HACIA UN MEJOR ENTENDIMIENTO DE LOS ATAQUES AL PROTOCOLO ARP, A TRAVÉS DE LA IDENTIFICACIÓN DE ÁRBOLES DE ATAQUE EN UNA RED CERRADA

Chiang, Luis [1] ; Abad, Cristina Ms.Sc [2]
[1 2 3] Grupo de Visualización Científica y Sistemas Distribuidos
[1 2 3] Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
luis_chiang@fastmail.fm, cabad@fiec.espol.edu.ec

1. Introducción

ARP (Address Resolution Protocol), protocolo utilizado en redes Ethernet, sirve para obtener la dirección física de un computador (MAC Address) de la red preguntando a toda la red mediante un mensaje broadcast por el propietario de la dirección IP. Quien tiene esa dirección IP responde directamente a quien hizo la solicitud.

El protocolo ARP es un protocolo sin estado, y no tiene información de cuáles fueron las solicitudes realizadas, ni las respuestas anteriores. Cada respuesta nueva sobreescribe a la anterior en la tabla cache ARP.

El funcionamiento estándar de ARP está documentado en el RFC 806, pero pequeños detalles de implementación del protocolo dependen del sistema operativo, los cuales pueden agregar algunos mecanismos sencillos de seguridad.

El problema de los ataques a este protocolo radican en que la respuesta no puede ser autenticada y por lo tanto, alguien más que no sea el autentico dueño de esa IP puede enviar una respuesta falsa y hacerse pasar por otra computadora. Para una mayor eficiencia, la asociación IP-MAC recibida en la respuesta ARP se almacena por un cierto tiempo en la tabla cache ARP. En el caso de darse un ataque como el descrito, se dice que la tabla cache del host fue “envenenada”. De esta manera quien hace la solicitud inicial no se comunicara con el computador correcto si no con el falso y le enviará la información que era para el destinatario original.

Un agravante de este problema es que no es necesario ser un hacker experto para montar este tipo de ataques, ya que hay herramientas que uno puede bajarse de Internet para realizarlos. El problema del envenenamiento ARP es un problema grave, que compromete la confidencialidad de los datos enviados en nuestras redes de área local (y desde ahí, hacia Internet), y que hasta el momento no tiene una solución ideal.

Uno de los motivos por los que todavía no hay disponible una solución eficiente y económica al problema es que lamentablemente no existen estudios detallados y exhaustivos del problema. Mucha de la información para realizar los ataques ARP se encuentran en sitios Web de piratas, los cuales no son nada técnicos ni muy explicativos. Además, dicha información está incompleta y se encuentra disponible de manera desorganizada. Lastimosamente no existen estudios donde se examinen todas las combinaciones para realizar los envenenamientos ARP. Estos estudios ayudarían a detectar este tipo de fallas en las redes o para validar la eficiencia de alguna solución.

Dada la importancia del problema descrito, y de la necesidad imperativa de estudios académicos en el área, un equipo de investigación de la FIEC, con fondos del programa VLIR-ESPOL (Componente 8) está estudiando en paralelo el problema y su solución [1, 2].

En este trabajo presentamos un primer paso hacia un estudio académico, detallado y

exhaustivo de las diferentes maneras que se pueden montar ataques al protocolo ARP. Este estudio servirá como base para trabajos posteriores, como: (1) evaluación de los mecanismos de seguridad existentes que pretenden bloquear (ciertos tipos de) ataques ARP, (2) diseño de nuevos esquemas de seguridad para ARP, (3) dejar sentadas las bases para futuros estudios del protocolo Neighbor Discovery (ND), el cual reemplazará a ARP en las redes IPv6.

2. Materiales y Métodos

Una de las mejores maneras para analizar las diferentes formas de los ataques ARP es realizando un árbol de ataque.

Los árboles de ataque, propuestos por el experto en seguridad informática Bruce Schneier [3], proveen una descripción formal y metódica sobre la seguridad de los sistemas basados en las variantes de los ataques. Se representan en estructuras de árboles, siendo la meta el nodo raíz, y las diferentes maneras de lograr esa meta son los nodos hojas.

En este caso particular la meta o nodo raíz es el envenenamiento ARP y las hojas serán las diferentes variaciones de envenenamiento.

Para poder crear estos árboles hemos armado una red de pruebas aislada en la que nuestros experimentos no comprometan la seguridad de otros usuarios. En seguridades, a este tipo de experimentos se los llama experimentos en cajas de arena (sandboxes) como se muestra en la Figura 1.

