Cyber Security:

By accident or by design?

Software Improvement Group

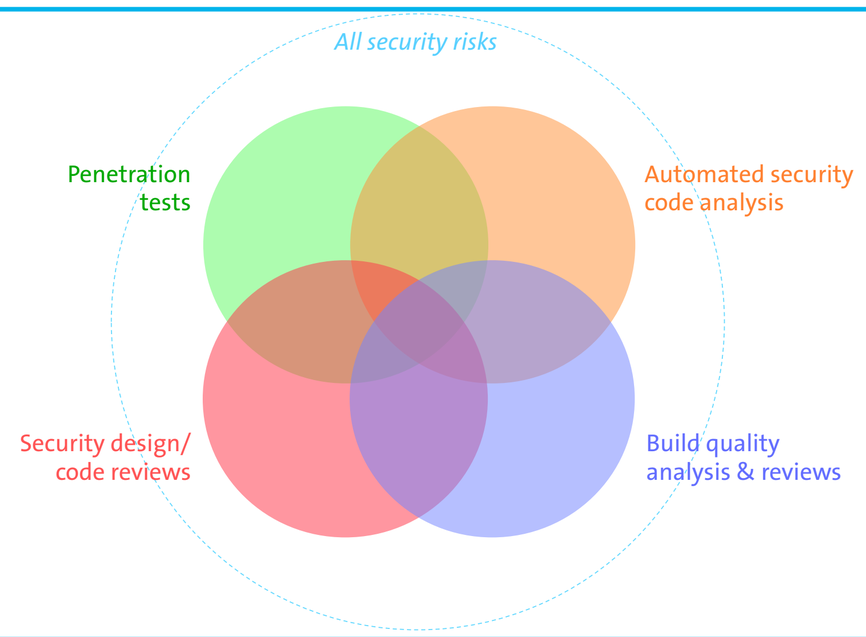
Radboud Universiteit Nijmegen

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

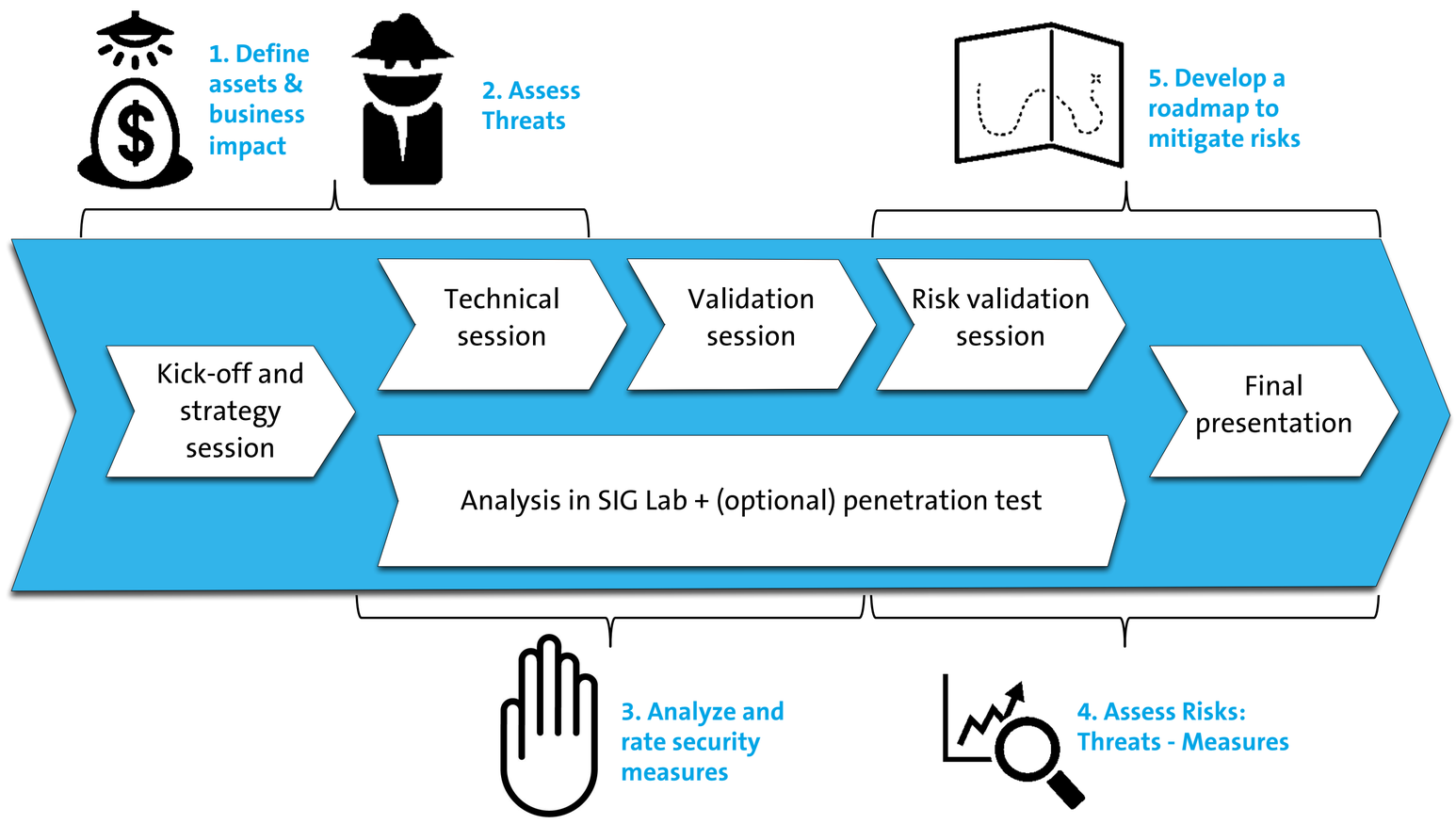
	Secure data transport	Identification strength	Access management strength	Session maangement strength	Authorized access	Input and output verification	Secure data storage	Evidence strength	Secure user management	Overall rating	
Rating	★★★★☆	★★★★☆	★★☆☆☆	★★★★☆	★★★★☆	★★☆☆☆	★★★★☆	★★★★☆	★★☆☆☆		
Confidentiality & Integrity	X				X	X	X				★★★☆☆
Non-repudiation & Accountability		X						X			★★★☆☆
Authenticity			X	X					X		★★☆☆☆

