Una Implementación de Autenticación para Mensajes DHCP

D. Rubel Salas[1], M. Villapol[1] y D. Pérez Abreu[1]

[1]Universidad Central de Venezuela, Escuela de Computación, Laboratorio ICARO, Venezuela

RESUMEN

En el presente artículo, se describen y exploran múltiples métodos de autenticación en DHCP como antesala al trabajo desarrollado, una implementación de DHCP con autenticación. También en este trabajo se describen las consideraciones de diseño y detalles de implementación en la versión de mensajes DHCP autenticados desarrollada; en la cual se usaron los métodos Configuration Token y Delayed Authentication, esperando que esta experiencia pueda ser tomada en consideración por otros investigadores. Adicionalmente, se presentan los resultados de diversas pruebas ejecutadas en diferentes escenarios. Los resultados obtenidos permiten concluir que es factible la construcción de un sistema DHCP funcional y robusto usando diferentes métodos de autenticación.

Palabras Clave: DHCP, Autenticación, Configuration Token, Delayed Authentication.

ABSTRACT

In this paper, we describe and explore multiple methods of DHCP authentication as a way to introduce our work, a functional implementation of DHCP with authentication. Also, this work describes the design considerations and details for the implementation of Authentication for DHCP Messages using Configuration Token and Delayed Authentication methods, with the hope that our experience can be taken in consideration by other researches. In addition, we present the results of several tests conducted using different scenarios. These results lead us to think that it is possible to build a robust and proper DHCP system with various authentication methods.

Keywords: DHCP, Authentication, Configuration Token, Delayed Authentication.

1. Introducción

El crecimiento de Internet junto a los datos que esta alberga ha creado una necesidad en las personas de estar conectados a dicha red. Para poder conectarse a Internet, un dispositivo de comunicación necesita tener configurado de manera correcta diversos parámetros de la pila de protocolos TCP/IP. Sin embargo, una gran cantidad de personas, las cuales usualmente poseen poco o ningún conocimiento de los parámetros de la pila de protocolos TCP/IP, desean tener acceso a Internet sin la necesidad de que un administrador de red deba configurar las interfaces de comunicación de sus equipos. De esta manera, resulta deseable poseer un mecanismo que permita a los dispositivos obtener de forma automática los parámetros de configuración necesarios para poder acceder a Internet.

El Protocolo de Configuración Dinámico de Estaciones (DHCP – Dinamic Host Configuration Protocol) permite a una estación ubicada en una red basada en TCP/IP, obtener de manera automática la información necesaria para configurar la interfaz de comunicaciones, eliminando de esta manera la necesidad de que el administrador de red configure manualmente la interfaz [Dro97]. Cuando DHCP fue desarrollado a inicios de los años noventa, cuando la seguridad en Internet no representaba una gran preocupación, este no proveía ningún soporte de seguridad. Sin embargo, existen dos grandes problemas de seguridad asociados al protocolo DHCP. El primero, un servidor DHCP no autorizado podría proveer información de configuración incorrecta al cliente, con la intención de establecer bien sea un ataque de hombre en el medio (Man-in-The-Middle) o un ataque de negación de servicios (DoS – Denial-of-Service). El segundo, un cliente DHCP no autorizado podría obtener información de configuración de la red con la intención de comprometer la seguridad de la misma en el futuro. De manera similar, un cliente no autorizado podría causar que las direcciones IP válidas del servidor se agotaran o en general que se agotara cualquier recurso compartido en la red, por ejemplo, enviando múltiples solicitudes al servidor (ataque de DoS) [Rub11].

En los últimos años, se han llevado a cabo varias investigaciones con la intención de mitigar los problemas de seguridad del protocolo DHCP descritos anteriormente. Uno de estos esfuerzos se describe en [DA01], donde se define una nueva opción de autenticación mediante el intercambio de *tickets* para DHCP, así solo las estaciones clientes y servidores que posean un *ticket* válido podrán estar involucrados en el proceso de configuración de interfaces. Dos métodos de autenticación son definidos en [DA01]: *Configuration Token* y *Delayed Authentication*. El método *Configuration Token* implica el envío de un *token*, como una clave en texto plano, desde el cliente al servidor y viceversa para realizar la autenticación entre ambos. En

contraste con el método anterior, *Delayed Authentication* autentica clientes y a un servidor usando una llave simétrica conocida por ambas partes, esto antes de que ocurra cualquier comunicación relacionada con el protocolo DHCP.

Tomando en cuenta los mecanismos de autenticación planteados en el RFC 3118, algunos investigadores han realizado propuestas alternativas de autenticación para DHCP, por ejemplo, Hornstein et al. [HLA*01] plantean un esquema de autenticación similar al método *Delayed Authentication* pero usando el protocolo Kerberos [NHR05] para la generación de *tickets*. Un método de autenticación para DHCP usando certificados digitales se expone en [GHS03]. En esta investigación Glazer et al. proponen el envío de certificados X.509 [HFP*99] en lugar de una clave compartida como se especifica en el método *Delayed Authentication* [DA01]. Propuestas más recientes como la de Xu et al. [XMW11] sugieren el uso de certificados digitales entre clientes y servidores DHCP, y adicionalmente incorporar un "servidor de confianza" el cual será el encargado de lidiar con los certificados. En este método de autenticación clientes y servidores utilizan el "servidor de confianza" para validar los certificados de su contraparte; usando para esto mensajes de autenticación con un formato similar al definido en [GHS03].

