Gestión de la confianza en redes ad hoc

Helena Rifà-Pous Jordi Herrera-Joancomartí

Universitat Oberta de Catalunya, Rb. del Poble Nou, 156
08018 Barcelona
{hrifa,jordiherrera}@uoc.edu

Resumen El despliegue de un esquema de confianza es fundamental para poder desarrollar servicios de seguridad que permitan administrar y operar una red. Sin embargo, las soluciones empleadas en las redes tradicionales no se adaptan a un entorno ad hoc debido a la naturaleza dinámica y sin infraestructura de estas redes. En el presente trabajo se propone un esquema de confianza práctico y eficiente basado en una infraestructura de clave pública distribuida, umbral y jerárquica, que no requiere sincronización temporal entre todos los nodos de la red. La autorización de usuarios en el sistema se hace a través de certificados de corta duración que eliminan la necesidad de mantener la publicación y diseminación de unas listas de revocación. Por otro lado, una entidad externa de confianza permite alargar la reputación de un usuario de la red más allá de la existencia de la propia red.

Palabras clave: redes ad hoc, seguridad, criptografía, gestión de claves, confianza.

1. Introducción

La cooperación y la confianza son características fundamentales para el despliegue funcional de una red ad hoc.[1] En este tipo de redes no existe una infraestructura de red dedicada ni un control centralizado, las transmisiones se realizan a través de la colaboración de los miembros de la red y éstos, en general, son usuarios anónimos, móviles y temporales. Establecer una red operativa en tales circunstancias requiere el uso de mecanismos de seguridad en los protocolos básicos de la red: acceso, transmisión y encaminamiento de paquetes, etc.

En el presente trabajo nos centraremos en los procesos de acceso y conexión a la red. Para ofrecer propiedades de seguridad a dichos procesos es importante definir un sistema de gestión de confianza. De forma más detallada, las acciones más importantes a tener en cuenta son las siguientes:

Identificación de usuarios Es necesario verificar la identidad de los usuarios, sino un adversario podría adoptar diferentes perfiles para entrar en el sistema una vez se le haya vetado el acceso con una credencial (ataque Sybil [1]). La identificación se realiza a través de servicios de autenticación.

[1] Ad hoc (latin): para esto, a propósito

Acceso a la red Una vez autenticado el usuario se tiene que tener en cuenta la elegibilidad para poder connectarse a la red. Sin un control de acceso seguro la red no tiene protección contra nodos maliciosos. El control de acceso se realiza a través de servicios de certificación.

Expulsión de la red Los usuarios maliciosos tienen que ser expulsados de la red para no comprometer la funcionalidad de la misma. La expulsión de usuarios se realiza a través de servicios de revocación.

Autogestión Los miembros de la red son los responsables de su administración. A través de esquemas de compartición de claves el control del sistema se puede repartir entre distintos nodos.

Existen dos modelos generales para autenticar a los nodos en una red ad hoc, los basados en clave simétrica y los basados en clave asimétrica. Los primeros, aunque más eficientes computacionalmente, tienen el inconveniente que previamente al establecimiento de la red ad hoc los nodos tienen que haberse comunicado a través de un canal confidencial y auténtico, y haber acordado un secreto compartido. Por otro lado, los modelos asimétricos están basados en criptografía de clave pública lo que permite una gestión de la confianza mucho más eficiente. En este tipo de sistemas la identificación de los usuarios en un grupo puede ser local o global. Los identificadores locales sólo tienen sentido dentro de la propia red (direcciones MAC, IPs, nombres únicos de usuario, etc..) mientras que los globales son vinculaciones permanentes entre una persona y una etiqueta y, por lo tanto, permiten crear sistemas con memoria.

El control de acceso de los usuarios a una red ad hoc se realiza a partir de su identidad y de otros datos que puedan aportar información sobre su adecuación en la red (historial del usuario, listas de acceso..). Cuando se concede el acceso a un usuario se le expide un token o certificado que así lo avale. Estos certificados de autorización tienen que ser emitidos por personas o entidades pertenecientes a la red, ya que en una red ad hoc la conexión con una autoridad externa no está garantizada.

La expulsión o revocación de miembros de una red es una de las partes más sensibles y menos solventadas en los esquemas propuestos para redes ad hoc. El problema principal estriba en que la adaptación a una red ad hoc del modelo tradicional basado en repositorios de acceso público con las listas de revocación de certificados (CRLs) no es simple. En este tipo de escenarios puede que la red no tenga conexión a ningún repositorio o servidor central con lo que es imposible acceder a la información de revocaciones. Actualmente las propuestas para solventar este inconveniente se basan en sistemas en los cuales un usuario es revocado cuando es acusado de fraudulento (por uno o más nodos), lo que implica una transmisión en broadcast de la acusación y un almacenaje y gestión local en cada nodo de las listas de control de acceso. Esta aproximación puede ser peligrosa si no se ponen medidas para salvaguardar la reputación de los usuarios honestos ya que estos podrían ser acusados injustamente por otros nodos maliciosos.

