(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 554 491**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/00 (2013.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.01.2011 E 11700203 (0)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2548353**

(54) Título: **Aparatos y método de aplicación de una directiva de ordenador**

(30) Prioridad:

11.01.2010 GB 201000288

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.12.2015

(73) Titular/es:

SCENTRICS INFORMATION SECURITY TECHNOLOGIES LTD (100.0%)
3 Brassey Hill
Limpsfield, Surrey RH8 0ES, GB

(72) Inventor/es:

CHANDRASEKARAN, GURUPARAN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Aparatos y método de aplicación de una directiva de ordenador

La presente invención se refiere a un método, a un dispositivo cliente y a un servidor para realizar una operación de firma criptográfica.

Las políticas de seguridad corporativa (PE) son una parte vital de la gobernanza de la seguridad corporativa. Estas políticas se ponen en grave riesgo cuando a los empleados se les permite vagar con el activo más vital de una organización – información. Este es un problema extremadamente importante que es también muy difícil de tratar satisfactoriamente.

Por ejemplo la política corporativa podría requerir a cualquier portátil corporativa proteger los datos almacenados en él, incluso en caso de robo, es decir, incluso si un adversario tiene acceso físico al ordenador portátil y se lleva fuera de los límites de la empresa (en el que la política se aplica típicamente). Del mismo modo, los ordenadores portátiles corporativos llevados a casa de una manera autorizada por los empleados todavía deben regirse por la política corporativa, a pesar de que el portátil esté fuera de las instalaciones corporativas.

Las políticas de seguridad existentes son típicamente complejas y requieren mucho tiempo para gestionarse debido a la necesidad de replicar las claves de cifrado cuando empleados se mueven entre las oficinas y trabajan en una variedad de diferentes dispositivos informáticos, tanto dentro como fuera del ámbito corporativo. Cuando un empleado deja el empleo, todas las claves de cifrado correspondientes deben ser revocadas. Estas cuestiones de gestión de claves representan costes significativos a las empresas que intentan hacer cumplir las políticas de seguridad en una fuerza de trabajo móvil y cambiante.

Es un objeto de la presente invención, al menos aliviar estas dificultades.

De acuerdo con un primer aspecto de la presente invención, se proporciona un método de acceso a una clave criptográfica específica del usuario almacenada en un servidor remoto con el fin de realizar una operación de firma criptográfica tal como se establece en la reivindicación 1.

Este aspecto se extiende a un dispositivo cliente como se establece en la reivindicación 8.

Este aspecto se extiende además a un servidor tal como se establece en la reivindicación 12.

La condición de acceso puede estar relacionada con la clave criptográfica y/o a los datos almacenados en forma cifrada en el dispositivo cliente.

El dispositivo cliente comprende un módulo de seguridad criptoprocesador o hardware seguro. De esta manera se puede proporcionar un entorno seguro (por ejemplo, un módulo de plataforma segura).

"Implementing Trusted Terminals with TPM and SITDRM" por S. Stamm, NP Sheppard, y R. Safavi-Naini, Electronics Notes in Theoretical Computer Science 197 (2008) 73-85, describe el uso de módulos de plataforma fiables para controlar el uso y la difusión de la información electrónica.

El dispositivo cliente está configurado preferentemente para contener la clave de cifrado en la memoria volátil (por ejemplo, RAM) y para borrar la clave criptográfica de la memoria después de realizar la operación criptográfica.

La identidad del usuario puede ser verificada por el dispositivo cliente y/o el servidor remoto.

El dispositivo cliente puede ser configurado para validar la identidad del servidor.

La condición de acceso puede constituir una política de seguridad.

En contraste con los métodos existentes de la aplicación de una directiva de equipo, en la realización preferida:

-claves criptográficas (utilizadas para proteger los datos) preferentemente no son almacenadas a largo plazo en los dispositivos cliente;
-el sistema puede controlar si las claves de cliente se ponen a disposición de los dispositivos cliente (la aplicación de la política de este modo) debido a su capacidad para identificar de forma remota tanto dispositivos como usuarios, y para verificar la integridad de los dispositivos remotos.

Esto permite que la aplicación de políticas centradas en el servidor incluso en dispositivos remotos. Esta aplicación de políticas puede tener lugar a través de cualquier entorno distribuido como la nube.

Además de y separada de la noción de la identidad del usuario, la identidad de la máquina se utiliza para permitir que las políticas complejas y más expresivas se definan y se ejecuten. Esto permite a los administradores del sistema especificar lo que un usuario particular puede hacer, y también lo que un usuario puede hacer cuando utiliza una máquina en particular.

El servidor remoto puede transmitir uno o más certificados junto con la clave criptográfica. Se puede transmitir una pluralidad de claves criptográficas en el dispositivo cliente.

En algunas realizaciones, computación de confianza se utiliza para la aplicación de la política con la descarga de un perfil de usuario que contiene claves secretas específicas del usuario.

