

Tecnológico de estudios superiores de jocotitlán

Ingeniería en sistemas computacionales

Redes inalámbricas

Investigación

Abdalan Ismael Bernardino Hidalgo

Grupo: 801

ICMP Router Discovery

Es un protocolo que utiliza mensajes ICMP router advertisement y router solicitation para permitir a un nodo descubrir la dirección de routers operacionales en una subred IPv4. Este protocolo es utilizado en IP móvil para cuando un nodo móvil se encuentra cambiando constantemente de subred sin tener que perder comunicación con su Home Agent.

Funcionamiento

Para que un nodo pueda enviar paquetes dentro de la red a la cual se encuentra conectado, este debe encontrar al menos un enrutador operativo en dicha subred. Usualmente esto se logra mediante dos técnicas, al leer una lista con una o más direcciones de enrutadores desde un archivo de configuración, o bien, al escuchar en enlaces multicast el tráfico de paquetes de protocolos de enrutamiento. Estos métodos tienen inconvenientes, en el caso del archivo de configuración, este debe ser mantenido manualmente, y en el caso de escuchar el tráfico de paquetes de protocolos de enrutamiento, el nodo debe conocer el protocolo en particular que es usado en la subred a la cual se encuentra conectado.

Como solución se utilizan mensajes ICMP Router discovery que son llamados Router Advertisements (RA) y Router Solicitations (RS). Los routers envían mediante multicast mensajes RA a través sus interfaces la dirección de cada una de ellas. De este modo los nodos simplemente deben escuchar dichos mensajes multicast para descubrir las direcciones de los routers vecinos. También el nodo puede transmitir mensajes RS cuando se conecta a una subred, de esta forma no debe esperar a recibir la llegada de mensajes RA. Solo si no recibe respuesta, el nodo retransmite los mensajes RS, esto solo un número limitado de veces, una vez pasado dicho número, el nodo desiste su solicitud.

VoIP (Voz sobre el protocolo de internet)

Este es un grupo de recursos que hacen posible que la señal de voz viaje a través de internet empleando un protocolo IP. Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla a través de circuitos utilizables solo para telefonía como una compañía telefonía o PSTN.

Los protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. Pueden ser visto como implementaciones comerciales de la Red experimental de protocolo de voz inventada por ARPANET.

El tráfico de voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a internet, como ejemplo redes de área local (LAN).

Ventajas

Evita los cargos altos de telefonía que son usualmente de las compañías de la red pública, algunos ahorros en el costo son debido a utilizar una misma red para llevar voz y datos, especialmente cuando los usuarios tienen sin utilizar toda la capacidad de una red ya existente en la cual pueden usar para VoIP sin un costo adicional.

Funcionalidad

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas comunes:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar donde se esté conectado a la red.
- Los agentes de Call center usando teléfono VoIP pueden trabajar en cualquier lugar con conexión a internet lo suficientemente rápida.
- Algunos paquetes de VoIP incluyen servicios extra por los que PSTN cobra un cargo extra.

Teoría de agentes para móviles

Los agentes móviles son programas de software inteligentes que realizan un objetivo y pueden estar construidos con herramientas de desarrollo estructuradas, orientadas a objetos o concurrentes. Normalmente involucran desarrollos soportados en técnicas de Inteligencia Artificial.

Los agentes actúan de manera autónoma; están programados para que perciban y aprendan de su entorno a través de sensores, razonan sobre lo aprendido; eligen una o varias soluciones para resolver problemas o consultar requerimientos automáticos o humanos; viajan sobre la plataforma de comunicaciones de una red LAN o WAN; sirven para automatizar tareas que se ejecutan repetidamente en una red; se programan una única vez y posteriormente no requieren manipulación humana.

Autonomía

El software tradicional suele ejecutarse en entornos interactivos de tal forma que responde a órdenes directas del usuario, es decir, el usuario tiene que decir paso a paso qué es lo que se tiene que hacer. La idea de los agentes consiste en crear programas informáticos que tengan una serie de objetivos y posean unos conocimientos del mundo, de tal forma que partiendo de sus conocimientos, sean capaces de aproximarse lo más posible a sus objetivos sin necesidad de que ningún usuario los guíe paso a paso hacia ellos.

