Implementación del esquema de Shamir sobre una red P2P DHT para proveer un servicio de almacenamiento de contraseñas

A. Enrique[1], J. Ramith[2]
{ a. enrique[1], j. ramith[2]}@unisimon.edu.co

Resumen - Hoy en día la seguridad es un atributo fundamental para la construcción de cualquier sistema de información de una compañía. Dentro de las diferentes estrategias de aseguramiento, la autenticación de los usuarios del sistema es una de las más importantes, porque permite posteriormente la caracterización del mismo. Existen muchos métodos de autenticación, el más común es el uso de contraseñas. En este caso, el usuario memoriza estos caracteres, o los consignas en algún otro sitio. Sin embargo, este proceso puede convertirse difícil sí los requerimientos en el número de caracteres y contraseñas a usar son cada vez mayor [1], por lo que es importante introducir mecanismos para el almacenamiento seguro y confiable de estos caracteres. En este artículo se presenta un mecanismo usando criptografía umbral para distribuir un secreto (contraseña) sobre una red P2P DHT.

Palabras clave— P2P,DH, PAS, Esquema de Shamir

Nowadays security is a key to building any information system of a company attribute. Among the different insurance strategies, the user authentication system is one of the most important, because then allows characterization. There are many authentication methods, the most common is the use of passwords. In this case, the user memorizes these characters, slogans or elsewhere. However, this process can become difficult if the requirements on the number of characters and passwords to use are increasing [1], so it is important to introduce mechanisms for the safe and reliable storage of these characters. This article using threshold cryptography mechanism to distribute a secret (password) on a P2P DHT network is presented.

Keywords— P2P,DH, PAS, Shamir scheme

I. INTRODUCCIÓN

Hoy día es muy común hablar o quizás ver como entre más crece y avanza la tecnología, aumenta la inseguridad en las redes, en el envió de nuestros datos, poniendo en riesgo nuestra información la cual puede ser utilizada de tal manera que pueda afectar la integridad de su dueño, es por ello que se han creado muchas técnicas de seguridad en la transferencia de archivos las cuales permitan que la información solo llegue al destinatario que nosotros queremos,

Con ello apareció la criptografía, esta se encarga de enmascarar las referencias originales de dichos archivos por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información. El uso de esta u otras técnicas, permite un intercambio de mensajes que sólo puedan ser leídos por los destinatarios designados como 'coherentes'. Un destinatario coherente es la persona a la que el mensaje se le dirige con intención por parte del remitente.

En el presente artículo proponemos y describimos una nueva forma de seguridad web mediante las redes peer to peer tomando en cuenta el esquema de Shamir, basado en el compartimiento de secretos donde cada secreto se divide en partes y donde para reconstruir el secreto es fundamental hallar esa partes colocadas en este caso en diferentes peer en forma de anillo. Nuestra propuesta es atacar la disponibilidad de los dispositivos para reconstruir un secreto divido en varias partes.

II. ESTADO DEL ARTE

Un sistema P2P basado en DHT es un sistema estructurado que utiliza funciones hash para la ubicación y localización de nodos y datos. Un sistema DHT usualmente tiene las siguientes propiedades [7]:

1. Eficiencia en enrutamiento. Como utilizan funciones hash para la localización de nodos y objetos, las búsquedas se pueden resolver fácilmente. Estos sistemas proveen O(log n) como límite superior en la longitud del camino de búsqueda.

2. Balanceo de carga. Existen un balanceo entre el número de datos asignados a los nodos del sistema. Esto se debe al uso de una función hash de distribución uniforme tal como SHA-1. Con esto, la sobrecarga en almacenamiento y mantenimiento de nodos crece solo logarítmicamente de acuerdo al número de nodos en el sistema.

3. Auto-organización. El sistema DHT es totalmente distribuido. La entrada y salida de los nodos se maneja automáticamente sin la necesidad de la coordinación de una entidad central de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Pastry [6] es uno de los sistemas basados en DHT más utilizado actualmente. Varias aplicaciones tales como SCRIBE [3] y PAST [4], se han desplegado utilizando Pastry como el sistema DHT subyacente. Cada nodo en Pastry tiene un único identificador de 128 bits. Los identificadores se escogen de manera aleatoria y uniforme. Una manera de generar identificadores para los nodos es aplicando una función de hash a las direcciones IP. Pastry utiliza prefix-matching para enrutar mensajes.

