A cyber security modeling language

Hannes Holm,

Industrial Information and Control Systems, Royal Institute of Technology (KTH)

SWITS 2011

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 interviews with researchers and network penetration testers. Furthermore, it declares 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.

Done so far…

Validating the qualitative structure and populating the model with quantitative information takes a lot of effort. Some effort has been done so far, namely:

Expert elicitation using questionnaires and interviews. How do experts perceive the ease of performing various cyber attacks given different architectural scenarios and countermeasures? We have queried both suited researchers and professional penetration testers regarding arbitrary code execution attacks, performance of intrusion detection, denial of service attacks and how often unknown services can be found. Approximately 300 respondents fully answered the questions. The performance of respondents was assessed through Cooke's classical method.

How accurately does the Common Vulnerability Scoring System (CVSS) portray the security of a system? This model uses the CVSS for classifying vulnerabilities. But how valid is the CVSS. To assess this we carried out a study comprising statistical analysis of how 15 security estimation metrics comprising CVSS data relate to the time-to-compromise of 41 successful attacks. Results suggest that security modeling through CVSS data alone doesn't accurately portray the security of a system. However, it also implies that the amount of CVSS information which is used by the metric is of relevance to its accuracy: a metric employing more CVSS data also explains time-to-compromise better.

Testing network vulnerability scanners. One common solution by practitioners is to utilize network vulnerability scanners. We have tested seven of the more utilized ones.

Literature elicitation of quantitative data. Some aspects, e.g. the possibility of breaking different hashes under various conditions, have already been studied in great detail. Such data is used in the proposed PRM.