El NoticIEEEro

VOLUMEN 31, NÚMERO 3

SEPTIEMBRE 2003

Celebración de 31º Aniversario de IEEE Sección Panamá

Este año se celebró el trigésimo primer aniversario del IEEE Sección Panamá con una serie de actividades realizadas durante la semana del 9 al 13 de Septiembre, conmemorando a las diferentes generaciones de la Sección que han aportado su contribución al IEEE y a Panamá.

Iniciamos el martes 9 de septiembre con la publicación de una pauta en el periódico La Prensa en la cual se destacó la colaboración de los miembros IEEE con el desarrollo de la ingeniería en Panamá por 31 años.

El día miércoles 10 de septiembre, realizamos una gira técnica al Centro de Simulación, Investigación y Desarrollo Marítimo del Canal de Panamá. Este centro incluye dos simuladores de maniobras de buques, uno de ellos de 360 grados de visual y otro de 150 grados, un simulador de remolcadores y un simulador de incendios en buques.

El capitán Altafulla nos mostró la operación de estos 3 simuladores que son utilizados para capacitar a los pilotos del Canal. También son utilizados para realizar investigaciones y desarrollo de proyectos ya que conducen a definiciones más realistas y precisas, ahorrando así en costos de diseños y ejecución de proyectos. Posteriormente personal técnico nos mostraron los sistemas de bases de datos geográficas y de redes utilizados para manejar estos sistemas de simulación. Finalmente pudimos apreciar a 2 pilotos del Canal realizando simulaciones en el manejo de barcos con casos reales en donde se intentaba estacionar un barco de contenedores en un muelle de difícil acceso.

Miembros IEEE durante la visita del Simulador de 360 grados de visual

El jueves 11 de septiembre se realizó una misa de acción de gracias por los miembros de IEEE Sección Panamá en el Santuario Nacional del Corazón de María.

El viernes 12 de septiembre, día de nuestra formación como Sección, se entregó una canastilla a un recién nacido de parto normal llamado Eduardo Díaz quien nació a las 12:55 de la mañana y quien peso 7 libras con 9 onzas.

Momento en que se hace entrega de una canastilla al recien nacido Eduardo Díaz

Continúa en la página 12

EN ESTE NUMERO:

31º Aniversario	1
Editorial	2
Premios y Reconocimientos	3
Artículo: Desafíos de la Seguridad en Redes Inalámbricas 802.11b	6
Capítulos Técnicos	13
CONCAPAN XXIII	14
IEEE y la Robótica	15
Agenda de Eventos	16

Editorial

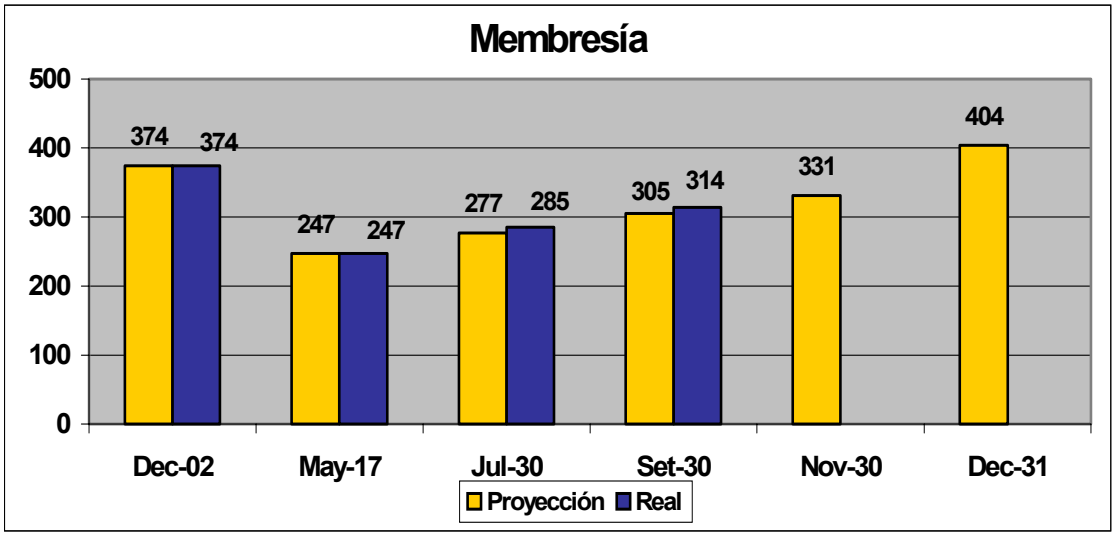
Nos llena de orgullo el haber celebrado el trigésimo primer aniversario del IEEE Sección Panamá, ver como hemos crecido y al mirar hacia los inicios ver como generación tras generación sigue involucrada y exhortando a las más recientes generaciones en continuar con el desarrollo de la Sección. En esta edición queremos compartir con ustedes estimados miembros, la serie de actividades realizadas durante los días 9, 10, 11, 12 y 13 de septiembre en conmemoración del aniversario de la sección. Además, encontraran la ponencia ganadora del concurso IEEE CONESCAPAN 2003 presentada por el joven Carlos Kan titulada "Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b", a quien le reiteramos las felicitaciones por el logro alcanzado. Y, continuando con las buenas noticias, les traemos lo acontecido en el primer seminario realizado por el IEEE en el interior del país cuyo tema fue el Código Eléctrico NEC y sus aplicaciones el mismo se llevo a cabo en la ciudad de Santiago de Veraguas. Adicionalmente les presentamos un resumen de los talleres de Robótica dictados por el Ing. Román Altamiranda quien cautivo a la audiencia con los detalles de las exposiciones. Y por supuesto no podíamos dejar de traerles los detalles de la reunión del Grupo Gold, quienes no dejan que nuestro clima tropical sea un impedimento para llevar a cabo los famosos Get Together Gold en los cuales compartimos siempre tan amenamente, esperamos noticias de otro próximamente. En este aniversario queremos extender las felicitaciones a todos ustedes, ya sean miembros o colaboradores, ya que sin ustedes el éxito del IEEE Sección Panamá no seria la realidad que tenemos hoy día, mil gracias y sigamos trabajando en pro de la Sección.

Sofía Cuevas
Comité Editorial

Noticias del Comité de Membresía

Para el IEEE Sección Panamá es un gran reto mantener y aumentar la membresía durante el año 2003 y para eso se fijaron metas específicas. Para este año hemos proyectado alcanzar la cifra de 404 miembros, lo que representa un 8.02% de incremento con respecto a diciembre del 2002. Sin embargo, esto no será una tarea fácil, ya que para el próximo año el IEEE, nuevamente, ha incrementado el costo de la membresía anual de $114.00 a $117.00 dólares para los miembros profesionales de la región, debido a los costos de la inflación. Los costos de membresía estudiantil permanecen iguales para el 2004. También se incrementó el costo en algunas sociedades técnicas, como por ejemplo IEEE Power Engineering Society, PES que incrementó su membresía de $22.00 a $25.00 dólares.