Una red ad hoc puede ser gestionada a través de una entidad centralizada o un quórum de miembros. El modelo más adecuado para una red colaborativa,

dinámica, sin infraestructura y cuyos miembros tienen todos los mismos derechos y deberes, es un modelo distribuido entre éstos. Esta funcionalidad se consigue con esquemas de compartición de secretos que permiten distribuir el control de una infraestructura de clave pública (PKI) entre un grupo de participantes de forma que la confianza de todo el sistema no recaiga en un único nodo.

En el siguiente apartado pasamos a comentar la bibliografía más relevante relacionada con la temática.

1.1. Trabajos relacionados

El núcleo de un modelo de confianza radica en los protocolos de generación y actualización de la clave central del sistema. Los esquemas de generación y compartición de secretos fueron introducidos independientemente por Blakley [2] y Shamir [3] en 1979. En sus esquemas un agente de confianza es el responsable de generar y distribuir los fragmentos del secreto.

En 1985 Chor et al. [4] introducen la idea de la compartición verificable de secretos (VSS). Los esquemas propuestos permiten verificar la corrección de los fragmentos de clave distribuidos por el agente.

En 1995 Jerecki et al. [5] introducen el concepto de compartición proactiva de secretos (PSS) en la cual los fragmentos de la clave son actualizados periódicamente para incrementar la confidencialidad del secreto. Los fragmentos comprometidos en diferentes periodos no se pueden unir para formar la clave final y por lo tanto, asumiendo que en un ciclo de refresco el número de nodos que pueden ser comprometidos es menor que el umbral de recuperación de la clave, el esquema es robusto.

A partir de aquí empiezan a aparecer modelos de PKIs distribuidas que emplean y mejoran los protocolos de gestión de claves descritos.

En [6] Zhou y Haas proponen un modelo basado en una autoridad de certificación (CA) distribuida entre t nodos de una red. En el momento de la inicialización una entidad de confianza reparte los fragmentos de la clave de la CA entre unos servidores. Posteriormente, el protocolo de gestión de claves emplea un refresco proactivo de los fragmentos con tal de adaptarse a los cambios de configuración de la red. Los costes computacionales y de transmisión de este protocolo son muy altos para dispositivos móviles de mano.

Kong et al. [7] presentan un esquema de CA distribuida entre todos los nodos de la red. La existencia de fragmentos de clave redundantes distribuidos en diversas islas de usuarios facilita la emisión de certificados para nuevos miembros de la red. De todas formas, Leahne [8] probó que el sistema no es eficiente.

Yi y Kravets proponen en [9] un esquema llamado Mobile Certificate Authority (MOCA). Este modelo limita los candidatos que poseen un fragmento de la clave de la CA a un subconjunto de nodos que son más confiables, tienen mayor poder computacional, y físicamente son menos vulnerables.

El inconveniente tanto de [6] como de los esquemas de [7,8,9] es que requieren un agente de confianza, aunque los últimos sólo lo necesitan en la fase de puesta en marcha. En [10] Pedersen implementa la primera CA umbral sin un servi-

dor de confianza que genere y distribuya los fragmentos de clave. El algoritmo está basado en el criptosistema de Desmedt y Frankel [11].

Gennaro et al. [12] mejoran la CA de [10] en cuanto a seguridad y eficiencia. La versión propuesta en su artículo es robusta incluso ante adversarios adaptativos. El criptosistema de firma usado es DSS.

Los algoritmos criptográficos basados en el problema del logaritmo discreto (cifrado ElGamal o firmas DSS) permiten construir esquemas proactivos mucho más eficientes que los basados en RSA. La regeneración de los fragmentos del secreto implica operaciones distribuidas sobre las claves y las claves, en el caso del logaritmo discreto, pertenecen a un dominio cuya estructura algebraica es pública (un grupo de orden conocido). Por el contrario, cuando utilizamos criptosistemas como RSA, el problema es más complicado porque la clave está definida sobre un dominio secreto (el orden del grupo no puede ser conocido públicamente o por los servidores involucrados). Existen algoritmos que permiten la proactivación de criptosistemas distribuidos RSA ([13]), pero la eficiencia de estos algoritmos no es tan buena como los basados en DSS.

