**Measuring software security**

**Who:** The Software Improvement Group (SIG) specializes in measuring software quality (security, maintainability, reliability, performance) and provides actionable recommendations to improve design, source code and the development process.

**What:** Through SBIR-funded research SIG further develops its method for finding security weaknesses using a mix of design/code review, build quality analysis, code scanning and penetration tests, in order to assess the level of security in 1-5 stars. The research involves 20 pilots with various organizations.

**Why:** 75% of worldwide security incidents are caused by mistakes in software. SIG’s approach provides a thorough, structured, consistent and repeatable way to have continuous insight in software security, from the very start of development. It includes the analysis of build quality in order to prevent making software mistakes.

**Software Security Model**

The SIG software security model is based on the ISO/IEC 25010 standard 'System and Software Product Quality Model'.

**Security Risk Assessment Process**

SIG looks at the design, code, software development process and optionally at the system in operation (penetration test). Findings on design, code, process and operation are summarized in a star rating and lead to recommendations.

A Security Risk Assessment follows a well defined process to establish to what extent a software system is protected against security issues and defines what steps are necessary to get security at the right level.

**Risk Based Roadmap**

**Publication and Partners**

H. Xu, J. Heijmans and J. Visser.  
*A Practical Model For Rating Software Security*.  

Our partner is Radboud University Nijmegen and the project is funded by Netherlands Enterprise Agency.