Otro trabajo relacionado con la autenticación de mensajes en DHCP se presenta en [KS02]. En dicha investigación, Komori et. al. sugieren un mecanismo de autenticación donde el cliente debe ser previamente certificado usando un identificador de usuario y una clave, esto con la intención de prevenir el uso ilegítimo de direcciones IP. Bajo este escenario los servidores deben almacenar cierta información del cliente certificado (Identificador del Usuario, dirección MAC, y dirección IP); de este modo el servidor permitirá el tráfico de datos desde el cliente hacia Internet a través de la puerta de enlace de la red.

A pesar de que el RFC 3118 fue publicado en el año 2001 y que se han realizado varias investigaciones para brindar autenticación al protocolo DHCP, los autores de este trabajo no consiguieron una implementación completa y funcional que permita agregar seguridad a DHCP. El desarrollo más cercano a una implementación funcional de seguridad para DHCP se presenta en el artículo [JH05], donde los autores presentan un método de autenticación para mensajes DHCP usando un algoritmo de llaves de una vía (HMAC-MD5). El desarrollo de dicha propuesta utiliza los formatos de mensajes propuestos en el RFC 3118; sin embargo, no utiliza ninguno de los métodos de autenticación descritos en el RFC, por lo que no es posible validar la implementación.

Este artículo presenta la experiencia de los autores al implementar los mensajes de autenticación para DHCP tal como se describen en [DA01]. En la implementación desarrollada se siguió un enfoque incremental, donde en primera instancia se implementaron los mensajes de autenticación usando el método *Configuration Token*, para luego desarrollar el método *Delayed Authentication* [Rub11]. Para ambas implementaciones fue necesario tomar en cuenta un conjunto de consideraciones adicionales a las descritas en [DA01], las cuales se explican a profundidad en este trabajo.

El presente trabajo de investigación se encuentra estructurado de la siguiente manera. La Sección 2 describe el soporte de autenticación para mensajes DHCP tal como se específica en el RFC 3118. En la Sección 3 se explican detalladamente los aspectos relacionados al proceso de implementación de la solución de seguridad para DHCP usando los métodos *Configuration Token* y *Delayed Authentication*. Con la finalidad de validar el correcto funcionamiento de la implementación desarrollada, esta fue sometida a diferentes escenarios de prueba, los cuales se presentan en la Sección 4. En esta sección también se incluye el análisis de los resultados para cada escenario de prueba ejecutado. Finalmente, en la Sección 5 se concluye acerca de los resultados obtenidos en esta investigación, y se plantean algunos trabajos futuros.

2. Autenticación para Mensajes DHCP

La autenticación en mensajes DHCP es una opción definida en el RFC 3118 [DA01] que se basa en un *ticket* de autenticación; usando este *ticket*, solo a las estaciones clientes autorizadas se les permite configurar sus interfaces de red de manera automática vía un servidor DHCP. La autenticación no se limita solo a los clientes, también puede ser usada para autenticar los mensajes enviados por un servidor DHCP.

La Figura 1 muestra el formato de la opción de autenticación para mensajes DHCP, y su descripción se presenta a continuación:

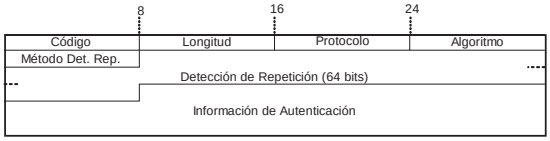

Figura 1: *Formato de la opción de autenticación para mensajes DHCP.*

- **Código**: El código que corresponde a éste tipo de mensajes es el número 90.
- **Longitud**: Contiene la longitud en bytes de los campos "Protocolo", "Algoritmo", "Método Det. Rep.", "Detección de Repetición" e "Información de Autenticación".
- **Protocolo**: Indica la técnica en particular para la autenticación usada en esa opción.
- **Algoritmo**: Indica un algoritmo a utilizar en base al protocolo indicado en el campo anterior.
- **Método Det. Rep. (Método de Detección de Repetición, o RDM)**: Indica el método a utilizar para detectar posibles mensajes duplicados.
- **Detección de Repetición**: Contiene un valor utilizado para detectar ataques de repetición que varía según el "Método Det. Rep.".
- **Información de Autenticación:** Este valor varía dependiendo del tipo de autenticación usado.