Zhu et al. [14] introducen un esquema de PKI distribuida en estructura jerárquica. Los nodos de la red se dividen en áreas gestionadas por CAs subordinadas virtuales. De esta forma un usuario sólo tiene que contactar con los nodos de su zona para poder conseguir un certificado y a su vez, puede verificar la autenticidad de certificados de nodos de otras zonas siguiendo la cadena de certificación. Aunque este esquema es muy flexible y escalable, los dispositivos tienen que tener unos requisitos mínimos -memoria y potencia- para poder formar parte de una red de gran tamaño.

Wu et al. [15] proponen un esquema de gestión de claves llamado SEKM. La clave privada de la CA no está distribuida entre todos los miembros de la red sino solo en un subgrupo de servidores. El tráfico entre los responsables de mantener un fragmento de la clave de la CA es elevado, por lo que crear un subgrupo de nodos servidores supone una mejora en el coste computacional y de transmisión de la red. Por otro lado, el protocolo de refresco de los fragmentos de la clave de la CA está optimizado de forma que la carga de la red sea mínima. Uno de los inconvenientes de SEKM es que los certificados externos que utiliza para la identificación de los nodos de la red necesitan unas extensiones no estándares.

Finalmente, en [16] Capkun et al. describen una arquitectura totalmente distribuida basada en un modelo P2P. Los nodos tienen un repositorio con todos los certificados que han generado y los que les han sido emitidos. Cuando dos nodos se comunican combinan sus repositorios de claves para evaluar las cadenas de confianza entre ellos. El modelo de Hubaux [17], basado en PGP, sigue el mismo esquema. El inconveniente de estos sistemas es la dificultad de encontrar la métrica de autenticación apropiada para cada entorno, y la carga que supone reconstruir repositorios locales de certificados en todos los nodos.

Las carencias generales para la aplicación de los modelos de PKIs distribuidas en redes ad hoc son la falta de un esquema de repudio eficiente y efectivo, y un sistema de autorización íntegro que tenga en cuenta las acciones pasadas de un nodo a la hora de tomar una decisión.

En este artículo proponemos un esquema de confianza flexible y con la autonomía suficiente para adaptarse a las necesidades de un grupo heterogéneo, dinámico y sin el soporte de una infraestructura de red. El algoritmo de generación distribuida de una CA está basado en el protocolo definido en [12] sobre firmas DSS, y la gestión de claves se apoya sobre el modelo jerárquico de Zhu et al. [14]. Las mejoras principales del modelo propuesto respecto al descrito por Zhu et al. son las siguientes:

- Los fragmentos de la clave de la CA no están distribuidos entre todos los miembros de la red sino una parte. De esta forma se reduce la sobrecarga debido a las operaciones y comunicaciones entre los titulares.
- El criptosistema umbral (t, n) de las CAs de nivel inferior en la jerarquía puede actualizarse a (t', n') para adaptarse al entorno de red. De no ser así la PKI resultante puede tener muchos niveles jerárquicos y no ser práctica.
- Se independiza el ciclo de vida de los certificados de las marcas temporales absolutas, tolerando de esta forma que no haya sincronía entre todos los miembros de la red.
- Se eliminan las listas de certificados revocados y la necesidad que cada usuario de la red evalúe las características de autorización de los demás nodos. La posesión de un certificado de la red ya garantiza el acceso.
- Se introduce una una entidad de confianza que permite mantener y gestionar el comportamiento y la reputación de un usuario en redes colaborativas de forma que esta información sirva para evaluar la autorización de los usuarios en la propia red o en otras nuevas.

El resto del artículo está organizado de la siguiente manera. La sección 2 describe la arquitectura general del sistema. En la sección 3 se presenta el esquema de PKI distribuida y el modelo de certificados atemporales. La sección 4 detalla las funciones de una autoridad externa de soporte para el esquema de confianza. Finalmente, en la sección 5 se exponen las conclusiones.

2. Visión general del sistema

El sistema de confianza propuesto está centrado en un esquema de autorización de los nodos a la red ad hoc basado en un modelo de PKI distribuida y jerárquica. Internamente la red trabaja con los certificados de autorización emitidos por la PKI local, pero para poder conectarse a la red los usuarios deben identificarse y autenticarse con un certificado emitido por una CA externa. Todos los protocolos de gestión distribuida de claves necesitan establecer canales seguros y auténticos entre los nodos participantes y por lo tanto, la asunción de una CA externa o en su defecto un sistema de confianza P2P o de vista directa entre los miembros es necesario y requerido en todos los esquemas.

A continuación introducimos la arquitectura del sistema a partir de una ejemplificación del ciclo de vida de una red ad hoc.

1. **Inicialización de la red.**

Asumimos que todos los usuarios de la red deben poseer un certificado de identidad válido emitido por una CA externa y fuera de línea y que además, deben tener un repositorio de certificados de confianza (p.e. el repositorio del propio navegador web) que les permita validar certificados de CAs globales y reconocidas.

