Cuando se utiliza EAP junto con RADIUS se requieren cambios tanto para NAS como para RADIUS. Para la autenticación tradicional, la interacción NAS/RADIUS es un intercambio único de solicitud/respuesta. Pero en una autenticación EAP, NAS no puede recopilar información del cliente para la autenticación EAP a través de RADIUS, debido a que la información que RADIUS ha habilitado por EAP necesita estar oculta desde el NAS. Para resolver este problema, los administradores del sistema pueden configurar al NAS para que envíe un mensaje de identidad EAP al cliente, el cual a su vez envía el nombre de usuario y los datos de dominio al NAS. NAS presenta estos datos a RADIUS en una solicitud EAP-START, y luego se vuelve transparente para el resto del proceso de autenticación. RADIUS envía y contesta los mensajes EAP a través de NAS al cliente hasta que la autenticación sea satisfactoria o falle.

CERTIFICADOS

Un certificado (o certificado de clave pública) es una estructura de datos firmada digitalmente por una autoridad certificada (CA)—una autoridad en la que pueden confiar los usuarios del certificado. El certificado contiene una serie de valores, tales como el nombre y uso de certificado, información que identifica al propietario de la clave pública, la clave pública misma, la fecha de terminación y el nombre de la autoridad certificada. Esta última utiliza su clave privada para firmar el certificado. Si el receptor conoce la clave pública de la autoridad certificada, el receptor puede verificar que el certificado sea realmente de una autoridad certificada, y que por lo tanto contiene información confiable y una clave pública válida. Los certificados se pueden distribuir de manera electrónica (a través del acceso Web o correo electrónico), con tarjetas inteligentes o discos flexibles.

El soporte de autenticación certificada de clave pública en Windows NT permite que las aplicaciones del cliente se conecten a servicios seguros en nombre de los usuarios que no tienen una cuenta de dominio Windows NT. A los usuarios que pueden ser autentificados con base en un certificado de clave pública emitido por una Autoridad certificada confiable, se les puede permitir el acceso a los recursos Windows NT. Las herramientas de administración del Servicio de directorio permite que los administradores, o autoridades delegadas, se asocien con uno o más usuarios externos a una cuenta Windows NT existente para el control de acceso. El nombre del tema en el certificado versión 3 de X.509 se utiliza para identificar al usuario externo que está asociado con la cuenta.

Las cuentas de clientes son válidas en contraste con la base de datos del usuario Windows NT, y sólo pueden conectarse aquellos que cuentan con permisos válidos. Las claves que se usan para encriptar datos se derivan de las credenciales del usuario, y no se transfieren por cable. Cuando se termina la autenticación, se verifica la identidad del usuario, y se usa la clave de autenticación para la encriptación.

Los negocios pueden compartir información de manera segura con personas seleccionadas de otras organizaciones sin tener que crear varias cuentas individuales Windows NT. Una o varias correlaciones de certificados para los objetos de usuario Windows NT proporcionan autenticación absoluta que se basa en los certificados de clave pública y permisos de control de acceso común. La autenticación de cliente de usuarios externos requiere todavía que el administrador del sistema configure la Autoridad certificada para certificados de usuario externo como una autoridad certificada confiable. Esto evita que alguien que tenga un certificado emitido por una autoridad desconocida entre al sistema con otra identidad.

Autenticación certificada de máquina

Un certificado de máquina se utiliza para validar a un emisor o receptor a nivel de sistema. Los certificados de máquina se diferencian de los certificados del servidor en el hecho de que representan a la máquina misma, y en que pueden ser utilizados para servicios múltiples.

Aunque los certificados de máquina identifican a una computadora a nivel de sistema, no reconoce a un usuario específico que usa tal máquina. Por lo tanto, son más seguros para aplicaciones tales como la autenticación de usuario de marcación, certificados de usuario, que se describirán más adelante, ya que identifican al usuario y no a la máquina del cliente. Esta identidad puede ser utilizada para proporcionar acceso seguro a los recursos.

Autenticación de certificado de usuario

Un certificado de usuario se utiliza para la validación de un usuario específico y para hacer que la clave pública del usuario sea accesible para las funciones de encriptación/desencriptación. Los elementos de un certificado de usuario son el nombre de usuario relacionado con el sistema de directorio (tales como un nombre de usuario X.500), la clave pública de usuario, el nombre de la autoridad certificada que firma y la fecha de terminación del certificado.

Los certificados del usuario se pueden almacenar en tarjetas inteligentes o en la computadora del usuario. Por lo general, en ambos casos están protegidos del acceso de alguna forma de contraseña. También pueden almacenarse en un sistema de directorio para compararse con los certificados presentados por un usuario, que solicita acceso a la red.

Integración Active Directory

Con Windows 2000, se utiliza el Servicio de directorio para publicar certificados de clave pública para los usuarios, y para localizarlos se utilizan los protocolos estándar de acceso al directorio. Las claves privadas y los certificados emitidos para los usuarios se mantienen en un almacenamiento seguro, ya sea en el sistema local o en la tarjeta inteligente. Este almacenamiento seguro se proporciona con las tecnologías de seguridad de Internet y se conoce como *Wallet*.

La implementación del *Wallet* se basa en la arquitectura CryptoAPI de Microsoft para Windows NT. CryptoAPI proporciona funcionalidad de administración clave y otra funcionalidad criptográfica para la creación de un almacén seguro. La implementación de los protocolos de seguridad basados en clave pública Windows NT utilizará las claves y certificados almacenados en *Wallet* como credenciales del usuario para acceder servidores basados en Internet. En muchos casos, las propiedades de certificados definidas por el usuario en *Wallet* permiten que los protocolos de seguridad seleccionen y utilicen de manera automática el certificado correcto y la clave de firma. Los avances en los protocolos de seguridad de Internet (SSL3/TLS) permiten que un servidor solicite credenciales específicas del cliente que se utilizarán automáticamente del *Wallet,* si acaso están disponibles.

