Transición IPv4 a IPv6: Aspectos relacionados con Seguridad Informática

Propuesta de Investigación

Silvia J. Pineda

Ingeniería de Sistemas

spineda82@unab.edu.co

Universidad Autónoma de Bucaramanga

RESUMEN

Debido al crecimiento acelerado de Internet, se ha producido un agotamiento de direcciones IPv4, razón por la cual se ha iniciado el despliegue de IPv6 a nivel mundial, para responder a la demanda de los usuarios de Internet. Lo anterior ha implicado el desarrollo de un proceso de transición entre los dos protocolos, para asegurar el adecuado despliegue de IPv6. En este documento es presentada una propuesta de investigación para el desarrollo de un estudio sobre la transición de IPv4 a IPv6 tomando en consideración aspectos relacionados con seguridad informática.

ABSTRACT

Due to the accelerated rise of the Internet in the world, there was an IPv4 address depletion, reason why it has started IPv6 globally deploying. This has involved the development of a transition process between the two protocols, to ensure an adequate IPv6 deployment. In this paper it is presented a research proposal for transition IPv4 to IPv6 development study taken in consideration computer security aspects.

Área de Conocimiento

Ingenierías.

Palabras Clave

IPv4; IPv6; mecanismos de transición; seguridad informática.

INTRODUCCIÓN

En un principio, la idea de Internet, fue introducida sólo para conectar a unas cuantas agencias estadounidenses, pero a medida que el tiempo pasaba y con él aparecían nuevos avances tecnológicos, Internet se convirtió en lo que hoy conocemos como la red de redes. El sistema de direccionamiento utilizado desde el nacimiento del Internet es el protocolo de IPv4 limitada a 2^{32} direcciones, un protocolo inherente, ligero y sencillo.

Debido a la expansión de la cobertura mundial del Internet, el uso de direcciones IP empezó a crecer, lo cual generó la necesidad de introducir una gran cantidad de extensiones, para contrarrestar el sumergimiento del protocolo IPv4 por sus características simples. Con la aparición de estás extensiones el funcionamiento de IPv4 a través de redes públicas se volvió complicado y, al mismo tiempo, se evidenció la escasez de direcciones IP para cubrir la demanda mundial.

A partir de los problemas mencionados anteriormente, fue creado el protocolo IPv6 (capacidad de 2^{128} direcciones, cerca de 670mil billones de direcciones por cada milímetro cuadrado de la tierra) y robustez, diseñada para reemplazar IPv4 mejorando el servicio de Internet [1].

Para poder implementar este nuevo protocolo, es necesario hacer una transición de IPv4 a IPv6, que en la actualidad es una extensa e importante área de investigación. En este documento, es presentada una propuesta de investigación para realizar un estudio sobre los problemas relacionados con seguridad informática en la transición de IPv4 a IPv6, para lo cual se ha propuesto la ejecución del ataque *"man-in-the-middle"*. En la Sección 2, se presentan los objetivos de la proyecto. La Sección 3 expone la metodología de investigación para la realización del proyecto. En la Sección 4 son presentados los referentes teóricos. La Sección 5 corresponde al cronograma para el desarrollo de la investigación. La Sección 6 presenta los resultados esperados del proyecto. En la Sección 7 es presentada la identificación del proyecto. Finalmente, la Sección 8 presenta las referencias bibliográficas consultadas.

OBJETIVOS

Para el desarrollo del proyecto de investigación se han propuesto los siguientes objetivos:

Objetivo General

Elaborar un estudio sobre métodos de transición de IPv4 a IPv6 haciendo énfasis en problemas relacionados con seguridad informática.

Objetivos Específicos

Elaborar un estado del arte sobre de mecanismos de transición de IPv4 a IPv6 existentes.

Realizar un diagnóstico sobre los principales problemas de seguridad existentes en la comunicación entre los protocolos IPv4 e IPv6.

Diseñar una red controlada con direccionamiento IPv4 e IPv6 para ejecutar y analizar un ataque "Man-in-the-middle".

METODOLOGÍA DE LA INVESTIGACIÓN PROPUESTA

Para el desarrollo del proyecto se han propuesto tres fases, que se relacionan directamente con los objetivos específicos del proyecto (Ver Figura 1), las cuales se describen a continuación:

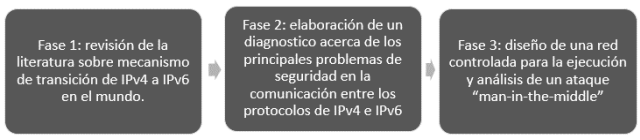

Figura 1: Fases del proceso investigativo.

Fuente: Elaboración propia.

A continuación se mostrarán las actividades que se deberán realizar para cumplir en su totalidad las fases del proyecto.

Fase 1: (i) Búsqueda y revisión de literatura sobre mecanismos de transición de IPv4 a IPv6; (ii) Lectura, análisis y clasificación de acuerdo a su importancia de las fuentes bibliográficas consultadas.