Suponemos que inicialmente hay 3 usuarios que se quieren comunicar y deciden crear una red cooperativa con una CA compartida umbral de tipo $(3, 3)$. Los usuarios se autentican mutuamente utilizando sus certificados de identidad. Si la autenticación no se lleva a cabo con éxito se aborta la operación.

Si la autenticación de los usuarios es satisfactoria se procede a generar una CA local cuya clave privada es calculada de forma distribuida por los 3 miembros de la red. Una vez generados los fragmentos de la clave privada se genera un certificado autofirmado para la CA local. Los certificados se generan a partir de la combinación de las firmas parciales que genera cada nodo sobre los datos del certificado.

Finalmente, los 3 miembros del grupo generan un par de claves criptográficas y se envían mutuamente una petición de certificación. Los certificados que obtienen son certificados de autorización emitidos por la CA local.

2. **Adición de usuarios.**
   Cuando un usuario se quiere unir a la red genera un par de claves criptográficas y envía una solicitud de acceso a los miembros del grupo. Es necesario que los 3 miembros originales identifiquen y autentiquen al nuevo usuario y le den un pase de acceso a la red, esto es, un certificado parcial de autorización. El nuevo usuario combina los 3 certificados parciales obtenidos para generar su certificado de autorización en la red.

   En la solicitud de acceso al grupo, el usuario puede manifestar también su voluntad de unirse como titular de la CA. En este caso, cada nodo genera una parte del fragmento de la clave privada que utilizará el nuevo miembro.

   Es importante que los nodos con suficientes recursos se incorporen como miembros con poderes en la red. Esto facilita la emisión de certificados a nuevos miembros y la red es más robusta y tolerante a fallos.

   La aceptación de nuevos usuarios y titulares de CA a la red se hace a través de la validación de su certificado de identidad en los repositorios de CAs de confianza y, si el nodo evaluador tiene conexión a Internet, mediante la información obtenida en las listas de revocación y las Autoridades de Reputación (ver sección 4).
3. **Revocación de un usuario.**
   Cuando un nodo de la red detecta el comportamiento fraudulento de otro nodo, firma una evidencia de repudio con su certificado local que es enviada en multicast a los titulares de la CA. De esta forma se generan unas listas negras administradas localmente por cada nodo que participa en la gestión de la red.

   Las listas negras contienen un contador de las acusaciones que se han emitido sobre cada usuario y permiten configurar un margen de cargos que se pueden aceptar antes de expulsar a un nodo del grupo.

Cuando un usuario tiene conexión a Internet, puede transferir las evidencias de repudio a las Autoridades de Reputación (RPA) que mantienen información sobre el comportamiento de los usuarios en las redes cooperativas.

4. **Renovación de fragmentos de claves y certificados.**
   El proceso de actualización de los fragmentos de clave de la CA ocurre bajo dos condiciones. Una es la renovación periódica de los secretos. La otra sucede durante algunas operaciones de unión y separación de usuarios en la red.
   De forma periódica se deben regenerar todos los fragmentos de las claves de CA para evitar que sean expuestos suficientes nodos como para comprometer la confianza de la PKI. Para reducir el coste de la operación, durante el tiempo de vida de una región o rama de la PKI, no se puede cambiar el esquema umbral del secreto compartido.
   Cuando se renuevan los fragmentos del secreto compartido también se deben reemitir los certificados de autorización de los miembros de la red. Este hecho permite expulsar del grupo aquellos usuarios que han sido declarados fraudulentos.

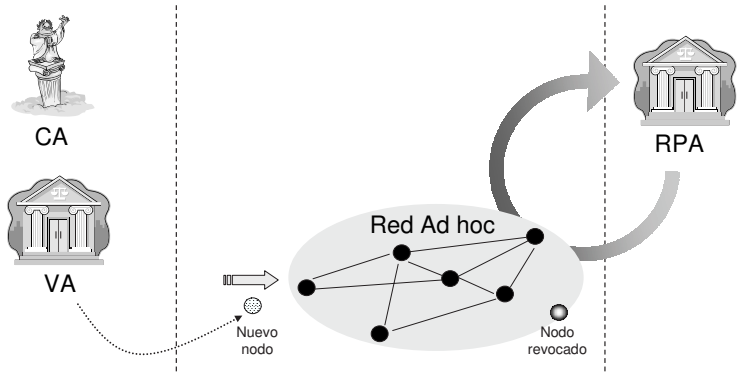

Figura 1. Arquitectura del sistema de confianza de una red ad hoc

La figura 1 muestra gráficamente los módulos involucrados en el sistema. Como se ha comentado, el esquema de confianza propuesto puede funcionar de forma autónoma, aunque utiliza información de autoridades externas cuando la conexión a éstas es posible.

