56. YOSHA

AI-BASED AUTOMATIC ATTACK PLANNER FOR SMART CITIES

ABSTRACT:

America's critical infrastructure is becoming “smarter”and increasingly dependent on highly specialized computers called industrial control systems(ICS).Networked ICS components now called the industrial Internet of things(IIoT) are at the heart of the “smartcity”,controlling critical infrastructure, such as CCTV security networks, electric grids, waternetworks, and transportation systems. Here, we describe an AI planning system design that can enumerate a setofmulti-step attack plans capable of penetrating and compromising systems across IP-networked devices. Importantly, our proposed method is “industry sectoragnostic”meaning thatitis designed to accommodate a wide range of organizations and computing systems. We call it “master” attack ontology because our goal is to design an attack ontology that accommodates any IP networked system in any industry sector.This technique uses various standardised cyber security frameworks like Lockheed Martin Cyberkill chain, OWASP surface areas, MITRE’S CAPECs and ATTACK MATRIX, Kali Linux tools for representing the anatomy of an attack. By using this, it generates attack trees automatically easing the operational burden. By combining attack frameworks from a number of respected authorities, we have developed a master attack method that can be used with classical planners to generate automated attack trees. With further testing and refinement, will be useful across multiple critical infrastructure sectors ,thereby easing the operational burden of cyberrisk enumeration.