Threat Modelling for Digitalized Power Systems

Engla Ling (KTH) englal@kth.se

Abstract for the 20th Seminar within the Framework of a Swedish IT Security Network for PhD students (SWITS 2020)

In our modern world, the dependency of electric energy is large and therefore power systems must be kept secure. If power systems are maliciously shut down, the consequences can be devastating because hospitals, public transportation and other important parts of society are reliant on them. Because of these severe consequences, power systems can be a target for cyber attackers that wish to cause disruption or cyber warfare.

Due to the digitalization of power systems the ways of how to attack them have increased. There are more components added to the infrastructure and interfaces are created to enable, for example, remote management. The digitalization makes it more difficult to get an overview over the potential vulnerabilities of power systems. A solution to this problem is to use threat modelling. In threat modelling, a model of the system is created that illustrate the different potential vulnerable components of a system and the different ways in which to attack them. A threat model can also include the likelihood of different attacks to be successful and potential defenses of attacks.

My research topic is threat modelling for digitalized power systems and during my presentation I will describe the progress that I have done, as well as my current plans. So far, I have created a threat model of a substation based on the Substation Configuration description Language (SCL), which is part of the IEC 61850 standard. I have also conducted a systematic literature review to investigate what different information sources that have been used in previous research when creating threat models for the power systems domain.