ENCRIPTACION

La seguridad VPN se mejora con el uso de encriptación para proteger contraseñas además del contenido de paquetes de datos. Las claves que se utilizan para encriptar datos se derivan de las credenciales del usuario y no se transfieren por cable. Cuando se termina la autenticación, se verifica la identidad del usuario, y se utiliza la clave de autenticación para la encriptación.

Tanto los protocolos de encriptación y compresión opcionales inherentes PPTP y L2TP como la seguridad adicional de encriptación, pueden agregarse implementando el protocolo IPSec, ya que la implementación Microsoft de L2TP está permitida para la encriptación IPSec. Se pueden utilizar varias tecnologías de encriptación para proporcionar seguridad de datos con las VPNs.

Encriptación simétrica (Clave privada)

La encriptación simétrica o de clave privada (también conocida como encriptación convencional) se basa en una clave secreta que se comparte por dos partes que están en comunicación. La parte que envía, utiliza la misma clave secreta como parte de la operación matemática para encriptar (o cifrar) el texto sencillo a *ciphertext.* La parte que recibe, utiliza la misma clave secreta para desencriptar (o descifrar) *ciphertext* a texto sencillo. Algunos ejemplos de los esquemas de encriptación simétrica son: el algoritmo RAS RC4 (que sienta las bases para la Encriptación de punto a punto de Microsoft), Estándar de encriptación de datos (DES), el Algoritmo internacional de encriptación de datos (IDEA) y la tecnología de encriptación Skipjack propuesta por el gobierno de los Estados Unidos para utilizarse en el chip Clipper.

Encriptación asimétrica (Clave pública)

La encriptación asimétrica o de clave pública utiliza dos claves diferentes para cada usuario: una es la clave privada que sólo conoce el usuario. La otra es la clave pública correspondiente que puede acceder cualquier persona. Las claves privadas y públicas están relacionadas matemáticamente por el algoritmo de la encriptación. Una clave se utiliza para la encriptación, y la otra para la desencriptación, dependiendo de la naturaleza del servicio de comunicación que se esté implementando. Asimismo, las tecnologías de encriptación de clave pública permiten que se coloquen firmas digitales en los mensajes; una firma digital utiliza la clave privada del emisor para encriptar una parte del mensaje. Cuando se recibe el mensaje, el receptor utiliza la clave pública del emisor para descifrar la firma digital y verificar la identidad del emisor.

Con la encriptación simétrica, tanto el emisor como el receptor tienen una clave secreta compartida. La distribución de la clave secreta debe ocurrir antes que cualquier comunicación encriptada (con protección adecuada). Sin embargo, con la encriptación asimétrica, el emisor utiliza una clave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una clave pública para descifrar estos mensajes. La clave pública puede distribuirse libremente a cualquiera que necesite recibir los mensajes encriptados o firmados digitalmente.

El emisor necesita proteger cuidadosamente sólo la clave privada.

Encriptación Stateful y Stateless

Al seleccionar los esquemas de encriptación, es importante observar las diferencias que hay entre la encriptación *Stateful y Stateless*.

Con la encriptación Stateless, cada paquete es autosuficiente y contiene toda la información necesaria para desencriptar el paquete. Con la encriptación Stateful cada paquete depende del paquete o paquetes anteriores para desencriptarlo de manera satisfactoria.

La opción de encriptación Stateless versus Stateful es una negociación entre la fuerza de encriptación y el desempeño en ambientes de alta pérdida o ambientes sin petición de soporte. La encriptación Stateless requiere que cada paquete sea descifrable como unidad autónoma. Esto tiene menos solidez que la encriptación Stateful, en la cual se requiere el conocimiento del paquete anterior con el fin de descifrar cualquier paquete individual. Pero debido a que la desencriptación de un paquete depende de la llegada del anterior, la encriptación Stateful pierde uno adicional por cada serie contigua de paquetes perdidos. Por lo que el rendimiento se ve afectado por los paquetes perdidos por la entrega fuera de secuencia.

Los mecanismos de encriptación IPSec utilizan regularmente los métodos de encriptación Stateless por la simple razón de que un ambiente de red IP no puede garantizar la entrega del paquete. Los mecanismos de encriptación PPP, por lo regular, utilizan la encriptación Stateful debido a que el ambiente de punto a punto para el que fueron inventados garantiza la entrega del paquete y la secuencia correcta.

IPSec y encriptación Stateless

Los esquemas de encriptación IPSec encriptan cada paquete por separado y no dependen de la encriptación de paquetes anteriores. Por lo tanto, la pérdida de uno solo afectará únicamente a ese mismo paquete, pero esto no evitará que los demás se decripten. Cuando los protocolos de túnel de Nivel 2 (tales como PPTP y L2TP) se ejecutan sobre IPSec, es posible utilizar los mecanismos de encriptación Stateless de IPSec en lugar de los mecanismos de encriptación Stateful de PPP.

IPSec se crea con base en el modelo IETF combinando la criptografia de clave secreta y clave pública, y proporcionando administración de clave automática para mayor seguridad y conexión más rápida. Esto origina una combinación de autenticación, integridad y antireproducción y opcionalmente de confidencialidad, para asegurar una comunicación segura. Debido a que la Seguridad IP Windows está por debajo del nivel de red, es transparente para los usuarios y las aplicaciones existentes. Las organizaciones automáticamente obtienen altos niveles de seguridad de red.

Por lo general, las implementaciones IPSec ofrecen soporte a una variedad más amplia de algoritmos de encriptación que la de los protocolos de túnel de Nivel 2,

los cuales están basados en la encriptación PPP. Sin embargo, cuando los protocolos de túnel de Nivel 2 se ejecutan sobre IPSec, se puede disponer de todos los algoritmos de encriptación IPSec para encriptar el trafico de túnel de Nivel 2.

