Índice

1. Resumen

Cada vez está tomando más importancia la web, y actualmente están apareciendo multitud de aplicaciones, ya sea por parte de empresas o de instituciones, como Universidades, etc. Estas aplicaciones normalmente requieren autenticación, y la mayoría de ellas basan dicha autenticación en bases de datos locales.

Con el crecimiento de las aplicaciones, crece el número de usuarios de estas, y por parte del usuario, crece el número de cuentas creadas para diferentes aplicaciones. Para paliar este problema, nace el Single Sing On(SSO), que proporciona una única cuenta, y un único punto de autenticación, para diferentes aplicaciones web de una misma entidad, por ejemplo la Universidad de Sevilla.

El siguiente paso natural, es el uso de aplicaciones de otras entidades, y aquí es donde radica la importancia de la **federación de identidad**.

La federación de identidad consiste en que una serie de entidades **confían** en otras para la autenticación de los usuarios. Es decir, que una aplicación de una entidad, acepta usuarios de otra entidad. Además estos usuarios se autenticarán en su entidad, por lo que la gestión de usuarios, contraseñas, y atributos, queda delegada a cada entidad. Por tanto el usuario final tiene acceso a todas las aplicaciones federadas, de todas las entidades que conforman la federación de identidad.

Esto facilita enormemente la gestión de usuarios, por parte de las entidades, puesto que tan solo tienen que gestionar sus propios usuarios, y prestan servicio a usuarios de otras entidades, gracias a que la autenticación es delegada.

La idea principal de este proyecto es llevar las facilidades que proporciona la federación de identidad fuera del ámbito de la web, más concretamente al ámbito del **SSH** (Secure SHell).

Para el caso del SSH, si un usuario tiene acceso a diferentes máquinas, tendrá diferentes cuentas, y diferentes contraseñas que recordar, almacenar y gestionar, con la problemática que eso conlleva. Además sus contraseñas estarán en máquinas que no tiene por qué controlar, por lo que si se compro-

mete alguna de estas máquinas, estará comprometida su contraseña.

Utilizando SSH sobre la federación de identidad, se pueden eliminar estos problemas e incrementar la comodidad, tanto por parte de los usuarios, como por parte de los administradores. Para poder acceder por SSH, un usuario tendría que autenticarse en la federación, y una vez autenticado, podrá entrar en todas las máquinas que ofrezcan el servicio de SSH federado, sin necesidad de poner contraseña, basándose en el mecanismo de clave pública y clave privada, y estando el servidor en cualquier entidad de la federación.

Así pues, por parte del usuario, se tiene acceso a diferentes máquinas necesitando recordar y gestionar una sola contraseña. Además esta contraseña nunca se entrega a un servidor extraño, sólo a la entidad de la cual procedes (a través de una páginas web segura), y en la cual confías puesto que es la encargada de gestionar tu identidad.

Y por parte del administrador, se puede delegar la gestión de usuarios, confiando en la federación. Automatizando la creación y destrucción de cuentas, y sin necesidad de proporcionar ninguna contraseña.

2. Introducción

2.1. Objetivos

Las facilidades que ofrece la federación de identidad son más que evidentes, y podría ser interesante en muchos casos, tener estas facilidades para otros servicios que requieran autenticación.

El principal objetivo de este proyecto es llevar las facilidades de la gestión de identidad del ámbito de la web a otros servicios, como por ejemplo el SSH. En este proyecto nos hemos centrado en integrar la federación de identidad con el acceso por SSH, y puede servir como prueba de concepto a la hora de llevar la autenticación por federación de identidad a servicios diferentes de la web.

Las características más importantes de la federación de identidad, que nos serán útiles en el SSH son:

1. **Acceso a recursos de otras entidades**: La base de la federación de identidad es poder acceder a recursos de otra entidad con la misma cuenta con la que accedes a los recursos o servicios de tu propia entidad.

2. **Gestión de identidad distribuida**: Al encargarse cada entidad de la federación de sus propios usuarios, y basándonos en las relaciones de confianza de la federación, se puede dar servicio a un mayor número de usuarios gestionando tan solo una pequeña cantidad de ellos. Esto puede crear algún tipo de duda, puesto que se pierde el control sobre los usuarios, pero no hay que olvidar que la federación es una red de confianza, donde cada entidad debe confiar en las demás, y para ello hay mecanismos seguros, como por ejemplo los certificados.

3. **Unicidad de contraseña**: La federación de identidad nos brinda la posibilidad de acceder a diferentes servicios, que requieren autenticación, con la misma cuenta y la misma contraseña, y sin necesidad de replicar esta en los diferentes servicios, sino estando en tu propia entidad, incrementando así la seguridad de la misma, y la comodidad a la hora de cambiar de contraseña, o de nombre de usuario.

4. **Login único**: También se busca implementar el Single Sing On(SSO) para el SSH sobre federación, de tal forma que un usuario sólo tenga que autenticarse una vez, y a partir de ahí, tener acceso, sin necesidad de introducir ningún tipo de contraseña, a todos los servidores SSH disponibles.

2.2. Antecedentes

(feide, parche opensshldap)

3. Análisis del problema

3.1. Necesidad de federación

3.2. Uso de la federación fuera de la web

3.3. La importancia del ssh

(túneles, importación X ...)

4. Solución propuesta

4.1. Parche para openssh (proceso de autenticación sshd)

4.2. Servidor de claves, flexibilidad, LDAP, python...

4.3. Aplicación de login.

4.4. Ejemplo aplicación creación de cuentas.

5. Implementación y despliegue

5.1. Código del openssh, (mínimas variaciones)

5.2. Código de las aplicaciones federadas, (ssh, useradd)

5.3. Necesidades para montar la plataforma

6. Conclusiones

6.1. Por qué es importante, y por qué soy el mejor

7. Anexos

7.1. Aplicación del parche sobre openssh

7.2. Despliegue del servidor ssh con el parche

7.3. Seguridad mínima (permisos, cambiar passwd, etc)

7.4. Despliegue de la aplicación federada

7.5. Schemas ldap utilizados, dónde encontrarlos, cómo instalarlos en openldap