ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

OFERTA CIBER PARA ESTUDIANTES.

Análisis de Canal Lateral (Side-Channel Analysis) de algoritmos criptográficos en laboratorio.

El alumno colaborará en la actividad del laboratorio de ciberseguridad de IKERLAN, utilizando equipamiento altamente especializado para evaluar la seguridad de distintos productos electrónicos. Se centrará en el manejo del equipamiento de Side-Channel Analysis (SCA), utilizado para romper la seguridad de implementaciones criptográficas y obtener la clave secreta, mediante el análisis de variables físicas como el consumo de potencia o las emisiones electromagnéticas. Las mediciones obtenidas deberán ser procesadas, utilizando para ello distintas técnicas estadísticas y de procesamiento de señal, hasta encontrar la información buscada.
Se requieren conocimientos de electrónica y procesamiento de señal, así como una gran iniciativa e ingenio para buscar nuevas vías de ataque a través de estas técnicas.

OBJETIVOS DEL PROYECTO:

- Adquirir conocimiento teórico y experiencia práctica en la técnicas y herramientas existentes de análisis de canal lateral.
- Evaluar el nivel de protección de distintas implementaciones criptográficas.
- Proponer nuevas técnicas y métodos de evaluación.

LAS FASES SERÁN:

- Estudio de los métodos más comunes para la realización de ataques SCA.
- Prueba y manejo de las herramientas.
- Elección de circuitos a atacar (claramente vulnerables, probablemente vulnerables, protegidos...).
- Realización de ataques sobre diseños escogidos.
- Análisis y comparación de resultados.

TUTOR DE IKERLAN:

Unai Rioja / Servio Paguada

Nuestra cultura Ikerlaniana.

- El mundo no se nos ha dado para contemplarlo sino para transformarlo.
- La tecnología, nuestra actitud.
- Un Proyecto cooperativo vivo de todos y para todos.
- Una filosofía de trabajo que apuesta por la excelencia, cercanía y autonomía.

¡YA ERES PARTE DE NUESTRO EQUIPO!

Nacimos para mejorar y transformar nuestro entorno a través de la tecnología. Por eso, no es casualidad que seamos líderes en transferencia de tecnología a las empresas. Nos gusta soñar e imaginar el futuro. Pero sobre todo nos encanta crear tecnología útil para responder a los retos de las empresas y de la sociedad. Los retos de personas como tú.

En 45 años de historia, hemos conseguido ser pioneros en aplicar la robótica y la inteligencia artificial a la industria, colaborar con la NASA en mejorar sus experimentos en el espacio, aplicar con éxito tecnologías de inducción para mejorar las prestaciones de los aviones o desarrollar el primer tranvía sin catenaria y el primer sistema de almacenamiento de energía para parques fotovoltaicos del Estado.

Toda esta experiencia, junto a la capacidad de aplicación de la tecnología más innovadora, nos permite mejorar y facilitar tu vida, por ejemplo, desarrollando sistemas que consiguen que la energía que consumes sea cada vez más limpia, segura y económica o que el transporte que utilizas a diario sea más cómodo y sostenible. En definitiva, desarrollamos tecnología útil, que impacta en tu día a día y transforma nuestro futuro.

Trabajamos con las empresas líderes en retos que nos hacen crecer y desplegar nuestro mejor talento. Trabajamos en cooperación, en un entorno de aprendizaje continuo y superación y con un equipamiento singular. Y sobre todo disfrutamos creando la tecnología que transformará el futuro.

Si crees en el poder transformador de la tecnología y quieres ser protagonista en los retos tecnológicos del futuro, **IKERLAN es tu lugar.**