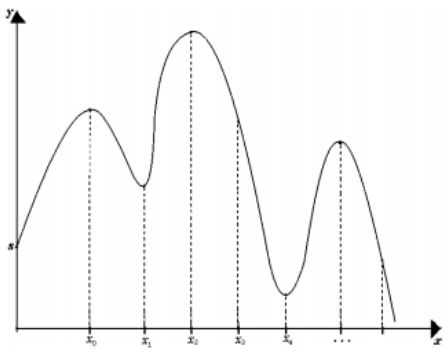
Cada nodo mantiene una tabla de enrutamiento, donde la entrada en la fila n, comparte los primeros n dígitos con ese nodo. Además, cada nodo mantiene un conjunto de vecinos que contiene las direcciones IP de los l/2 nodos cuyos identificadores son los más cercanos numéricamente mayores, y los l/2 nodos cuyos identificadores son los más cercanos numéricamente menores.

Para ingresar al sistema, un nuevo nodo debe conocer a algún nodo que hace parte del sistema. El nuevo nodo puede inicializar su estado contactando al nodo existente y enviando un mensaje de ingreso con su identificador como la llave. El mensaje se enruta a otro nodo existente cuyo identificador es numéricamente más cercano al del nuevo nodo. Luego, todos los nodos encontrados durante el camino envían sus tablas de enrutamiento al nuevo nodo. Este luego inicializa sus propias tablas basadas en la información recibida. Finalmente, el nuevo nodo informa a aquellos nodos que necesitan saber de su llegada.

El proceso de mantenimiento se maneja periódicamente intercambiando mensajes de vida entre los nodos vecinos. Cuando se detecta una falla de un nodo, todos los miembros del conjunto leaf del nodo que ha fallado son notificados y estos actualizan sus respectivos conjuntos.

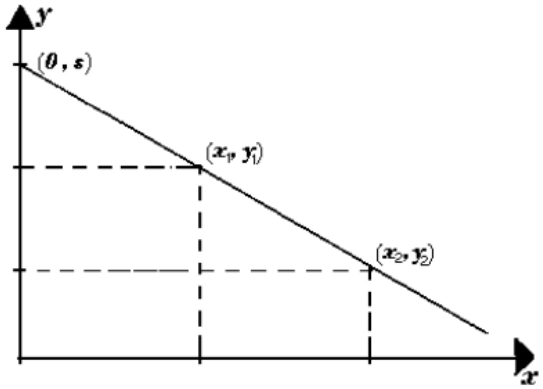
A. Esquema De Shamir

Esquema de Shamir es un esquema criptográfico de umbral [5], en donde un secreto se divide en partes y se da a cada participante al menos una de estas partes. Posteriormente, un subconjunto de estas partes se usan para reconstruir el secreto.
La idea detrás de los sistemas de secretos compartidos (shared secret systems) es la protección o la privacidad de la información, vía su distribución. algunas de las aplicaciones de los SSS son las firmas colectivas digitales, la custodia de claves, el almacenamiento de información, etc., en los cuales un número de participantes desea coordinar sus actividades para obtener algún objetivo. Generalmente se asume que el distribuidor de los fragmentos es una entidad confiable y que los fragmentos son entregados de manera segura a los participantes.
En general, los esquemas de compartición de secretos de umbral están definidos por medio de algoritmos probabilísticos, en los que se considera como entrada al secreto, que es un elemento de un conjunto finito, y su salida son los fragmentos del secreto.
Por otra parte, el secreto es recuperado con el umbral t, es decir, en el que al menos t fragmentos pueden recuperar el secreto; y si menos de t fragmentos son conocidos, entonces no se sabe absolutamente nada sobre el mismo (en el sentido teórico de la información). shamir formalizó las nociones de privacidad y exactitud en los esquemas de umbral. En su esquema propuso elegir un polinomio (aleatorio) de grado t-1, y la recuperación del secreto se basa en la interpolación polinómica de la forma de lagrange.
El esquema de shamir se describe así:
Entrada: números enteros positivos l y $t \leq l$, y un secreto $k \in \{0,..,s-1\}$.
Salida: número enteros positivos fragmentos del secreto distribuidos en S_i
1. se elige un número primo p > max{s,l + 1}
2. se eligen aleatoria e independientemente a_1,..,a_(t-1),∈Z
3. se construye el polinomio de grado t-1,q(x)=K+ Σ_(i=1)^(t-1) a_i x^i
4. se distribuye el secreto en las particiones s_i=q(i)∈Z,i=1
Los miembros del colectivo t podrán recuperar el polinomio q(x), puesto que conocen
Las imágenes de t puntos y en este polinomio el término independiente es el secreto. Ahora bien, t-1 miembros no obtendrían información adicional sobre la que ya tenían, ya que cualquier término independiente sería compatible con la construcción.
El esquema de Shamir es un tipo de esquema de umbral, el cual está basado en la interpolación de polinomios.
Consideramos a un polinomio de grado t-1 sobre el campo finito K
p[x]= a_0+ a_1 x+ a_2 x^2+..+ a_(t-1) X^(t-1)
Este polinomio lo construimos de tal manera que el coeficiente a_0 es el secreto y los demás coeficientes son elementos aleatorios en el campo K.
Cada uno de los n fragmentos serán los puntos (x_i,p[x_i])$1 \leq i \leq n$, donde:
$x_i \neq x_j$ Para todo $i \neq j$ y p[0] = a_0
Tales puntos son elementos de la curva definida por el polinomio anterior sobre el plano R^2



