TROPICS: Timely and RObust Patching of Industrial Control Systems

Prof. dr. ir. H.J. Bos & Prof. dr. C Kruegel

Juist de meeste vitale industrial control systemen (ICS) worden vaak het slechtst beschermd tegen cyber-aanvallen. Hiervoor zijn verschillende, elkaar versterkende redenen. Vaak is het bijvoorbeeld helemaal niet duidelijk is hoe ernstig het veiligheidsprobleem is. Daarnaast kan het installeren van een security-update (als die er al is) er ook toe kan leiden dat je super-essentiële systeem instabiel wordt, bijvoorbeeld omdat de patch bugs bevat. Tenslotte is updaten van een industrial control system een alles-of-niets operatie: je voert de patch helemaal uit (en dan is je systeem beschermd tegen de cyberaanval, maar mogelijk minder stabiel vanwege bugs in de update zelf), of helemaal niet (en dan is je systeem stabiel, maar ben je kwetsbaar voor de aanval). In de praktijk wegen de risico's van instabiliteit zwaarder dan de cyberveiligheidsrisico's en worden de belangrijkste industrial control systemen niet of pas maanden later ge-update. Met een toenemende afhankelijkheid van ICS/SCADA wordt deze situatie onhoudbaar en het doel van het TROPICS project is dan ook de ontwikkeling van een oplossing waarbij ICS beheerders:

1. kunnen inschatten hoe ernstig een gevonden kwetsbaarheid is zodat duidelijk is hoe urgent tegenmaatregelen zijn,
2. vervolgens kunnen bepalen hoe risicovol de urgente update is voor de stabiliteit van de software,
3. en tenslotte de mogelijkheid hebben om een urgente, maar risicovolle update te vervangen door een veilige tussenoplossing die de mogelijke aanvallen tegenhoudt, maar niet de stabiliteit in gevaar brengt.

Met andere woorden, TROPICS stelt beheerders in staat om te bepalen of er iets aan een veiligheidslek moet worden gedaan en zo ja, dan biedt het ze een alternatieve maar veilige versie van de software die het lek dicht, terwijl de officiële update (door-)ontwikkeld, getest en gedebugt wordt tot ze echt kan worden doorgevoerd.