FILTRACION

La filtración brinda a los administradores de red una importante función de seguridad. Es decisión del administrador permitir que únicamente los usuarios habilitados y autentificados por VPN se conecten a la red corporativa desde Internet. Al filtrar paquetes que no son PPTP o L2PT se evita el riesgo de que alguien atente contra la red corporativa a través del servidor de central internacional de la VPN. La filtración evita que los demás paquetes entren a la red privada. En combinación con la encriptación PPP, esta práctica asegura que sólo los datos encriptados y autorizados entren o salgan de la LAN privada.

Filtración en un servidor VPN-R/RAS

El Servidor de acceso remoto y encaminamiento de Microsoft integra el encaminamiento con soporte VPN y RAS; puede establecer filtros de paquete en puertos individuales y soporta L2TP con Windows 2000.

En un servidor R/RAS-VPN, se pueden aplicar los filtros L2TP o PPTP a las puertas de entrada del servidor de túnel, de esta manera se bloquean los paquetes que no cumplan con las especificaciones designadas del protocolo como se implementaron en el servidor. Tales especificaciones podrían incluir paquetes cuya dirección de destino corresponda a un servidor específico, y que su dirección esté incluida en una serie de direcciones IP de fuente, donde el servidor de túnel asignó las direcciones válidas de red privada y donde la dirección de fuente de red privada tiene validez.

Los filtros también pueden establecerse en las puertas de salida del servidor de túnel para filtrar paquetes de datos a medida que *abandonan* la red privada. Por ejemplo, un esquema podría implementarse para verificar la dirección de destino de un paquete comparado con un conjunto de direcciones aceptables que R/RAS mantiene. Por el contrario, las direcciones de la fuente del paquete podrían verificarse de la misma manera.

Filtración IPSec

IPSec puede visualizarse como un nivel por debajo de la pila TCP/IP. Este nivel está controlado por una política de seguridad en cada máquina y una asociación de seguridad negociada entre el emisor y el receptor. La política consiste en una serie de filtros y comportamientos de seguridad relacionados. Si una dirección IP del paquete, protocolo y número de puerto coincide con un filtro, entonces el paquete queda sujeto al comportamiento de seguridad relacionado.

VPNs y *firewalls*

Firewalls son otro método para asegurar la integridad de la red corporativa regulando estrictamente qué datos pueden entrar a la red privada desde Internet. Existen dos enfoques para la utilización de las técnicas *firewall* con una VPN.

Un servidor de túnel VPN puede instalarse al frente de un *firewall*, detrás de un *firewall* o en la misma máquina. La configuración más segura requiere que el

servidor VPN se coloque al frente del *firewall*. Al utilizar Windows NT, el túnel VPN podría configurarse para filtrar paquetes que no sean del PPTP. Una vez que se filtran los paquetes PPTP, estos se decriptan y descomprimen. Posteriormente, pasa la comunicación al *firewall*, donde éste puede proporcionar más servicios de filtración y mostrar dentro del contenido encriptado y encapsulado con anterioridad. Este enfoque, con el servidor al frente del *firewall,* es la configuración más segura, es la que se recomienda para cualquier aplicación extranet de varios socios de confianza o por si los recursos financieros no excluyen la consideración.

(Nota Ejecutar el Servicio de acceso remoto y encaminamiento en el servidor Windows NT puede dar algo de filtración estática para filtrar los paquetes de acuerdo con las direcciones de destino y fuente, protocolo, puerto u otros criterios de filtración. Aunque esto puede proporcionar cada vez más seguridad, no se debe entender como un equivalente a una solución *firewall*).

Asimismo, como ya se mencionó antes, un *firewall* puede colocarse al frente de un servidor VPN. Esta solución, aunque posible, da como resultado paquetes que son analizados por el servidor. Además, existe más riesgo si se permite el paso a los paquetes basados en PPTP a través de un servidor VPN. Estos paquetes no los puede contabilizar el *firewall*, ya que ambos están comprimidos y encriptados. El riesgo de seguridad que conlleva dicha configuración se confina a quien posee un empleado que se le ha permitido el acceso remoto. El empleado que tiene acceso LAN también enfrenta cada día este riesgo interno. Esta configuración y los riesgos que implican, son suficientes para una aplicación Intranet.

Algunas organizaciones, debido a los recursos restringidos, quizás también deseen instalar *firewall* en la misma máquina que el servidor VPN. Bajo estas circunstancias, una sola máquina dirige el tráfico VPN a su destino específico y dirige el resto del tráfico que recibe el servidor al *firewall* para ser analizado. Este enfoque es el más económico y se recomienda para Intranet o comunicaciones específicas de la compañía.

MEJORAR LA SEGURIDAD CON TRADUCTORES DE DIRECCION DE RED

Un Traductor de dirección de red (NAT) asigna direcciones privadas a los clientes, las cuales son traducidas por NAT en direcciones públicas IP aceptables para trafico en Internet. Algunas organizaciones utilizan NAT detrás de su *firewall* para que la seguridad adicional que surge no exponga su estructura de dirección interna.

NAT se instala típicamente como un componente de encaminamiento de protocolos múltiples. En general, existen dos tipos de implementaciones NAT. En el primer tipo, una LAN pequeña puede tener direcciones privadas y luego recibir un número correspondiente de direcciones desde InterNIC. Un NAT se configura para correlacionar cada dirección privada a una dirección individual de Internet, o viceversa. En el segundo caso la LAN tiene más direcciones privadas que direcciones de Internet. Un NAT establece una tabla de correlación interna de direcciones. Cuando un paquete proveniente de un cliente LAN pasa por el NAT para llegar a Internet, el NAT cambia el campo de dirección de origen del paquete, mantiene un registro de la dirección original del cliente, además del campo de dirección de fuente compatible con Internet y proporcionado de manera más reciente por NAT. Después, el NAT transmite el mensaje a Internet. Cuando NAT recibe los mensajes de Internet, éste utiliza su tabla de traducción de dirección para volver a correlacionar el campo de dirección de la fuente al cliente original, y enviar el paquete por su ruta.

