DEPICT: DEep Packet Intelligence for industrial ConTrol systems

Prof. Dr. Sandro Etalle & Dr. Alvaro A. Cardenas

Zoals recente aanvallen laten zien is betere bescherming van kritieke infrastructuur en andere industriële controle systemen (ICS) essentieel en dit vereist oplossingen die bestaande systemen niet hinderen in hun werking. Dit laatste is zeker voor al bestaande 'legacy' systemen onontbeerlijk. Het DEPICT (DEep Packet Intelligence for industrial Control sysTems) project zal nieuwe tools, algoritmen en software ontwikkelen die een betere 'situational awareness', i.e. inzicht in de huidige status van het systeem bieden. Dit wordt bereikt door informatie over bedreigingen uit externe bronnen te combineren met analyse van het netwerk verkeer uit verschillende perspectieven. Eerst wordt er met automatische ondersteuning een overzicht gemaakt van de recourses van het system. Dit wordt gelinkt met de gevonden informatie over bedreigingen. Verder wordt semantische informatie geëxtraheerd uit netwerk berichten wordt vergeleken met modellen van het ICS en de processen die hierop draaien. De beheerder wordt zo een beeld geboden van gevaarlijke en onverwachte situaties met voldoende context informatie om hier adequaat op te kunnen reageren. DEPICT is een samenwerking tussen drie partijen met uitgebreide kennis op dit gebied en belangrijke faciliteiten zoals ICS netwerk datasets en test-beds; het Cyber-Physical Security Laboratory van de University of Texas at Dallas (UTD), de security groep van de at Technische Universiteit Eindhoven (TUE) en ICS beveiligings expert SecurityMatters BV.