LINEAS DE INVESTIGACIÓN EN REDES DE COMPUTADORAS DESARROLLADAS EN EL CENTRO DE INVESTIGACIÓN Y DESARROLLO EN INFORMÁTICA APLICADA

Redes Móviles Ad Hoc, Extensiones de Seguridad para DNS, Virtualización en la enseñanza de redes, Cableado Estructurado inteligente

Daniel Arias Figueroa, Ernesto Sanchez, Sergio Rocabado, Alejandro Barrena, Miguel Angel Aguirre

C.I.D.I.A. (Facultad de Ciencias Exactas.) / Universidad Nacional de Salta
Dirección: Av. Bolivia 5150 – Salta Capital (4400)
Tel.: +543874258614
Mails: daaf@cidia.unsa.edu.ar; esanchez@cidia.unsa.edu.ar; srocabad@cidia.unsa.edu.ar

RESUMEN

Desde el año 2000, cuando se crea el C.I.D.I.A. en el ámbito de la Facultad de Ciencias Exactas de la UNSa, a la fecha, se vienen desarrollando diferentes trabajos y proyectos de investigación relacionados con la temática de redes de datos y sistemas operativos. Actualmente esta línea de investigación se consolidó gracias a la especialización formal de los docentes e investigadores que la conforman.
En ella confluyen actividades de investigación realizadas por varios grupos de investigación con resultados visibles en su producción académica y en la formación de recursos humanos mediante el desarrollo de trabajos finales de pregrado, grado y tesis de postgrado.
Los principales ejes temáticos, que abarca la investigación en redes en el centro son las Redes Móviles Ad Hoc, Seguridad, MANET, DNS Seguro, DNSSEC, DNSCurve, Nuevas tendencias en el Cableado Estructurado, Simulación y Virtualización aplicadas a la enseñanza de redes.

Palabras clave:
Redes Móviles Ad Hoc, Seguridad, MANET, DNS Seguro, DNSSEC, DNSCurve, Nuevas tendencias en el Cableado Estructurado, Simulación y Virtualización aplicadas a la enseñanza de redes.

CONTEXTO

Una de las líneas de investigación que se desarrolla en el ámbito del C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada dependiente de la Facultad de Ciencias Exactas de la Universidad Nacional de Salta es la de redes de computadoras y sistemas operativos. Trabajamos en colaboración con el L.I.N.T.I. – Laboratorio de Investigación en Nuevas Tecnologías Informáticas perteneciente a la Facultad de Informática de la Universidad nacional de La Plata. La mayoría de los proyectos generados en este ámbito son acreditados en el Consejo de Investigación de la UNSa y otros quedan en el ámbito interno del centro hasta que adquieren mayor relevancia.

LINEAS DE INVESTIGACION y DESARROLLO

“Integración segura de MANETs a redes de infraestructura”

Motivación / Estado del arte del tema

Una de las principales ventajas de una MANET es la posibilidad de integrarla a una red de infraestructura con diferentes fines, entre otros podemos mencionar: el acceso a Internet o sistemas de información de una organización desde un dispositivo móvil y la posibilidad de transportar información a lugares sin cobertura de red.
La seguridad y el rendimiento son factores importantes para el éxito de esta integración. La “seguridad”, porque las MANETs utilizan

un medio compartido (aire) para transmitir los datos y se encuentran expuestas a posibles "ataques" y/o accesos no autorizados, y el rendimiento porque algunos o todos los dispositivos móviles de la MANET tienen capacidad de procesamiento limitada, ancho de banda reducido y son alimentados por baterías con energía limitada.

En este contexto nos propusimos investigar sobre diferentes protocolos y mecanismos de seguridad que permitan realizar una integración y/o comunicación "segura" entre redes móviles ad hoc (MANETs) y redes de infraestructura (GPRS, LAN/WAN), bajo dos premisas:

- Garantizar el cumplimiento de los siguientes aspectos de seguridad: Confidencialidad, integridad, autenticación.
- La implementación de la seguridad, en lo posible, no debe comprometer el rendimiento del dispositivo móvil: Utilización del ancho de banda, utilización de los recursos físicos (Procesador, Memoria) y consumo de energía.