L2TP da a las VPNs de Microsoft la capacidad de pasar a través de una traducción de dirección de red, ya que está estratificada hasta arriba de UDP. En contraste, PPTP está estratificada hasta arriba de la encapsulación de ruta genérica, la cual carece de la capacidad de trabajar con NATs.

SELECCION DE SU SOLUCION VPN

En la industria de seguridad de computadoras existe una broma que trata acerca de asegurar por completo una computadora, lo cual consta de dos pasos:

1) Cubrirla de concreto.

2) Arrojarla desde un muelle.

La idea es que la seguridad nunca es absoluta, pero tampoco es absoluta la magnitud de la seguridad. La buena noticia es que la seguridad que proporcionan las VPNs habilitadas por PPTP de Microsoft y la Encriptación de punto a punto es segura. Microsoft y sus empleados utilizan esta tecnología a diario para transmitir información privada de manera económica con seguridad mediante las redes privadas y públicas.

Con el soporte Windows 2000 de L2TP, la protección de extremo a extremo de la Seguridad IP, las tarjetas inteligentes del Protocolo de autenticación mejorada, y el uso de certificados Kerberos, permiten que los administradores de red tengan una amplia gama de soluciones de seguridad de Microsoft de las que pueden elegir al implementar una VPN.

Realización del análisis de riesgo

Es por eso que un buen primer paso es que un administrador de red lleve a cabo un análisis de riesgos para considerar la vulnerabilidad de la red, la probabilidad de un ataque y la consecuencia de un ataque exitoso.

Otra parte del análisis es determinar el impacto de la solución. Por ejemplo, una compañía que considere una solución completa de Seguridad IP quizás tendría que actualizar todas sus 486 o computadoras Pentium para que cumplan con las demandas adicionales de la CPU por soportar la Seguridad IP. Para las aplicaciones *hosting* una red que involucra información extremadamente sensible y con altas probabilidades de ataque, la decisión de cambiar a IPSec podría ser una inversión prudente. Un negocio con menos riesgo de atraer intrusos podría eliminar el gasto de actualizar las máquinas e implementar una VPN PPTP.

El soporte Microsoft del Protocolo de autenticación mejorada en Windows 2000 permite que las compañías implementen tarjetas inteligentes o sistemas de seguridad basados en tarjetas *token* en las que los usuarios tiene que llevar físicamente un dispositivo parecido a una tarjeta de crédito para conectarse a sus computadoras. El nivel extra de seguridad que se enfrenta deberá considerarse en relación con los problemas pragmáticos reales de la gente que deja las tarjetas inteligentes en casa o las pierde.

De manera similar, la seguridad adicional, proporcionada por los certificados Kerberos, podría ser esencial para algunas operaciones. Pero otros administradores de red dudarían en comprometerse con integrar sus redes para dar soporte a una infraestructura de clave pública.

Aumento de seguridad a través de la política de contraseña

La facilidad de implementación y administración, junto con la absoluta seguridad y soporte de encriptación de datos MPPE, hacen que las VPNs habilitadas por PPTP de Microsoft sean unas de las soluciones que más se utilizan. De nuevo, cada administrador de red debe determinar la solución de seguridad que mejor se adapte a sus análisis de riesgos, pero para un gran porcentaje de organizaciones, incluyendo Microsoft, las VPNs habilitadas por PPTP proporcionan la seguridad extrema que se requiere para implementar de manera segura las redes privadas virtuales.

Aunque la autenticación de PPTP basada en contraseña es más fácil de administrar que las tarjetas inteligentes o certificados, es de vital importancia que los administradores de red protejan la seguridad de sus VPNs de PPTP (además de otros recursos de red) mediante la política de contraseñas que refuerza:

- El uso de contraseñas Windows NT
- El uso de cadenas de caracteres complejos (letras mayúsculas y minúsculas, númericos, puntuación y longitud mínima)
- Cambio constante de contraseña

La buena política de seguridad también incluye temas prácticos, tales como recordar al usuario de no mostrar notoriamente su contraseña, por ejemplo, pegándola en su monitor.

Viendo hacia el futuro

Microsoft es líder en desarrollo e implementación de encriptación y otras tecnologías de seguridad. Debido a que la seguridad es importante para mantener la integridad de las redes de computadoras del mundo, el desarrollo e investigación en Microsoft y en otras partes es un proyecto continuo. Por ejemplo, el grupo de trabajo de protocolo de seguridad de protocolo Internet esta desarrollando mejoras para la Seguridad IP, y la seguridad de datos RCA está realizando un esfuerzo de consorcio para implementar la iniciativa S/WAN, y asegurar la interoperabilidad entre los productos *firewall* y TCP/IP. A medida que las nuevas tecnologías de seguridad se desarrollan, serán evaluadas en cuanto a su integración con Microsoft VPN.

RESUMEN

Microsoft sigue evolucionando su Operación de red privada virtual a fin de proporcionar a los usuarios soluciones seguras VPN y bien integradas. El protocolo de túnel de punto a punto permite que las organizaciones aprovechen la conveniencia y los ahorros de túnel a través de redes públicas, sin permitir acceso no autorizado. La Encriptación de punto a punto de Microsoft proporciona la seguridad adicional de encriptación de los datos de túnel; Windows 2000 dará la opción de usar el Protocolo de túnel nivel 2, Seguridad IP y el Protocolo de autenticación ampliable para soportar métodos adicionales de autenticación, tales como tarjetas inteligentes.

Microsoft reconoce que la seguridad es una amenaza dinámica y responde proactivamente a las demandas de cambio de la seguridad de red evolucionando constantemente la tecnología que se necesita para proporcionar las operaciones seguras de red. Este compromiso ha dado una solución aún más extrema de PPTP VPN a través de mejoras que incluyen:

- Mejora de autenticación con MS-CHAP
- Opción para Requerir autenticación más sólida de contraseñas
- Mejoras de encriptación con la Encriptación de punto a punto de Microsoft (MPPE)
- Protección del canal de control

Las organizaciones enfrentan una serie de desafíos de seguridad. Algunas redes, como aquellas que soportan información sumamente sensible y que enfrentan una alta probabilidad de ataque, requieren soluciones más seguras que puedan implementarse, mientras que otras requieren una VPN básica, quizás con la encriptación de datos. Microsoft soporta la variedad completa de la tecnología, proporcionando a los clientes una extensión de soluciones integradas de seguridad.