En la gráfica de abajo se puede observar que al mes de septiembre de 2003 se han alcanzado las proyecciones realizadas de la membresía de 314 miembros, sin embargo, continuaremos trabajando ya que para los próximos meses las metas son más altas.



Noticias del Comité de Premios y Reconocimientos

El ganador del concurso estudiantil de trabajos para CONESCAPAN 2003 fue el estudiante Carlos Kan, miembro de la Rama de la Universidad Santa Maria La Antigua. El estudiante Kan nos representó el pasado mes de agosto en CONESCAPAN 2003 el cual se realizó en la ciudad de San Salvador, El Salvador. El trabajo que presentó Carlos esta titulado "Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b". Y se publica en este edición del NoticIEEEro.

Además, el pasado 17 de septiembre se realizó, con una gran concurrencia, el Concurso IEEE CONCAPAN 2003 en el Hotel El Ejecutivo de esta ciudad. En este concurso se presentaron las ponencias: “Análisis de Pérdida de Energía en el Sector de Distribución Eléctrica”, por Marianela Herrera; “Opciones para una Reducción Tarifaria”, por Nicanor Ayala; y “Detección de Fallas en Sistemas No Aterrizados”, Enrique Tejera, quien resultó ganador del Concurso. El premio consiste en gastos pagados de pasaje, hospedaje e inscripción a la CONCAPAN XXIII a realizarse en la ciudad de Tegucigalpa, Honduras el próximo mes de noviembre. Los otros dos concursantes recibirán los gastos pagados del hospedaje e inscripción.

Felicidades a los concursantes por el buen desarrollo de su trabajo y los incentivamos a que sigan investigando y trabajando en el área de la electrotecnología objetivo primordial del IEEE.

Momentos en que Carlos Kan recibe el premio del Concurso IEEE CONESCAPAN 2003 de parte del Coordinador de Act. Estudiantiles, Ing. Jorge Him

Vista de los participantes del Concurso IEEE CONCAPAN 2003 junto a la Presidenta de la Sección, Ing. Tania Quiel

Seminario del NEC en Santiago

Por primera vez en la historia del IEEE Sección Panamá se realiza un seminario en el interior del país.

En esta ocación se escogió a el Hotel Galería en la ciudad de Santiago de Veraguas para realizar este evento técnico. Fue así como el pasado 19 de julio se llevó a cabo el Seminario del Código Eléctrico NEC y sus Aplicaciones. El mismo fue dictado por renombrados profesionales panameños de la ingeniería eléctrica como son el Ing. Rodrigo Chanis, Ing. Gustavo Bernal y el Ing. Lucas Halpen.

Este evento fue un rotundo éxito desde el punto de vista técnico, logístico y financiero que contó con la participación de 31 profesionales de diferentes empresas de la capital y del interior del país, destacándose una importante asistencia del cuerpo de bomberos de las ciudades de Las Tablas, Chitré y Santiago.

De esta manera IEEE Sección Panamá cumple una vez más con su misión de llevar a todas partes el conocimiento de la ingeniería eléctrica y electrónica.

Asamblea General

El pasado 24 de julio, se realizó la Asamblea General de Miembros de la Sección Panamá. Esta reunión inició con la excelente participación del Ing. Henry Stec, quien nos expuso la conferencia titulada "Aplicación de Sistemas de Comunicación en la Autoridad del Canal de Panamá".

El Ing. Henry Stec, mientras dictaba la conferencia

También se realizo la presentación de los diferentes informes de actividades y eventos más sobresaliente de cada uno de los comités de trabajo y de los capítulos celebrados en este año.

El comité organizador del CONCAPAN XXII aprovecho la reunión anual de los miembros para presentar el informe final de este gran evento celebrado en el mes de noviembre de 2002.

Se aprovechó la oportunidad para entregar a los miembros de la Junta Directiva del Capítulo de Potencia, Gustavo Bernal, Mario de la Ossa y Leonardo Pérez, un certificado de reconocimiento al Segundo Lugar como Mejor Capítulo del año 2002, cabe mencionar que este es un premio internacional. Adicionalmente, se hizo entrega por parte del Capítulo de Comunicaciones de un cheque de $250.00 que le diera la Sociedad de Comunicaciones por sus actividades durante el año 2002.

La reunión finalizó con un sorteo de obsequios entre los miembros que nos acompañaron en esta reunión anual.

Miembros de la Junta Directiva durante la Asamblea General

Promoción del IEEE en la Universidad Latina

En días pasados el Comité de Actividades Estudiantiles presidido por el Ing. Jorge Him visitó dos de las instalaciones de la Universidad Latina, ULAT, con el objetivo de promover el IEEE entre los estudiantes de esta casa de estudios e involucrarlos con el Instituto para que en un futuro cercano puedan formar la cuarta Rama Estudiantil de nuestra Sección Panamá.

Ing. Jorge Him explicando el formulario de inscripción al IEEE a los estudiantes de la Universidad Latina

Estudiantes de Ingeniería Biomédica de la Universidad Latina

Las visitas efectuadas fueron el 25 de julio en las facilidades de la ULAT en Justo Arosemena en la cual estudiantes de Ingeniería Biomédica se mostraron sumamente interesados en pertenecer al IEEE, lo cual se demostró con las membresías nuevas que se hicieron después de concluir la charla. La segunda visita se realizó en la sede central de la ULAT, en la Avenida Ricardo J. Alfaro, esta vez estudiantes de Ing. enTelecomunicaciones fueron los que atentamente escucharon la charla de promoción para posteriormente inscribirse al IEEE.

El interés que demuestran estos estudiantes en las actividades del IEEE nos vaticina que antes que finalice el 2003 la ULAT tendrá la cuarta Rama Estudiantil de Panamá.

Estudiantes de Ingeniería Biomédica inscribiéndose al IEEE

RICHARDS EAGLE GROUP

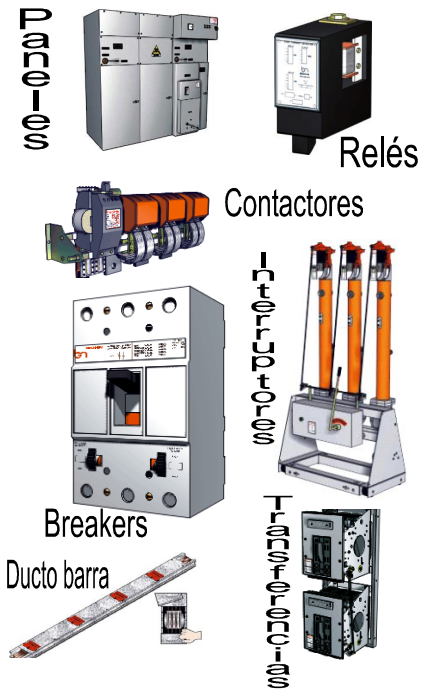
Romanos 10:9

RICHARDS EAGLE GROUP es una empresa panameña con la visión de brindar a nuestros clientes la más alta calilidad y tecnología del mercado en tiempo real.