Esto difiere de otras aplicaciones (por ejemplo, la aplicación de descarga de software de confianza) de las siguientes maneras:

-un perfil de usuario es algo específico a un usuario, no una pieza del software de propósito general;
-control basado en políticas de acceso a partes específicas del perfil de usuario permite un control basado en políticas de acceso a las claves secretas y privadas de manera flexible - por ejemplo, la política puede permitir la liberación de teclas de bajo grado a las plataformas en una clase amplia, pero solo permitir la descarga de claves de alto grado a plataformas muy específicas en un conjunto muy específico de posibles estados de software;
-control basado en políticas de un perfil de usuario permite muchas otras aplicaciones posibles, ya que da un acceso flexible a las claves criptográficas (que pueden ellas mismas ser utilizadas para controlar el acceso a otros servicios y/o información).

Cualquier característica opcional de uno de los aspectos puede ser una característica opcional de cualquier otro aspecto, siempre que sea apropiado.

Ciertas realizaciones preferidas de la invención se describirán ahora a modo de ejemplo solamente.

Componentes

Una realización preferida incorpora los siguientes dispositivos:

1. un dispositivo informático de servidor, preferentemente ofreciendo servicios web;

2. un dispositivo de cliente de agente de usuario que está equipado con un módulo de plataforma segura (TPM) que se ajusta a las especificaciones del grupo de computación de confianza (o cualquier otro dispositivo o sistema que ofrezcan servicios de seguridad similares).

Cada TPM de agente de usuario está equipado con un par de claves criptográficas pública/privada, proporcionando la base para una identidad (máquina) única de agente de usuario. Debido a la forma en que está diseñada, y teniendo en cuenta sus propiedades inviolables, la clave privada TPM no está disponible fuera del TPM, por lo que el robo de identidad del dispositivo cliente es extremadamente difícil.

Protocolo cliente-servidor

Para que el servidor verifique la identidad del agente de usuario, y así utilizarlo en la aplicación de políticas, se aplica el siguiente protocolo:

1. El dispositivo de agente de usuario/cliente verifica el servidor. Esto se hace mediante la verificación de una firma producida por el servidor y la comprobación de la clave pública del servidor (programada en el agente de usuario).

2. El servidor verifica el agente de usuario interrogando al TPM. El servidor desafía el TPM, solicitando la TPM para calcular una firma utilizando una clave privada que pertenece al TPM. Tenga en cuenta que la clave privada del TPM nunca sale del TPM en forma no cifrada, y por lo tanto no puede ser robada (por ejemplo a través de software malicioso ejecutado en la plataforma de cliente).

Una vez que la identidad de dispositivo físico del agente de usuario ha sido autentificada, la verificación del usuario se realiza a través de un mecanismo de autenticación de usuario adecuado, por ejemplo, involucrando contraseñas, pares de claves criptográficas, y/o biometría. El sistema permite la identificación de combinaciones arbitrarias de los dispositivos y usuarios, es decir, un único usuario puede emplear múltiples dispositivos, y un único dispositivo puede ser empleado por múltiples usuarios. La política entonces se puede hacer cumplir en consecuencia.

Verificación remota del agente de usuario

La política puede limitar la funcionalidad del sistema, por ejemplo mediante la desactivación de la conectividad a Internet sin control cuando se conecta a una VPN corporativa con el fin de evitar la fuga de datos a través de la Internet (insegura). El agente de usuario puede ser programado para hacer cumplir estas políticas.

Sin embargo, mediante el uso de la combinación de control de servidor de claves y el TPM en la plataforma de cliente, la solución que se describe puede también proporcionar una seguridad al servidor que en realidad se está aplicando la política. Supongamos que un agente de usuario modificado, malicioso, informa al servidor que está aplicando la política, cuando en realidad no lo hará. El servidor puede verificar la integridad del sistema remoto a través de su TPM, y por lo tanto detectar la presencia de un agente de usuario modificado, utilizando el siguiente procedimiento.

1. En el momento del arranque, el TPM comprueba la integridad del sistema operativo, y registra con seguridad mediciones características del software que se ha cargado.

2. El sistema operativo, cuya integridad está garantizada por las medidas TPM hechas en el momento de arranque, verifica la integridad de la aplicación del usuario. Los resultados de esta medición también se almacenan internamente en el TPM.

3. Cuando el servidor autentica la identidad del dispositivo remoto, también confirma su integridad. Es decir, el proceso de autenticación implica la transferencia del TPM en el servidor de las mediciones de integridad a que se hace referencia en las etapas 1 y 2; esta transferencia se lleva a cabo de tal manera que el servidor puede verificar que las mediciones de hecho provienen de un TPM genuino incrustado en la plataforma con la que se está comunicando. Esto se logra mediante el TPM firmando digitalmente las mediciones de integridad utilizando una clave privada verificable única para ese TPM. Este proceso se conoce como atestación.

4. El servidor procesa las mediciones de integridad para la plataforma del cliente, y decide si son o no indicativas de un entorno de procesamiento coherente con la política de seguridad en vigor.