Concretamente, un usuario hace uso de las entidades de confianza en dos ocasiones:

- Previamente a la conexión a la red ad hoc. Los nodos deben poseer un certificado de una de las CAs comunes de Internet o de una CA reconocida por la red de usuarios que se quieren reunir.
- Durante el proceso de aceptación de un nuevo usuario a la red. Los nodos responsables del control de acceso deben verificar las credenciales presentadas

por los usuarios que se quieren unir a la red. Esto implica validar que la identidad del usuario es auténtica (verificar el certificado de identidad y comprobar que el estado del certificado es correcto), y que la reputación del usuario está por encima del mínimo que fija la red.

Por otro lado, los usuarios pueden reportar información a la RPA en cualquier momento.

3. Gestión de claves

Comoy a se ha comentado anteriormente, la gestión de claves se apoya sobre el modelo jerárquico de Zhu [14] aportando una serie de mejoras. La PKI es un árbol cuyas hojas representan nodos reales, mientras que las ramas sólo tienen una existencia lógica. Los fragmentos de la clave secreta del sistema son generados y custodiados por los nodos que son titulares de la CA. Estos usuarios son los que voluntariamente se han ofrecido para dar el servicio y la comunidad de miembros de la red ha aceptado. Por lo tanto son nodos que no tienen una limitación importante de recursos y que su reputación en la red es buena.

El número de nodos óptimo que deben forman la CA depende de diversos parámetros de la red:

- *Densidad*. En redes poco densas es importante que la proporción de titulares de la CA sea alta para no afectar a la disponibilidad. En redes muy densas, una gran candidad de titulares disminuye la eficiencia en los procesos de renovación de claves y certificados.
- *Entorno*. En entornos hostiles una mayor proporción de titulares dificulta el compromiso de la clave.
- *Dinamismo*. Las redes muy dinámicas -de tamaño muy variable- deben tener una alta proporción de titulares que garanticen la continuidad de las funcionalidades de la CA.

Los fragmentos de clave distribuidos entre todos los nodos de la red permiten obtener la clave privada del nodo raíz del sistema -la CA raíz-. Por otro lado, la combinación de los fragmentos de un grupo determinado de nodos tiene como resultado un secreto que podemos ver como la clave privada de una CA subordinada. Los titulares de la clave secreta de la CA se ordenan en grupos anidados formando una estructura jerárquica. Los grupos más pequeños corresponden a las CAs subordinadas virtuales de nivel inferior. Los grupos que contienen otros subgrupos forman CAs subordinadas de nivel superior, y los certificados emitidos por éstas tienen un nivel de confianza mayor.

La clave privada de la CA se genera en la fase de inicialización de la red por los nodos que en aquel momento formaran el grupo. Una vez generados los fragmentos de la clave privada se genera un certificado autofirmado que lleva la información mostrada en el cuadro 1.

Los campos del identificador de la red ad hoc y la fecha son acordados de mutuo acuerdo entre los iniciadores de la red.

Campos firmados	
`PublicKey`	Clave pública (equivalente) de la CA
`Initiators`	Lista con de los usuarios/entidades que han iniciado la red (Campo `Subject` del certificado de PKI)
`Id`	Identificador de la red ad hoc
`Date`	Fecha de inicio
`Count`	Número de renovación del certificado *(inicialmente 0)*

Cuadro 1. Certificado de la CA de la red

Una vez inicializado el sistema, los fragmentos de la clave de la CA tienen que ser redistribuidos y actualizados periódicamente con los siguientes propósitos:

- Adaptar la disponibilidad de la CA a las características de la red
- Evitar que la clave privada sea comprometida

Cuando uno de los titulares de la CA quiere proponer una actualización del secreto, envía un mensaje *UpdateShareReq* al resto de miembros. El mensaje *UpdateShareReq* especifica la causa de la actualización, que puede ser `Resize` o `Timeout`. Los nodos interesados en renovar su titularidad en la CA responden a esta petición con un mensaje. Si el quórum es suficiente, se procede a la renovación de la clave.