Dos métodos de autenticación *Configuration Token* y *Delayed Authentication* son detallados en el RFC 3118. En los mensajes del tipo *Configuration Token* se hace envío de un valor conocido previamente por el cliente y el servidor que es utilizado como un método básico de autenticación semejante al provisto por una contraseña. Dado que en este método no es usado ningún algoritmo de cifrado el valor del campo Algoritmo debe ser cero (0); adicionalmente en este tipo de mensajes solo es soportado un tipo de Detección de Repetición básico, el cual básicamente consiste en un contador monótono creciente (por ejemplo, una marca de tiempo utilizando un protocolo de manejo de tiempo como NTP – Network Time Protocol). El Método de Detección de Repetición descrito anteriormente se denota con el valor cero (0) en el campo correspondiente.

Los mensajes del tipo *Delayed Authentication* son definidos por el valor uno (1) en el campo Protocolo y estos usan una función criptográfica estilo *hash*, como MD5, para autenticar los mensajes intercambiados por los clientes y servidores DHCP. En este tipo de mensajes el campo Información de Autenticación se divide en dos subcampos, uno de ellos se utiliza para almacenar un identificador usado para calcular el *hash*, y el otro representa el valor del *hash*. El valor del campo Algoritmo es uno (1), lo cual denota el uso del algoritmo HMAC-MD5.

Independientemente del método de autenticación usado, un mensaje es considerado válido por el receptor si el valor en el campo Detección de Repetición es coherente con el método descrito por el campo RDM, y el emisor del mensaje puede demostrar que conoce la llave compartida o contraseña.

3. Diseño e Implementación

En esta sección se describen las consideraciones y detalles de la implementación desarrollada para añadir soporte de autenticación a mensajes DHCP usando los métodos *Configuration Token* y *Delayed Authentication* [Rub11].

3.1 Consideraciones de Diseño

En primer lugar, dado que el interés de esta investigación se basó en la implementación de los métodos de autenticación en DHCP y no en desarrollar por completo una implementación del protocolo, se seleccionó una implementación funcional de DHCP conocida como ISC (Internet Systems Consortium - Consorcio de Sistemas de Internet) para modificarla e incluirle el soporte de autenticación descrito en el RFC 3118. Esta implementación fue seleccionada ya que es de código abierto, y además es ampliamente usada en sistemas estilo UNIX. Adicionalmente, el hecho de trabajar con una implementación bien conocida del protocolo facilitó la realización de las pruebas.

En segundo lugar, dado que algunas partes del RFC 3118 son ambiguas y no profundizan en aspectos que se consideraron claves, la implementación desarrollada se basa en las siguientes consideraciones y asunciones:

- El procesamiento de la opción de autenticación debe ser transparente para DHCP. Esto es, luego de ser procesada la opción de autenticación, la misma es removida del mensaje DHCP. El mensaje resultante será procesado por el código original del ISC DHCP como si nunca hubiese existido dicha opción.
- Un mensaje DHCP debe contener solamente una opción de autenticación, aún cuando no hayan indicaciones al respecto en el RFC 3118.
- Los archivos que contienen los registros de llaves utilizadas, así como las marcas de tiempo para prevenir ataques de repetición, sólo serán actualizados luego de que un mensaje DHCP sea procesado por completo.
- Al usar el método de *Configuration Token* no será obligatorio el uso de la opción *Client Identifier*; sin embargo, será obligatorio en el método *Delayed Authentication*.
- Al usar el método de *Delayed Authentication* si no se especificó previamente en el archivo de configuración del cliente algún *Client Identifier*, se añadirá esta opción al momento de construir la opción de autenticación. El valor de *Client Identifier* en este caso corresponderá a la dirección MAC de la interfaz por la que el cliente esté enviando el mensaje.
- El único método de detección de ataques de repetición soportado es el contador monótonamente creciente.
- Las llaves a utilizar por cada uno de los dispositivos serán distribuidas siguiendo el enfoque de predistribución de llaves. La distribución manual de cada conjunto de llaves con sus respectivos identificadores es tarea del administrador del sistema.

3.2 Detalles de Implementación

Como se mencionó en la Sección 3.1, se modificó la implementación de DHCP desarrollada por ISC para agregarle soporte de autenticación a los mensajes DHCP, en particular en esta sección se detallan los cambios realizados para incluir los métodos *Configuration Token* y *Delayed Authentication*.

Con la intención de activar el uso del método de autenticación, los demonios DHCP (servidor/cliente) son iniciados vía línea de comando usando un argumento especial que indica el método de autenticación a utilizar, el valor de este argumento podría ser el método *Configuration Token* o el método *Delayed Authentication*. Al usar el soporte de autenticación, la función de autenticación que se ha implementado debe establecer los valores adecuados a todos los campos de la opción de autenticación en los mensajes DHCP salientes. En el otro extremo de la comunicación, el receptor debe determinar si el mensaje de autenticación recibido es válido antes de iniciar su procesamiento, en caso de que el mensaje recibido sea inválido el mensaje es descartado. Específicamente, los siguientes criterios fueron tomados en cuenta para validar el mensaje:

- La opción de autenticación debe estar presente.
- El valor del campo Detección de Repetición debe ser mayor que el valor que se haya recibido desde el mismo emisor en cualquier mensaje previo. Esta verificación pretende prevenir ataques de repetición.