5. Si se cumplen los requisitos de la política, el servidor transfiere las claves criptográficas en el dispositivo de tal manera que la plataforma de cliente solo será capaz de descifrar si las mediciones de integridad que se ha enviado en el mensaje 3 siguen siendo válidas. Esto utiliza la funcionalidad conocida como almacenamiento sellado (como se describe por ejemplo en el documento The Trusted Platform Module (TPM) and Sealed Storage, Bryan Parno 21 de junio de 2007, disponible en www.rsa.com/rsalabs/technotes/tpm/sealedstorage.pdf). Esto une de manera efectiva la política de seguridad al conjunto de claves descargadas en la plataforma del cliente, es decir, para que las claves solo estén disponibles para las plataformas de cliente que cumplan los requisitos de la política.

Este procedimiento muestra la importancia de la noción de identidad de la máquina para asegurar que la política se está aplicando en un entorno remoto. Se cree que la combinación de la gestión de claves centradas en el servidor y el uso de medidas de integridad basadas en TPM (incluyendo certificación y almacenamiento sellado) son únicos en la presente realización.

Aplicación de políticas basadas en claves

La política puede y suele limitar el acceso a información sensible mantenida en el dispositivo cliente. Los datos encriptados pueden ser divulgados libremente, asumiendo que las claves necesarias para el descifrado se mantienen en secreto. Por lo tanto, el problema de limitar el acceso a los datos puede ser transformado a un problema de gestión de claves; al negar a un usuario acceso a las claves, el usuario no puede acceder a los datos (cifrados).

Realizar el control de la política de esta manera proporciona ventajas significativas, especialmente con dispositivos remotos. Si un dispositivo remoto mantiene datos en texto común y fue robado, los datos se pueden leer mediante el análisis de los contenidos del disco duro directamente, independientemente de cualquier restricción de acceso aplicada del sistema operativo o la presencia de un TPM. Esto es imposible si los datos son encriptados y las claves de descifrado necesarias no se almacenan en el dispositivo cliente.

Para hacer cumplir las políticas en relación con el tratamiento de los datos sensibles, se utiliza el siguiente mecanismo:

1. Los datos se cifran con una clave generada y se mantienen en el servidor.

2. Si se permite que un usuario acceda a los datos por la política en vigor, el servidor da a conocer la(s) clave(s) de descifrado necesaria para el agente de usuario, solo después de la máquina principal del agente de usuario y el usuario se han autenticado. El usuario final nunca conoce la clave del agente de usuario dado que la clave nunca se almacena (en texto plano) en el disco duro de la máquina del cliente, y se almacena solo en la memoria protegida,

inaccesible desde (dichos) depuradores. Estas propiedades se aplican debido a que la integridad del sistema ha sido verificada por el servidor, por ejemplo, usando un procedimiento de certificación TPM. Debido a que el usuario final nunca conoce las claves de descifrado, es posible revocar dichas claves y por lo tanto revocar el acceso a los datos, por la simple eliminación de claves de la memoria del agente de usuario.

3. Para permitir el acceso a datos sin conexión, el agente de usuario puede (sujeto a la política) almacenar la clave de cifrado de datos en el disco de forma encriptada. La clave utilizada para cifrar la clave de datos está protegida mediante la función de almacenamiento de sellado del TPM, con lo que la recuperación de formas no autorizadas es impracticable debido a las propiedades inviolables del TPM. Solo cuando el sistema cliente está ejecutando el conjunto adecuado de software (incluyendo el agente de usuario válido) permitirá el TPM que la tecla clave de encriptación sea descifrada - utilizando la funcionalidad de almacenamiento sellado.

La nueva combinación de *centricidad del servidor* para gestionar las políticas (y las claves), y el uso de un entorno seguro, como un TPM para verificar el cumplimiento de políticas y permitir el uso de datos fuera de línea, permite una sólida gestión de la política empresarial basada en el servidor y la aplicación en los dispositivos remotos.

Transferencia de perfil

Pasamos ahora a una explicación detallada de la transferencia de perfiles de usuario desde un servidor a un dispositivo cliente.

Introducción

La palabra "perfil" se utiliza aquí para referirse a un conjunto de datos específicos del usuario almacenados en un servidor central. Este perfil incluye cosas tales como claves criptográficas e información de políticas relativas a esa persona, por ejemplo, las aplicaciones que él/ella está autorizado a utilizar, y en qué circunstancias deben descargarse las claves a un cliente. El término perfil se utiliza libremente - bien puede ser apropiado para descargar solo partes de la información de perfil a una máquina cliente, con la elección de los elementos en función del tipo de cliente que se utiliza, y/o las necesidades específicas de los usuarios en el momento de descargar.

Dividimos la descripción del protocolo de transferencia de perfil en tres fases: una fase preliminar (configuración), y dos fases principales. Mientras que la fase de configuración solo se realiza una vez por cada entidad pertinente, las otras dos fases se llevarán a cabo cada vez que un usuario desea hacer uso de una máquina cliente, es decir, para cada sesión. Las principales fases (*Fases I* y *II*) se describen aquí por separado para simplificar la explicación; sin embargo, en la práctica, las implementaciones pueden solaparse por ejemplo, mensajes que implementan la Fase I podrían ser enviados al mismo tiempo que algunos de los mensajes que implementan la Fase II.