LAS PREGUNTAS QUE SE HACEN CON MAS FRECUENCIA SOBRE SEGURIDAD VPN

¿Es segura la red privada virtual basada en Windows NT 4.0?

Crear un ambiente seguro de sistemas requiere atención en la política de seguridad y seguridad física, así como asegurar el software. No hay algo tan absoluto como la seguridad. Para la mayoría de los fines de negocio, el costo por quebrantar la seguridad PPTP probablemente excederá el valor de la información obtenida. En este contexto, Windows NT 4.0 proporciona una infraestructura segura para la Red privada virtual (VPN). Las claves de encriptación de 128 bits o iniciales 40 bits se generan automáticamente para cada sesión de VPN, permitiendo la rápida y absoluta encriptación de datos que usan el algoritmo de encriptación RC4. Además, Windows NT 4.0 da a los administradores del sistema las herramientas adicionales necesarias para asegurar sus instalaciones. Esto incluye la autenticación integrada de usuario e instalaciones para reforzar la sólida seguridad de contraseña.

Tome en cuenta que la política del gobierno de los Estados Unidos generalmente restringe la distribución de software de encriptación de 128 bits a sitios en los Estados Unidos y Canadá y a bancos, instituciones financieras y subsidiarios de grandes compañías de Estados Unidos en otras ubicaciones (bajo ciertas circunstancias). Dada la tecnología actual, es posible quebrantar claves de 40 bits dentro de un periodo que disminuye constantemente a medida que la tecnología avanza. Esto es verdad sin tomar en cuenta la tecnología VPN. Por esta razón recomendamos que los clientes utilicen claves de 1280 bits si es posible, cuando necesiten sólida confidencialidad de datos.

¿Hay otros aspectos de seguridad que debería considerar al tomar una decisión sobre una solución VPN?

Sí. El diseño integrado, la facilidad de uso e implementación y el costo son factores importantes. Un sistema mal diseñado puede abrir brechas adicionales en la seguridad mientras la gente trata de simplificar su operación. Por ejemplo, un sistema que requiere administración manual de claves de encriptación puede causar que la gente mantenga estas claves en lugares accesibles, reduciendo la dificultad de un ataque. Además, una de las fuerzas principales detrás de la adopción corporativa de tecnología VPN ha sido la reducción de costos.

¿Son diferentes los temas de seguridad para RAS que para el acceso VPN?

Sí, en particular, la necesidad de encriptación es mucho mayor en el caso de VPN. Esto se debe a que el tráfico de datos pasa a través del Internet, el cual es más susceptible a ser descubierto que una línea telefónica. El acceso físico al cable o al interruptor de la compañía de teléfonos es necesario para intervenir o redirigir una línea telefónica y, aunque tales incidentes sean documentados, este acceso es difícil de llevar acabo. Por otro lado, el tráfico de Internet confía en muchos dispositivos (tales como asignadores de ruta y servidores de nombre) en la ruta

desde su cliente PPTP al servidor PPTP. El número total de dispositivos aumenta la posibilidad de que un intruso pueda entrar sin problemas con el fin de redireccionar o interceptar el tráfico de datos.

Además, un mayor número de agresores en potencia pueden intentar alterar un servidor VPN y pueden lanzar tales ataques con mayor rapidez en el caso de un servidor de marcación. Esto aumenta la importancia de autenticación de usuario para servidores VPN y enfatiza la necesidad de establecer contraseñas sólidas.

¿Qué funciones de seguridad se incluyen en PPTP?

PPTP[1] confía en las funciones de seguridad del protocolo de punto a punto (PPP) para proporcionar autenticación y proteger la confidencialidad de datos del usuario. PPP[2, 3,4] es el protocolo que se utiliza para transportar datos dentro del túnel PPTP. Los métodos de autenticación PPP soportados en Windows 9*x* DUN y Windows NT 4.0 RAS incluyen PAP, SPAP, CHAP y MS-CHAP. En Windows 2000 se proporciona el Protocolo de autenticación ampliable (EAP). La encriptación de punto a punto de Microsoft (MPPE) es soportada en Windows 9*x* DUN y Windows NT 4.0 RAS. MPPE usa la cifra de flujo RC4.

¿Cuán seguro es el PPTP?

PPTP depende de dos protocolos propietarios para proteger los datos del usuario a nivel PPP: el Protocolo de autenticación de intercambio de señales de desafío de Microsoft (MS-CHAP)[5] y MPPE[6].

Las versiones más recientes de PPP y PPTP soportan una nueva versión de MS-CHAP (MS-CHAP versión 2)[7], la cual brinda autenticación mutua, claves de encriptación de datos iniciales más sólidas y claves separadas de encriptación para las rutas de recepción y transmisión.

¿Qué tipos de ataques se utilizan contra las VPNs?

Las agresiones de red se clasifican en cuatro categorías:

- Sustitución
- Integridad
- Revelación
- Negación del servicio

---

1 K. Hamzeh, et al., “Protocolo de punto a punto --PPTP,” draft-ietf-pppext-pptp-05.txt (trabajo en progreso), Octubre 1998.
2 W. Simpson, "El protocolo punto a punto (PPP)," RFC 1661, Julio 1994.
3 D. Rand, "Protocolo de control de compresión PPP (CCP)," RFC 1962, Junio 1996.
4 G. Meyer, "Protocolo de control de encriptación (ECP)," RFC 1968, Junio 1996.
5 G. Zorn y S. Cobb, “Extensiones PPP CHAP de Microsoft,” RFC 2433, Octubre 1998.
6 G. S. Pall y G. Zorn, “Protocolo de encriptación punto a punto de Microsoft (MPPE),” draft-ietf-pppext-mppe-02.txt (trabajo en progreso), Agosto 1998.
7 G. Zorn, “Extensiones PPP CHAP de Microsoft, versión 2,” draft-ietf-pppext-mschap-v2-00.txt (PPP CHAP), Agosto 1998.