Richards Eagle Group empezó en 1973, como Carlos A. Richards, nombrado así como su fundador y CEO. En 1999, el nombre de la compañía fue cambiado a Richards Eagle Electrical, Inc. Solamente cuatro años más tarde, en 2000, Richards Eagle Supply Inc. nace. Estas dos compañías junto con Richards Eagle Communication Inc. Comprenden el Grupo Richards Eagle.

BEGHIM www.beghim.com.br

EQUIPOS BAJO Y MEDIO VOLTAJE



Richards Eagle Electrical Inc.

General Contractors & Project Developers

- Diseño de AUTOCAD
- Inspección
- Electricidad en general
- Sistema de alarma
- Auditoría energética
- Mejoramiento sistema de tierra
- Mejoramiento factor de potencia
- Análisis de facturación
- Generación de planes y programas de mantenimiento industrial y comercial

Richards Eagle Supply Inc.

Venta de equipos eléctricos y materiales de construcción

- Representantes y distribuidores de Beghim para Centro América, el Caribe, Colombia, Estados Unidos y Panamá.
- Pararrayos, sistemas de tierra, CALDWELD
- Video portero electrónico
- Materiales y equipos a prueba de explosión
- Casas prefabricadas de madera y galeras de metal

Richards Eagle Communication Inc.

- Diseño de planos en AUTOCAD
- Diagramas asesoría y consultoría
- Cableados estructurados
- Infraestructuras disponibles para seminarios, conferencias y reuniones ejecutivas

Algunos de nuestros clientes:

ABB ERICSSON ALSTOM SIEMENS NEC TOSHIBA CATERPILLAR PIRELLI

Parque Industrial de Cocolí · Apdo. 1429, Balboa Ancón · Panamá, Rep. de Panamá
Email: resupply@cwpanama.net · Richardseagle@hotmail.com
Tel. (507) 316-4092 · Telefax: (507) 316-4108 · Cel. (507) 618-6807

Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b

Presentado por: Carlos H. Kan, IEEE Student Member # 41363577
Ponencia presentada en CONESCAPAN, El Salvador

EXTRACTO

La actual demanda de servicios inalámbricos tiene un crecimiento exponencial, lo que augura el descuido de muchos usuarios en el tema de la seguridad. Este documento presenta una introducción a las especificaciones y vulnerabilidades del estándar IEEE 802.11, seguidamente unos mecanismos de seguridad con un caso práctico único en su clase, una red inalámbrica con unidades móviles flotantes. Además, unas recomendaciones y reflexiones para este tipo de eventos.

INTRODUCCION

La movilidad ha supuesto una revolución y está siendo alimentada por el gran número de empresas que están instalando redes inalámbricas (WLANs, *Wireless Local Area Networks*) bajo el estándar de la industria IEEE 802.11b. La aceptación global de las WLANs depende de la estandarización de la industria para asegurar una compatibilidad y confiabilidad de todos los fabricantes. El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ratifico originalmente la especificación 802.11 en el año 1997, como el estándar para las WLANs. Aquella versión proveía transferencia de datos de 1 y 2 Mbps, así como también métodos fundamentales de señalización y otros servicios.

El asunto mas crítico que ha afectado las WLANs ha sido su limitado rendimiento de procesamiento. Los porcentajes de datos soportados por el estándar IEEE 802.11 original, eran muy bajos para lo requerido para las funciones de las empresas y negocios. Razón por la cual se ratifico el estándar IEEE 802.11b para aumentar las transmisiones a 11 Mbps. Con las WLANs IEEE 802.11b, los usuarios tendrán niveles de funcionamiento, rendimiento y disponibilidad parecidos a los encontrados en Ethemet.

Desde la ratificación del estándar IEEE 802.11b en 1999, las WLANs han llegado a ser mas frecuentes. Hoy, las WLANs están desplegadas extensamente en lugares tales como, salas de conferencias de corporaciones, almacenes industriales, aulas de clase listas con Internet, cafeterías, y por supuesto, la Autoridad del Canal de Panamá. El estándar IEEE 802.11 basado en WLANs presenta nuevos desafíos para los administradores de la red, e igualmente para los administradores de seguridad de la información. Relativamente distinto al despliegue de las redes cableadas, las WLANs IEEE 802.11 difunden los datos mediante señales de radio frecuencia (RF, *Radio Frequency*) para que las estaciones del cliente puedan tener servicio de red.

Esto presenta nuevas y complejas medidas de seguridad que involucran el aumento del estándar IEEE 802.11. La necesidad reinante de políticas de seguridad en los lugares donde se despliegan las WLANs ya no es una opción, es una necesidad recomendada en cualquier despliegue de tecnologías de redes inalámbricas. Las WLANs se han convertido en uno de los objetivos más interesantes para los *hackers* en estos días. Las organizaciones están desplegando tecnología inalámbrica a una tasa más rápida que la mayoría de los departamentos de tecnología pueden establecer. Este rápido despliegue es debido en parte a, los bajos costos de los equipos, su fácil instalación, y la gran productividad que generan. Los equipos de WLANs son empacados con todas las opciones de seguridad deshabilitadas, esta dispersión atrajo la atención de la comunidad *hacker*. Varios sitios Web han empezado a documentar la disposición de servicio y conexión inalámbrica mundialmente. Aunque muchos *hackers* están utilizando este tipo de conexión, como medio para obtener acceso gratis de Internet o para ocultar su identidad. Un pequeño grupo considera esta situación como una oportunidad de interrumpir en las redes, y difundir el caos entre ellas.

Cuando antenas de alta ganancia son utilizadas en edificios, estas cubren hasta sectores que están afuera de la edificación. Este escenario crea ambientes en los que los controles de seguridad tradicionales de redes cableadas son inefectivos, porque los paquetes (*packets*) pueden ser vistos por cualquiera en el espectro radio eléctrico.