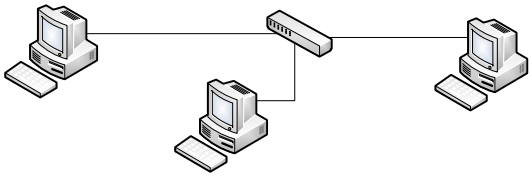

Figura 1. Ambiente de caja de arena para las pruebas de ataques ARP.

En la Figura 1 se muestra al computador Mallory, que representa al host malicioso, y es quien realizará los ataques de envenenamiento a las comunicaciones realizadas entre Alice y Bob.

Para que Alice se pueda comunicar con Bob , Alice necesita saber cuál es la dirección MAC de Bob. Para esto, envía un paquete ARP con la consulta: “Quién tiene la IP_{Bob}? Conteste a MAC_{Alice}”. Bob normalmente recibiría esa consulta y le contestaría a Alice. Pero si Mallory estaba planeando un ataque ARP, entonces le envía a Alice una respuesta falsificada, indicando que la IP_{Bob} la tiene el host con $MAC_{Mallory}$. El atacante puede proceder a envenenar de manera equivalente la caché ARP de Bob, y así montar un ataque de hombre en el medio (man-in-the-middle attack).

Existen varias variantes del ataque, las cuales estamos estudiando y serán plasmadas en el árbol de ataque que estamos desarrollando.

Mallory repite este procedimiento cada vez que Alice o Bob hacen una solicitud ARP y puede de esta manera hacer un ataque de hombre en el medio, logrando así leer los datos transferidos entre Alice y Bob.

Un pequeño árbol de ataque ARP (representado a manera de lista sangrada) se muestra en la Figura 2. En la Figura 3, se muestra lo mismo pero en forma de árbol.

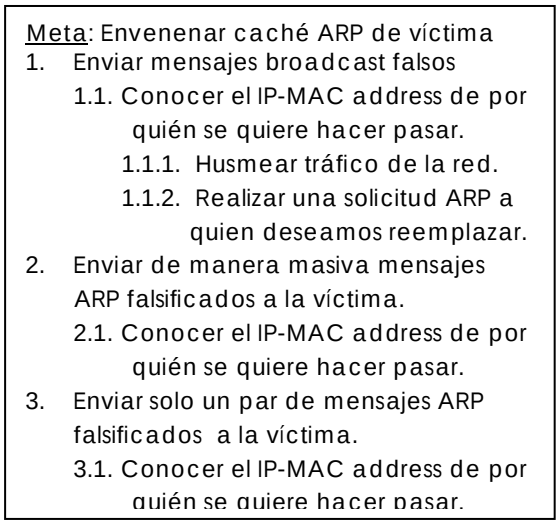

Figura 2. Árbol de ataque ARP (representación de lista sangrada)

El árbol mostrado en las Figuras 2 y 3 es una versión limitada y preliminar del árbol en el que estamos trabajando. Antes de tener el árbol final, estamos realizando una serie de pruebas de ataques ARP sistematizados y a computadores con diferentes sistemas operativos, de manera que el árbol final sea completo y sirva de referencia para trabajos futuros en el área.

3. Resultados y Discusión

Los resultados de esta investigación son importantes, ya que describirán un problema de seguridad muy grave: alguien con poca experiencia podría obtener de manera muy fácil información confidencial que podría caer en manos inapropiadas. Este problema se encuentra en todas las redes TCP/IP sobre Ethernet. Esta combinación es la más común en la actualidad y para agravar el estado del problema, éste no tiene una solución eficiente hasta el momento [1].

Esperamos sentar las bases para trabajos futuros que intenten resolver el problema de envenenamiento ARP. Nuestro estudio también podrá ser utilizado para validar las posibles soluciones al problema, como la que está realizando en paralelo un grupo de investigación del Grupo de Visualización Científica y Sistemas Distribuidos de la FIEC [2].

Esperamos que los resultados de esta investigación sirvan también como guía para un completo entendimiento del problema y los alcances del mismo, y por lo tanto, para ayudar a administradores de redes a conocer de mejor manera las vulnerabilidades de las redes frente a los ataques ARP.

4. Conclusiones

En este trabajo presentamos un primer paso hacia una documentación exhaustiva del problema de los ataques ARP por medio de árboles de ataque. La arquitectura del ambiente de caja de arena, y un árbol de ataque preliminar fueron presentados.