Cada usuario y todos los servidores deben realizar la fase de configuración antes de participar en el protocolo. Esta fase establecerá todas las claves y perfiles de usuario necesarios a largo plazo. Una vez realizado, no será normalmente necesario realizar la fase de configuración de nuevo, a menos que haya ocurrido un compromiso de seguridad o si el estado del usuario ha cambiado.

La Fase I tiene por objeto permitir a la plataforma del cliente y al servidor compartir una clave de sesión secreta, que luego puede ser utilizada tanto para proteger la transferencia del perfil de usuario en la Fase II.

En la Fase II, el cliente (con seguridad) pide el perfil del servidor - la solicitud se puede autenticar utilizando la clave de sesión establecida en la Fase I. La solicitud podría, por ejemplo, indicar que tipos de clave se requieren. El servidor entonces selecciona las partes pertinentes del perfil para enviar al usuario, genera algunos pares de claves y/o claves secretas necesarios a corto plazo, genera los certificados de clave pública necesarias a corto plazo, y monta el material que se enviará al usuario. Este paquete de datos de perfil es entonces encriptado y protegida la integridad utilizando la clave de sesión establecida en la Fase I, y el paquete se envía al cliente. Tras la recepción de los datos del perfil del servidor, el cliente lo verifica y lo descifra, y procesa la información lista para su uso.

Fase de configuración

Los objetivos de esta fase preliminar son dotar a las partes implicadas en el esquema con los recursos que necesitan para participar en el protocolo. Dividimos esta discusión en tres partes, que cubren los requisitos de configuración para el servidor, el usuario y el cliente.

Configuración de servidor

Para establecer un servidor para soportar el esquema, se llevan a cabo las siguientes etapas:

1.-El software necesario se instala.

2.- Se prevé permitir el almacenamiento seguro de los perfiles de usuario y las contraseñas de usuario.

Configuración de usuario

Para que un usuario pueda empezar a utilizar el programa, se realizan las siguientes etapas:

1. El usuario establece una relación con un servidor. Esto podría, por ejemplo, ser una relación de pago de tasa contractual (donde el servidor está proporcionando un servicio al usuario), o una relación que surge 'por defecto', con el empleo del usuario en que el servidor está ejecutado por, o en nombre de, el empleado.

2. El usuario selecciona una o más autoridades de certificación (CAs) que serán las responsables de generar los certificados de claves públicas de los usuarios. Por supuesto, dependiendo de la relación del servidor con el usuario, esto puede hacerse automáticamente para el usuario por el servidor.

3. El usuario establece una contraseña secreta compartida con el servidor.

4. El servidor crea un perfil para el usuario. El usuario especifica (o ha seleccionado automáticamente) qué tipos de claves se requieren. El servidor generará entonces las claves secretas necesarias y pares de claves asimétricas, y obtener certificados para las claves públicas de una o más CAs. (Tenga en cuenta que la única clave a largo plazo necesaria como parte del perfil de usuario puede ser un par de claves de firma.)

5. El servidor entonces almacena de forma segura el perfil (que contiene, por ejemplo, claves secretas, pares de claves asimétricas y certificados de clave pública que se acompañan) junto con la contraseña de usuario u otros datos de identificación del usuario. Tenga en cuenta que cada clave tiene cierta información asociada con ella, incluyendo un identificador para el algoritmo con el que se va a utilizar, el uso previsto (por ejemplo, el cifrado, la generación de MAC, la generación de la firma, etc.), y un período de validez.

Configuración del cliente

Para que un dispositivo cliente sea empleado por un usuario como parte del plan, se realizan las siguientes etapas:

1. El software adecuado está instalado en el cliente (sin embargo, esto podría llevarse a cabo de forma dinámica mediante la descarga desde el servidor, por ejemplo, como un applet de Java, en el momento de uso).

2. El TPM del equipo cliente se inicializa, y el servidor se hace capaz para hacer frente a una plataforma que contiene el tipo de TPM u otro entorno de seguridad en uso en la máquina cliente.

Fase I

El principal objetivo de esta fase es establecer una clave de sesión secreta de corta duración entre la máquina cliente y el servidor. Ahora discutiremos posibles formas de realización de esta fase del protocolo.

Tenga en cuenta que, con el fin de asegurar que el perfil solo se pone a disposición una plataforma que ejecuta el software de confianza, la funcionalidad informática de confianza puede ser utilizada para verificar el entorno de software en la plataforma (cliente) destinataria. Esto debe hacerse de tal manera que solo una plataforma confiable tendrá acceso a la clave de sesión de corta duración. Sin esta clave, el perfil enviado desde el servidor al cliente no se puede descifrar, y por lo tanto no estará disponible para el cliente, es decir, el control de la política se ejerce a través del acceso a la clave de sesión de corta duración.

Posibles medios para establecer la clave de corta duración se discuten a continuación. Las formas en que este proceso se puede hacer dependiendo de la informática de confianza se discuten más adelante.