VULNERABILIDADES DEL ESTANDAR IEEE 802.11

El WEP (*Wired Equivalent Privacy*) es un algoritmo de encriptación del estándar 802.11, originalmente

Continúa en la página 7

Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b

Viene de la página 6

diseñado para proveer de seguridad a las WLANs con el mismo nivel de privacidad disponible en las redes cableadas. WEP utiliza una llave secreta compartida entre los nodos de la red inalámbrica encriptando los *frames* (capa 2, Enlace de Datos), y mediante la llave secreta compartida en la transmisión, es posible descifrar el mensaje. Estas llaves secretas pueden ser de 40 y 128 bits, generadas por un algoritmo Generador de Números Pseudo Aleatorios (PRNG, *Pseudo Random Number Generator*). Cuando se habilita esta función, cada estación (tanto clientes como puntos de acceso) tiene una clave que se utiliza para cifrar los datos antes de transmitirlos por las ondas de radio. Si una estación recibe un paquete que no se encuentra cifrado con la clave apropiada, el paquete es desechado y no es entregado al *host*; de esta manera se evita el acceso no autorizado y la recepción de señal no autorizada.

El SSID (*Service Set Identifler*) es una identificación que se anexa a cada paquete enviado a través de la red, y opera como una clave que da acceso a la red, todos los puentes inalámbricos y puntos de acceso usan la misma SSID, los paquetes con otro SSID son ignorados, esto también aplica para los usuarios inalámbricos (*clients*). El SSID no provee ningún tipo de funciones de seguridad contra la data, ni tampoco una autenticación de los clientes que intentan asociarse al punto de acceso. El SSID es publicado en los *frames* del mensaje de faro (*beacon*) que se envían a los puntos de acceso para obtener el servicio de red, los mensajes de faro son transparentes para el usuario. Esta información puede ser determinada por un analizador de paquetes como *Sniffer Pro*. Algunos fabricantes han incluido en la configuración, la opción de poder deshabilitar la transmisión del SSID en los mensajes de faro. Esto puede afectar redes inalámbricas mixtas, con equipos de una diversidad de fabricantes.

El estándar IEEE 802.11 esta basado en la autenticación de una estación o equipo inalámbrico, y no basados en autenticación de usuarios. Las especificaciones establecen dos modos de autenticación: autenticación abierta (*Open Authentication*) y autenticación de llave compartida (*Shared Key Authentication*). Y tres estados que se describen a continuación, primero, no autenticado y no asociado (*unauthenticated and unassociated*), segundo, autenticado y no asociado (*authenticated and unassociated*), tercero, autenticado y asociado (*authenticated and associated*).

La autenticación abierta es proveniente de un algoritmo nulo (*null*) de autenticación. La autenticación en el estándar IEEE 802.11 del año 1997, fue diseñada para permitir a los equipos obtener rápido acceso a la red. La autenticación abierta consiste en dos mensajes, en la petición de autenticación y en la respuesta de autenticación, porque lo que es orientado a la conectividad (*connection-oriented*). Para algunos investigadores les resulta sin sentido la utilización de tal algoritmo, porque le da autorización de establecer la comunicación a cualquiera estación.

Cualquier dispositivo que conozca el SSID puede obtener acceso a la red, con la adición de la encriptación WEP en la autenticación abierta, la llave de WEP se convierte en un control de acceso. Pero la autenticación abierta por si sola no provee seguridad, ya que es imposible para los equipos determinar si un cliente es valido o no. Existe la posibilidad de una validación mediante listados, puede estar ubicada dentro del equipo inalámbrico o en un servidor externo. Esto dependerá si el fabricante habilito estos campos de opción en el equipo inalámbrico, pero la utilización de un equipo externo como un servidor es más costoso. Y aquí se retoma lo expresado en un principio, dependerá de las políticas de seguridad, y de las funciones de los usuarios dentro de la WLAN.

La autenticación de llave compartida tiene solamente una variante en su utilización, el uso de una llave WEP estática que es recompartida en el proceso de autenticación. Este proceso de intercambio es vulnerable a ataques de tipo "hombre en el medio" (*man-in-the-middle*), que es básicamente una situación en donde el atacante se encuentra localizado en la mitad, escuchando la transmisión y obteniendo la llave WEP, porque como su nombre lo identifica es estática, que se mantiene igual en toda la transmisión.
Existe la autenticación mediante direcciones MAC (*Media Access Control*), el cual no esta especificado en el estándar IEEE 802.11, pero que muchos fabricantes han optado por utilizar. Se tiende a autenticar las direcciones MAC de los

Continúa en la página 8

Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b

Viene de la página 7

clientes, mediante un listado donde están las direcciones MAC validas que tienen acceso, reduciendo el posible acceso de equipos no autorizados. Esta autenticación mediante direcciones MAC puede ser "engañada" (*spoofing*) por un atacante, con la utilización de un analizador de protocolos para determinar una dirección MAC valida, y así engañar al sistema con una dirección MAC rescrita. Esto se realiza a nivel de las NIC (*Network Interface Card*), y es posible en ambientes con plataformas Windows. El estándar IEEE 802.11 no especifica mecanismos de administración de las llaves WEP. El WEP solo se definió para soportar llaves estáticas y recompartidas. La integridad de la red mediante la autenticación es vital, sin mecanismos de generación y distribución de llaves, los administradores tienen que ser cautelosos en las NICs y los usuarios.

MECANISMOS DE SEGURIDAD

Después de realizar una introducción a las especificaciones y vulnerabilidades del estándar IEEE 802.11, proseguimos a presentar dos sistemas que se han implementado anteriormente en redes cableadas, y se han identificado por sus mecanismos de seguridad. Estos son las murallas de fuego (*firewall*) y las redes privadas virtuales (VPN, Virtual *Private Network*). Es razón por la cual distinguir entre "instalar" y "configurar" una WLAN es un punto básico en lo que sigue a continuación, siendo dos temas muy diferentes y que una instalación no garantiza la seguridad en si misma.

Cuando se especifican las políticas de seguridad en una red, es reglamentario definir ciertos procedimientos para salvaguardar el contenido de la red, y los daños y pérdidas de usuarios de la misma. Visto desde esta perspectiva, las políticas de seguridad juegan un papel vital en el esfuerzo global de las políticas, que definen a una organización como tal. Una parte crítica de la solución global de seguridad es un firewall en la red, el cual monitorea el tráfico que atraviesa los perímetros de la red e impone restricciones acordes a las políticas de seguridad. Las políticas de seguridad de una red se enfocan en el control de tráfico y utilización de la red. Este identifica los recursos y amenazas, define el uso y responsabilidades de la red, y detalla los planes de seguridad cuando las políticas de seguridad son violadas.