Hemos visto que es factible documentar árboles de ataque ARP, los que una vez culminados, servirán para sentar bases para futuros trabajos de investigación en el área. De hecho, el presente trabajo forma parte de un proyecto mayor financiado con fondos del programa VLIR-ESPOL. En dicho proyecto se utilizarán los árboles de ataque ARP para mejorar y validar el diseño de un mecanismo eficiente y económico para evitar ataques ARP en redes de área local.

5. Agradecimientos

Este trabajo ha sido posible gracias al financiamiento del programa VLIR-ESPOL y a la donación de equipos de la FIEC.

6. Referencias

[1] Abad, Cristina y Bonilla, Rafael. “An Analysis of the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks”. En *Proceedings of the IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2007 Workshops)*, Toronto, Canadá, Junio 2007, ISBN: 0-7695-2838-4.

[2] Marcos, Xavier; Ortega, Andre; Abad, Cristina. “Hacia un Mejor Entendimiento de los Ataques al Protocolo ARP, a Través de la Identificación de Árboles de Ataque en una Red Cerrada.” (enviado para su revisión a) *ESPOLciencia 2007*. Guayaquil, Ecuador. 2007.

[3] Scheneier, Bruce. Attack Trees. Disponible en línea en: http://www.schneier.com/paper-attacktrees-ddj-ft.html. (Ultima vez accesado en octubre 5 de 2007).

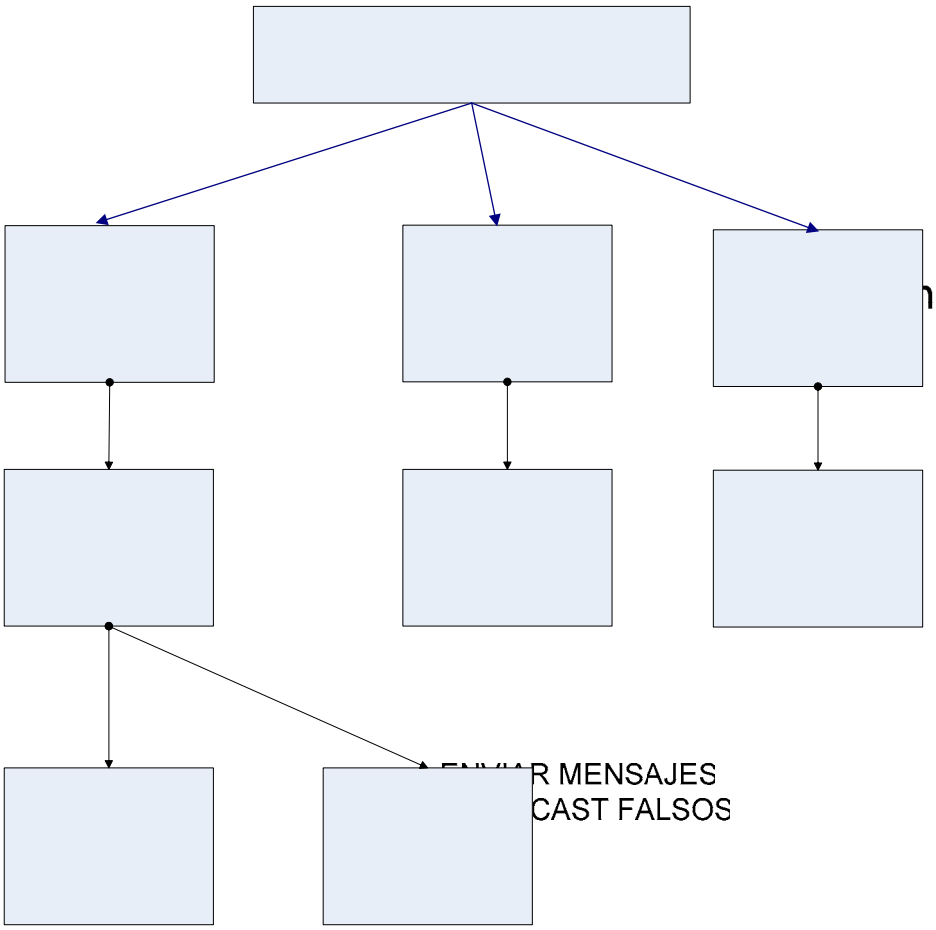

Figura 3. Árbol de ataque ARP.

CONOCER EL IP-MAC
ADDRESS DE POR QUIEN
SE QUIERE HACER PASAR

HUSMEAR TRAFICO DE LA
RED

HACER UNA
ARP A QUIEN
REEMPL