Un enfoque trivial

Un enfoque muy simple es que ambas partes deriven simplemente una clave de la contraseña secreta compartida. Con el fin de garantizar que una clave diferente se utiliza para cada sesión, una de las dos partes podría primero generar un número aleatorio r, por ejemplo, de 128 bits, y enviarlo a la otra parte. Tanto el servidor y el cliente entonces podrían generar la clave de sesión como $K = h(p||r)$, donde h es una función de comprobación aleatoria criptográfica (por ejemplo, SHA-256, [5]), p es clave secreta del usuario, y || denota concatenación de cadenas de bits.

Aunque muy simple, este enfoque tiene una gran debilidad. Si un atacante intercepta *r* y también intercepta algunos datos cifrados utilizando la clave de sesión *K*, a continuación, el siguiente *ataque de diccionario fuera de línea* es posible si *p* se extrae de un conjunto de posibilidades demasiado pequeño:

- El atacante trabaja a través del conjunto de todas las contraseñas posibles de una en una, eliminando incorrectas 'conjeturas' de la siguiente manera sencilla. Supongamos que p* es un valor candidato para la contraseña. El atacante calcula la clave de sesión candidato correspondiente K* = h(p*||r), utilizando el valor interceptado de r. El

atacante intenta descifrar el texto cifrado interceptado usando K*; si el resultado no produce un texto claro significativo luego la contraseña candidata puede ser eliminada.

De hecho, es algo difícil de memorizar fácilmente las contraseñas que se toman a partir de un conjunto suficientemente grande para evitar este tipo de ataques. Incluso si suponemos que los usuarios eligen contraseñas de 8 caracteres, con cada carácter siendo una letra o un número, entonces el número de posibles contraseñas es solo $36^8 \approx 2{,}8 \times 10^{12}$. Trabajando a través de un conjunto de este tamaño no es factible (aunque no trivial).

Por tanto, es deseable utilizar un enfoque más sólido, por ejemplo, a lo largo de las líneas que se proponen a continuación.

Un enfoque basado en SSL

Otro enfoque relativamente simple es exigir al servidor establecer primero una sesión de capa de zócalos seguros (SSL) con la máquina cliente. La máquina cliente debe tener un medio para verificar que la sesión se ha establecido con el servidor apropiado. Esto podría, por ejemplo, implicar que el software descargado al cliente sea equipado previamente con una copia de confianza de la clave pública del servidor.

Una vez que la sesión SSL está en su lugar, el software de cliente podría entonces solicitar al usuario introducir su contraseña, que puede ser enviada al servidor (a través del canal SSL) para su verificación. Dado que la contraseña se comunica sobre un canal cifrado (según lo dispuesto por SSL), está protegida contra el compromiso por un interceptor.

El canal SSL también se podría emplear en la Fase II para proporcionar un medio seguro de transmisión para el perfil.

Hay una desventaja importante de este enfoque. El cliente debe tener los medios para verificar que se está hablando con el servidor correcto, o de otra forma pueden ser lanzados ataques intermediarios. Si el software que es utilizado por el cliente contiene la clave pública del servidor, entonces, se evita este problema - sin embargo, esto significa que el software que se utilizará en una máquina cliente debe ser personalizado para incluir la clave pública del servidor en particular con el que el usuario tiene una relación de confianza.

Puede haber situaciones en que esto puede ser difícil de organizar. El problema anterior se evita mediante la solución que se describe inmediatamente a continuación.

Un enfoque basado en estándares

Hay una serie de protocolos bien establecidos que están diseñados para permitir que una clave de sesión secreta sea establecida usando una contraseña del usuario memorizable de tal manera que los ataques de diccionario fuera de línea no son posibles. Además, dichos protocolos también pueden ser diseñados para frustrar ataques más activos (siempre y cuando alguna medida está en su lugar para contar los intentos de autenticación fallidos y tomar contramedidas apropiadas).

Tres de estos protocolos se especifican en la cláusula 6 de la norma ISO/IEC 11770-4 [6], llamados allí *Mecanismos de Acuerdo de Claves 1, 2 y 3*. Todos estos mecanismos se cree que son seguros, y cualquiera de ellos sería adecuado para su uso en el esquema. A continuación consideramos sus ventajas y desventajas relativas.

Propiedades de seguridad

Los tres de los mecanismos en ISO/IEC 11770-4 tienen características de seguridad muy similares. La única diferencia significativa (con los conocimientos actuales) es que el mecanismo 1 requiere que el servidor conozca la contraseña, mientras que los otros dos mecanismos solo requieren que el servidor almacene el hash de la contraseña. Esta última propiedad puede tener algunas (pequeñas) ventajas prácticas.

Cuestiones de aplicación

Hay algunas diferencias en las propiedades entre las opciones, como sigue:

-El mecanismo 1 (SPEKE) puede ser implementado utilizando tres flujos de mensajes; mecanismos 2 (SRP6) y 3 (AMP) requieren al menos cuatro flujos de mensajes;
-Los mecanismos 1 y 3 se pueden implementar tanto en la configuración de registro discreta "estándar" y el ajuste de la curva elíptica;
-El mecanismo 2 solo se puede implementar en el la configuración de registro discreta "estándar";
-Se cree que los tres mecanismos tienen costes de computación similares, aunque las diferencias no han sido revisadas en detalle.