Los firewalls separan comúnmente las redes internas (privadas) y las redes externas (públicas). El firewall opera en las capas superiores del modelo OSI, y tienen información sobre las funciones de la aplicación en la que basan sus decisiones. Los firewalls también operan en las capas de red y transporte en cuyo caso examinan los encabezados IP y TCP (paquetes entrantes y salientes), y rechazan o pasan paquetes con base a reglas de filtración de paquetes programadas. Los filtros están diseñados para evitar que un usuario irreconocible, ataque un equipo por Internet y al mismo tiempo este equipo quede inmune a la penetración. Un firewall puede ser un dispositivo basado en hardware o software, es decir, un equipo físico dedicado a esa función (Cisco PIX Firewall, Symantec Firewall, etc), o bien un programa que se instala en un computador (Sygate Firewall, Zone Alarm Pro, Linux, etc).

Las VPN han compartido mercado con los firewalls, debido a su gran robustez y su variedad de sabores que hay en el mercado actual. Algunos fabricantes realizan híbridos con capacidad de firewall y *VPN* a la vez (Symantec Firewall/VPN Appliance, Cisco PIX Firewall 5xx), y otros más ortodoxos, que son dedicados exclusivamente a funciones de VPN (Cisco VPN Concentrator).

Un VPN es una extensión de una red privada, que mantiene enlaces compartidos a través de una red pública como es el Internet. El VPN permite enviar datos entre dos computadores a través de la red compartida o la red pública, de manera que emula las propiedades de un enlace punto a punto. Para emular un enlace punto a punto, los datos son encapsulados, o envueltos en un encabezado (*header*) que provee información de enrutamiento, proveyendo la travesía de la red compartida o transito público de la red, hasta llegar al punto final. Para emular un enlace privado, los datos son enviados encriptados para la confiabilidad. Los paquetes que son interceptados en la red compartida o red pública, son indescifrables sin la llave de encriptación. La porción de la conexión en que los datos privados son encapsulados es llamada túnel (*tunnel*). La porción de la conexión en que los datos privados son encriptados es llamada "la conexión a la red privada virtual".

En algunas corporaciones interconectadas, los datos departamentales son tan sensitivos que la

Continúa en la página 9

Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b

Viene de la página 8

LAN departamental es físicamente desconectada del resto de la red corporativa. Aunque esto proteja la confidencialidad departamental de la información, crea problemas en poder acceder esa información para aquellos usuarios que no están físicamente conectados a dicha LAN. Las VPNs permiten que la LAN departamental sea conectada físicamente a la red corporativa, pero separada por un Concentrador de VPN. Con el uso de las VPNs, el administrador de red puede asegurar que solamente los usuarios con los derechos y credenciales aprobados, puedan tener acceso a la red corporativa (basados en una política de *need-to-know*) estableciendo una sesión VPN con el Concentrador de VPN, y ganar acceso a esta zona protegida de recursos departamentales. Además, todas las comunicaciones a través del VPN pueden tener los datos encriptados para mayor confiabilidad. Aquellos usuarios que no tengan los derechos y credenciales aprobados no podrán tener acceso a la LAN departamental.

CASO PRÁCTICO

Nuestro caso se establece en la red inalámbrica de la Autoridad del Canal de Panamá. Esta red inalámbrica tiene como usuarios principales al equipo flotante de la institución, como los remolcadores, dragas, barcazas y lanchas, estos utilizan la vía acuática en sus operaciones diarias, y necesitan de este servicio inalámbrico para realizar trabajos en las aplicaciones corporativas existentes. Tales como, *Oracle Financials*, EVTMS (*Enhanced Vessel Traffic Management System*, es una aplicación donde se despliega el horario de trafico de los buques, la cantidad de pilotos, remolcadores, locomotoras y personal a asistir el mismo); otros servicios como correo electrónico, actualización en tiempo real de la base de datos de mantenimiento de las flotas, información del servicio meteorológico, etc.

Es una red con una topología celular, los puntos de acceso ubicados estratégicamente en las orillas del Canal de Panamá. Provee servicio de roaming entre celdas, para que las embarcaciones mientras se desplazan a través de la vía acuática, tengan acceso a la red. El equipo flotante que son las estaciones móviles, tienen un puente inalámbrico que permite interactuar la red cableada interna con la Intranet terrena. La embarcación puede contar con dos y hasta cuatro computadoras, que se encuentran interconectadas a través de un switch y este switch posee un puerto configurado para establecer el puente entre las dos redes, por medio de la interfase inalámbrica.

Esta red inalámbrica esta basada en el estándar IEEE 802.11b, supliendo las necesidades y criterios iniciales del diseño, que tenían como objetivo principal la alta capacidad del canal de transmisión, es decir la velocidad. La red inalámbrica cada día tiene mas auge, y los clientes están satisfechos con el desempeño. Pero es aquí, donde se retoma lo que anteriormente se ha mencionado, las vulnerabilidades del estándar IEEE 802.11 y la aplicación de soluciones de seguridad. Para mantener la integridad y seguridad de los usuarios, protegiéndolos así de posibles ataques.

Se decide utilizar el concepto de redes perimetrales (*Perimeter Networks*), el cual evoca mecanismos de seguridad para proteger la red, tales como firewalls y VPNs. Es necesario entender que todos los productos pueden ser vulnerables a ataques, solo que dependerá de las políticas de seguridad y la configuración que se les implanten, para poder mitigar estos posibles ataques. Se evaluaron los tipos de amenazas a los que son susceptibles los equipos basados en el estándar IEEE 802.11 (se mencionaron al inicio de este documento), seguido este paso, es posible conocer de que manera se pueden desplegar y configurar redes inalámbricas seguras.

Detallado el tipo de usuarios y sus funciones dentro de la red, se procedió a reducir el factor riesgo, esto se realizo mediante el aislamiento de la red inalámbrica, colocándola en un segmento controlado o DMZ (*Desmilitarized Zone*), que de por si representa una defensa perimetral proveída por el firewall. La red inalámbrica ahora se encuentra en un segmento controlado, para el acceso hacia la Intranet e Internet, es decir, se mantiene aislado de la red corporativa y así se tiene otro perímetro de seguridad. Hasta ahora tenemos aislada la red inalámbrica y a sus usuarios, pero son estos usuarios, los asiduos clientes de las aplicaciones corporativas. Es aquí donde la premisa "Todo acceso de, hacia y dentro del segmento debe ser controlado" se concretiza, se preguntaran como se puede controlar este acceso dentro de un segmento aislado y dar

Continúa en la página 10

Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b

Viene de la página 9

acceso hacia las aplicaciones corporativas, la solución mas conveniente es un concentrador de VPN [Figura 1].

