Diseño Preliminar de un Sistema para Evitar Ataques al Protocolo ARP en Redes de Área Local

Marcos, Xavier [1]; Ortega, Andre [2]; Abad, Cristina Ms.Sc.[3]
[1 2 3]Grupo de Visualización Científica y Sistemas Distribuidos
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
{xmarcos,aortega,cabad}@fiec.espol.edu.ec

1. Introducción

La información a través de una red de computadoras se envía en paquetes de datos. El computador debe conocer la dirección física de la máquina destino para que la capa de enlace pueda proceder con la transmisión de tramas (nombre que reciben los paquetes de capa de enlace de datos). Para ello se hace uso del protocolo de resolución de direcciones ARP, cuyas siglas en inglés corresponden a Address Resolution Protocol. La función de ARP es averiguar la dirección física (MAC) asociada a una dirección IP. Cuando se envían datos en la red, desde un computador a otro, el equipo que envía transmite un pedido ARP a la dirección de broadcast para que la consulta llegue a toda la red de área local. El computador que hace la consulta ARP espera que la máquina con la IP correspondiente devuelva su respuesta con su dirección MAC. Adicionalmente, se optimiza el protocolo con la introducción de cachés de ARP. En estas cachés se almacena la correspondencia entre direcciones MAC del segmento de red y las direcciones IP, de forma que antes de enviar una petición ARP se trata de resolver la dirección buscándola en las propias entradas de la caché.

El protocolo ARP trabaja bien en circunstancias regulares, pero no fue diseñado para lidiar con hosts maliciosos, de esta forma, durante el tiempo entre la transmisión de la petición ARP y la respuesta, los datos son vulnerables a modificaciones, secuestros o redireccionamiento hacia un tercero no autorizado. Cuando un host añade un mapeo <IP, MAC> incorrecto a su caché ARP, esto se conoce como envenenamiento a la caché o falsificación, a través del cual un intruso puede hacerse pasar por otro host, forzando a la víctima a que envíe los paquetes al host atacante en lugar de hacerlo al destino deseado y así ganar acceso a información sensitiva.

Los distintos ataques que pueden ser realizados a este protocolo, comprometen la seguridad de una red. Es así que existen diversos esquemas para añadir protección al protocolo ARP ya sea previniendo, detectando o mitigando el problema, pero no existe una solución perfecta pues cada una tiene sus desventajas como no haber sido probados con todos los tipos de ataques ARP, ser costosos de implementar, y además complejos de administrar. Todos estos problemas han sido estudiados y analizados previamente [1].

Nuestro objetivo es presentar un nuevo esquema para asegurar ARP y combatir los problemas a los que este protocolo es susceptible, de manera que cumpla con un número de requerimientos que la constituyan como una solución ideal.

2. Materiales y Métodos

La siguiente lista de requerimientos se debe cumplir para diseñar un esquema ideal que combata los problemas de seguridad del protocolo ARP en redes de área local [1]:

- La solución no debería requerir cambios en cada uno de los hosts de la red, por ejemplo, no se tendría que realizar la instalación de un software específico en cada host, ya que esto

incrementaría los costos administrativos.

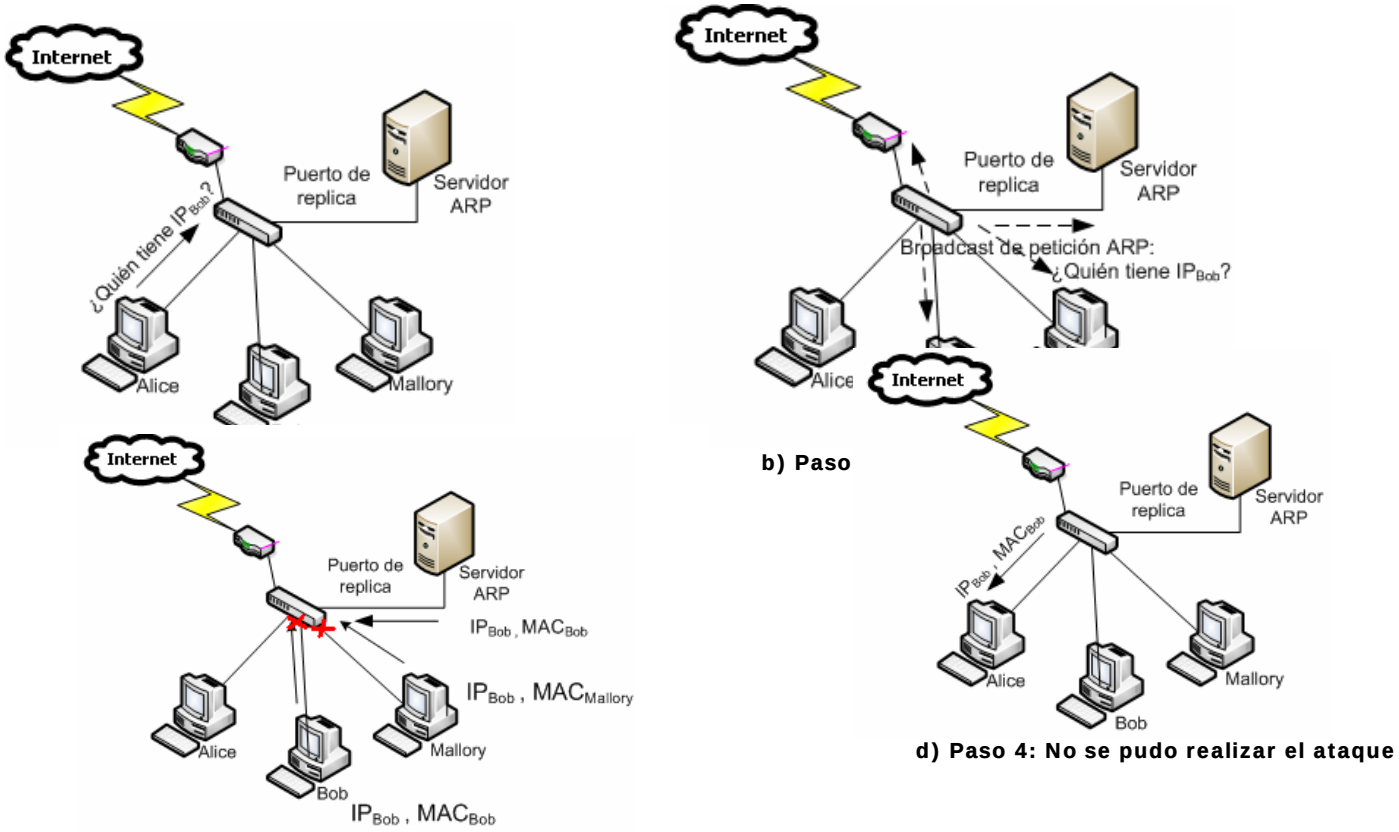
- Se deben evitar técnicas criptográficas pues disminuyen la rapidez del protocolo.
- El esquema debe estar disponible ampliamente y debe ser fácil de implementar.
- Las técnicas para prevenir o bloquear son mejores que las de detección.
- Se debe minimizar en lo posible requerimientos costosos de hardware.
- Todos los tipos de ataques ARP deben ser combatidos.

