JORNADA IK4

“Ciberseguridad en aplicaciones industriales: situación actual y tendencias”

Parque Científico-Tecnológico de Gipuzkoa, Orona Fundazioa
Campus Hernani-Galarreta (Gipuzkoa)
Martes, 17/10/17

1. DESCRIPCIÓN DE LA JORNADA

En estos últimos años el auge y crecimiento generalizado de internet y las posibilidades que esto ha abierto en cualquier campo, está provocando el traslado al ámbito industrial de herramientas y estrategias hasta ahora prácticamente aplicadas sólo en sectores comerciales, de servicios o ligadas a productos de consumo. Esto supone un paso trascendental para cualquier empresa de este tipo, las cuales, en general, sólo utilizaban internet en sus actividades de marketing y comunicaciones.

La ubicuidad de las redes de telefonía y datos con capacidad de transmitir grandes cantidades de información de forma fiable y en tiempo real; los grandes avances en electrónica, tanto en miniaturización como en precisión y precio, que han facilitado la aparición de infinidad de sensores y sistemas de monitorización y comunicación; la globalización de los mercados y, por tanto, la mayor lejanía física de los clientes y la aparición de nuevos competidores; la obligación de poner en el mercado nuevos productos de alto valor añadido que compensen esa mayor competencia y fidelicen a los clientes, por ejemplo ofreciendo máximos niveles de personalización … todo esto en poco tiempo se ha convertido es una realidad inexorable que crece por momentos y, a su vez, abre nuevas líneas, necesidades y posibilidades.

Pero, como es normal, estas nuevas oportunidades llevan aparejadas la aparición de nuevos riesgos y uno principal y muy grave es la seguridad de las comunicaciones y de la información que intercambiamos. No hace falta recordar los sonados casos de entidades de primera línea que han visto cómo sus sistemas han sido ciber-atacados y sus datos o perdidos o expuestos, cuando no secuestrados, con el consiguiente perjuicio económico y de prestigio.

Nuestras empresas industriales empiezan a utilizar masivamente equipos conectados a internet y esta explosión del “internet of things” (IoT) o internet de las cosas, obliga absolutamente a disponer de capacidades avanzadas en ciberseguridad, para minimizar los riesgos mencionados.

En este marco, IK4 Research Alliance organiza esta jornada dirigida a empresas, universidades, centros de investigación y cuantos otros agentes estén interesados en conocer las últimas realidades, tendencias y retos a futuro en este ámbito, desde un punto de vista técnico.

Contaremos con la presencia del Gobierno Vasco y la Diputación de Gipuzkoa, que nos explicarán las iniciativas que lideran en este campo. Y abrirá las ponencias técnicas un experto de Daimler Trucks, que nos describirá su experiencia, las futuras líneas de trabajo y su visión general respecto de las implicaciones, oportunidades y retos de la progresiva introducción de estas herramientas en su estrategia industrial y de servicios.

Los diferentes ponentes abordarán posteriormente diversos aspectos de esta tecnología, con el fin de tratar de concretar el panorama que se nos presenta en un futuro cercano, centrándose en los aspectos de mayor novedad o nivel científico-tecnológico con sus aplicaciones concretas.

PROGRAMA

09h30 – 09h35 Saludo y Presentación de la jornada: IK4 Research Alliance

09h35 – 09h50 Diputación Foral de Gipuzkoa. Estrategia de la administración guipuzcoana en materia de ciberseguridad industrial.
Ainhoa Aizpuru, Diputada Foral de Promoción Económica, Medio Rural y Equilibrio Territorial

09h50 – 10h05 Gobierno Vasco. Estrategia e intereses de la administración vasca en materia de ciberseguridad industrial.
Estíbaliz Hernáez, Viceconsejera de Tecnología, Innovación y Competitividad

10h05 – 10h25 IK4 Research Alliance. Panorama general actual de la ciberseguridad industrial.

10h25 – 11h05 DAIMLER TRUCKS. Cyber attacks – an emerging risk for vehicle control !

11h05 – 11h35 pausa café

11h35 – 11h55 CEIT-IK4. Ciberseguridad en entornos IoT y evaluación de impacto en infraestructuras críticas.