En caso de una actualización por `Resize`, ésta no se hace de toda la PKI sino sólo de la región afectada. Las operaciones que la provocan son:

- *Cambio del umbral de un criptosistema.* Sucede cuando una región de la red es administrada por una CA que tiene pocos titulares. A medida que nuevos usuarios se unen al grupo administradores la relación entre el umbral del criptosistema y el número de nodos que poseen un fragmento de la clave disminuye, provocando que la CA sea más vulnerable. Una renovación de los fragmentos de clave de todos los nodos de la región permite incrementar el umbral de confianza.
- *Partición de una región.* El coste computacional y temporal de las operaciones de gestión de una PKI con estructura plana en una red ad hoc es exponencial con el número de usuarios titulares de la clave de la CA. Cuando una región de la red es administrada por un gran número de nodos, da servicio a muchos usuarios, y los retardos inducidos por la CA no son tolerables. En esta situación decimos que la región está saturada. Es este caso es aconsejable dividirla en dos regiones más pequeñas, cada una de las cuales está en el mismo nivel jerárquico que la región original. Una de las nuevas regiones tiene la misma clave privada virtual que tenía la región original y por lo tanto mantiene el certificado de CA. A la otra región le corresponde un nuevo fragmento de la clave de CA del nivel superior (obtenido a partir de los nodos de las otras regiones que están al mismo nivel) y por lo tanto un nuevo certificado. Se ha realizado una ampliación horizontal de la PKI.
- *Expansion de la PKI.* Cuando una región está saturada y no se puede particionar porque la CA de nivel superior no admite incrementar el número de

regiones que comparten su clave secreta para no vulnerar la seguridad del sistema (el umbral k de las CAs formadas por nodos virtuales no puede se puede modificar), la ampliación de la PKI es vertical. La región es dividida en r subregiones que contienen n' titulares cada una. Los fragmentos de clave de los n' titulares forman la clave secreta virtual sobre el que se emite el certificado de CA de la subregión. La combinación de las claves secretas de las subregiones constituyen la clave secreta de la región, que es la misma clave que tenía la región original.

Las renovaciones por `Timeout` se hacen regularmente e implican una actualización de claves de toda la red y la expedición de nuevos certificados, desde la CA raíz hasta el último nodo. El nuevo certificado de CA tiene los mismos datos que su predecesor excepto que el campo `Count`, que indica el número de renovaciones del certificado, se incrementa en una unidad.

El hecho de renovar regularmente todos los certificados de la red permite trabajar con certificados de corta duración -efímeros- y, por lo tanto, no es necesario establecer un mecanismo de emisión y gestión de listas de certificados revocados porque la revocación de éstos deja de tener sentido. Los nodos titulares de la red gestionan listas de usuarios maliciosos con el fin de no renovarles el certificado de autorización en la red. Los usuarios que no son responsables de la gestión de la PKI no realizan ningún control de acceso, confían en todos los usuarios que les presentan un certificado de autorización válido.

La arquitectura de la PKI es dinámica y se adapta a las necesidades de la red. Inicialmente la estructura es siempre plana pero a medida que el tamaño de la red aumenta, es aconsejable dividir la PKI en regiones más pequeñas y fáciles de gestionar. Las operaciones de expansión permiten agrupar los titulares de la CA en grupos independientes. Estos grupos pueden emitir certificados a usuarios finales en nombre del propio grupo -no de la CA del sistema-. El identificador del grupo es una clave pública generada a partir de los fragmentos de clave que poseen los usuarios miembros. Esta clave está certificada por la CA del sistema con la colaboración de usuarios de otras regiones. De esta manera se crea una PKI en estructura jerárquica cuyas ramas están formadas por nodos virtuales equivalentes a las CAs subordinadas de una arquitectura con infraestructura, y las hojas de la cual son los miembros titulares de la red ad hoc.

El certificado de un nodo virtual de la PKI (CA subordinada) contiene los datos mostrados en el cuadro 2.

En una red ad hoc es muy difícil mantener una sincronización de los relojes de todos los usuarios. Es por ese motivo que la gestión de claves y certificados tiene que tener la mínima dependencia con el instante temporal. Normalmente los certificados tienen un tiempo de vida limitado. Los certificados que se generan en una CA distribuida no pueden llevar este parámetro por dos motivos:

1. Los emisores del certificado no están sincronizados
2. La fecha de validez del certificado la puede definir el usuario final, pero en este caso la utilidad de la misma pierde el sentido.

Por otro lado, pueden ser los nodos que validen dicho certificado los que estén desajustados.

Campos firmados	
`PublicKey`	Clave pública (equivalente) de la CA
`Id`	Identificador del nodo (hash de la clave pública)
`Threshold`	Umbral del nodo emisor
`Issuer`	Identificador del nodo emisor
`Count`	Número de renovación del certificado *(inicialmente 0)*
`ICount`	Número de renovación del certificado del emisor

Cuadro 2. Certificado de CA subordinada

Estos pequeños desajustes temporales no son especialmente significativos en redes estables y con una infraestructura de soporte. En estas redes los certificados tienen un tiempo de vida longevo (un certificado de identidad de usuario tiene unos 2 años de vida) y hay entidades de soporte que pueden comprobar el estado de los certificados. En un entorno ad hoc no existe una entidad dedicada a publicar, diseminar o evaluar la validez de los certificados. Además, en caso de certificados de corta duración, el tiempo de validez adquiere mayor importancia.