Los ataques de cambio de personalidad son aquellos en los que un agresor se hace pasar por otra persona. Los sólidos métodos de autenticación soportados en PPTP pueden reducir la efectividad de los ataques de cambio de personalidad.

Los ataques exitosos de *integridad* dieron como resultado la modificación no detectada de los datos del usuario, por ejemplo, cambiar el contenido de un mensaje de correo electrónico en tránsito. Los ataques contra la integridad son casi imposibles de prevenir. Lo mejor que se puede hacer es detectar la modificación; las firmas digitales de varios tipos son formas de defensa útiles contra agresiones de integridad.

Ataques de *revelación* ocasionan la exposición de datos a una persona que no es la indicada. Con frecuencia, el daño causado por los ataques de revelación dependen del contenido de los datos revelados: una petición de reunión puede tener poco valor para un oponente, mientras que la revelación de proyectos confidenciales de ventas podría ser fatal. La defensa típica contra ataques de revelaciones es el uso de encriptación sólida para ocultar tráfico de red, el cual esta disponible en PPTP.

Los ataques de *negación de servicios* son los más difíciles de proteger y los más fáciles de perpetrar. El propósito de dicho ataques, como lo sugiere el nombre, es negar el servicio a usuarios válidos. Windows NT 4.0 se ha hecho más difícil contra un número de agresiones conocidas de negación de servicios que incluyen todo tipo de esfuerzos.

¿Qué ha hecho Microsoft para protegerse de los ataques?

Microsoft toma en serio la seguridad. Para defenderse de un ataque, hemos diseñado nuevamente MS-CHAP y modificado la forma en la que se derivan las claves MPPE. En el futuro, también agregaremos autenticación sólida, protección de integridad y encriptación al canal de control PPTP. La siguiente discusión describe las agresiones en potencia contra PPTP y los pasos que Microsoft ha tomado para evitarlos.

Ataques de diccionario

Los ataques *de diccionario* ocurren cuando un adversario usa una extensa lista de palabras para tratar de adivinar una contraseña. La contraseña encriptada se compara con cada palabra de la lista (también encriptada) hasta que se encuentra una igual. Todos los métodos de autenticación basados en contraseñas son vulnerables a agresiones de diccionario. Sin embargo, la autenticación de administrador LAN es en particular susceptible, debido a la forma en que la contraseña se procesa.

Para corregir este problema, la autenticación del administrador LAN no está soportada en MS-CHAP versión 2. Únicamente se soporta el método de autenticación Windows NT más sólido. El método de autenticación Windows NT es mucho más resistente a los ataques ya que los datos aleatorios están incluidos en las credenciales de autenticación. El método de autenticación Windows NT está

planeado para ser soportado en Windows 95, Windows 98 y Windows NT.

Servidor falso

Debido a que sólo el cliente PPTP se autentica, puede ser posible que un servidor PPTP falso se haga pasar como un servidor PPTP real. El servidor falso no podrá desencriptar los datos transmitidos por el cliente, pero podría recopilar dos o más grupos de datos encriptados con la misma clave de encriptación, lo cual sería de gran utilidad. Asimismo, es posible que un servidor falso solicite al usuario cambiar su contraseña utilizando una versión obsoleta de la facilidad para cambio de contraseña MS-CHAP (Change Password versión 1 o CPW1). Debido a la manera en que CPW1 fue diseñado, el servidor falso podría poseer la contraseña actual del usuario, lo cual podría usarse para impersonar al usuario a un servidor PPTP o RAS real.

Para corregir este problema, MS-CHAP versión 2 proporciona autenticación mutua, lo que dificulta la falsificación del servidor. La *autenticación mutua* significa que no sólo se autentica el cliente para el servidor PPTP, si no también el servidor se autentica al cliente. Además, se ha eliminado el soporte para Change Password versión 1.

Claves débiles de encriptación

Las claves de encriptación utilizadas en MPPE se derivan de la contraseña del usuario. Si la contraseña se elige mal, la clave de encriptación resultante será relativamente débil y fácil de alterar.

Para manejar este problema, Microsoft proporcionó un mecanismo para reforzar la seguridad de contraseña en Windows NT 4.0 Service Pack 2. El administrador de sistemas puede forzar a todos los usuarios a cambiar sus contraseñas (una vez o periódicamente). Durante la operación de cambio de contraseña, el sistema puede inspeccionar la elección de contraseña del usuario para asegurar que cumpla los requisitos mínimos de longitud y aleatoriedad. Sin embargo, es decisión de los usuarios y administradores asegurarse de utilizar la herramienta y no olvidar la seguridad.

Uso repetido de la misma clave de encriptación

Cuando MS-CHAP versión 1 se usa para la autenticación y se negocia la encriptación de 40 bits, se utiliza la misma clave inicial de encriptación para cada sesión PPTP iniciada mientras la contraseña del usuario sea la misma. Esto se debe a que únicamente se usa la contraseña para derivar la clave inicial de 40 bits, sin ninguna otra información para la sesión en sí. Las claves de 128 bits no tienen este problema, ya que los datos específicos de la sesión se utilizan para derivarlas. Sin embargo, se usa la misma clave tanto para enviar como para recibir datos, lo que significa que en cualquier caso se encriptan datos con la misma clave.

En MS-CHAP versión 2 se incorporan los únicos datos a la sesión actual dentro de todas las claves de encriptación, de 40 y 128 bits. Las claves de encriptación separadas se derivan de las direcciones del vínculo de enviar y recibir.

