



VÍDEO intypedia004es

LECCIÓN 4: INTRODUCCIÓN A LA SEGURIDAD EN REDES TELEMÁTICAS

AUTOR: Justo Carracedo Gallardo

Universidad Politécnica de Madrid, España

BERNARDO

Hola amigos, bienvenidos a intypedia. En las últimas semanas he estado estudiado sobre un tema muy interesante: la seguridad en las redes telemáticas, un tema complejo con múltiples matices que afecta a numerosos usuarios y empresas. En esta lección junto a Alicia vamos a introducirnos en este apasionante tema. Por favor, ¡Acompáñanos!

ESCENA 1: REDES TELEMÁTICAS. DEFINICIONES

ALICIA

Desde tiempos ancestrales el hombre ha necesitado superar sus obstáculos de tiempo y espacio desarrollando mecanismos de comunicación cada vez más precisos. Hoy en día, en pleno siglo XXI el uso de la telefonía móvil o de Internet es un claro ejemplo de estos avances. Sin embargo, no siempre el usuario final tiene noción de la complejidad de estas tecnologías y de los inconvenientes que acarrea usarlas de forma incorrecta... Para adentrarse en estas tecnologías es necesario conocer la esencia del funcionamiento de las redes de telecomunicación, y en nuestro caso concreto de las redes de ordenadores y las comunicaciones entre ellas. Es por tanto interesante centrarse en el caso de las redes telemáticas.

BERNARDO

En general, una red telemática es un conjunto de equipos conectados mediante un medio de transmisión de datos, como pueden ser cables que transmiten señales, ondas que se propagan por el espacio, etc., lo que permite compartir información, recursos y servicios, con la intención de proporcionar un valor añadido a las entidades finales que las utilizan.

ALICIA

¿Algún estudiante aventajado podría preguntarse cómo funcionan estas redes telemáticas?

BERNARDO

Es una buena pregunta Alicia. Una respuesta inicial puede verse en la existencia de protocolos telemáticos. Un protocolo es un conjunto estricto de reglas que define la sintaxis y la semántica de la comunicación. Es decir, establece qué se puede y qué no se puede hacer en esa comunicación. Para facilitar la interconexión entre equipos y permitir el buen funcionamiento de los protocolos telemáticos es necesario contar con elementos de interconexión, como por ejemplo son los routers. Gracias a todo esto puede existir Internet, una red mundial de comunicación que consiste en la interconexión entre millares de redes y, por tanto, la interconexión de millones de ordenadores.

ALICIA

Tengo una duda... ¿es necesario conocer esos protocolos para poder comunicarse a través de una red telemática?

BERNARDO

En tecnología siempre que sea posible es interesante abstraer al usuario final de la complejidad tecnológica. Así por ejemplo, elementos esenciales para que una persona pueda leer un correo electrónico o navegar por la Web, como es la torre de protocolos TCP/IP o el protocolo DNS, no tienen por qué ser conocidos en profundidad. Actualmente, es común oír hablar de sistemas de información y de las TIC. Sistemas de información y tecnologías que permiten el tratamiento y la transmisión de grandes cantidades de datos para cubrir la necesidad concreta. Por suerte, para el usuario final gran parte de la complejidad de su funcionamiento es transparente para él. No obstante, el uso de sistemas de información implica una serie de riesgos a tener en cuenta, muchos de ellos derivados precisamente del desconocimiento de la tecnología usada. A continuación, vamos a analizar este asunto con un poco más de detalle.

ESCENA 2: RIESGOS Y PROTECCIONES EN LAS REDES TELEMÁTICAS

BERNARDO

Hoy día las redes telemáticas se utilizan para comunicar no sólo a individuos sino que tienen una gran utilidad en las comunicaciones empresariales, bancarias, estatales, diplomáticas, militares, entre ciudadanos con la administración pública, etc. Mucha información, en algunos casos sensible, circula por estas redes. Existe un riesgo real de que personas no autorizadas intenten tener acceso ilegítimo a ella.

ALICIA

¿Pero la criptografía no soluciona esto? Hasta lo que yo sé la criptografía es la base de multitud de protocolos telemáticos seguros que permiten proteger la información.