Una implementación usando SPEKE

Para aclarar la discusión anterior, damos una descripción simplificada de la Fase I en el caso en que se utiliza Mecanismo 1 de la norma ISO/IEC 11.770-4.

1. Proporcionar el nombre de usuario y contraseña. El usuario tendrá que ejecutar el software cliente y equiparlo con el nombre del usuario y la contraseña. Puede ser apropiado para el usuario proporcionar información adicional en esta etapa, como los tipos de claves que al usuario le gustaría haber descargado del servidor (por ejemplo, la información que se utilizaría en la fase II).

2. Solicitar perfil (fase I). El software de cliente le enviará un mensaje al servidor para solicitar el inicio del proceso de descarga del perfil.

3. Establecer la clave de sesión (fase I). El servidor y el cliente ahora utilizan el protocolo SPEKE, tal como se especifica en la cláusula 6.1 de la norma ISO/IEC 11770-4 [6], para establecer una clave secreta compartida.

Ahora explicamos en un poco más de detalle cómo las etapas 2 y 3 podrían aplicarse. Se hace referencia a las descripciones en la cláusula 6.1 de la norma ISO/IEC 11.770-4 [6]. Suponemos que el cliente corresponde a A en 11770-4 y el servidor corresponde a *B*.

1. El software cliente realiza la etapa de construcción del testigo del símbolo de clave (A1) que se especifica en la cláusula 6.1.3 utilizando la contraseña proporcionada por el usuario n.

2. El software de cliente envía wA a B, junto al nombre de usuario y una solicitud para inaugurar la descarga del perfil.

3. Una vez recibido el mensaje del cliente, el servidor recupera la contraseña de usuario π del perfil de usuario (indexados por el nombre de usuario) y lleva a cabo la etapa de construcción del testigo de clave (B1) especificado en la cláusula 6.1.3 usando π.

4. El servidor envía wB a A.

5. El servidor utiliza el valor recibido de wA en la etapa B2 para obtener la clave secreta compartida Ki.

6. Una vez recibido el mensaje del servidor, el cliente utiliza el valor recibido de wB en la etapa A2 para obtener también la clave secreta compartida Ki.

Tenga en cuenta que las etapas de confirmación clave se omiten, dado que la fase II proporciona un grado de (solo ida) confirmación de la clave. Tenga en cuenta también que puede ser útil para el cliente (A) generar un identificador de sesión aleatoria y enviarlo al servidor (B) en la etapa 2 anterior. El servidor debe enviar ésta de vuelta al cliente en la etapa 4, que permite al cliente hacer coincidir las respuestas con las solicitudes.

Fase II

El principal objetivo de esta fase es descargar de forma segura los datos de perfil de usuario desde el servidor a la máquina cliente.

Hay una variedad de maneras en que esto podría ser implementado. Le damos una opción.

El protocolo de transferencia tiene la siguiente forma general.

1. Cliente → Servidor: Solicitud de perfil

Este mensaje de solicitud especifica qué tipos de clave se necesitan por la máquina cliente. Por ejemplo, si el usuario solo necesita llevar a cabo operaciones de firma, entonces la información de perfil que debe proporcionarse al usuario solo necesita incluir una clave privada de firma (y el certificado para la clave pública correspondiente).

Tenga en cuenta que este mensaje podría ser enviado al mismo tiempo que uno de los mensajes en la Fase I. Sin embargo, puede ser necesario proteger a la integridad y, posiblemente, cifrar este mensaje. Si es así, entonces solo puede ser enviado después de que el equipo cliente ha obtenido una copia de la clave de sesión.

2. Servidor: Preparar el perfil

Una vez que la solicitud ha sido recibida (y verificada) por el servidor, realiza las tareas necesarias para preparar los datos que se envían a la máquina cliente.

Todas las claves y certificados necesarios son puestos en un perfil con formato, listo para ser descargado al cliente.

3. Servidor → Cliente: Perfil cifrado

Una vez que los datos del perfil han sido montados por el servidor, incluyendo claves y certificados, pueden ser enviados al cliente. Antes de la transmisión deben ser cifrados por el servidor utilizando la clave de sesión. El método de cifrado debe proporcionar tanto la confidencialidad y la protección de la integridad, y una de las técnicas que figuran en la norma ISO/IEC 19772 [7] es muy recomendable.

Tenga en cuenta que este mensaje podría ser enviado al mismo tiempo como uno de los mensajes en la Fase I, siempre y cuando la clave de sesión necesaria esté disponible en el servidor.

4. Cliente: Proceso del perfil recibido

Por último, en el recibo del perfil de cifrado, el cliente puede verificar y descifrar con la clave de sesión secreta.

Como se discutió anteriormente, un perfil normalmente será generado para cada usuario. Un perfil de usuario contiene una serie de claves y certificados. Algunas o todas estas claves y certificados se pueden enviar a continuación a la máquina cliente cada vez que se establece una sesión.

