

Miércoles 2 de diciembre – Sesión divulgativa

Seguridad y privacidad desde el Diseño

Pedro Alberto González González – AVPD – Vitoria-Gasteiz

Las necesidades de seguridad y en particular de privacidad hacen necesaria una filosofía de diseño de aplicaciones teniendo en cuenta estos requerimientos y no como un añadido posterior. Se estudia en particular el caso de la privacidad en el contexto de la Internet de las cosas.

Un análisis ético de los riesgos del *big data*

Txetxu Ausín Díez – Instituto de Filosofía – CSIC – Madrid

Los datos personales, como por ejemplo los datos de salud, son extremadamente sensibles y requieren un especial cuidado y protección. Sin embargo, la analítica de big data entraña una serie de importantes riesgos: Re-identificación, brechas en la seguridad del almacenamiento de grandes cantidades de datos, reutilización y transferencia de los datos, opacidad y escasa información en la recogida de datos, determinismo de los datos ("datificación") y discriminación ("perfilamiento"), entre otros. Para abordar estos desafíos y minimizar los riesgos se plantean una serie de principios éticos y buenas prácticas para los procesos de *big data*.

Vulnerabilidades de ciberseguridad en los entornos industriales

Isidro Calvo Gordillo – DISA, EUI Vitoria-Gasteiz

Hasta hace unos años, los Sistemas de Control y Automatización Industrial o IACS (Industrial Automation and Control Systems) estaban en gran medida aislados de los sistemas corporativos, lo cual facilitaba su seguridad frente a ciberataques. Sin embargo, la generalización del uso de Internet y las comunicaciones inalámbricas ha cambiado este panorama.

Durante los últimos años se han detectado múltiples evidencias de ciberataques que explotan las vulnerabilidades de los protocolos utilizados en los IACS. Desafortunadamente, estos ataques han ido aumentando de manera significativa en el último lustro.

En esta ponencia se describe en qué consisten algunas de las vulnerabilidades más habituales en los IACS.

Safety & Security: una necesidad actual

Xabier Larrucea Uriarte – TecNALIA, División ICT, Derio

Los temas relacionados con la seguridad (*Safety & Security*) están adquiriendo una relevancia prioritaria no solo en el mundo industrial sino también en el día a día de la ciudadanía. El diseño de los sistemas según principios de Seguridad es vital para poder desarrollar sistemas fiables. Aspectos como performance o assurance cases son necesarios y requeridos en entornos industriales como la automoción y aviónica.

Martes 15 de diciembre – Sesión técnica

Comunicación segura con IPv6

José Manuel López Guede – DISA, EUI Vitoria-Gasteiz

A la hora de garantizar la seguridad en las comunicaciones existen dos factores que son de vital importancia: la conducta de los propios usuarios de dichas comunicaciones, y los protocolos de comunicaciones utilizados. Dentro de estos últimos, hay uno que aborda de modo integral el tema de la seguridad junto con otros aspectos más pragmáticos: el protocolo *Internet Protocol v6 (IPv6)*. En la charla se analizarán las facilidades que aporta dicho protocolo para todo lo concerniente a la seguridad en las comunicaciones.

La investigación digital y la ciencia forense cibernética

Ismael Etxeberria Agiriano – LSI, EUI Vitoria-Gasteiz

Es habitual relacionar el término forense directamente con la medicina, sobre todo por su extensa utilización en películas y series de televisión. En el campo de la informática las técnicas forenses implican la recogida, análisis y conservación de las evidencias del crimen informático. Estas técnicas no siempre tendrán un uso legal en cuyo caso es típico hablar de investigación digital.

Esteganografía mediante ejemplos

Ekaitz Zulueta Guerrero – DISA, EUI Vitoria-Gasteiz

En esta presentación se mostrarán diferentes algoritmos desarrollados en Matlab para ocultar información relevante sobre información redundante.

Se mostrarán fundamentalmente algoritmos donde se introduce información en ficheros de imágenes o audios.

Análisis de la seguridad de Contenedores Docker

Pablo González Nalda – LSI, EUI Vitoria-Gasteiz

Erlantz Sáenz Fraile – Innotec, Madrid

Análisis de las ventajas e inconvenientes en cuanto a seguridad del uso de contenedores Docker. Amenazas y vulnerabilidades por el uso de contenedores, y controles que las minimizan. Vulnerabilidades que se pueden evitar en un sistema genérico por el uso de contenedores para dar servicios al exterior, como un servidor web.

Organizan: Departamentos de Lenguajes y Sistemas Informáticos (LSI) e Ingeniería de Sistemas y automática (DISA) – EUI – Vitoria-Gasteiz

Colaboran: Agencia Vasca de Protección de Datos (AVPD) Vitoria-Gasteiz, Instituto de Filosofía – CSIC Madrid, División ICT Tecnalia, Derio

Patrocina: EUI Vitoria-Gasteiz (UPV/EHU), Proyecto CPS4PSS ETORTEK14/10 (GV/EJ), Proyecto Kontuz! Ref. FFI2014-53926-R, MINECO. <http://kontuz.weebly.com/>

Más información: <http://lsi.vc.ehu.es/wdocs/>

Contacto: Ismael Etxeberria Agiriano, ismael.etxeberrria@ehu.eus

