Enpresa-Erakundea / Empresa- Entidad

IKERLAN S.COOP

Lanpostua / Puesto:

Tesis doctoral sobre técnicas de análisis de canal lateral para evaluación de ciberseguridad en laboratorio

Lantokia / Lugar de trabajo:

Arrasate

Egin beharreko zereginak edo eginkizunak / Tareas o funciones a realizar:

La ciberseguridad hace referencia a la protección de los activos digitales ante los riesgos de intrusión, modificación o robo. Aunque históricamente se han considerado principalmente los activos contenidos en las plataformas digitales accesibles a través de Internet, el crecimiento de dispositivos conectados los hace también objeto de análisis. Por ejemplo, en dispositivos IoT como coches o teléfonos inteligentes, el hardware se ha convertido en un activo digital objeto de ataques. Compañías cuyos productos están basados en tales tecnologías están cada vez más interesadas en proteger el hardware.

Los ataques físicos son aquellos ataques orientados a explotar una implementación insegura de algoritmos criptográficos sobre elementos hardware. Dentro de este tipo de ataques se encuentran los ataques de canal lateral, o Side-Channel Attack (SCA), y de inyección de faltas, o Fault Injection (FI).

Un canal lateral es una interfaz que poseen los dispositivos físicos sin que el fabricante haya tenido la intención de disponerla. Surgen por diferentes motivos, principalmente debido a las propiedades físicas del hardware. Por ejemplo, un canal lateral es la potencia que el dispositivo consume al procesar datos e instrucciones, o la emisión electromagnética que genera. Al capturar estas variables, un atacante dispone de lo que se conoce como información de canal lateral. Dicha información puede ser utilizada para inferir los datos que el dispositivo está procesando. Por lo tanto, un dispositivo que implementa un algoritmo criptográfico (por ejemplo AES) puede fugar información a través de distintos canales laterales. Un atacante podría extraer la clave secreta a través del procesamiento y análisis de esta información.

El estudio de la efectividad de los ataques de canal lateral contra una implementación criptográfica es de particular interés para los investigadores. La elaboración de nuevas contramedidas para proteger los dispositivos de tales ataques es una constante. De esta forma surge una lucha entre pares: mientras investigadores y desarrolladores analizan los ataques para poder protegerse a través de la implementación de contramedidas, los atacantes analizan las protecciones para poder derrotarles.

Esta propuesta de tesis doctoral persigue objetivos desde uno o ambos puntos de vista. La propuesta comprende (pero no está limitada a) las siguientes líneas de investigación:

- Análisis del estado del arte de los ataques de canal lateral, para determinar las propuestas que permitirán incrementar la eficiencia y eficacia de tales ataques. Algunas

técnicas del estado del arte para la implementación de ataques de canal lateral son las siguientes:

* Algoritmos de estimación de la distribución.

* Redes neuronales.

* Ataques de canal lateral basados en grafos.

- Análisis de la efectividad y eficacia de los ataques de canal lateral, utilizando trazas de grandes dimensiones para determinar la posibilidad de explotar las fugas de información contenidas en las mismas.

- Análisis de las métricas actuales para determinar los posibles aspectos de mejora con el fin de reducir la incertidumbre de los resultados de las evaluaciones de canal lateral.

- Análisis de las contramedidas actuales (masking, hiding) para determinar cómo incrementar su efectividad ante los ataques de canal lateral.

- Investigación de las tecnologías de inserción de instrucciones automáticas actuales, para determinar perspectivas de mejora (como la expansión a otros microcontroladores).

- Diseño y desarrollo de herramientas que ayuden a mitigar la incertidumbre y la enorme dependencia humana que implica actualmente llevar a cabo una evaluación de seguridad frente a ataques de canal lateral.

Eskatzen diren betekizunak / Requisitos exigidos:

- Máster ya terminado o que termine en el curso académico 2022/2023: Ingeniería

Telecomunicaciones, Ingeniería Electrónica, Ingeniería Informática, Física, Matemáticas...

- Ingles hablado y escrito fluido.

- Conocimientos de programación en C y Python.

- Se valorará haber realizado el TFG (Trabajo Fin de Grado) o el TFM (Trabajo Fin de Máster) en

el área que se indica en la oferta.

- Capacidad de relación, organización del trabajo, iniciativa, autonomía y trabajo en equipo.

- Capacidad de comunicación oral y escrita.

- Inteligencia emocional y habilidades sociales.

Eskaintzen dena / Se ofrece:

¿Qué te ofrecemos?

Ser miembro de un equipo que trabaja en temáticas punteras de investigación, junto con investigadores con experiencia, doctorandos y estudiantes, aportando soluciones reales a empresas:

- Flexibilidad de horario y calendario.

- Participación en la toma de decisiones.

- Posibilidad de teletrabajar.

- Compañerismo y ¡buen ambiente!