- Al utilizar el método *Configuration Token* los campos Algoritmo, Protocolo y Método Det. Rep deben valer cero. En su lugar, al utilizar el método *Delayed Authentication* los campos Algoritmo y Protocolo deben valer uno, y Método Det. Rep debe valer cero, de acuerdo a lo expuesto en la Sección 2.
- El valor de la clave usado por el cliente y el servidor debe ser exactamente el mismo.
- Solo una opción de autenticación debe estar presente.

Un archivo destinado a la detección de repetición se procesa cada vez que inicia el demonio DHCP en el sistema. Dicho archivo inicialmente se encuentra vacío. Luego de la recepción y validación de un mensaje DHCP con soporte de autenticación, el valor del campo Detección de Repetición y un identificador del equipo se almacenan en dicho archivo con la finalidad de comparar estos valores con el de los próximos mensajes. En particular, para el mecanismo *Delayed Authentication*, se crean tres archivos adicionales: el primer archivo contiene los valores de las llaves a utilizar y sus respectivos identificadores; el segundo archivo, que inicialmente se encuentra vacío, almacena el identificador de la última llave utilizada por cada equipo que se haya autenticado exitosamente. El tercer archivo solo se crea en el cliente y almacena la dirección IP del servidor DHCP del cual se ha recibido la última dirección IP usada por el cliente.

La implementación de los métodos *Configuration Token* y *Delayed Authentication* difiere en las actividades de inicialización del demonio, así como en el intercambio de mensajes DHCP. A continuación se presentan las diferencias de implementación entre ambos métodos de autenticación. Para el método *Configuration Token* se establece una única contraseña para todos los equipos con los que exista alguna comunicación, la cual se incluye en cada uno de los mensajes DHCP intercambiados entre cliente y servidor. En el método *Delayed Authentication* se establece el algoritmo de cifrado a usar y se inicializan ciertas estructuras de datos necesarias para la construcción del *hash*. A diferencia del método anterior, en *Delayed Authentication* el cliente envía un primer mensaje *DISCOVER* con el campo Información de Autenticación vacío y es el servidor quien selecciona la llave a utilizar en el intercambio de mensajes. La llave es seleccionada al azar de entre todas las llaves disponibles. Una vez seleccionada la llave, sólo se revela su identificador en los mensajes DHCP, es decir, nunca se transmite el valor de la llave a través de la red. El valor del campo Información de Autenticación contiene un *hash* (HMAC-MD5) calculado usando el mensaje DHCP y el valor de la llave. De forma análoga, el cliente debe realizar el proceso de verificación del campo Información de Autenticación calculando nuevamente el *hash* del mensaje, y determinar si dicho mensajes es procesado o descartado.

Las acciones realizadas por el cliente y el servidor durante el intercambio y validación de los mensajes en los métodos *Configuration Token* y *Delayed Authentication* se observan en la Figura 2 y Figura 3 respectivamente.

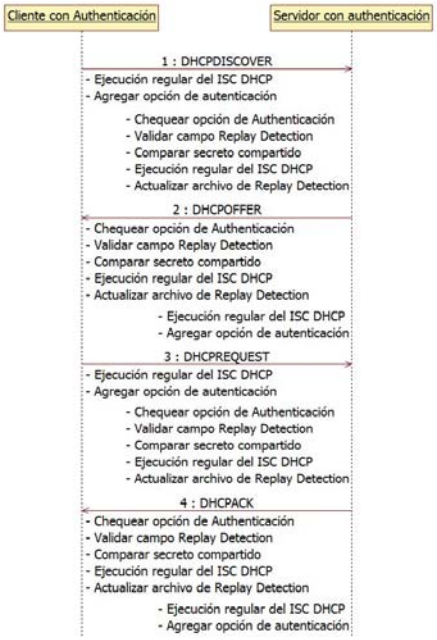

Figura 2: *Proceso de autenticación usando el método Configuration Token.*

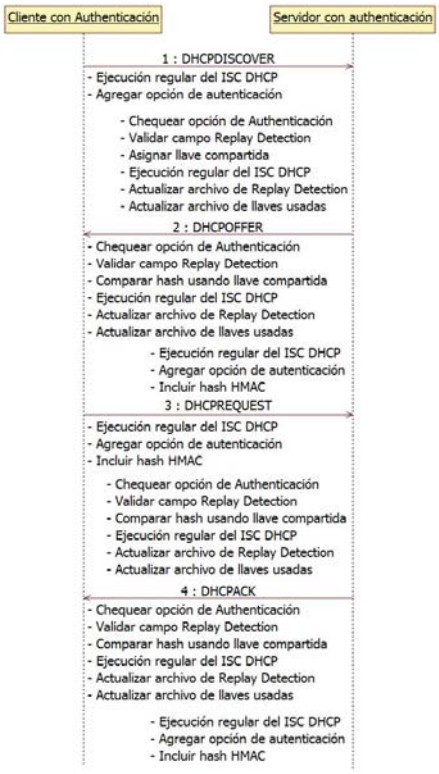

Figura 3: *Proceso de autenticación usando el método Delayed Authentication.*

4. Resultados y Discusión

La implementación desarrollada fue sometida a diversos escenarios de prueba, con el propósito de evaluar que su comportamiento es coherente con las especificaciones definidas en el RFC 3118, en lo que respecta a la correcta validación de mensajes DHCP. Las pruebas descritas en esta sección fueron ejecutadas para ambos métodos de autenticación: *Configuration Token* y *Delayed Authentication*.