Nuestro diseño preliminar adapta algunas ideas de la inspección dinámica de ARP (DAI) implementada por Cisco, pero de manera que no se requiere el uso de switches costosos como ésta lo hace. Es un esquema centralizado compuesto por un servidor, un switch y las computadoras que conforman la red local. La función del servidor consiste en receptar todas las consultas ARP que se transmitan en la red de área local, y emite una respuesta ARP correcta (en base a una tabla de mapeos <MAC, IP> que mantiene el host utilizando una técnica conocida como DHCP snooping o en base a una tabla estática configurada por el administrador). El switch está configurado de tal manera que bloquea todas las respuestas ARP, excepto las que provengan de nuestro servidor ARP.

De esta forma, respuestas maliciosas no son transmitidas, y los ataques ARP no serán exitosos. Para que la solución funcione correctamente, necesitamos ayuda del switch, el cual debe estar configurado para bloquear respuestas ARP que provengan de cualquier puerto que no sea el de nuestro servidor ARP. Este bloqueo puede ser realizado a través de la configuración de ACLs en el switch, o de otro tipo de reglas (por ejemplo, usando reglas arptables en switches programables basados en Linux). Las siguientes reglas formarían parte del firewall implementado con arptables, el cual se utilizaría para programar el switch:

```
arptables -A INPUT -s IPSERVER --opcode 3 -j ACCEPT
arptables -A INPUT -s ! IPSERVER --opcode 3 -j DROP
```

La Figura 1 ilustra la solución propuesta.



b) Paso

c) Paso 3: Respuesta ARP del servidor ARP

d) Paso 4: No se pudo realizar el ataque

3. Resultados

Paralelamente a este trabajo de investigación se están desarrollando árboles de ataque contra ARP [2] derivados de la investigación en diferentes escenarios, los cuales nos ayudarán a comprobar que nuestra solución combate todos los tipos de problemas que este protocolo enfrenta.

De acuerdo a nuestra investigación, no se encuentra disponible ninguna herramienta que pueda ser descargada por administradores de redes y utilizada para evitar los ataques ARP. Un mecanismo similar al propuesto está disponible en los switches más costosos de Cisco y Allied Telesis, los cuales por su costo no representan una solución asequible para pequeñas y medianas empresas o para aquellas que ya tienen instalada una infraestructura de switches de una generación previa a este tipo de soluciones (las cuales ingresaron en el mercado recién en el 2005).

Nuestro diseño preliminar será validado con los árboles de ataque ARP en los que nuestro equipo de investigación está trabajando, y su rendimiento será evaluado posteriormente. Creemos que la solución propuesta representará una sobrecarga despreciable al rendimiento de la red, ya que no depende de costosos mecanismos criptográficos, y de hecho, puede ser implementada directamente en un switch Ethernet programable, prescindiendo así del computador que hace de servidor ARP (ver Figura 1).

Quisiéramos también indicar que una vez que tengamos lista la herramienta final, la publicaremos con código abierto, para su descarga e implementación en cualquier red de área local. Adicionalmente, la red necesita tener un switch Linux programable (o basado en Linux) o con soporte de ACLs. Esto no representa un impedimento, ya que existen switches basados en Linux desde $60 como el switch Linksys modelo WRT54GL.

4. Conclusión

En una red de área local existe un gran riesgo de que la comunicación sea interceptada y la información manipulada, lo que podría llegar a comprometer datos confidenciales o a interrumpir servicios. Creemos que la protección contra el robo de la información por los ataques generados contra ARP es de suma importancia tanto para los usuarios de redes hogareñas, como para aquellos de grandes empresas. Por esta razón nos vimos motivados a implementar un esquema ideal desde el punto de vista económico y técnico que pueda ser utilizado en cualquier área de red local. El diseño presentado en este artículo es un primer paso hacia la implementación de un mecanismo eficiente, eficaz, económico y asequible para proporcionar seguridad a los 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]Chiang, Luis y 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.