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

Security Risk Assessment Process

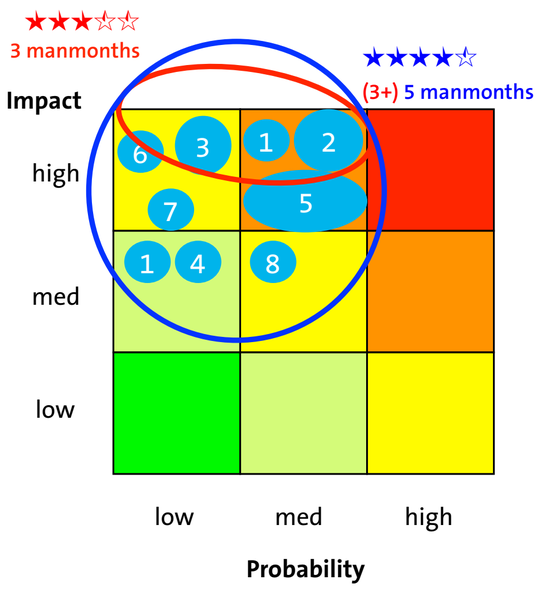
SIG looks at the *design*, *code*, *software development process* and optionally at the *system in operation* (penetration test). Findings on design, code, process and operation are summarized in a star rating and lead to recommendations.

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

Risks
1. Missing certificate check by mobile app is abused
2. Passwords in database get descrypted by code in database and leak
3. Access management is hacked since location and version are exposed
4. Passwords leak from registration log
5. Developers create a data leak because of high complexity in website architecture
6. Backdoor in the application interface is abused
7. Injection attack abuses browser-only input for validation of date of birth
8. Attack is missed because logging/monitoring of key process is not in place



Diameter represents indication of effort

Publication and Partners

H. Xu, J. Heijmans and J. Visser.
A Practical Model For Rating Software Security.
The 7th International Conference on Software Security and Reliability.
Washington, D.C., USA, June 2013.

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

Netherlands Enterprise Agency

Radboud Universiteit Nijmegen