La herramienta de captura de tráfico Wireshark [WIR13] fue utilizada para validar los mensajes DHCP con soporte de autenticación. En los resultados presentados en esta sección, se han resaltado los datos de interés para facilitar la discusión en cada escenario. Adicionalmente, los clientes y servidores involucrados en cada uno de escenarios de prueba fueron configurados usando VMware Workstation [VMW13] con las siguientes características:

- **Sistema Operativo:** Debian 6.0.1 (Squeeze).
- **Procesador:** Intel i7 2.6 GHz (1 núcleo).
- **Memoria RAM:** 256 MB.
- **Versión DHCP:** ISC DHCP 4.2.1-P1 [ISC13].

Con la intención de validar el comportamiento y coherencia de la implementación de DHCP con autenticación desarrollada, se definieron diferentes topologías de red sobre las cuales posteriormente se ejecutaron diversos escenarios de pruebas. La primera topología de red solo involucra un cliente y un servidor DHCP sobre la misma subred como se ilustra en la Figura 4. Esta topología se utilizó en los escenarios de prueba del 1 al 5.

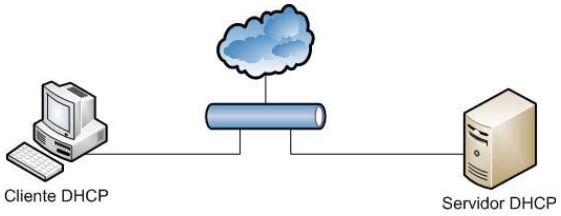

Figura 4: *Topología de red simple para DHCP con autenticación.*

En la segunda topología se introdujo un agente de relevo DHCP entre el cliente y el servidor, esto con la finalidad de comprobar si los mensajes de DHCP con autenticación atraviesan sin inconveniente el agente de relevo. Esta topología se utilizó en el escenario de prueba 6.

Figura 5: *Topología de red con agente de relevo DHCP con autenticación.*

Para la última topología se consideraron varios clientes y servidores DHCP en la misma subred como se muestra en la Figura 6. En esta oportunidad los clientes y servidores usaban o no algún método de autenticación; del mismo modo, compartían algún secreto o llave que permitía el intercambio de mensajes con otro dispositivo, es decir, en esta topología los clientes solo podían adquirir una dirección IP de aquellos servidores con los que se compartía el mismo secreto o llave y adicionalmente usaban el mismo método de autenticación; o bien si no utilizaban ningún método de autenticación. La topología descrita recientemente se empleó en las pruebas del escenario 7.

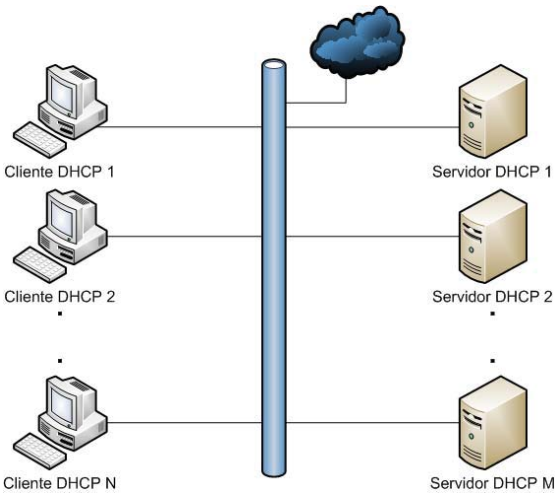

Figura 6: *Topología de red con múltiples clientes y servidores DHCP con autenticación.*

4.1 Escenario 1: Validación de la Opción de Autenticación

El escenario 1 se diseñó con la intención de corroborar si un cliente es capaz de adquirir información de configuración de red vía mensajes DHCP con la opción de autenticación habilitada. Durante la realización de esta prueba el cliente y el servidor DHCP se iniciaron usando el mismo método de autenticación, además de utilizar el mismo secreto compartido o conjunto de llaves. En las Figura 7 y Figura 8 se puede apreciar el intercambio de mensajes con autenticación (mensajes *DHCPDISCOVER*) usando los métodos *Configuration Token* y *Delayed Authentication* respectivamente.

```
Option: (t=90,l=21) Authentication
    Option: (90) Authentication
    Length: 21
    Value: 000000507a4b050008555f746573745f746f6b656e
    Protocol: configuration token (0)
    Algorithm: 0
    Replay Detection Method: Monotonically-increasing counter (0)
    RDM Replay Detection Value: 507a4b050008555f
    Authentication Information: 746573745f746f6b656e
End Option
```