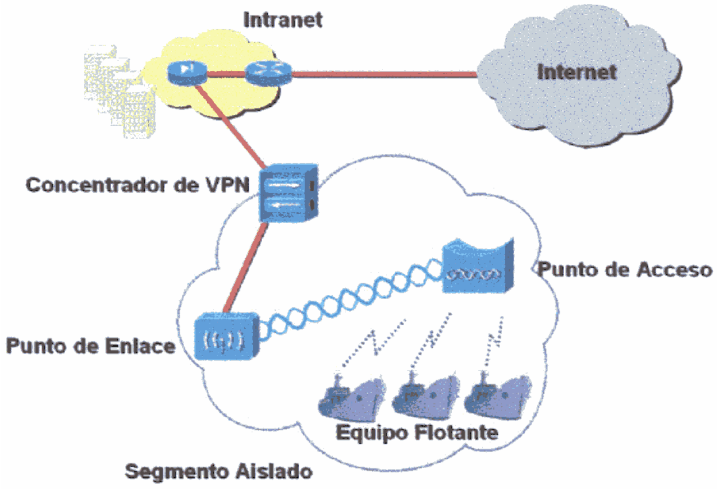


Figura 1. Diseño Experimental de Seguridad en la Red Inalámbrica

El concentrador de VPN proveerá una comunicación segura a través de su túnel, utiliza una encriptación mediante *hardware*. Hay también encriptación mediante *software*, pero dependerá de la elección del tipo de equipo para la encriptación, por presupuesto y rigidez de las políticas de seguridad que hemos comentado anteriormente. La encriptación mediante *hardware* provee un rendimiento mayor y mejora el funcionamiento de todo el sistema. Se decidió utilizar la tecnología de túneles (*tuneling*) *IPsec*, siendo el más utilizado hoy en día, porque provee escalabilidad hacia las nuevas tecnologías que se avecinan. *IPsec* es un grupo de extensiones de la familia del protocolo IP, que trabajan en la capa de red. *IPsec* provee servicios criptográficos de seguridad.

Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. *IPsec* provee servicios similares a *SSL* (*Secure Socket Layer*), pero mucho más complejos que *SSL*; de un modo que es completamente transparente para las aplicaciones y mucho más robusto. Es transparente porque las aplicaciones no necesitan tener ningún conocimiento de *IPsec* para poder usarlo. Se puede usar cualquier protocolo IP sobre *IPsec*. Por naturaleza *IPsec* enmascara las direcciones dentro de la DMZ, por lo que un *NAT* (Network Address Translator) no es requerido.

Este *IPsec* utiliza algoritmos de encriptación tales como *DES* y *3DES*. Algoritmos de *hash*, que proveen autenticación e integridad, tales como *HMAC-MD5*, *HMAC-SHA-I*. La autenticación se realiza mediante *RSA digital*, llaves recompartidas y certificados. Esto representa 4 puntos tangibles, la confidencialidad de la data que es encriptada, la integridad de la data, la autenticación del punto de origen de la data, y la protección de data rescrita.

Así mismo, se explora la posibilidad de desplegar un nuevo sistema de encriptación, basado en la tecnología pre estandarizada *TKIP* (*Temporal Key Integrity Protocol*), el cual no ha sido ratificado como un estándar aun, pero que fabricantes como Cisco han optado por implementar en sus productos. Esta técnica es desarrollada por el grupo de seguridad inalámbrica IEEE 802.11i, el *TKIP* promueve tres componentes que realzan la encriptación WEP. Uno, la revisión de integridad del mensaje o *MIC* (*Message Integrity Check*), que provee autenticación eficaz de los *frames* para mitigar las vulnerabilidades de ataques de tipo *"man-in-the-middle"*. Dos, el proveerle llaves a cada paquete (*Per-Packet Keying*), para así proporcionarle una llave nueva y única de *WEP* a cada *frame*, mitigando los ataques de llaves *WEP* derivadas. Tres, difusión de llaves mediante rotación (*Broadcast Key Rotation*), estas realizan un proceso dinámico para la entrega de llaves, como estas llaves se entregan antes de realizar la autenticación, los puntos de acceso no necesitan estar pre configurados con la misma llave, reduciendo así la oportunidad de ataques de derivación de llaves estáticas.

RECOMENDACIONES

Se recomienda:
-No utilizar el SSID como método de seguridad en las WLANs.
-No desplegar una WLAN sin habilitar la encriptación WEP.
-No utilizar control de acceso a la red mediante direcciones MAC.
-La autenticación de usuarios para prevenir

Continúa en la página 11

Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b

Viene de la página 11

accesos NO autorizados hacia los recursos de la red.
-El aislamiento de los datos para proteger la integridad y privacidad de los datos transmitidos.
-La creación de políticas de seguridad, las cuales dejaron de ser una opción.
-La actualización del personal de administración de las WLANs, mediante revistas, *journals*, grupos de investigación o de seguridad, inscripción a grupo de noticias tales como HISPASEC, etc.

CONCLUSIÓN

Es necesario reconocer las vulnerabilidades del sistema, y tener de manifiesto que todo equipo puede ser susceptible a ataques. El sistema del caso práctico en cuestión, se encuentra totalmente desplegado, asegurado, y con bondades de escalabilidad. La implementación de políticas de seguridad es costosa, pero a la larga representa ahorro en la integridad y privacidad de la información que se manipula. Los profesionales de estas áreas, necesitan comprender las facilidades y riesgos, para así poder evitar el caos, para un desarrollo que augure niveles eficientes y seguros para los sistemas inalámbricos y demás. Es imperante la necesidad de actualización constante en estos temas tan ambiguos, pero necesaria para un fin.

RECONOCIMIENTOS

El autor quisiera agradecer a todo el personal de la Unidad de Interconexión de Redes de la Autoridad del Canal de Panamá, por proveer el conocimiento que se despliega en este documento. Al Grupo de Desarrollo e Investigación de Redes Inalámbricas de la Universidad Santa María La Antigua, del cual es miembro e investigador. Sin más y por ultimo, agradecer por la oportunidad de presentar este trabajo de investigación, para participar del concurso de trabajos estudiantiles de IEEE Sección Panamá 2003.

REFERENCIAS

[1] W. Odom, "Cisco CCNA Exam #640-607 Certification Guide", Cisco Press, Indianapolis, 2002.
[2] M. Castelli, "Network Consultants Handbook", Cisco Press, Indianapolis, 2001.
[3] 3Comm, "IEEE 802.11 b Wireless LANs", 2002.
[4] Cisco Networkers 2002, "Deploying and Managing Wireless LANs", Session ACC-231, 2002.
[5] W. Arbaugh, N. Shankar, Y. Wan, "Your 802.11 Wireless Network has No Clothes", Maryland, Marzo, 2001.
[6] D. Halasz, "IEEE 802.11i draft & Call for Interest on Link Security for IEEE 802 Networks", Noviembre, 2002.
[7] Microsoft, "Virtual Private Networking Ín WÍndows 2000: An Overview", Septiembre, 2001.
[8] "How to build a Secure WLAN", Cisco Packet Magazine, pp. 40-44, Vol 14, No 2, Second Quarter 2002.

