Criptografía Liviana y Ciberseguridad aplicados a Sistemas Ciberfísicos.

Marcelo Cipriano; Jorge Eterovic; García, Edith; Luis Torres; Bianchi, Sebastián
Instituto de Investigación en Ciencia y Tecnología.
Dirección de Investigación Vicerrectorado de Investigación y Desarrollo.
Universidad del Salvador.

Lavalle 1854 – C1051AAB -Ciudad Autónoma de Buenos Aires - Argentina
{marcelo.cipriano; jorge.eterovic; edith.garcia}@usal.edu.ar
luis.antonio.torres@kyndryl.com; sbianchi@usal.edu.ar

DESCRIPCIÓN DE LA LÍNEA DE INVESTIGACIÓN

CONTEXTO

El Vicerrectorado de Investigación y Desa-rrollo (VRID), de la Universidad Nacional del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndolas como un servicio a la comunidad, entendiendo que los nuevos conocimientos son la base de los cambios sociales y productivos. Se desarro-llan acciones conducentes a concretar pro-yectos de investigación uni/multidisci-plinarios, asociándose a la docencia de grado y postgrado, de universidades nacionales e internacionales.
La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación y a sus investigadores para el desarrollo de Proyectos y Programas de Investigación, nacionales e internacionales, como así también, apoyo y orientación de recursos para la investigación.

A ella pertenece el Instituto de Investigación en Ciencia y Tecnología (RR 576/12) en el cual se enmarca este proyecto con una duración de 2 años (2023-2025).
El mismo se encuentra aprobado por Disposición Decanal No 58/22 con el Nro. Trámite SIGEVA 80020220200024US.

LINEAS DE I+D

RESULTADOS ESPERADOS

RESUMEN

Los llamados Sistemas Ciberfísicos (CPS: cyber-physical system) son mecanismos físicos controlados o monitoreados por equipos informáticos. Se integran mediante una red de datos y de comunicaciones, siendo Internet la mayormente empleada.
Este nuevo conjunto de sistemas, agrupa prácticamente la totalidad de los equipos industriales modernos (Industria 4.0), como así también los recursos y sistemas de las Ciudades Inteligentes (Smart-Cities), Cibermedicina (e-Health), Internet de las Cosas (Internet of Things), solamente por mencionar algunos de los más conocidos.
El proyecto persigue el estudio y análisis de la seguridad de los protocolos de comuni-caciones de los Sistemas Ciberfísicos y los mecanismos y algoritmos criptográficos. En particular aquellos mecanismos de autenti-cación, confidencialidad e integridad ofreci-dos por la llamada Criptografía Liviana o Ligera (LiCrypt: Lightweigh Cryptography).
También se propone la difusión y promoción de estas temáticas en la comunidad científica y tecnológica local.

Se persigue el estudio y análisis de algoritmos criptográficos livianos y protocolos de seguridad, observando fortalezas y debilidades matemáticas y criptográficas, test y pruebas de seguridad, conocer e indagar sobre los nuevos estándares criptográficos en el campo de la Criptografía Liviana. Además comprender los ataques criptoanalíticos recientes y su incidencia sobre los algoritmos y protocolos.

También se persigue la difusiòn de los nuevos algoritmos y estándares criptográficos, como así también sus características de seguridad y su ámbito de aplicación, para transferir a la comunidad académica, científica nacional o internacional, docentes e ingenieros del ámbito IT y OT, la información y resultados obtenidos. En procura de lograr un nexo entre la investigación científico/aca-démica y el mundo de la producción en el marco de Industria 4.0.

FORMACIÓN DE RECURSOS HUMANOS

El equipo de investigadores pertenece al cuerpo docente de Tecnologías Aplicadas en la Facultad de Ingeniería, el área de la Seguridad Informática, de la Universidad del Salvador.

Se espera la incorporación de más docentes investigadores y alumnos. Ya que redundará en un aumento del activo académico e investigativo representado por su cuerpo de docentes participantes, como así también sembrando las bases para la investigación del futuro, a través de la participación de alumnos de la Facultad de Ingeniería.

Se espera la pronta aprobación de la *Diplomatura en Ciberseguridad IT/OT,* la que al sumarse a las propuestas educativas ofrecidas por la Facultad de Ingenierìa, posibilite la incorporación de más docentes investigadores y alumnos.

USAL
UNIVERSIDAD DEL SALVADOR
Ciencia a la mente y virtud al corazón