Sociabilidad

Cuando se habla de agente no se suele pensar en una única entidad que se ejecuta de forma aislada. Más bien se piensa en sistemas complejos (multi-agente) en los que una serie de agentes colaboran entre sí para llevar a cabo una tarea. Este modelo denominado tradicionalmente como “divide y vencerás” presupone que los agentes son capaces de interactuar entre sí y al mismo tiempo, hacerlo con entidades externas al propio sistema como es el caso del usuario.

Reactividad

A pesar de su autonomía, un agente debe ser capaz de percibir estímulos externos tanto para actuar de acuerdo a su entorno cambiante como para poder “conocer” en todo momento cómo es el “mundo” que le rodea. Es decir, que el agente debe tener estímulos y actuar de acuerdo con ellos. Estos estímulos afectarán a las acciones realizadas por él para alcanzar sus objetivos.

Pro-actividad

Es una de las consecuencias de la autonomía de un agente. Éste es capaz de elegir, en cada momento, cuáles son las acciones a realizar para alcanzar sus objetivos. Es decir, un agente no

solo actúa en función de los estímulos que recibe desde el exterior, sino que puede ejecutar acciones como resultado de sus propias decisiones.

Inteligencia

Un agente es inteligente si es racional, coherente, adaptable y móvil, en mayor o menor medida. Podemos decir que será más inteligente cuanto más desarrolladas tenga estas características.

Seguridad en Redes Inalámbricas

La seguridad en Internet comienza en el proveedor que ofrece la conexión, que debe mantener su servicio y servidores protegidos para evitar que sus clientes sean víctimas de alguna intrusión.

El objetivo final es que el usuario pueda disponer de una red a la que se conecte él de forma exclusiva, o todas aquellas personas con las que conviva. Al mismo tiempo, debe estar protegida debidamente para evitar que personas ajenas se aprovechen para conectarse a internet utilizando una red que no es suya, o impedir también que usuarios con malas intenciones detecten vacíos de seguridad para robar datos o cometer otros actos delictivos.

Ventajas y desventajas de la seguridad en las redes inalámbricas

La principal ventaja es la facilidad para modificar la contraseña y proteger la conexión del uso no autorizado o indebido por parte de personas ajenas. Además, también existen los protocolos de cifrado WEP, WPA o WPA2, cuya función es codificar toda la información que se transmite a través de esta conexión y protegerla así ante cualquier intromisión.

Sin embargo, se debe también tener muy presente que en ciertos aspectos una red Wi-fi puede presentar vulnerabilidades. Al tratarse de una conexión inalámbrica, puede verse afectada por interferencias producidas por otras señales, o incluso factores externos como la climatología. Esta inestabilidad puede afectar a la velocidad o disponibilidad de conexión en momentos puntuales.

WEP

Wired Equivalent Privacy es una técnica de encriptación de datos, que se encarga de cifrar cada uno de los paquetes 802.11 antes de su transmisión, usando el algoritmo de cifrado RC4. Este algoritmo puede usar claves de 40 a 128 bits, aumentando la seguridad usando claves de mayor tamaño. WEP no provee mecanismos para el control de claves. Todos los cambios deben hacerse de forma manual en cada dispositivo inalámbrico.

Esta técnica tiene una serie de vulnerabilidades que permite que dicha clave pueda ser descubierta. WEP es una manera sencilla de evitar el acceso no controlado a nuestra red inalámbrica, pero es inadecuada si se requieren unas mínimas medidas de seguridad.

WPA

WPA es un subconjunto de la especificación IEEE 802.11i, el estándar de la seguridad en las redes Wi-Fi.

Las características principales son:

- Uso del protocolo Temporal Key Integrity Protocol (TKIP) para evitar la reutilización de claves.
- Testeo de la integridad de los paquetes enviados (MIC) para evitar errores de transmisión o manipulado de datos.

