Suggested Thesis Topic: “Defence in depth principles for industrial IoT”

Intent

Defence in depth is a security architecture principle that implies layering diffrerent controls to eliminate single point of failure and therefore increase overall reliability of security design. It rendered itself being even more important due to dramatic growth in complexity of attack vectors and resources available to threat actors.

IoT apperared to be a golden mine for cyberattackers because typical very primitive or absent security mechanisms on the one hand and greate scale on the other. At the same time industry is quite a conservative area being now actively transformed: legacy software, propriate protocols and deprecated standards meet introduction of emerging technologies like modern hardware, web-based protocols, sending data to the cloud and automated decision making (aka AI) algorithms. Such kind of cooperation provides attacker an enormous attack surface and access to unprotected critical systems.

Traditionaly, security in industry mostly relied upon physical controls: LANs and buses are isolated from the internet, fences and guards restrict access to the facility. Nowadays internet access is much more common and at the same time very valuable for business. So there can be an endpoint standing between industrial network and internet by accident or by design. And also the physical isolation is not enough without an appropriate enforced security policy.

For example, Stuxnet worm enters industrial network by means of infected USB drive, spreads across the network targeting Siemens Step7 control software and performes actions on target. During Stuxnet incident in Iran about 1/5 of nuclear centrifuges of the country.

Relevant experience

From my university studies a have learned a lot about networks and servers design and administration. And from my work experience I’ve got a good knowledge on building network applications using different protocols.

- IT Security course in XAMK
- IT Security course in HS Esslingen (course description: https://intranetportal.hs-esslingen.de/uploads/tx_femanagement_module_en/ITSecurity_20150305-2118.pdf)
- Study project “Running mirai botnet in lab environment” (on github: https://github.com/kribesk/security-project-mirai)

- Recently completed Cisco CyberOps Scholarship Program (electronic proof: https://www.youracclaim.com/badges/27e47c39-3096-4eb2-bb93-01dd25c503bc)
- Distributed Energy Production at Siemens (building hardware+software prototype for demonstrating cooperation scenarios)

For more information please see my CV (http://kribesk.github.io/cv.pdf).

Possible subtopics and activities

Some or all of these topics can be included in research:

1. Overview, classification and estimation of available solutions (study part)
2. Overview of related security incidents (additional study part)
3. Industrial network survivalence part 1: IDS for IoT protocols (PoC)
4. Industrial network survivalence part 2: Applying ML algos for detecting suspicious activity, moving on to IPS (PoC)
5. Gathering and listing best practicies, that can be used in security policies (study)