A Meta-Model for the Assessment of Systems

Submitted by Katie Dey on Thu, 04/23/2015 - 7:49pm. Contributor:
Jennifer Guild

Abstract:
In this poster, we will provide an overview of a methodology that maps mathematical models to assessment evidence, including formal proofs, in a human friendly manner for certification processes. This is relevant to HCSS as it provides an assessment methodology that integrates formal proofs without requiring the assessor to be an expert in formal modeling. The methodology (meta-model) provides a way for the assessor to represent, organize, and refine the various aspects of the assessment: the flaws, countermeasures, threats, vulnerabilities, risk, etc. This provides a level of assessment detail not provided in the current approaches, a more precise basis for the properties that must be maintained in the operational system and the ability to reuse the assessment of a system by another entity without reassessing the system.
National Security Systems are assessed to determine our confidence in their level of robustness, where robustness is the characterization of strength of a security function, mechanism, service, or solution, and the assurance that it is implemented and functioning correctly. For National Security Systems, current practice requires a single assessment that does not address formal proofs to be conducted against a system's implementation. The current approach combines two types of assessments. The first, the technical assessment, is conducted on an implementation in a laboratory environment and is conducted prior to placement of the system in the operational setting. The second, the operational site assessment, is conducted once the system is implemented at the operational site, and may include physical connection to live networks.
Currently, there is no assessment methodology in use by the US government that provides a model and methodology for assessing technical and operational evidence and risk individually. Such a methodology and models would provide a level of reciprocity not available reducing assessment costs and allow better reuse of systems.
We propose a methodology that revisits individual models to enable the assessor to represent their knowledge of the system's capabilities and correlate the models to the evidence, including formal proofs. The content of these models is refined from generalized to specific as the assessment progresses. The individual models will, in combination, comprise the meta-model, mapping the completed models to the evidence of the assessment.
We propose the use of mathematical models for a number of aspects that an assessor must consider when assessing a system, regardless of its complexity or connectivity. Mathematical models detail the flaws, countermeasures, vulnerabilities, threats, probabilities, attack vectors, impacts, and risk on the operational environment. Vulnerabilities are defined as those flaws with perceived, partial, or no countermeasures. The impact is in terms of the value of the asset with the vulnerabilities and the associated threats.

Other available formats:

A Meta-Model for the Assessment of Systems
Switch to normal viewerSwitch to experimental viewer