Celebración de 31º Aniversario de IEEE Sección Panamá

Viene de la página 1

En la noche de ese mismo día, se celebró un sencillo cóctel en el cual brindamos y celebramos 31 años de existencia de IEEE Sección Panamá. Durante la noche, se proyectó los logros sobresalientes acompañados de una secuencia fotográfica de los sucesos y personajes que han tenido que ver con la Sección en todo este tiempo. Durante el acto de la noche se hizo un brindis por la salud y éxitos de todos nuestros miembros y se entregaron placas de reconocimiento internacional al Capítulo de Comunicaciones de Panamá y al Ing. Gustavo Bernal. Culminamos la velada con un animado cóctel y una rifa de premios para los asistentes.

Presidenta de la Sección, Ing. Tania Quiel dirigiendose a los presentes durante el cóctel de Aniversario

Entrega de premios durante el Cóctel de Aniversario

Entrega de Reconocimientos durante el Cóctel de Aniversario.

La semana culminó, el sábado 13, con la realización de una de las metas del año, el Proyecto IEEE en la Comunidad, que en esta ocasión nos llevó a la ciudad de Penonomé provincia de Coclé. Se destacó la participación de los miembros IEEE, Ing. Gustavo Bernal, Ing. Román Altamiranda, Ing. Tania Quiel, Judith Pino, Rafael Asprilla, Eduardo Rodríguez y dos voluntarios no miembros Oscar Aguilar y Frank Barragán, quienes donaron desinteresadamente todo su sábado para trabajar por este proyecto. Además, se contó con el apoyo de la empresa Electrocentro, S.A., propiedad del LSM, Ing. Ernesto Richa quien donó todos los materiales utilizados.

Vistas de trabajos realizados en Penonomé

El próximo 11 de octubre tenemos proyectado realizar el segundo Proyecto del 2003 de IEEE en la Comunidad, el cual se realizará en la Escuela José Isabel Herrera en Nombre de Dios, Colón.

Seminario de Seguridad en Operaciones de Alto Voltaje

El día 26 de Julio de 2003 en el Hotel Holiday Inn el Capítulo de Potencia (Power Engineering Society) presentó el Seminario de Seguridad en Operaciones de Alto Voltaje dictado por el Lic. Igor Tello, quien cuenta con una amplia experiencia en el área de seguridad en instalaciones eléctricas por lo que el evento tuvo una gran acogida ya que tuvimos una participación de 51 profesionales de diferentes empresas como Edemet, S.A., Zoluciona, ETESA, BLM, Panamá Port, Manzanillo Internacional y otras empresas del sector eléctrico en Panamá. Los participantes se mostraron muy satisfechos por el dinamismo y fuerza con que fue presentado el Seminario por el Lic. Tello. Los principales temas presentados en este seminario fueron: reglas generales, efectos de la corriente eléctrica, equipos y herramientas de trabajo, equipos de protección personal, sistemas de distribución aérea y subterránea y situaciones de emergencia.

Vista de los asistentes y el expositor, Lic. Igor Tello, en el Seminario.

Seminario de Mantenimiento de Transformadores

El Capítulo de Potencia presentó el día 26 de agosto el Seminario de Mantenimiento de Transformadores de Potencia dictado por el Ing. Jorge Fernández Daher de nacionalidad Uruguaya y conferencista regional de la Sociedad de Potencia del IEEE. En este seminario participaron 50 profesionales panameños de las diferentes empresas del sector eléctrico en Panamá, los puertos y otras empresas del área. Los principales temas tratados en este importante seminario fueron instalación de transformadores, aislación dieléctrica, accesorios, ensayos, monitoreo de transformadores y capitalización de pérdidas.

Vista del Seminario de Mantenimiento de Transformadores

Seminario de Acceso de Banda Ancha

Participantes al Seminario de Acceso de Banda Ancha

El pasado 28 y 29 de noviembre se llevó a cabo el Seminario “Acceso de Banda Ancha” ofrecido por el Capítulo de Comunicaciones, en el marco del Distinguished Lecturer Tour (DLT) que incluyó a Panamá, Ecuador, Colombia y Perú. El expositor fue el Dr. Hikmet Sari, Catedrático del Ecole Supérieure d Electricité, en París, Francia. En este seminario se trataron temas tales como la especificación DOCSIS 2.0 y tecnologías de banda ancha de microondas, como es el caso de LMDS. El seminario fue de provecho para los participantes, los cuales tuvieron la oportunidad de intercambiar experiencias con el Dr. Sari, así como también se llevó a cabo una comparación entre las tecnologías de banda ancha con mayor penetración en Panamá: Cable MODEM y ADSL.

Segundo Get Together GOLD

La lluvia y por ende el tranque, bautizaron una vez más nuestra actividad, mas no impidieron que realizáramos nuestra reunión. El 20 de Agosto pasado se llevó a cabo el segundo Get Together GOLD, esta vez nos reunimos en la Taberna de Benningan´s en donde compartimos entre un par de Margaritas (¿les comenté que había Open Margarita?); temas varios entre ellos el famoso ataque del Welchia y sus estragos, recomendaciones para el trabajo, troubleshooting en la red, estudios de mercado, en fin de todo un poco.

Luego pasando más concretamente a actividades de IEEE, tuvimos la oportunidad de conocer los detalles y las "fotos" del que fue nuestro representante ante el CONESCAPAN en El Salvador de este año, el recién graduado y por ende nuevo miembro GOLD: Ing. Carlos Kan.

Definitivamente que pasamos un buen rato escuchando las anécdotas e impresiones del compañero. Como todo en IEEE, esta reunión tenía un objetivo: compartir, expresar dudas, intercambiar contactos y conocimientos entre los presentes. Acompañados de unas riquísimas quesadillas, buffalo wings y otras cosas más, fue interesante observar una vez más ese lazo invisible de compañerismo. De escuchar recomendaciones que valen oro, anécdotas y chistes.

Misión Completa.

Vista del Segundo Get Together GOLD

CONCAPAN XXIII Tegucigalpa, Honduras

Con el lema “El reto de la tecnología en pos de una mejor calidad de vida”, IEEE Sección Honduras está organizando la Vigésima Tercera Convención de Centroamérica y Panamá – IEEE CONCAPAN XXIII. Este tradicional evento congrega anualmente a los profesionales de las ingenierías eléctrica, electrónica y de computación de toda la región para actualizarse y compartir conocimientos con sus colegas y con empresas especializadas.

Esta convención a lo largo de los años ha ido ganando preponderancia como lugar de encuentro idóneo para los ingenieros, técnicos y público en general que desean conocer los últimos avances en materia de tecnología. Las características de rotación anual de CONCAPAN en distintas ciudades de la región brindan la posibilidad de difundir la información entre los países participantes y permite conocer la multiplicidad de culturas con que contamos.