Sincronización de claves MPPE

En un principio MPPE cambiaba la clave de encriptación cada 256 paquetes o cuando se perdía un paquete. Si el paquete perdido era detectado por el receptor, éste enviaba una solicitud autenticada al emisor para cambiar la clave a fin de resincronizar. Este comportamiento permitía que un intruso emprendiera un ataque de negación de servicio a través de la modificación del contabilizador en un paquete MPPE, o rechazando una petición de resincronización.

Para manejar este problema, en PPTP de manera predeterminada las claves MPPE ahora se cambian de manera predeterminada en cada paquete. Este cambio evita el ataque a la resincronización de claves.

Liberación de bits

MPPE utiliza el algoritmo de encriptación RC4, inventado en los laboratorios RSA. Una de las características de RC4 es que proporciona soporte no inherente para la protección de la integridad de datos. Esto significa que es posible *liberar* aleatoriamente los bits en el flujo de datos sin que se detecten los cambios.

Este aspecto será manejado en la próxima versión mediante el rediseño del canal de datos PPTP para incluir protección de integridad.

Falsificación de negociación PPP

Las negociaciones PPP entre el servidor y cliente PPTP no están autenticadas ni encriptadas. Por esta razón, es posible que un adversario falsifique los paquetes de negociación PPP, tales como los que contienen la dirección del servidor DNS o la dirección IP interna para que sea utilizada por el cliente. Con este fin, sería necesario insertar o modificar paquetes en el flujo de datos PPTP.

Este aspecto se tratará en la próxima versión agregando autenticación por paquete y protección de integridad para el canal de datos PPTP.

Monitoreo pasivo

Al monitorear el control PPTP y los canales de datos durante la inicialización del túnel, se puede obtener información sobre el servidor y cliente PPTP. Esta información incluye las direcciones IP de servidor y cliente, la dirección IP interna asignada al lado del cliente del túnel PPTP, las direcciones de cualquier servidor DNS interno dadas al cliente, y el nombre de usuario del cliente.

Este aspecto será tratado en la próxima versión mediante el rediseño del canal de datos PPTP.

¿Cuán importante es la buena seguridad de contraseñas?

Debido a que la seguridad PPTP esta basada en las contraseñas en Windows NT 4.0, la selección de una buena contraseña es una consideración importante de seguridad. Sin importar la longitud seleccionada de claves (40 ó 128 bits), el tamaño real del espacio de la clave se controla por la aleatoriedad de las contraseñas. El idioma inglés sólo proporciona aproximadamente 1.3 bits de

aleatoriedad por carácter.[8] Por lo que una contraseña en inglés de diez caracteres es el único equivalente para una clave de 13 bits, la cual es muy pequeña. En contraste, una contraseña de diez caracteres, compuesta de una recopilación aleatoria de mayúsculas y minúsculas, números y signos de puntuación proporcionaría la suficiente aleatoriedad para una clave de 40 bits. Por lo tanto, las contraseñas bien elegidas se pueden convertir en claves de encriptación razonablemente seguras, mientras las que se eligieron mal, no.

En la práctica, se aconseja proporcionar aleatoriedad de contraseñas comparable con la longitud de la clave seleccionada. Por lo tanto, cuando se usan las claves de encriptación de 128 bits, se requerirán por lo general contraseñas más largas. En Windows NT 4.0, las contraseñas pueden tener una longitud máxima de 14 caracteres.

Las *contraseñas mal elegidas* incluyen aquellas que:

- Están compuestas únicamente de palabras de diccionario
- Tienen sólo un tipo de letras (mayúsculas o minúsculas)
- Están creadas con nombres de personas o cosas preferidas (el apellido de soltera no es una buena contraseña, se sorprendería al saber cuántas personas lo conocen).

Contraseñas bien elegidas

- Contienen por lo menos un número y un símbolo (por ejemplo, ?) en medio de la palabra.
- Parecen garabatos al observador casual.
- No contienen nombres propios ni palabras de diccionario

Windows NT 4.0, Service Pack 2, proporciona las facilidades para reforzar la seguridad de una buena contraseña.

¿Las VPNs basadas en IPSec son más seguras que las basadas en PPTP?

No necesariamente. Como con cualquier solución VPN, la seguridad de una solución VPN basada en IPSec depende de los aspectos de la implementación. Por ejemplo, la seguridad de una solución VPN basada en claves públicas es tan buena como los mecanismos que se usan para proteger las claves privadas del usuario.

La mayoría de las implementaciones IPPSec[9, 10, 11] actuales soportan los

8 T.M. Cover y R.C. King, “Un estimado juego convergente de Entropía,” Transacciones IEEE sobre teoría de información, v. IT-24, n. 4, Julio1978, pp. 413-421.
[9] R. Atkinson y S. Kent, “Arquitectura de seguridad para el protocolo Internet" draft-ietf-ipsec-arch-sec-05.txt (trabajo en progreso), Mayo 1998.
[10] S. Kent y R. Atkinson, "Iniciador de autenticación IP," draft-ietf-ipsec-auth-header-06.txt (trabajo en progreso), Mayo 1998.
[11]S. Kent y R. Atkinson, "Carga de pago de seguridad encapsulante de IP (ESP)," draft-ietf-ipsec-esp-v2-05.txt (trabajo en progreso), Mayo 1998.

certificados de claves públicas. En teoría estos pueden generar claves más sólidas de encriptación que los mecanismos basados en contraseñas compartidas. Sin embargo, la mayoría de las implementaciones IPSec dependen de los certificados de la máquina y en consecuencia no autentican las credenciales del usuario. Esto significa que el acceso se otorga con base en la autenticación de los puntos finales de la máquina; la identidad del usuario no debe conocerse, aunque en el caso del acceso VPN, por lo regular se requiere que una autorización esté soportada. En el caso de que una máquina cliente sea accedida por más de un usuario (por ejemplo usuarios móviles o máquinas de usuarios móviles), la autorización de acceso a la red corporativa se basa únicamente en los certificados con que la máquina crea un bucle de seguridad (tales como máquinas de usuarios múltiples o de usuarios de navegación).