Figura 7: *Autenticación vaílda usando Configuration Token.*

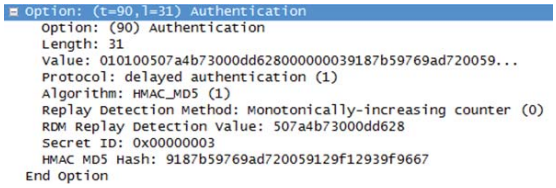

Figura 8: *Autenticación válida usando Delayed Authentication.*

4.2 Escenario 2: Opción de Autenticación no Presente

En este escenario el cliente se inició sin soporte de autenticación. El servidor recibió un mensaje *DHCPDISCOVER* sin opción de autenticación, por lo que descartó el mensaje y el cliente no pudo obtener información de configuración de red. De forma similar, un cliente que recibió un mensaje sin la opción de autenticación descartó dicho mensaje. En la Figura 9 se observa una captura de un mensaje DHCP que no posee la opción de autenticación.

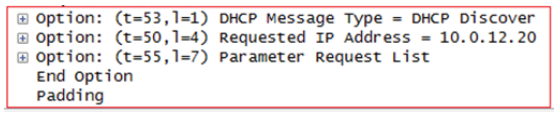

Figura 9: *Porción de una captura en Wireshark que muestra la ausencia de la opción de autenticación en un mensaje DHCPDISCOVER.*

4.3 Escenario 3: Uso de Clave o Llave Incorrecta

El uso de una clave o llave incorrecta debe ser detectado durante el proceso de autenticación en DHCP, es por esto que este escenario pretende validar el correcto funcionamiento de la implementación de autenticación para DHCP que se ha desarrollado. Específicamente en este escenario para el caso de *Configuration Token*, tanto el cliente como el servidor usaron un secreto distinto ("wrong_token" y "test_token" respectivamente), por lo que ambos descartaron cualquier mensaje que se enviaron entre sí, tal como lo establece el RFC 3118. Cuando se utilizó el método *Delayed Authentication*, si no se encontraba un identificador de llave o si la llave era distinta, el cálculo del *hash* no podía completarse o sencillamente resultaba en un *hash* distinto, por lo que se descartaba el mensaje. La captura en la Figura 10 muestra el uso de un *token* distinto, mientras que la captura en la Figura 11 muestra el uso de identificadores no aceptados en *Delayed Authentication* (el cliente sólo posee la llave con ID 1 y el servidor usa una llave con ID 2).

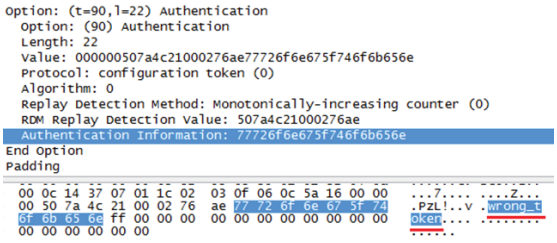

Figura 10: *Uso de clave incorrecta en el método Configuration Token.*

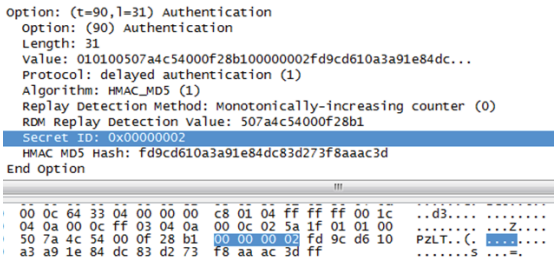

Figura 11: *Uso de llave incorrecta en el método Delayed Authentication.*

4.4 Escenario 4: Valor de Detección de Repetición Inaceptable

Para la realización de esta prueba se modificó en el servidor el archivo que contiene los valores de detección de repeticiones y se cambió la marca de tiempo del cliente a una fecha en el futuro como se aprecia en la Figura 12.

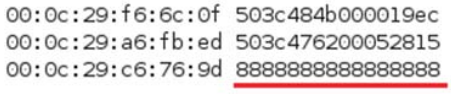

Figura 12: *Modificación en el archivo Replay Values del servidor*

El servidor recibió un mensaje con un valor de detección inferior (no aceptable) por lo que el mensaje fue descartado. En la Figura 13 se muestra que el valor de detección de repetición enviado por el cliente es menor que el valor encontrado en el archivo del servidor.

