Tecnológico de Costa Rica

Escuela de Ingeniería en Computación

Seguridad del Software - IC8071

Estudiante:
Axel Alexander Chaves Reyes

Profesor:
Herson Esquivel Vargas

Semestre I

2024

Identifying Near-Optimal Single-Shot Attacks on ICSs with Limited Process Knowledge

La investigación proporcionada plantea si se pueden realizar ataques comparables a sistemas de control industrial (ICS) sin tener conocimiento detallado del sistema y sin simuladores. Además, esto se acompaña del hecho de que un ICS puede contener cientos de componentes físicos de distintos tipos y que realizan interacciones entre sí que dificultan el proceso de encontrar un objetivo para atacar.

Asimismo, se describen los lazos de control cerrado, los cuales corresponden a componentes básicos como un punto de ajuste, un sensor, una función de control y un actuador. Todo este sistema se encarga de recibir entradas de entorno mediante sensores y reaccionar con una acción que compensa dicha entrada.

Por otra parte, se menciona que la parte fundamental de un ataque a un ICS es la comprensión del proceso por parte del atacante, ya que, según la habilidad de dicho sujeto, puede ser capaz de recolectar datos tales como capturas de procesos o tener acceso a la máquina de algún operador.

Por otro lado, también se hace hincapié en identificar ataques óptimos de un solo tiro, donde se destaca la importancia de utilizar conocimientos acumulados de vulnerabilidades conocidas y reconocer los flujos de funcionamiento del sistema mediante grafos del mismo, los cuales muchas veces no se manejan con la discreción adecuada.

Seguidamente, la investigación relata la implementación sobre el software neo4j donde buscan realizar consultas a través de datos en grafos, lo cual facilita el proceso de identificar sensores de ataque. Además, la implementación mencionada cuenta con una fase de preprocesamiento, otra de relacionar patrones y una etapa de post-procesado; todos estos pasos permitirán obtener una lista de objetivos para atacar.

Una interrogante durante la investigación fue si esta implementación era capaz de atacar sistemas de control industrial reales, por lo cual realizaron distintas simulaciones bajo diversos entornos con el objetivo de encontrar patrones de ataque y ejecutarlos. Seguidamente, la investigación halló que se podían causar disturbios bajo ciertos patrones. Asimismo, se propusieron estrategias de control para mitigar dichos ataques, mostrando las interrupciones del sistema y su comportamiento ante distintas configuraciones.

En síntesis, esta investigación se basa en sistemas de control industrial y su comportamiento ante ataques de un solo disparo en condiciones donde el atacante tiene conocimiento limitado del sistema, para el cual en esta ocasión utilizaron grafos del sistema a atacar. Además, los experimentos realizados mediante el procesamiento de información para obtener una lista de objetivos a atacar demostraron las implicaciones de tener acceso a información del sistema y también a su incapacidad de limitar su recolección.