BERNARDO

Vayamos por partes Alicia. Las redes telemáticas presentan muchas vulnerabilidades y es necesario protegerlas. En este sentido se define la seguridad en redes como todo aquel conjunto de técnicas que tratan de minimizar la vulnerabilidad de los sistemas o los problemas derivados de procesar la información en ellos contenida. Se trata de conseguir que el coste de la consecución indebida de un recurso sea superior a su valor. Con esta idea en mente se diseñan mecanismos de seguridad. Estos se utilizan para construir los protocolos seguros que facilitarán la prestación de servicios de seguridad, es decir, los mecanismos de seguridad son los “ladrillos” que permiten finalmente, gracias a los servicios de seguridad, proteger las comunicaciones de los usuarios frente a los distintos ataques. Principalmente los mecanismos de seguridad se apoyan en técnicas criptográficas, luego éstas son la base para los servicios de seguridad. Como puedes ver un servicio de seguridad es mucho más que una técnica criptográfica concreta.

Los 7 servicios de seguridad más significativos son: la autenticación de entidades, la confidencialidad de datos, la integridad de datos, el control de acceso, el no repudio, la disponibilidad y el anonimato.

La definición de servicios de seguridad es muy importante ya que existen múltiples ataques a minimizar, clásicamente **ataques sobre la identidad de las entidades** (interceptación y suplantación), **ataques sobre la información** (revelación, reenvío, manipulación y repudio de datos) y **ataques sobre los servicios** (negación del servicio y apropiación).

ALICIA

Tengo una duda sobre los ataques sobre los servicios. ¿Por qué alguien podría tener interés en impedir el acceso a un servicio o adueñarse de él, por ejemplo, tomar el control del equipo de un usuario final?

BERNARDO

Es fácil de entender. Hoy día tan importante es la información a proteger como los ordenadores o los servicios que permiten acceder a ella o tratarla. Actualmente los atacantes intentan comprometer ordenadores ya que éstos sirven para muchos usos. Pueden ser utilizados para ocultar el rastreo de actividades ilegales, como el envío de correos electrónicos no solicitados (el conocido como SPAM), la utilización de su conexión a la red para enviar peticiones masivas para intentar saturar servicios en Internet, por ejemplo para que una página web deje de funcionar, etc. Estos últimos son los conocidos como ataques DoS (negación de servicio). En este sentido, cada vez es más habitual hablar de la creación de botnets. Una botnet es una red de equipos comprometidos controlada habitualmente por una o más personas a través de un panel de control que aprovecha la capacidad de computación y la conexión de Internet de estos equipos para realizar habitualmente actividades ilícitas como las comentadas. En este tipo de ataques existe una componente económica muy importante y esto ha hecho que mafias y otros grupos organizados se hayan profesionalizado en esta tarea.

Además de todo esto, existen ordenadores y redes telemáticas que gestionan información y procesos muy críticos para un país. Un ejemplo de ello son las redes que gestionan infraestructuras críticas como las centrales de energía, los embalses, la red de transportes, etc. Como puedes suponer el mal funcionamiento de estas estructuras supondría consecuencias muy graves. En próximas lecciones profundizaremos en este tema tan complejo, que se conoce como protección de las infraestructuras críticas.

ESCENA 3: CONOCIENDO A TU ENEMIGO

ALICIA

Se me ha ocurrido algo. Si tuviéramos una idea aproximada del perfil de los atacantes, tal vez podríamos diseñar protocolos telemáticos más seguros.

BERNARDO

Exacto. En esa idea se ha ido trabajando en los últimos años, especialmente al verse la profesionalización de los ataques a redes telemáticas. Soluciones tecnológicas como los honeynets o honeypots apuntan en esa dirección. Respecto al peligro de los atacantes, seguro que has oído hablar de términos como hacker o cracker.

ALICIA

Sí... y tengo entendido que un hacker es una persona que disfruta explorando los sistemas informáticos y redes de telecomunicación accediendo a éstos sin permiso para demostrar su habilidad y conocimientos. Y, por el contrario, un cracker invierte las medidas de protección de una red telemática o sistema informático para alcanzar un beneficio concreto, habitualmente económico.

BERNARDO

Bueno... eso podría ser una primera aproximación. En el ambiente tecnológico es común poner etiquetas a todo, a veces de forma errónea. Lo cierto es que existen personas con un conocimiento elevado sobre las tecnologías y protocolos en los que se apoyan las redes telemáticas. En ocasiones este conocimiento avanzado, con dosis de talento y trabajo, les permite descubrir fallos que permiten mejorar la tecnología, en otras ocasiones es utilizado con intereses particulares: económicos, morales, políticos, militares, etc. En la práctica, es difícil catalogar a los atacantes en blanco o negro, casi siempre hay niveles de grises.