¿Son las VPNs basados en L2TP más seguros que las VPNs basados en PPTP?

No necesariamente. Como con cualquier solución VPN, la seguridad de una solución VPN basada en el L2TP[12]- depende de los aspectos de la implementación. Las VPN basadas en L2TP que cumplen con los estándares que requieren seguridad utilizan IPSec para proporcionar confidencialidad así como protección de integridad de mensajes[13]. En tales implementaciones, la autenticación que se basa en PPP se usa típicamente junto con IPSec, para que se pueda proporcionar autorización al usuario. Por consecuencia, las VPNs basadas en L2TP, que usan IPSec, pueden asegurarse en diversos escenarios.

¿Son seguras las fuentes externas VPN?

En las fuentes externas de VPN, la seguridad es responsabilidad del proveedor de servicio. Los datos o incluso las contraseñas pueden estar disponibles en forma no encriptada para el proveedor. En tal situación, es muy importante que el proveedor de VPN sea confiable, ya que controlará los dispositivos por medio de los cuales sus datos fluyen. Por consiguiente, es importante tener un contrato sólido con un proveedor confiable.

¿Es una solución VPN basada de servidor a servidor más segura que una solución de servidor cliente?

Varios factores pueden ayudar a que la VPN de servidor a servidor sea más segura. Por ejemplo, las contraseñas que se usan pueden ser más largas, más fortuitas y no necesitan tener sentido ya que generalmente se almacenan en disco. Estos importantes beneficios son útiles si todo el tráfico VPN puede canalizarse a través de estos servidores. Una solución basada en servidor también demanda un

[12] K. Hamzeh, et al., "Protocolo de túnel nivel 2—L2TP," draft-ietf-pppext-l2tp-10.txt (trabajo en progreso), Abril 1998.
[13] B. Patel y B. Aboba, "Asegurando L2TP que usa IPSEC," draft-ietf-pppext-l2tp-security-02.txt, Mayo 1998.

requerimiento para que la sólida seguridad física proteja los servidores.

¿Qué son las tarjetas inteligentes?

Las tarjetas inteligentes son pequeños dispositivos del tamaño de una tarjeta de crédito. Las tarjetas contienen una CPU y una pequeña cantidad de memoria de acceso al azar, y tienen varias defensas contra daños eléctricos y mecánicos. Se usan comúnmente para almacenar credenciales de autenticación (como certificados de clave pública), claves de encriptación, información de cuenta, etc. La mayoría de las tarjetas inteligentes no funcionan sin un PIN u otra contraseña para abrir los contenidos. La mayoría de tarjetas útiles implementan algoritmo de encriptación, para que las claves de encriptación nunca dejen la tarjeta inteligente.

¿Soporta Microsoft la autenticación de tarjeta inteligente para las VPNs?

La autenticación de tarjeta inteligente no tiene soporte en Windows NT 4.0. sin embargo, en Windows 2000, Microsoft planea dar soporte a la autenticación de tarjeta inteligente para conectarse a Windows NT y usarse con RAS, IPSec, L2TP, y PPTP.

¿Qué son las tarjetas de contraseña?

Las tarjetas de contraseña de diferentes proveedores trabajan de distintas maneras, pero básicamente todos son generadores de contraseña de hardware. Por ejemplo, algunas tarjetas tienen una pequeña pantalla LCD y un teclado como el de una calculadora. El usuario registra un PIN y la tarjeta representa visualmente un código numérico, el cual se usa como contraseña. Normalmente, las tarjetas de contraseña se diseñan para que produzcan un solo código determinado. Las tarjetas de contraseña funcionan bastante bien para las aplicaciones de marcación (como RAS) o autenticación del *Host*. Debido a que las aplicaciones de red de tarjetas de contraseñas por lo general están basadas en servidor/cliente, las tarjetas de contraseñas (y otros esquemas de contraseña) pueden ser vulnerables a ataques repetidos y están expuestos a ser descubiertos casualmente.

¿Cuáles son los intercambios entre tarjetas inteligentes y tarjetas de contraseña y seguridad basada en contraseña?

Las tarjetas de contraseña frecuentemente son inconvenientes y en su mayoría están concesionadas. A menudo los servidores de autenticación de tarjeta de contraseña no producen claves de encriptación que se usen para proteger los datos de usuarios de red. Normalmente las soluciones de tarjetas de contraseña soportan autenticación inicial, pero sin la protección de integridad de mensajes ni encriptación de datos es posible que las sesiones inicialmente autenticadas sean capturadas después o descubiertas en la línea. Por consiguiente, se aconseja a los clientes que desean protección de robo o confidencialidad de datos usar

soluciones que proporcionen generación de claves, tales como tarjetas inteligentes basadas en clave pública. Las tarjetas inteligentes de clave pública son bastantes seguras y convenientes, pero son caras por el momento y sólo unos cuantos paquetes de acceso remoto dan soporte a su uso.

PARA MAYORES INFORMES

Para la información más reciente sobre Windows NT Server, verifique nuestro sitio World Wide Web en http://www.microsoft.com/ntserver y el Foro Windows NT Server en Microsoft Network (GO WORD: MSNTS).

Otros sitios para visitar incluyen:

The Windows NT Communication Services home page:

http://www.microsoft.com/communications

The Microsoft security Web site:

http://www.microsoft.com/security

Para mayores informes sobre PPTP:

http://www.microsoft.com/communications/pptp.htm

Para mayores informes en acceso remoto y ruta de Microsoft:

http://www.microsoft.com/communications/routing&ras.htm

Para mayores informes sobre tarjetas inteligentes:

http://www.microsoft.com/smartcard/

Para mayores informes sobre plataforma Windows:

http://www.microsoft.com/windows/

Para mayores informes sobre herramientas e información:

http://www.microsoft.com/msdn/

Para una serie de documentos de Windows NT Server:

http://www.microsoft.com/ntserver

Para mayores informes sobre el programa beta de Windows 2000:

http://ntbeta.microsoft.com