La arquitectura propuesta independiza la validez temporal de un certificado con la fecha absoluta a través del proceso de renovación de certificados. Los certificados de usuario están vinculados con el número de renovación del certificado de CA.

El certificado de CA se renueva cuando hay una regeneración de los fragmentos de la clave privada. Es aconsejable que los fragmentos se renuevan periódicamente por motivos de seguridad. Nuestro sistema aprovecha esta renovación para regenerar los certificados digitales asociados.

Cuando un nodo verifica el certificado presentado por otro usuario, tiene que validar tanto que procede de la CA de la red ad hoc, como que la emisión del certificado corresponde a la última renovación de certificados. El propio certificado lleva un campo que indica sobre que renovación de claves está emitido.

La información que lleva un certificado de autorización es la que se muestra en el cuadro 3.

Campos firmados	
`PublicKey`	Clave pública del usuario
`Id`	Identificador de usuario (`Subject`, `Issuer` y `SerialNumber` del certificado de PKI)
`Threshold`	Umbral del nodo emisor
`Issuer`	Identificador del nodo emisor
`Count`	Número de renovación del certificado *(inicialmente 0)*
`ICount`	Número de renovación del certificado del emisor

Cuadro 3. Certificado de autorización

4. Autoridad de Reputaciones (RPA)

La gestión de las revocaciones en el servicio de autorización propuesto abarca tanto el entorno local de la red ad hoc, como un entorno más global y duradero. Cuando un usuario detecta un nodo malicioso o fraudulento, éste emite una evidencia firmada de acusación que contiene:

Campos firmados	
`Id`	Identificador del usuario malicioso (`Subject`, `Issuer` y `SerialNumber` del certificado de PKI)
`Motivo`	Motivo de la revocación *(impersonación, denegación de servicio, ..)*
`Issuer`	Identificador del acusador (`Subject`, `Issuer` y `SerialNumber` del certificado de PKI)

Cuadro 4. Evidencia de acusación

Cuando un usuario emite una acusación la transmite en multicast al grupo de nodos responsables de la gestión de la PKI. Estos nodos mantienen localmente una lista negra de los usuarios presuntamente maliciosos. La lista contiene el número de acusaciones de diferentes nodos que ha tenido cada usuario, y la identidad de los acusadores. Cuando un usuario es acusado por más de t nodos (siendo t el umbral de gracia de la red), se decide que el nodo es fraudulento y a partir de ese momento no se le renueva el certificado de autorización y no se tienen en cuenta las revocaciones que este nodo ha emitido a otros miembros de la red.

Como las listas de acusaciones son personales de cada usuario, es posible que nodos que se incorporen posteriormente a la red no tengan información respeto de las revocaciones que han ocurrido previamente a su entrada. Además, es interesante guardar la información de revocación de los usuarios para tenerla en cuenta en futuras asociaciones de usuarios. Por este motivo, la arquitectura presentada incorpora una Autoridad de Reputaciones confiable que es externa a la red ad-hoc y que se encarga de la publicación, mantenimiento y administración de las reputaciones sobre certificados de identidad reconocidos que ocurren en redes ad-hoc.

Esta autoridad presenta información actualitzada de determinado certificado en las redes cooperativas. La organización de la información es en formato X.500 siguiendo la estructura jerárquica de los certificados de identidad. Las búsquedas al directorio se pueden hacer por Nombre Distintivo del sujeto, o bien por el identificador único del certificado, el publickKeyHash.

Cuando un usuario tiene conexión a Internet, puede publicar los informes obtenidos durante su participación en una red corporativa. La información que el usuario debe enviar a la RPA es por un lado el informe de acusación, y por el otro el certificado de autorización del nodo que firma la acusación junto con toda la cadena de certificación hasta la CA raíz de la red ad hoc. Esto permite

comprobar la veracidad de la denuncia y la pertenencia del acusador a la red ad hoc.

Un usuario, aunque no tenga ninguna evidencia de revocación que reportar, se puede conectar a la RPA para anunciar su pertenencia a la red ad hoc (demostrada por el certificado de autorización). Manifestando su apoyo a la red, un usuario respalda la información aportada por otros usuarios e incrementa el crédito que determinada información sea cierta.

La RPA abstrae y resume la información de reputación para cada certificado de PKI en estructuras que contienen el motivo de la reputación, el número reportado de informes de diferentes usuarios con ese motivo, y el respaldo que tiene la información. El respaldo que tiene la información se obtiene a partir del número de informes presentados y de la cantidad de usuarios que han dado su respaldo en las reputaciones presentadas por miembros de su red ad hoc.