Resultados y Objetivos

Los resultados de este trabajo están dirigidos a organizaciones que requieran integrar tecnologías móviles a su red de infraestructura.

Se busca concientizar a los distintos niveles jerárquicos de la organización sobre los riesgos que implica una integración "no segura", evitando así las posibles pérdidas económicas que pueden generarse por un "ataque" o acceso no autorizado a la información (activo de la organización).

Para lograr esto nos planteamos los siguientes objetivos:

- Presentar una revisión del estado del arte de seguridad en redes móviles ad hoc.
- Efectuar un análisis de alternativas para realizar comunicaciones seguras entre redes de infraestructura y redes móviles ad hoc.
- Presentar una propuesta de comunicaciones seguras para MANETs, que incluya un conjunto de recomendaciones y una guía de buenas prácticas para incorporar mecanismos de seguridad en los dispositivos móviles, teniendo en cuenta las características especiales de este tipo de redes e intentando minimizar el impacto de la seguridad en el rendimiento del dispositivo.

La revisión del estado del arte de seguridad en redes móviles ad hoc, servirá como guía para profesionales informáticos que requieran implementar políticas de seguridad en una organización.

El análisis comparativo de alternativas de seguridad para integrar MANETs a redes de infraestructura, facilitara al administrador de redes y a los programadores de aplicaciones móviles la elección de la alternativa que mejor se adapte a los requerimientos de seguridad de su organización.

La propuesta de comunicaciones seguras para MANETs, servirá como referencia para futuras implementaciones de seguridad en entornos móviles.

Referencias

1. AK Bayya, S Gupte, YK Shukla, A Garikapati, "Security in Ad Hoc Networks", Computer Science Department University of Kentucky (2007).
2. Carlton R. Davis, "Security Protocols for Mobile Ad Hoc Networks"; Phd thesis; McGill University, Montreal, QC, Canada (2006).
3. Virgil D. Gligor, "Security of Emergent Properties in Ad-Hoc Networks"; Electrical and Computer Engineering Department University of Maryland (2007).
4. Ramin Hekmat: "Ad-hoc Networks: Fundamental Properties and Network Topologies"; Delft University of Technology, The Netherlands (2006).
5. Madjid Nakhjiri, Mahsa Nakhjiri: "AAA and Network Security for Mobile Access"; John Wiley & Sons (2005)
6. H. Labiod, H. Afifi, C. De Santis: "WI-FI,BLUETOOTH,ZIGBEE AND WIMAX"; Springer (2007)

7. A. A. Adas, T. A. Shawly: “Simulation of IPSec Protocol in Ad-Hoc Networks”; Department of Electrical and Computer Engineering, Faculty of Engineering, King AbdulAziz University, Saudi Arabia (2010).

“Evaluación de Extensiones de Seguridad para DNS”

Motivación / Estado del arte del tema

Cuando el protocolo DNS fue diseñado, los principales objetivos fueron el de proporcionar un mecanismo de comunicación que fuera rápido, eficiente, escalable y de alta disponibilidad, omitiendo aspectos como la integridad y autenticidad de los datos. En la actualidad, estas omisiones han permitido un incremento significante de actividades maliciosas tales como; suplantación de identidad, distribución de malware, falsificación de respuestas DNS, entre otras. Tomado conciencia de estas fallas en el diseño original del protocolo DNS, es que organizaciones y particulares han puesto especial énfasis en la implementación de políticas y prácticas destinadas a dotar de seguridad al servicio proporcionado por DNS.

En consecuencia, a escala global, se viene trabajando en la implementación de lo que se conoce como DNSSEC (Extensiones de Seguridad para el Sistema de Nombres de Dominio), destinado a proteger el flujo de datos en el esquema DNS tradicional.

DNSSEC se presenta como un conjunto de extensiones para el sistema tradicional de DNS, diseñado para autenticar y proteger la integridad de las respuestas DNS, a través del uso de “firmas digitales basadas en clave pública”.