Fase 2: (i) Búsqueda y revisión de literatura enfocada a evidenciar de problemas de seguridad informática en la comunicación de estos dos protocolos; (ii) Elaboración de un diagnostico acerca de la situación actual de los problemas de seguridad informática en los mecanismos de transición de IPv4 a IPv6; (iii) Clasificación del ataque "man-in-the-middle" en el diagnóstico realizado.

Fase 3: (i) Diseño y construcción de una red controlada con direccionamiento IPv4 e IPv6; (ii) Ejecución de un ataque "man-in-the-middle" en la red controlada; (iii) Análisis del tráfico de red y el comportamiento del ataque.

REFERENTES TEÓRICOS

El despliegue de IPv6 ha sido posible gracias a diversos mecanismos de transición, que son categorizados como: (i) Dual stack: Mecanismo de transición más utilizado en el mundo, debido a su fácil implementación y soporte para los dos protocolos (IPv4 e IPv6). Este método permite que las direcciones IPv4 e IPv6 se asignen a cada nodo de la red, haciendo que sea posible utilizar ambos protocolos al tiempo; (ii) Tunneling: Utilizado para conectar dos nodos IPv6 que usan la red IPv4, encapsula los paquetes de un protocolo a otro, haciendo que así se propaguen a lo largo de la red IPv4; y (iii) Traducción: Mecanismo que está basado en la conversión de encabezados, en este sentido, cabeceras IPv4 e IPv6 se traducen entre sí. Debido a que los servicios de Internet fueron desarrollados para el protocolo IPv4, el periodo de transición puede tomar varios años, por esta razón es importante refinar los aspectos relacionados a la seguridad informática en estos mecanismos de transición [2].

Tanto en el protocolo IPv4 como en el protocolo IPv6 existen diferentes vulnerabilidades. En el contexto de IPv4 se pueden distinguir tres grandes vulnerabilidades que convergen en la fragmentación y reensamble de paquetes IPv6 en los router, un largo espacio de direcciones que hacen no práctico el escaneo de fuerza, y una capacidad de direccionamiento *end-to-end* que hacen innecesario el uso de traductores de direcciones de red (NAT). Con respecto a IPv6, las vulnerabilidades van enfocadas a cabeceras de extensión, reensamble de paquetes por dispositivos de seguridad, actualizaciones de DNS, múltiples direcciones y filtrado de ICMPv6 [3].

En este sentido, es importante identificar las técnicas de transición de IPv4 a IPv6 que contienen alguna amenaza a la seguridad, para estructurar un mecanismo que reduzca las diferencias entre los dos protocolos, con un enfoque especial a solventar las vulnerabilidades identificadas [4].

CRONOGRAMA

El cronograma de actividades para el desarrollo del proyecto, es presentado en la

Tabla 4.

Tabla 9. Cronograma de actividades

ACTIVIDAD		DURACIÓN (Meses)									
		1	2	3	4	5	6	7	8	9	10
1	Búsqueda y revisión en el mundo										
2	Lectura, análisis y clasificación										
3	Búsqueda y revisión										
4	Elaboración del diagnóstico										
5	Clasificación										
6	Diseño y construcción										
7	Análisis y Documentación										

RESULTADOS ESPERADOS

Con el desarrollo del presente proyecto de investigación se espera obtener los siguientes resultados:

Un documento que contiene el estado del arte sobre mecanismos de transición de IPv4 a IPv6 en el mundo.

Un documento que contiene el diagnóstico de los principales problemas de seguridad en la comunicación ente los protocolos de IPv4 e IPv6.

Un documento que contiene el análisis de tráfico antes, durante y después de la ejecución de un ataque "man-in-the-middle".

IDENTIFICACIÓN DEL PROYECTO

Nombre del Semillero	Semillero de Investigación en Seguridad Informática
Tutor del Proyecto	Diana Teresa Parra Sánchez
Grupo de Investigación	Grupo de Investigación en Tecnologías de Información
Línea de Investigación	Línea de Investigación en Telemática
Fecha de Presentación	Mazo 05 del 2016

REFERENCIAS

S. Kalwar, N. Bohra and A. A. Memon, "A survey of transition mechanisms from IPv4 to IPv6 — Simulated test bed and analysis," Digital Information, Networking, and Wireless Communications (DINWC), 2015 Third International Conference on, Moscow, 2015, pp. 30-34.

A. H. M. Taib and R. Budiarto, "Security Mechanisms for the IPv4 to IPv6 Transition," in 2007 5th Student Conference on Research and Development, 2007, pp. 1–6.

M. V. Vineeth and R. Rejimoan, "Evaluating the performance of IPv6 with IPv4 and its distributed security policy," in 2013 IEEE CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGIES, 2013, pp. 59–63.

A. S. Ahmed, R. Hassan, and N. E. Othman, "Security threats for IPv6 transition strategies: A review," in 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T), 2014, pp. 83–88.