Tiene dos versiones: la personal que controla el acceso usando una contraseña denominada Pre Shared Key (PSK), y la empresarial que provee un nivel de seguridad mayor, usando claves de sesión dinámicas y verificación de usuarios usando el protocolo 802.1X EAP. Al igual que su predecesor WEP utiliza el algoritmo de cifrado RC4 usando claves de 128 bits.

WPA2

Se basa en su predecesor WPA, tienen las mismas características, pero aumentando el nivel de seguridad, es la implementación completa de la especificación IEEE 802.11i. Una de las principales mejoras es el cambio del algoritmo de encriptado usado por WEP y WPA por otro más avanzado, el Advanced Encryption Standard (AES).

RADIUS

Radius es un sistema de autenticación y control de usuarios usado por muchos proveedores de acceso a Internet. Este forma parte de los mecanismos de seguridad del protocolo EAP. El servidor RADIUS es el encargado de validar el acceso de los usuarios de forma centralizada usando nombres de usuario y contraseña.

El cliente que desea conectarse a la red inalámbrica utiliza alguna de las variantes para autenticarse. Dicha petición EAP llega al punto de acceso el cual se encargará de transmitir la petición al servidor RADIUS, el cual se encarga de validar al usuario, usando su nombre de usuario y contraseña o su certificado. El resultado de la validación es devuelto al cliente inalámbrico, aceptando o denegando el acceso.

AES

Advanced Encryption Standard (AES) es uno de los algoritmos de cifrado más utilizados y seguros en la actualidad. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación "top secret". Su historia de éxito se inició en 1997, cuando el NIST (Instituto Nacional de Estándares y Tecnología) comenzó oficialmente a buscar un sucesor al envejecimiento cifrado estándar DES. Un algoritmo llamado "Rijndael", desarrollado por los criptógrafos belgas Daemen y Rijmen, sobresalía tanto en seguridad como en rendimiento y flexibilidad.

El nuevo estándar de cifrado AES en 2001. El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, cada una ejecutada en bloques de datos de 16 bytes - por lo tanto el término blockcipher. Esas operaciones se repiten varias veces, llamadas "rondas". Durante cada ronda, una clave circular única se calcula a partir de la clave de cifrado y se incorpora en los cálculos. Basado en la estructura de bloques de AES, el cambio de un solo bit, ya sea en la clave, o en el bloque de texto sin cifrado, da como resultado un bloque de texto cifrado completamente diferente - una ventaja clara sobre los cifrados de flujo tradicionales. La

diferencia entre AES-128, AES-192 y AES-256 finalmente es la longitud de la clave: 128, 192 o 256 bits - todas las mejoras drásticas en comparación con la clave de 56 bits de DES. Hasta el día de hoy, no existe un ataque factible contra AES. Por lo tanto, AES sigue siendo el estándar de cifrado preferido para los gobiernos, bancos y sistemas de alta seguridad en todo el mundo.

Algoritmo MD5

Este algoritmo está diseñado por Ronald Rivest del MIT en el año 1991, MD4 tuvo como pilares fundamentales en su diseño ser bastante rápido en las máquinas de 32 bits, además el algoritmo no necesita ninguna sustitución grande y puede codificarse de una forma bastante compacta. Este algoritmo es una extensión del algoritmo MD4, donde se persigue el mismo objetivo siendo MD5 más lento, pero más conservador en su diseño. MD5 fue creado dado que MD4 estaba diseñado para operar de una forma más rápida de la necesaria, trabajando al límite de lo que se conoce como criptoanálisis exitoso, corriendo riesgos de ataque de fuerza, por otra parte, MD5 cede en velocidad, pero aumenta las probabilidades éxito en su seguridad.