11h55 – 12h15 IK4-IKERLAN. Seguridad de los sistemas embebidos: factor clave para proteger el negocio

12h15 – 12h35 VICOMTECH-IK4. Aplicación del Big Data a la ciberseguridad.

12h35 – 13h15 coloquio entre los ponentes, preguntas y cierre

13h15 – 15h00 pinchos y contacto

NOTAS:

- Jornada gratuita, entrada libre previa inscripción.
- La ponencia de Daimler Trucks será en inglés, no habrá traducción simultánea.
- Modera y conduce la jornada: Javier Laucirica, Director Científico-Tecnológico de IK4.
- SERVICIO DE ASESORAMIENTO: al finalizar la jornada, personal de CDTI estará a disposición de las personas interesadas en obtener información sobre instrumentos y ayudas de este organismo para poner en marcha proyectos de I+D+i. Para ello se ruega que lo señalen en el momento de acreditarse en el acceso al evento.

COLABORADORES:

2. PONENCIAS

DAIMLER TRUCKS

Título:
Cyber attacks – an emerging risk for vehicle control !

Resumen:
La creciente automatización de la conducción de vehículos es posible gracias a los avances básicamente en electrónica y software. Sin embargo, esto abre la puerta a que los sistemas de control sean atacados informáticamente, pudiendo poner en grave riesgo a los pasajeros del vehículo afectado, a los de los demás vehículos con los que circula, a los peatones y a las infraestructuras.

Ponente: Roland Trauter
Manager Software Integration at Daimler Trucks Advanced Engineering in Stuttgart. In several positions within Daimler's research divison he has been working on software architecture, software analysis and reengineering of object-oriented software.
He has been leading Daimler's ecoDriver project work with focus on application prototype development, on- road tests, acceptance studies and follow-up data analysis.
He is now continueing this work on advanced navigation with focus on safety and security.
Previous work has been on Autosar development and software quality assurance for advanced driver assistance systems.

CEIT-IK4

Título:
Ciberseguridad en entornos IoT y evaluación de impacto en infraestructuras críticas.

Resumen:
Teniendo en cuenta que la seguridad del sistema completo la establece la seguridad del eslabón más débil de la cadena, es importante tener en mente toda la cadena de comunicaciones existente desde los dispositivos finales (IoT) hasta la nube. Se resaltarán aspectos importantes a tener en cuenta más allá del cifrado de las comunicaciones y se propondrán algunas claves para arquitecturas IoT ciberseguras. También se abordará la problemática de la evaluación del impacto de intrusiones y/o ataques mediante aproximaciones y ejemplos reales, que es fundamental sobre todo en infraestructuras críticas. Finalmente, se resaltarán las líneas de investigación actuales en esta temática.

Ponente: Javier Añorga
Doctor en Ingeniería Aplicada por la Escuela Superior de Ingenieros de la Universidad de Navarra (Tecnun) e Ingeniero de Telecomunicación por la Escuela Superior de Ingenieros de la Universidad de Navarra (Tecnun).
Certificado en CEH del EC-Council (Certified Ethical Hacker).
Investigador del grupo de Análisis de Datos y Gestión de la Información de la división de TIC en Ceit-IK4. Compagina labores de investigación dentro de Ceit-IK4 con las de docencia en Tecnun, incluyendo el liderazgo del Club de Seguridad y Hacking Ético. Su campo de trabajo actual se focaliza en las redes de comunicaciones de datos y ciberseguridad. Ha colaborado en varios proyectos de I+D y, así mismo, es autor o coautor de 13 publicaciones científicas entre las que se encuentran revistas indexadas y congresos internacionales.

IK4-IKERLAN

Título:
Seguridad de los sistemas embebidos: factor clave para proteger el negocio.