Este enfoque tiene la ventaja de que el servidor no necesitará generar nuevas claves o certificados cuando un cliente solicita un perfil, ya que todas las claves necesarias se generan por adelantado. Además, cada clave pública tendrá un único certificado asociado a ella, firmado por una CA de confianza

Sin embargo, este enfoque tiene la desventaja de que, si una máquina cliente está comprometida alguna vez, entonces las claves privadas de largo plazo del usuario también están comprometidas. Por otra parte, mientras que la revocación de la clave es posible, esto solo se produce si se detecta el compromiso, y esto no siempre será el caso.

Finalmente tened en cuenta que puede haber una necesidad de "descomprimir" el perfil para proporcionar claves y/o certificados de otras aplicaciones en el equipo cliente. Si las claves privadas están entonces fuera del control directo del sistema de la invención, puede ser difícil asegurar que estas claves se eliminan al final de una sesión.

El uso de informática de confianza

El hecho de que el dispositivo cliente puede no ser digno de confianza trae consigo importantes riesgos de seguridad. Si el servidor puede verificar que el software correcto se está ejecutando en un cliente (y que el entorno de sistema operativo cliente es seguro) antes de descargar el perfil al cliente, entonces, el perfil de seguridad se puede mejorar significativamente.

Tal capacidad es ofrecido por informática de confianza (véase, por ejemplo, [8]). Esta tecnología ya está presente en una proporción significativa de los nuevos PCs, en forma de un chip de seguridad de finalidad especial conocido como módulo de plataforma segura (TPM). La tecnología permite que un dispositivo verifique de forma remota la naturaleza del software que funciona en otra plataforma, y de restringir el acceso a los secretos a las configuraciones de software específicas. Estas propiedades parecen ser ideales para el modelo operativo descrito anteriormente.

Consideremos ahora las funciones de computación de confianza que pueden ser utilizadas para hacer el proceso de transferencia de la política de perfil controlado. Como se mencionó anteriormente, esto implica que el acceso a la clave de sesión condicionada efímera en el servidor esta contenido con el estado de la plataforma de cliente remota.

Trabajo relacionado

La noción general de solo permitir que se produzcan ciertas cosas si una plataforma remota está en un cierto estado (como se prueba utilizando la funcionalidad informática de confianza) es una bien establecida. El protocolo de conexión de red de confianza (TNC) utiliza la computación de confianza para decidir si procede o no admitir un PC cliente en una red. Un servidor requiere que el cliente proporcione evidencia de su configuración de software antes de decidir si admite o no al cliente en la red. El TNC ha sido estandarizado por el grupo de informática de confianza http://www.trustedcomputinggroup.org/) - para una simple descripción de su funcionamiento véase, por ejemplo, Rehbock y Hunt [9].

Esta idea general también ha sido propuesta como un medio de protección de software sensible solo mediante la descarga de este software a una plataforma verificable en un estado de confianza. Esta idea ha sido descrita por Gallery, Tomlinson, Delicata y Mitchell [1], [2], [3], [4].

Un enfoque simple

El enfoque más simple para el servidor es requerir la plataforma de confianza para dar fe de su configuración actual del software inmediatamente antes de iniciar el proceso de acordar una clave secreta. Esto supone que la plataforma de cliente tiene un TPM, y el software en el cliente es capaz de utilizar el TPM para almacenar mediciones indicativas del estado actual de la plataforma de cliente en las PCRs (Plataforma de Registros de Configuración) en el TPM. El proceso de certificación a continuación, opera en los siguientes términos.

1. El servidor envía un desafío al azar para el cliente, junto con los números de serie de las PCR de cuyos valores desea tener la seguridad.

2. El cliente pasa esta información a su TPM, que firma digitalmente una cadena que contiene el desafío al azar y los valores actuales de las PCR solicitadas (junto con sus índices).

3. Esta firma se pasa de nuevo al servidor que puede verificar la firma (y comprobar la frescura del desafío al azar para) y por lo tanto verificar que estos valores de PCR son un registro preciso del estado actual del software de la plataforma del cliente.

La firma se calcula utilizando una clave de identidad certificada, una clave de firma cuyo valor privado está disponible solo para el TPM. La validez de la clave pública asociada (utilizada para verificar la firma) puede ser verificada por el servidor de control de un certificado de clave pública también suministrado por el cliente.

El servidor puede verificar que los valores de PCR coinciden con una configuración de software considerado aceptable por la declaración de la política asociada con el perfil de usuario correspondiente. Si (y solo sí) la política considera aceptable esta configuración, el servidor a continuación, procede a establecer una clave secreta compartida, como se describió anteriormente.

Un enfoque más robusto

Uno de los problemas con el enfoque descrito inmediatamente antes es la posibilidad de que el estado del software del cliente puede cambiar entre el momento en que se lleva a cabo la medición y el tiempo (poco después) cuando se establece el secreto compartido. Este problema puede ser eliminado mediante la combinación del proceso de certificación con el establecimiento de la clave secreta compartida. Los métodos para lograr esto han sido descritos en la literatura - véase, por ejemplo, Gallery, Tomlinson, Delicata y Mitchell [1], [2], [3], [4].