La información necesaria para autenticar las respuestas es almacenada en un nuevo conjunto de Registros de Recursos: [1] [2] [3]

RRSIG: Contiene la firma digital para un conjunto de Registros de Recursos (RRSet). Cada RRSet de una Zona tiene un RRSIG asociado.
DNSKEY: Contiene la clave pública asociada a un RRSIG. Una Zona puede contener múltiples registros DNSKEY.
DS: Almacena un Digesto de la clave pública de una Zona Hija asociada a una Zona Padre. A través de un proceso de delegación permite posteriormente la validación de una Cadena de Confianza.
NSEC: Permite la autenticación de respuestas negativas, es decir, verificar si una respuesta del tipo NXDOMAIN fue recibida del host consultado.

Resultados y Objetivos

Como se ha especificado anteriormente, la implementación de DNSSEC implica contar con un mayor poder de procesamiento necesario para la generación y verificación de registros. Se observa también que dada la necesidad del intercambio de estos nuevos registros en un proceso de solicitud/respuesta, el recurso que se ve más comprometido es el del ancho de banda, ya que se requiere de un aumento significativo de éste. Por otra parte, un aspecto importante es que en el proceso de validación de la Cadena de Confianza, el protocolo DNSSEC debe estar implementado en toda la jerarquía, siendo este último aspecto quizás el que demore una implementación a nivel global dado que a la fecha no todos los Dominios lo han implementado aún.[4]

Por todo lo anterior es que actualmente nos encontramos realizando tareas de investigación vinculadas con:

- La recopilación de las formas más frecuentes de ataque al Sistema DNS.
- Impacto de la adopción de las extensiones de seguridad para DNS en el ámbito universitario.
- Integración de DNSSEC con otros mecanismos de seguridad tales como IPSEC y DNSCurve. [5]

Referencias

[1] RFC 4033: “DNS Security Introduction and Requirements”. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Internet Engineering Task Force. 2005.
[2] RFC 4034: “Resource Records for the DNS Security Extensions”. Internet Engineering Task Force. 2005.
[3] RFC 4035: “Protocol Modifications for the DNS Security Extensions”. Internet Engineering Task Force. 2005.
[4] DNSSEC Deployment Initiative. Sitio oficial disponible en: http://www.dnssec-deployment.org.
[5] DNSCurve: Usable security for DNS - Daniel J. Bernstein. Sitio oficial disponible en: http://www.dnscurve.org.

“Virtualización para la enseñanza de Redes IP”

Motivación / Estado del arte del tema

Las redes de computadoras son típicamente complejas. Contienen múltiples dispositivos (Routers, servers, etc.), múltiples interfaces, múltiples protocolos corriendo, interconexiones físicas que crean topologías complejas.
Comprender las redes de computadoras sin realizar experimentos prácticos es realmente dificultoso, por no decir casi imposible. Desafortunadamente, disponer y configurar de un laboratorio de redes puede ser de un costo muy elevado y en muchos casos impracticable.

Por otro lado, realizar experimentos en una red en producción, puede ser inviable (servicios críticos para los usuarios, coordinación entre departamentos, etc.).

Como solución alternativa, existe la posibilidad de poner en marcha programas (software) que emulen un dispositivo de red de la forma mas realista posible y construir la infraestructura de red necesaria de forma virtual, sin necesidad de incurrir en los gastos de tener los dispositivos físicos. Las herramientas de virtualización permiten orquestar la creación de dichos dispositivos virtuales y permiten interconectarlos para obtener la infraestructura de red necesaria. De esta forma es posible solucionar los problemas planteados anteriormente de forma eficiente y económica. Además, la virtualización muestra, a diferencia de los simuladores, un comportamiento real del sistema, por lo tanto, nos permite disponer y configurar infraestructuras de networking con costos muy bajos, facilitando la implementación de entornos de experimentación y de enseñanza.

Mediante el uso de la virtualización, los conceptos fundamentales de las redes de datos pueden aplicarse de forma práctica en ambientes casi reales.

Resultados y Objetivos

Se plantea por un lado una investigación tendiente a exponer la evolución y estado actual de la virtualización aplicada a la enseñanza de las redes de datos y en particular a las redes IP y por otro lado, la búsqueda, selección y prueba de las herramientas más difundidas de software libre de virtualización de redes.

