Probabilistic Relational Models for Security Risk Analysis

Teodor Sommestad
Industrial information and control systems, KTH

SWITS 2009

The project deals with the threats that arise when technical support systems in electric power utilities, e.g. SCADA, EMS, DMS, are increasingly integrated into utility-wide enterprise architecture. One result of this integration trend is that the process close systems are subject to new threats from intrusion from various networks. How the power generation and distribution processes should be protected from these new cyber threats is today generally only partly known. This project aims at developing a method for evaluate the security of technical support systems from a holistic point of view.

To aid decision makers secure these technical support systems, a metamodel expressed as a probabilistic relational model (PRM) is being developed. This PRM is intended to help decision makers by coupling a probabilistic inference engine to architectural models of systems and their environment. From an architectural model, a probabilistic model over attacks, countermeasures, assets, threats and threat agents is generated. With this probabilistic model, which is an Influence Diagram, risk can be inferred.

Until now, this project has been devoted to developing a high-level metamodel that sort out the relationship between various concepts that ought to be included in a metamodel to assess risk from instantiated architectural models. This high-level metamodel is sort of a core package that can be specialized into concrete metamodel-PRMs that facilitate automated analysis of security risk. In near time, these concrete metamodel-PRMs will be developed to a desirable level of detail. This includes collecting data from domain experts to establish the probabilistic relationship between different attacks, countermeasures, assets, threats and threat agents.

The project is partly a sub-project of the EU-financed project VIKING where other sub projects will investigate consequences of attacks (e.g. if an attack will cause a blackout or not). A testbed will also be constructed in the VIKING project. In this testbed some of the predictions the metamodel-PRMs makes will be tested/validated.