Dados t fragmentos, podemos determinar de manera única al polinomio, y en consecuencia podemos calcular a a_0 (el secreto) mediante la sustitución x = 0 en la función polinomial.

Por ejemplo el caso especial en que t = 2, solo requerimos 2 fragmentos para recobrar el secreto. En consecuencia la ecuación del polinomio describe una línea recta. El secreto es el punto en el que la línea intersecta al eje y



El esquema de Shamir está basado en la interpolación de polinomios por el hecho de que el polinomio invariante p[x] de grado t – 1 está determinado de manera única por t puntos (x_i,s_i) con distintos x_i pues estos puntos definen t ecuaciones independientes con t incógnitas en los coeficientes a_i .

Ejemplo:

Supongamos que el secreto es el número de una tarjeta de crédito: 1234

$$(S = 1234)$$

Queremos dividir el secreto en 6 partes (n=6), de forma que cualquier subconjunto (k=3) sea suficiente para reconstruir el secreto. Al azar obtenemos dos números por ejemplo 166, 94.

$$a_1 = 166;\ a_2 = 94)$$

El polinomio con el que operamos será por lo tanto:

$$f(x) = \ 1234 + 166x + 94x^2$$

Calculamos seis puntos a partir del polinomio:

(1,1494); (2,1942); (3,2578); (4,3402); (5,4414); (6,5614)

Damos a cada participe un único punto, que comprende el valor xy f(x)

Reconstrucción

Para reconstruir el secreto bastara con tres puntos.

Considérese

$$(x_0, y_0) = (2{,}1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5{,}4414)$$

Usamos la interpolación polinómica de LaGrange

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + 3\frac{1}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + 2\frac{2}{3}$$

Por lo tanto:

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= 1942 \cdot \left(\frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3}\right) + 3402 \cdot \left(-\frac{1}{2}x^2 + 3\frac{1}{2}x - 5\right) + 4414 \cdot \left(\frac{1}{3}x^2 - 2x + 2\frac{2}{3}\right)$$

$$= 1234 + 166x + 94x^2$$

Teniendo en cuenta que el secreto es el coeficiente de x_0 , ello significa que S= 1234.

III. Conclusión

En este artículo se ha mostrado una nueva arquitectura basada en el esquema de Shamir cuya característica es la búsqueda y reconstrucción de un secreto llevado desde un dispositivo servidor hacia varios dispositivos conectados por medio de redes peer to peer teniendo en cuenta las direcciones ip a las cuales dichos secretos fueron enviados, permitiendo así aumentar la seguridad en la transferencia de datos y archivos, usando la encriptación como base de una solución que permita erradicar la inseguridad a la cual día a día nos enfrentamos.

IV. REFERENCIA

[1] R. Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems”, Wiley, 2 ed. 2008

[2] E. Bertino, L. Martino, F. Paci, A. Squicciariani, “Security for Web Services and Service-Oriented Architectures”. Springer, 1ed., 2010

[3] M. Castro, P. Druschel, A-M. Kermarrec and A. Rowstron, "SCRIBE: A large-scale and decentralised application-level multicast infrastructure", IEEE Journal on Selected Areas in Communication (JSAC), Vol. 20, No, 8, October 2002.

[4] P. Druschel and A. Rowstron, "PAST: A large-scale, persistent peer-to-peer storage utility", HotOS VIII, Schoss Elmau, Germany, May 2001

[5] J. Hoffstein, J. Pipher, J. Silverman. “An Introduction to Mathematical Cryptography”. Springer, 1 ed., 2008

[6] A. Rowstron and P. Druschel, “Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems". IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), Germany, pp. 329-350, 2001.
[7] Shen, X., Yu, H., Buford, J., Akon, M. (Eds.), ”Handbook of Peer-to-Peer Networking”, Springer, 1 ed., 2010