Referencias

1. VNUML Virtual Network User Mode Linux, http://jungla.dit.upm.es/~vnuml/
2. The User-mode Linux Kernel Home Page, http://user-mode-linux.sourceforge.net/
3. NetKit, http://www.netkit.org/
   Vmware Server, http://www.vmware.com/products/server/
4. Virtual Box, home page: http://www.virtualbox.org/
5. Qemu Open source processors emulator, http://fabrice.bellard.free.fr/qemu
6. Xen, home page: http://www.xensource.com/

“Cableado Estructurado, Estándares y nuevos componentes”

Motivación / Estado del arte del tema

En la actualidad, los diseños de las redes locales de datos deben proveer calidad, flexibilidad, valor y funcionalidad, no sólo para cubrir las necesidades actuales, también deben soportar los requerimientos futuros. La supervivencia de las organizaciones actuales

depende de la confiabilidad y efectividad del intercambio de información y éste a su vez de la confiabilidad y efectividad del diseño de su infraestructura de red. Mediante la instalación de cableado estructurado se busca crear una infraestructura que sea altamente confiable con capacidad de ofrecer servicios de telecomunicaciones, de acuerdo con los nuevos requerimientos para el manejo de la información.

Tradicionalmente, la infraestructura de cableado de un edificio corporativo es en lo último en lo que se piensa; de hecho, los cables no son contemplados en el presupuesto de construcción inicial, su planeación e instalación se realiza cuando el edificio está listo para ocuparse y, generalmente, se utilizan varios tipos de cables para distintas funciones. Se podría afirmar que el cable ocupa una de las últimas jerarquías en las preocupaciones de propietarios, ingenieros y arquitectos.

Por lo antes expuesto y, considerando que existe una demanda permanente de este tipo de redes, y que en cualquier edificación nueva se debe instalar una red de cableado confiable para el transporte y distribución de los servicios de telecomunicaciones, se propone este trabajo tendiente a esclarecer el tema de cableado estructurado propuesto en cuanto a las normativas internacionales vigentes, normas en el país si es que existen y nuevos componentes desarrollados a fin de que constituya un material de referencia para las futuras obras de cableado estructurado.

Resultado y Objetivos

Realizar una investigación tendiente a exponer la normativa vigente de cableado estructurado y las nuevas tendencias en cuanto a la utilización de nuevos componentes tal como las patcheras inteligentes.

Referencias

1. ANSI/TIA/EIA-606A. Norma para la Administración de Infraestructura de Telecomunicaciones Comercial. Mayo, 2002.
2. ANSI/TIA/EIA-568-B.1. Norma para Cableado de Telecomunicaciones en Edificios Comerciales, Parte 1: Requerimientos Generales. Abril, 2001.
3. ANSI/TIA/EIA-568-B.1-1. Norma para Cableado de Telecomunicaciones en Edificios Comerciales, Parte 1: Requerimientos Generales. Apéndice 1: Radios de curvatura mínimos de cables UTP de cuatro pares y ScTP de cuatro pares para cordones de parcheo. Julio, 2001.
4. ANSI/TIA/EIA-568-B.2. Norma para Cableado de Telecomunicaciones en Edificios Comerciales, Parte 2: Componentes de Cableado de Par Trenzado Balanceado. Abril, 2001.
5. ANSI/TIA/EIA-568-B.2-1. Norma para Cableado de Telecomunicaciones en Edificios Comerciales, Parte 2: Componentes de Cableado de Par Trenzado Balanceado.

FORMACION DE RECURSOS HUMANOS

La estructura del equipo de investigación esta conformada por docentes y alumnos de la licenciatura en análisis de sistemas y asesores externos de empresas del medio y de otras instituciones de investigación. A continuación se describen:

Formación en postgrado

- Especialidad en Seguridad y Redes – UNLP “Virtualización para la enseñanza de redes IP” Expte. 3300-3489/11-000.
- Especialidad en Seguridad y Redes – UNLP “Cableado Estructurado, estándares y nuevos componentes” Expte. 3300-3768/11-000.
- Magister en Redes de Datos “Un estudio comparativo en extensiones de seguridad para el sistema de nombre de dominio (DNS)” Expte. 3300-2113/10-000.
- Magister en Redes de Datos “Caso de estudio de comunicaciones seguras sobre redes móviles ad hoc” Expte. 3300-1937/10-000.