Resumen:
Los sistemas embebidos tienen un papel fundamental en la industria (control de procesos) así como en otros muchos sectores (automoción, ferroviario, control de accesos, etc.). En el desarrollo de estos sistemas se han priorizado históricamente los requisitos de seguridad funcional (safety) y tiempo real, dotándolos de escasa o nula seguridad (security). La irrupción del paradigma IoT y el constante aumento de la conectividad han propiciado que estos dispositivos hayan quedado expuestos a ataques remotos, convirtiéndose en muchos casos en el eslabón más débil de los sistemas. Algunos factores que han contribuido a esta situación son la falta de concienciación de proveedor y del cliente final, así como la ausencia de una normativa de referencia.
En los últimos años esta situación está cambiando y los fabricantes están visualizando la necesidad de diseñar sus productos con las medidas de seguridad necesarias. Sin embargo, muchas de las tecnologías de seguridad disponibles provienen del ámbito de las TIs y no son fácilmente aplicables en un sistema embebido debido a la menor disponibilidad de recursos, presencia de protocolos especializados, exigencias de tiempo-real, la necesidad de compatibilizar las medidas de seguridad funcional o la dispersión de tecnologías.
En esta ponencia se profundizará en la seguridad de los sistemas embebidos como factor clave para proteger el negocio, garantizar la prestación del servicio de forma confiable, y posibilitar el despliegue de nuevos servicios. Se explicarán los riesgos, las ventajas de considerar la seguridad desde el diseño, las posibles soluciones tecnológicas, casos de aplicación, así como cumplimiento normativo y certificación.

Ponente: David González
Máster en procesamiento de señal y comunicaciones por la Universidad de Edimburgo, Ingeniero en Automática y Electrónica Industrial por Mondragón Unibertsitatea.
Responsable de Equipo de Investigación Industrial Security en IK4-IKERLAN.
Actualmente trabaja en el área de sistemas embebidos confiables de IK4-IKERLAN como responsable del equipo de investigación Industrial Security. Entre otros, es responsable de la colaboración en el ámbito de sistemas embebidos con empresas del sector de la aerogeneración, contribuyendo al desarrollo y mantenimiento de sistemas de supervisión y control de turbinas eólicas. Durante años se ha dedicado al diseño y desarrollo de plataformas embebidas para los sectores de salud y energía, participando a su vez en diversos proyectos de investigación en el ámbito nacional y europeo. Anteriormente también ha sido responsable de la actividad investigadora en plataformas hardware, virtualización y sistemas de criticidad mixta.

VICOMTECH-IK4

Título:
Aplicación del Big Data a la ciberseguridad.

Resumen:
La ponencia se centrará en la gestión de grandes columenes de datos; datos heterogéneos procedentes de video, imagen, audio, sensores, logs de procesos, etc., y su procesamiento en tiempo real para la detección de anomalías y comportamientos extraños. Todo este procesamiento debe llevarse a cabo en tiempo real, y complementado con herramientas de visual analytics que ayuden en la identificación de dichos patrones de un modo sencillo, rápido y eficaz..

Ponentes: Igor García Olaizola
Doctor en Informática por la Universidad del País Vasco (EHU-UPV) e ingeniero en Electrónica y Automática Industrial por la Universidad de Navarra (Tecnun).
Director del departamento de Data Intelligence en VICOMTECH-IK4, orientado al análisis estadístico y a la aplicación de técnicas de Big Data. También es profesor asociado en Tecnun.
Desarrolló su tesis de Master en el Fraunhofer Institut für Integrierte Schaltungen (IIS), en Erlangen (Alemania), en donde trabajó durante un año como asistente de investigación en varios proyectos relacionados con la decodificación de audio según el estándar MPEG (MP3 y AAC).
En 2002 entró a formar parte de personal investigador de VICOMTECH-IK4. En 2006 trabajó durante año y medio como consultor de tecnología en la empresa Vilau, spin-off del centro, en donde lideró varios proyectos de diseño y despliegue de cabeceras de TDT Interactiva. En 2007 pasó a ser director del departamento de Digital Media de VICOMTECH-IK4. Su trabajo de tesis está basado en la caracterización de imágenes a través de descriptores globales y en técnicas de inteligencia artificial.

3. LUGAR DE CELEBRACIÓN DE LA JORNADA

"Ciberseguridad en aplicaciones industriales: situación actual y tendencias"

Parque Científico y Tecnológico de Gipuzkoa, Orona Fundazioa
Campus Hernani-Galarreta
Camino Jauregi, s/n.
20120 Hernani (Gipuzkoa)
Tel: (+34) 943 335588

https://goo.gl/maps/dLUMdACToKT2
Latitud: 43°16'34.3"N | Longitud: 1°59'08.2"W