Conditional probabilities over security

Teodor Sommestad, Mathias Ekstedt
Industrial information and control systems, KTH

SWITS 2010

The project deals with the threats that arise when technical support systems in electric power utilities, e.g. SCADA-systems, electric management systems, distribution management systems 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) has been developed over IT security. 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 attack steps and countermeasures can be generated.

This PRM has been developed based on literature and declare a substantial number of conditional probabilities. These conditional probabilities are on the form *"Can attack step X be accomplished by adversary Y given conditions B, C and D"*, where the conditions [B, C, D] can be attack steps already accomplished or information about the system architecture as such.

The aim of this project is to now collect data on these conditional probabilities. A number of surveys will be sent to researchers and practitioners in the security-field to collect beliefs on these conditional probabilities. The agreement between these respondents' answers will be used to assess their credibility. Also, empirical data will be collected during security exercises (Cyberstorm).