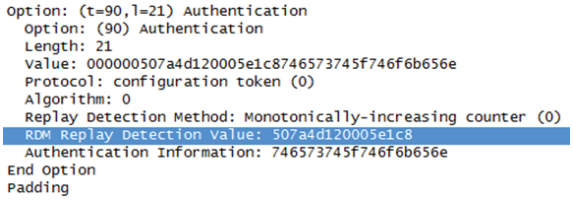

Figura 13: *Valor no válido para el método de detección de repetición.*

4.5 Escenario 5: Valores no Válidos en los Campos Protocolo, Algoritmo y RDM

El escenario 5 pretende determinar si mensajes DHCP con autenticación que contengan valores no válidos en sus campos son descartados con base a las especificaciones del RFC 3118. Para este escenario el cliente se modificó con la intención de que enviara valores no aceptados o conocidos por el servidor para los campos: Protocolo, Algoritmo y RDM. El servidor descartó todos y cada uno de los mensajes ya que los valores de los campos eran inválidos. Por ejemplo, al enviar un valor inválido en el campo RDM, el servidor descarto el mensaje, debido a que no conocía el método de detección de ataques de repetición usado por el cliente. La Figura 14 refleja este comportamiento y en ella se observa la palabra *Unknown*, que indica que el valor del campo RDM es un método no soportado actualmente.

```
Option: (t=90,l=21) Authentication
  Option: (90) Authentication
  Length: 21
  Value: 0000014fcba17500080867746573745f746f6b656e
  Protocol: configuration token (0)
  Algorithm: 0
  Replay Detection Method: Unknown (1)
  Replay Detection Value: 4fcba17500080867
  Authentication Information: 746573745f746f6b656e
End Option
Padding
```

Figura 14: *Valor desconocido para el campo de método de detección de repetición.*

4.6 Escenario 6: Soporte de Autenticación vía Agente de Relevo

En este escenario se ubicó al cliente y al servidor en dos sub redes distintas. Adicionalmente se agregó una tercera máquina conectada a ambas subredes, y se configuró como agente de relevo DHCP. El agente de relevo escuchaba y retransmitía peticiones DHCP hacia un servidor predeterminado. Se enviaron mensajes autenticados a través del agente de relevo y como resultado este modificó el valor del campo *giaddr* del mensaje DHCP, indicando que el mensaje pasó a través del agente de relevo señalado. Las capturas en la Figura 15 y la Figura 16 reflejan esta acción.

```
Option: (t=90,l=21) Authentication
  Option: (90) Authentication
  Length: 21
  Value: 000000507a4e66000b1840746573745f746f6b656e
  Protocol: configuration token (0)
  Algorithm: 0
  Replay Detection Method: Monotonically-increasing counter (0)
  RDM Replay Detection Value: 507a4e66000b1840
  Authentication Information: 746573745f746f6b656e
End Option
Padding
```

Figura 15: *Uso del método Configuration Token a través de un agente de relevo.*

```
Option: (t=90,l=31) Authentication
  Option: (90) Authentication
  Length: 31
  Value: 010100507a4ebf00096fa6000000032b908105364f31f139...
  Protocol: delayed authentication (1)
  Algorithm: HMAC_MD5 (1)
  Replay Detection Method: Monotonically-increasing counter (0)
  RDM Replay Detection Value: 507a4ebf00096fa6
  Secret ID: 0x00000003
  HMAC MD5 Hash: 2b908105364f31f139ef174965ac984f
End Option
```

Figura 16: *Uso del método Delayed Authetication a través de un agente de relevo.*

4.7 Escenario 7: Autenticación entre Múltiples Clientes y Servidores DHCP

Para las pruebas ejecutadas en este escenario se ubicó en una misma sub red a un gran número de clientes y servidores DHCP funcionando simultáneamente. Específicamente se contó con 10 servidores y 20 clientes con diferentes configuraciones, en general la configuración de cada uno de los equipos involucrados variaban en el método de autenticación soportado, y en las claves y llaves intercambiadas. Por limitaciones de espacio en este artículo no se expone la configuración de cada cliente y servidor; sin embargo, los valores utilizados durante las pruebas en este escenario se encuentran disponibles en [Rub11].

Dependiendo de la configuración establecida, un cliente sólo podía obtener los parámetros de configuración de red de aquellos servidores con los que se podía autenticar exitosamente. De este modo tanto el cliente como el servidor descartaban los mensajes que no estaban debidamente autenticados. Este comportamiento se refleja en la Figura 17 y la Figura 18 donde se pueden apreciar los *logs* de un cliente y de un servidor involucrados en este escenario.

Cliente DHCP

```
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
Key ID unknown.
HMAC not valid from 10.0.0.205, packet discarded.
Key ID unknown.
HMAC not valid from 10.0.0.203, packet discarded.
No Authentication option from 10.0.0.209, packet discarded.
DHCPOFFER from 10.0.0.201
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.0.0.201
bound to 10.0.0.13 -- renewal in 54 seconds.
```

Figura 17: *Extractos del log del cliente DHCP.*

Servidor DHCP

```
No Authentication option from 00:23:12:e7:37:89, packet discarded.
No Authentication option from a0:0b:ba:db:44:d3, packet discarded.
DHCPDISCOVER from 00:0c:29:4d:6c:1f via eth0
DHCPOFFER on 10.0.0.13 to 00:0c:29:4d:6c:1f via eth0
DHCPREQUEST for 10.0.0.13 (10.0.0.201) from 00:0c:29:4d:6c:1f via
eth0
DHCPACK on 10.0.0.13 to 00:0c:29:4d:6c:1f via eth0
Key ID unknown.
HMAC not valid from 00:0c:29:cd:62:ee, packet discarded.
Wrong PROTOCOL in use from 00:0c:29:a9:9c:0f, packet discarded.
```

Figura 18: *Extractos del log del servidor DHCP.*

Del lado del servidor se observa que las primeras dos líneas corresponden a mensajes que fueron descartados por no poseer una opción de autenticación. Las siguientes cuatro líneas corresponden a la autenticación y asignación de una IP de manera exitosa a un cliente. Las siguientes dos líneas corresponden al descarte de un mensaje por el uso de una llave desconocida y la última línea corresponde al descarte de un mensaje por usar un método de autenticación distinto al utilizado por el servidor.