Cuando la seguridad del sistema operativo de un servidor parte fundamental del usuario, se debe tener estricto cuidado con las descargas que en él se introducen, pero muchas veces se instalan programas de la web que provienen de páginas que nos son oficiales, o por otro lado de páginas oficiales que llevan mucho tiempo en la web y ha sido alterada su información por usuarios malintencionados el cual puede haber añadido al archivo a instalar virus o troyanos. Es importante la funcionalidad del algoritmo MD5 que se utiliza para varias aplicaciones, pero nos dirá con certeza en un caso como éste si la información que está no presenta ningún peligro para nuestro sistema operativo.

El funcionamiento del MD5, no tiene gran diferencia con el algoritmo MD4 ya que se persiguen los mismos objetivos generales, MD5 proporciona un código asociado a un texto o archivo, este código HASH o resumen del HASH viene unido a los archivos cuando se desean descargar. Para poder ver el código MD5 se debe recurrir a programas especiales para poder analizar los archivos descargados, para poder obtener un código y así poder acudir a la página del instalador original del programa o archivo, obteniendo su código y comparando con el nuestro para así poder ver si la información que estamos descargando es fiable, y no ha sido alterada.

SSL

SSL son las siglas de Secure Sockets Layer en resumen, es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger toda información confidencial que se envía entre dos sistemas, e impedir que los delincuentes lean y modifiquen datos que se transfieran, incluso datos que pudieran considerarse personales. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador), o de servidor a servidor (por ejemplo, una aplicación con información que se considere personal o con datos de nóminas). Esto lo lleva a cabo asegurándose de que todos los datos que se transfieren entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Utiliza algoritmos de cifrado para codificar los datos que se transmiten e impedir que los hackers los lean al enviarlos a través de la conexión. Esta información podría ser cualquier dato confidencial o personal, por ejemplo,

números de tarjeta de crédito y otros datos bancarios, nombres y direcciones. El protocolo TLS (Transport Layer Security) es solo una versión actualizada y más segura de SSL.

Bibliografía

- [1] A. Engst, 14 08 2013. [En línea]. Available:
] <https://cloudflare-ipfs.com/ipfs/bafykbzaceaw4augdossycsijxrwgbx5gwobbewthwvyaxm5wvwonhwva4w5ym?filename=Engst%20Adam%20-%20Anaya%20Multimedia%20Introduccion%20A%20Las%20Redes%20Inalambricas.pdf>. [Último acceso: 27 04 2021].
- [2] X. Garcia, 2017. [En línea]. Available:
] <https://cloudflare-ipfs.com/ipfs/bafykbzacedq5dvozmpf3csbczlpfejomthbdla2wv3nqc4cuyzioxb5yhpmk?filename=Clanar%20-%20Internet%20Y%20Redes%20Inalambricas.pdf>. [Último acceso: 27 04 2021].
- [3] «LinkFang,» 15 10 2017. [En línea]. Available:
] https://es.linkfang.org/wiki/ICMP_Router_Discovery_Protocol. [Último acceso: 27 04 2021].
- [4] C. d. Alfonso, 21 06 2005. [En línea]. Available:
] <http://www.dsic.upv.es/docs/bib-dig/informes/etd-06242005-121243/DSIC-II-04-05.TechReport.pdf>. [Último acceso: 27 04 2021].
- [5] «Blog todos somos ciencia,» 11 06 2020. [En línea]. Available:
] <https://todossomoscienciacyt.wordpress.com/2020/06/11/seguridad-en-redes-inalambricas-802-11/>. [Último acceso: 27 04 2021].
- [6] J. M. d. l. Torre, 03 10 2016. [En línea]. Available:
] <https://core.ac.uk/download/pdf/84137053.pdf>. [Último acceso: 27 04 2021].
- [7] M. I. H. Orrego, 03 07 2019. [En línea]. Available:
] http://opac.pucv.cl/pucv_txt/txt-8500/UCC8922_01.pdf. [Último acceso: 27 04 2021].
- [8] «Digicert,» 2020. [En línea]. Available:
] <https://www.websecurity.digicert.com/es/mx/security-topics/what-is-ssl-tls-https#:~:text=SSL%20Significa%20Secure%20Sockets%20Layer,se%20env%C3%A1Dan%20por%20la%20Internet..> [Último acceso: 27 04 2021].