En esta oportunidad la sede de CONCAPAN XXIII es el Hotel Clarión ubicado en la Ciudad de Tegucigalpa, capital de Honduras y se desarrollará los días 13, 14 y 15 de noviembre de 2003.

Entre las actividades más sobresalientes del evento se incluyen presentación de ponencias especializadas, exhibición técnica, cursos tutoriales y actividades de esparcimiento y camaradería. Adicionalmente, y siguiendo la tradición implantada el año pasado en la CONCAPAN XXII de la Ciudad de Panamá, se desarrollará un foro de interconexión centroamericana.

IEEE Sección Panamá está organizando un grupo para asistir juntos a la convención y representar así a nuestro país y apoyar a nuestros compatriotas que presentarán sus ponencias en el marco del evento. Para mayor información o inscribirte en el grupo de viajeros escribe un mensaje a sec. panama@ieee.org o llama al 223-7445.

IEEEE Sección Panamá y la Robótica

"Robot: Manipulador mecánico, reprogramable y de uso general. "

"Robótica: El diseño, fabricación y utilización de máquinas automáticas programables con el fin de realizar tareas repetitivas como el ensamble de automóviles, aparatos, etc. y otras actividades."

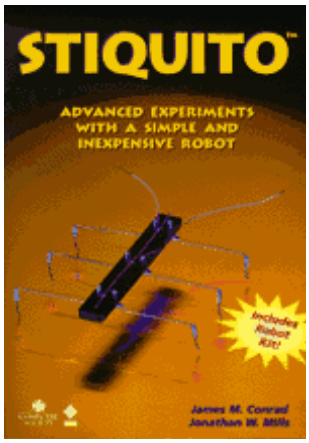
Recientemente el Ingeniero Román Altamiranda dicto sendos talleres orientados a introducir los conceptos de robótica. En los mismos participaron entusiastas estudiantes que tuvieron la oportunidad de aprovechar el aprender los conceptos básicos de introducción a la robótica. El primer seminario se realizó el 6 de septiembre en el colegio “Pureza de María” de Villa Lucre con una asistecia de 13 participantes y el segundo se realizó el 20 de septiembre en la Universidad Santa María La Antigua con una asistencia de 10 personas.

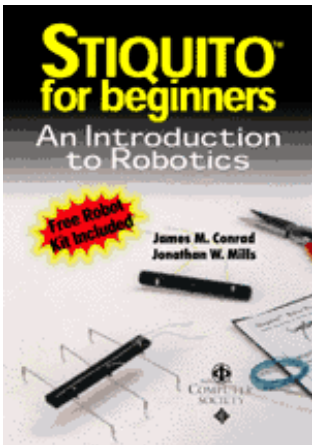
El Ing. Román Altamiranda mientras dictaba el Seminario de Robótica

El Ingeniero Altamiranda realizo un pasaje por los conceptos generales y específicos de la robótica, introdujo el origen del concepto en si; además planteo las diferentes aplicaciones y usos que a la robótica se le esta dando en la actualidad y sus oportunidades futuras. La parte practica fue realizada con la utilización de kits de robots conocidos como stiquito (www.stiquito.com) , los cuales son robots que utilizan tecnología de movimientos musculares a través de un material conocido como Nitinol. Stiquito fue creado por Jonathan Mills de Indiana University; se trata un robot hexápodo que utiliza Nitinol como actuador.

Stiquito es un robots económico y por sus características es ideal para utilizarlo como vehículo de introducción a la robótica ; es una excelente herramienta para la investigación.

IEEE Computer Society ha publicado dos libros donde desarrolla vastamente el tema: “Advanced Experiments with a Simple and Inexpensive Robot” y “Stiquito for Beginners: An Introduction to Robotics”.





Mas allá de la ciencia ficción estamos en el umbral de un sin número de posibilidades de aplicaciones en donde la robótica tiene y tendrá un uso cotidiano. Nuestro país tiene fronteras muy definidas y claras, contiene dentro de ellas un mercado bastante limitado. Las oportunidades de apertura a través de las diferentes iniciativas de tratados comerciales, nos posibilita nuevos horizontes. Es importante que estamos preparados para afrontar todos estos nuevos retos. El desarrollo tecnológico será una herramienta importante para cumplir con tal cometido.

Grupo de Escuela Secundaria asistentes al Seminario de Robótica STIQUITO

NUEVOS MIEMBROS IEEE

La Junta Directiva del IEEE Sección Panamá, da la más cordial bienvenida al instituto a los nuevos miembros del IEEE durante el periodo julio a septiembre del 2003. Ellos son:

■ Judith Pino ■ Beatriz Crespo ■ Edgardo Hull ■ Peter Arnoldo ■ Héctor Williams ■ José Matos ■ Abdo Rosa ■ Eyda Ríos ■ Yolanda Victoria Vega ■ Isaac Achurra ■ Charlie Davis ■ Jorge I. Echazabal B. ■ Edgard Chong ■ David Segovia ■ Esteban Ortiz ■ Javier Silva ■ Luis Eduardo Henao P. ■ Italio Castillo ■ Diego Luque ■ Issam Tejera ■ Gabriel Godoy ■ Iohann Robles ■ Julissa De León ■ Amlicar Pasco ■ Laura Mora ■ Eric Iglesias ■ Elvis Aguilar ■ Edelmira Atencio ■ Rolando Binns ■ Eric Alberto Morales ■

Felicidades!

IEEE Sección Panamá

Ave. Manuel Espinosa Batista
Edificio Ateneo de Ciencias y Artes
Oficina #3

Apartado 6-795
El Dorado
Panamá
Rep. de Panamá

Tel.: +507-223-7445
Fax: +507-223-7445
Email: sec.panama@ieee.org
Web: http://www.ieee.org/panama

CALENDARIO DE EVENTOS

SEPTIEMBRE 30, OCTUBRE 1 y 2
- Seminario del Código Eléctrico, NEC
  Hotel Miramar Intercontinental

OCTUBRE 4
- Seminario sobre Bibliotecas Digitales
  Dr. Ricardo Baeza, Chile
  Hotel Holiday Inn

OCTUBRE 15
- Conferencias para Jóvenes Profesionales GOLD

OCTUBRE 9
- CICONTEC 2003. Ciclo de Conferencias 2003 IEEE UTP

OCTUBRE 21 y 22
- Seminario de Sistemas de Aterrizaje
  Ing. Freddy Villalta, El Salvador
  Hotel Miramar Intercontinental

NOVIEMBRE 13 al 15
- CONCAPAN XXIII
  Tegucigalpa, Honduras

NOVIEMBRE 15
- Cierre del Concurso AT&T

DICIEMBRE 16 – 7:30pm
- Fiesta de Navidad