Los informes de reputación generados por la RPA son certificados con una firma de la entidad. De esta forma, cuando un nodo se encuentra en una red ad hoc y tiene acceso a la RPA, puede evitar la entrada de usuarios maliciosos distribuyendo entre los nodos titulares de la red la información de reputación de estos candidatos.

Todas las evidencias en las que se basan los informes de la PRA son ordenadas y almacenadas para facilitar los procesos de auditoría de la entidad.

La Autoridad de Reputaciones recibe este nombre porque guarda información de informes positivos y negativos de los usuarios. Por ejemplo, ser el titular de una red ad hoc o el hecho de reportar información del comportamiento de otros usuarios en la red incrementa el nivel de voluntad cooperativa del propio usuario.

5. Conclusiones

En el presente artículo, se ha presentado un modelo de confianza práctico y eficiente basado en una PKI distribuida y jerárquica. A diferencia de las propuestas anteriores, el ciclo de vida de los certificados que se utilizan en el esquema diseñado no tiene una dependencia temporal fija. Esto permite trabajar con certificados de corta duración y se evita la expedición de listas de revocación.

El esquema propuesto permite una comunicación mucho más eficiente entre los nodos. No son los usuarios finales los que tienen que evaluar los permisos de los demás nodos con los que quieren interactuar sino que el control de acceso es gestionado de forma única y global por los nodos responsables de la seguridad del sistema, nodos que por otra parte tienen suficientes recursos para hacerlo.

El hecho que se tengan que renovar las claves y los certificados de toda la red de forma periódica no supone una penalización drástica en el rendimiento de la red. El tiempo medio para renovar un certificado de 1024 bits en una red administrada por 100 nodos es de unos 50ms [14].

Por otra parte se ha introducido el concepto de una Autoridad de Reputaciones. Esta autoridad es externa a la red ad hoc pero realiza funciones de soporte. Permite ordenar y custodiar un histórico de la reputación de los nodos en las

redes cooperativas de forma que el comportamiento de un nodo tenga valor más allá de la vida de la red ad hoc de la que formó parte.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia y Tecnología con el proyecto SEG2004-04352-C04-04 PROPRIETAS-WIRELESS.

Referencias

1. Douceur, J.: The sybil attack. In: Proceedings of the IPTPS02 Workshop. (2002)
2. Blakley, G.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference. Volume 48. (1979) 313–317
3. Shamir, A.: How to share a secret. Commun. ACM **22** (1979) 612–613
4. Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In: Proceedings of the 26th IEEE Annual Symposium on Foundations of Computer Science. (1985) 383–395
5. Herzberg, A., Jarecki, S., Krawczyk, H., Yung, M.: Proactive secret sharing or: How to cope with perpetual leakage. In: CRYPTO '95: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, London, UK, Springer-Verlag (1995) 339–352
6. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network **13** (1999) 24–30
7. Kong, J., Zerfos, P., Luo, H., Lu, S., Zhang, L.: Providing robust and ubiquitous security support for mobile ad-hoc networks. In: International Conference on Network Protocols (ICNP). (2001) 251–260
8. Lehane, B., Doyle, L., O'Mahony, D.: Shared RSA key generation in a mobile ad hoc network. In: Proceedings of IEEE Military Communications Conference (MILCOM 2003). (2003)
9. Yi, S., Kravets, R.: Moca: mobile certificate authority for wireless ad hoc networks. In: 2nd Annual PKI Research Workshop Program (PKI 03). (2003)
10. Pedersen, T.: A threshold cryptosystem without a trusted party. In Davies, D.W., ed.: Advances in Cryptology – EUROCRYPT'91. Volume 547 of Lecture Notes in Computer Science. (1991)
11. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Advances in Cryptology – CRYPTO 89. Lecture Notes in Computer Science (1990) 307
12. Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Secure distributed key generation for discrete-log based cryptosystems. Lecture Notes in Computer Science **1592** (1999) 295–310
13. Frankel, Y., MacKenzie, P., Yung, M.: Robust efficient distributed RSA-key generation. In: The Thirtieth Annual ACM Symposium on Theory of Computing – STOC '98. (1998) 663–672
14. Zhu, B., Bao, F., Deng, R.H., Kankanhalli, M.S., Wang, G.: Efficient and robust key management for large mobile ad hoc networks. Comput. Networks **48** (2005) 657–682
15. Wu, B., Wu, J., Fernandez, E., Ilyas, M., Magliveras, S.: Secure and efficient key management in mobile ad hoc networks. In: Proceedings of IEEE Parallel and Distributed Processing Symposium, (19th). (2005) 288a– 288a

16. Capkun, S., Buttyán, L., Hubaux, J.P.: Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing **2** (2003) 52–64
17. Hubaux, J., Buttyan, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, New York, NY, USA, ACM (2001) 146–155