ALICIA

¿Existen, quizás, otras formas de clasificar a los atacantes?

BERNARDO

Existen varias... Una clasificación interesante es clasificar a los atacantes en función de su conocimiento, en lugar de sus motivaciones o de los efectos que produzcan en el sistema final. De esta forma se puede hablar de atacantes que intentan maximizar sus resultados con el mínimo esfuerzo. En este caso muchas de las medidas de seguridad que se irán estudiando en las próximas lecciones servirán para evitar o minimizar esos ataques. Otro tipo de atacantes, estos son los más peligrosos, son aquellos que provocan ataques dirigidos, es decir, ataques contra un objetivo concreto, entrando en juego no sólo los conocimientos técnicos del atacante y del defensor, sino también el tiempo y el dinero que puedan invertir ambos en proteger o atacar la red o los equipos. Actualmente, es común que los atacantes se dirijan especialmente a entornos empresariales y que por lo general estos ataques provengan de personal interno, ya que poseen un mejor conocimiento de la infraestructura de comunicación implementada.

ALICIA

Muy interesante... pero supongo que una empresa o un particular no podrá invertir todo el dinero del mundo en proteger su red o su equipo.

BERNARDO

Efectivamente. Tu pregunta abre un nuevo tema, el de la gestión de riesgos. La inversión en seguridad debe ser proporcional al valor de la información o de los elementos a proteger. En la práctica deben definirse normas claras de actuación para analizar potenciales amenazas, el impacto de los ataques, etc. Ya tendremos tiempo en un futuro de profundizar en este aspecto.

ESCENA 4. PROTEGIENDO LA RED

ALICIA

Por todo lo que estoy viendo, proteger una red telemática y la información almacenada o intercambiada no es nada sencillo.

BERNARDO

Así es. Idealmente un administrador debería proteger y vigilar todos los puntos susceptibles de recibir un ataque. Al atacante, no obstante, le sirve únicamente que un punto de éstos no esté debidamente protegido para realizar su ataque e ir escalando privilegios en la red o máquina destino para conseguir su objetivo. No existe la seguridad total: ante cualquier coraza de protección, siempre se podrá encontrar un elemento capaz de romperla. No obstante, no debe olvidarse que el estado actual de las tecnologías de seguridad permite ofrecer en las redes telemáticas una protección superior en varios órdenes de magnitud a la que se ofrece en el mundo ordinario, por ejemplo, en el intercambio de documentos en papel.

ALICIA

En seguridad se dice que habitualmente el eslabón más débil es el ser humano.... Ya me puedo imaginar por dónde pueden venir los ataques.

BERNARDO

Tienes toda la razón. En muchas ocasiones la forma más fácil de acceder a una red telemática, sustraer una información o falsificar una autenticación, es manipulando, engañando o coaccionando a personas. En esto tiene que ver mucho la denominada ingeniería social, esto es la habilidad para hacer que otras personas trabajen en tu beneficio, en muchos casos sin ser éstos conscientes del engaño al que están siendo sometidos. La solución a este problema en la mayoría de los casos consiste en una concienciación en seguridad en redes telemáticas y en la definición de **políticas de seguridad** claras, que impidan por ejemplo, que un usuario pueda dar la clave de autenticación de un servidor por teléfono a un desconocido.

En próximas lecciones hablaremos de los certificados de clave pública y de las infraestructuras de seguridad que existen, basadas en autoridades de seguridad de confianza, que sirven para ayudar a los usuarios a protegerse lo mejor posible de los muchos riesgos y ataques que puedan aparecer en las redes telemáticas.

También tendremos tiempo para profundizar en cada uno de los ataques posibles y hablar de nuevos conceptos como: firewalls, IDS, logs, sniffers, etc.

Pero esto será en otra ocasión...

BERNARDO

¡Adiós! Cuidado ahí afuera....

ALICIA

Hasta pronto.

Guión adaptado al formato intypedia a partir del documento entregado por el Dr. Justo Carracedo Gallardo de la Universidad Politécnica de Madrid, España.

Madrid, España, enero de 2011

<http://www.intypedia.com>

<http://twitter.com/intypedia>