4.8 Resultados Generales de las Pruebas Realizadas

Luego de haber ejecutado las pruebas descritas en la Sección 4, se pudo corroborar que la implementación desarrollada en este trabajo cumple con las funcionalidades necesarias para llevar a cabo correctamente la autenticación en mensajes DHCP tal como lo describe el RFC 3118.

5. Conclusiones

En este artículo se ha descrito la posibilidad de incorporar la opción de autenticación a los mensajes DHCP usando los métodos *Configuration Token* y *Delayed Authentication*. La posibilidad de incorporar autenticación en los mensajes DHCP permite aliviar los problemas de seguridad asociados al protocolo. La principal ventaja de la autenticación vía los métodos *Configuration Token* y *Delayed Authentication* es la factibilidad de incorporarlos al protocolo DHCP. A pesar de que los mecanismos de autenticación mencionados fueron publicados en el año 2001, estos no han sido implementados o incorporados a alguna implementación funcional de DHCP.

En esta investigación se modificó una implementación de DHCP bien conocida, llamada ISC DHCP, para incorporarle soporte de autenticación. La implementación desarrollada siguió un enfoque incremental al incorporar los métodos *Configuration Token* y *Delayed Authentication*. Los resultados obtenidos durante las pruebas demuestran que la implementación desarrollada es sencilla y funcional, lo cual permite concluir que el uso de un mecanismo de seguridad que restrinja a quién se le otorga una dirección IP se puede llevar a cabo sin incluir elementos o equipos adicionales que pudiesen añadir complejidad a una red existente.

El principal aporte de este trabajo de investigación es el hecho de proveer una solución real y factible para la implementación de mecanismos de autenticación para la obtención de una dirección IP en dispositivos funcionando bajo la plataforma Linux. Adicionalmente, la implementación desarrollada representa una contribución para la comunidad de administradores de sistemas ya que provee una alternativa segura y sencilla para la asignación de direcciones IP.

Como trabajos futuros a esta investigación se propone extender el conjunto de pruebas sobre la implementación desarrollada, por ejemplo, la implementación podría someterse a pruebas de estrés. Adicionalmente sería interesante determinar la sobrecarga que genera el procesamiento de los mensajes de autenticación sobre el protocolo básico de DHCP. Finalmente, sería conveniente adaptar la implementación desarrollada a las opciones de autenticación para el protocolo DHCPv6.

Referencias

[DA01] DROMS, R. and ARBAUGH, W.*: Authentication for DHCP Messages*. (2001). RFC 3118.

[Dro97] DROMS, R.: *Dynamic Host Configuration Protocol*. (1997). RFC 2131.

[GHS03] GLAZER, G., HUSSEY, C., and SHEA, R.: *Certificate-Based Authentication for DHCP*. (2003). Internal report, University of Calgary.

[HFP*99] HOUSLEY, R., FORD, W., POLK, W., and SOLO, D.: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. (1999). RFC 2459.

[HLA*01] HORNSTEIN, K., LEMON, T., ABOBA, B., and TROSTLE, J.: *DHCP Authentication via Kerberos V*. (2001). IETF Internet-Draft.

[ISC13] Internet System Consortium: *http://www.isc.org/software/dhcp*. (2013).

[JH05] HONGIL, J. and HAN, J.: *DHCP Message Authentication with an Effective Key Management*. (2005). In Proceedings of IS'2005, Information Society.

[KS02] KOMORI, T. and SAITO, T.: *The Secure DHCP System with User Authentication.* (2002). In Proceedings of the 27th Annual IEEE Conference on Local Computer Networks.

[M*00] MILLS, D. et al.: *Network Time Protocol Version 4: Protocol and Algorithms Specification*. (2010).

[NHR05] NEUMAN, C., HARTMAN, S., and RAEBURN, K.: *The Kerberos Network Authentication Service (V5)*. (2005). RFC 4120.

[Rub11] RUBEL, D.: *Una Propuesta para Diseñar y Desarrollar un Sistema de DHCP con Mensajes de Autenticación.* (2011). Reporte Interno, UCV.

[VMW13] VMware: *http://www.vmware.com.* (2013).

[WIR13] Wireshark: *http://www.wireshark.org*. (2013).

[XMW11] XU, Y., MANNING, S., and WONG, M.: *An Authentication Method based on Certificate for DHCP*. (2011) IETF Internet-Draft.