Referencias

[1] E. Gallery y A. Tomlinson, ‘Secure delivery of conditional access applications to mobile receivers’, en: C.J. Mitchell (ed.), Trusted Computing, IEE Press, 2005, pp.195 hasta 237.

[2] E. Gallery y A. Tomlinson, ‘Protection of Downloadable Software on SDR Devices’, en: Software Defined Radio Technical Conference SDR 05, noviembre de 2005.

[3] E. Gallery, A. Tomlinson y R. Delicata, ‘Application of Trusted Computing to Secure Video Broadcasts to Mobile Receivers’, Technical Report RHUL-MA-2005-11, Department of Mathematics de la Royal Holloway, Universidad de Londres, junio de 2005.

[4] E.M. Gallery y C.J. Mitchell, ‘Trusted computing technologies and their use in the provision of high assurance SDR platforms’, en: Proc. de 2006 Software Defined Radio Technical Conference, Orlando, Florida, noviembre de 2006.

[5] ISO/IEC 10118-3: 2003, Information technology - Security techniques - Hash-functions: Part 3: Dedicated hash-functions. International Organization for Standardization, Ginebra, 2003.

[6] ISO/IEC 11770-4: 2006, Information technology - Security techniques - Key management: Part 4: Mechanisms based on weak secrets. International Organization for Standardization, Ginebra, 2006.

[7] ISO/IEC 19772: 2009Informafion technology - Security techniques - Authenticated encryption. International Organization for Standardization, Ginebra, 2009.

[8] C. Mitchell (ed.), Trusted Computing. IEE Press, Londres 2005.

[9] S. Rehbock y R. Hunt, ‘Trustworthy clients: Extending TNC to web-based environments’. Computer Communications 32 (2009) 1006-1013.

REIVINDICACIONES

1. Un método de acceso a una clave criptográfica específica del usuario almacenada en un servidor remoto con el fin de realizar una operación de firma criptográfica, que comprende:

determinar la identidad de un usuario;
validar criptográficamente la identidad de un dispositivo de cliente usando un criptoprocesador seguro del dispositivo cliente;
determinar si la identidad del usuario y la identidad del dispositivo cliente satisfacen una condición de acceso que se almacena en el servidor remoto;
transmitir de forma segura la clave criptográfica específica del usuario desde el servidor remoto al dispositivo cliente cuando la condición de acceso está satisfecha; y
usar el criptoprocesador seguro para firmar los datos con la clave criptográfica sin revelar la clave criptográfica al usuario.

2. Un método según la reivindicación 1, en el que el criptoprocesador seguro comprende un módulo de plataforma segura.

3. Un método según la reivindicación 1 o 2, que comprende que el dispositivo cliente mantenga la clave criptográfica en la memoria volátil y limpie la clave criptográfica de la memoria después de realizar la operación de firma criptográfica.

4. Un método según cualquiera de las reivindicaciones anteriores, que comprende que el servidor valide la identidad del dispositivo cliente.

5. Un método según cualquiera de las reivindicaciones anteriores, que comprende que el servidor verifique la identidad del usuario.

6. Un método según cualquiera de las reivindicaciones anteriores, que comprende que el dispositivo cliente valide la identidad del servidor.

7. Un método según cualquiera de las reivindicaciones anteriores, que comprende que el servidor remoto transmita uno o más certificados junto con la clave criptográfica.

8. Un dispositivo cliente configurado para:

utilizar un criptoprocesador seguro del dispositivo cliente para permitir que la identidad del dispositivo sea validada criptográficamente;
recibir una clave criptográfica específica de usuario transmitida de forma segura, desde un servidor remoto; y
utilizar el criptoprocesador seguro para firmar los datos con la clave criptográfica sin revelar la clave criptográfica a un usuario

9. Un dispositivo cliente según la reivindicación 8, que comprende un módulo de plataforma segura.

10. Un dispositivo cliente según la reivindicación 8 o 9 configurado para contener la clave criptográfica en la memoria volátil y para borrar la clave criptográfica de la memoria después de realizar la operación criptográfica.

11. Un dispositivo cliente según cualquiera de las reivindicaciones 8 a 10 configurado para validar la identidad del servidor.

12. Un servidor en el que se almacena (i) una clave criptográfica específica del usuario para realizar una operación de firma criptográfica y (ii) una condición de acceso, en el que el servidor está configurado para:

determinar si la identidad de un usuario y la identidad de un dispositivo cliente satisfacen la condición de acceso; y
transmitir la clave criptográfica de forma segura al dispositivo cliente cuando se satisface la condición de acceso.

13. Un servidor según la reivindicación 12 configurado para validar la identidad del dispositivo cliente.

14. Un servidor según la reivindicación 12 o 13 configurado para verificar la identidad del usuario.

15. Un servidor según cualquiera de las reivindicaciones 12 a 14 configurado para transmitir uno o más certificados junto con la clave criptográfica.