

The SHIELDS project benefits

Assurance – effectiveness – quality

- *Higher assurance for users*
 - Tool capabilities become known
 - Tools can remain up-to-date
 - Tools can be updated faster
- *Less duplication of effort*
 - Models can be used by many tools
 - Development resources can be used in more productive ways
 - Better management of security knowledge
- *More secure software*
 - Developers get access to tailored security information
 - Security methods and tools can cover more security issues
 - Improved trust in software and services

The SHIELDS project benefits

From case studies evaluation

SHIELDS has been acknowledged as:

- Being able to improve customer trust and the quality of software with a marked reduction in security problems in the software (6 evaluators out of 8 found that using these methods will improve the software development lifecycle)
- Appropriate for both software developers and security experts thanks to its simple but targeted methods (5 evaluators out of 8 found that user friendliness of Shields methods is quite high)
- Being able to reduce time and manpower for finding vulnerabilities in the project through focused code analysis systems (7 evaluators out of 8 perceived that SHIELDS ability to detect vulnerabilities is quite high)

The SHIELDS consortium



Linköpings universitet (Sweden)



SINTEF (Norway)



European Software Institute (Spain)



Fraunhofer IESE (Germany)



Institut TELECOM/TELECOM SudParis (France)



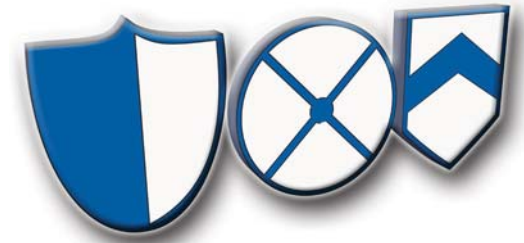
Montimage SARL (France)



SEARCH-LAB Ltd (Hungary)



TXT e-solutions SPA (Italy)



SHIELDS

Detecting known vulnerabilities from within design and development tools

Official site

<http://www.shields-project.eu>

Contact SHIELDS

✉ Professor Nahid Shahmehri
@ nahsh@ida.liu.se
☎ +46 13 282066

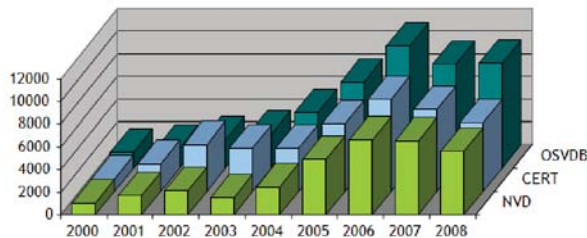


The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 215995

Why SHIELDS?

Software vulnerabilities are a critical problem

- *With software controlling*, protecting and affecting more and more critical information and systems, the consequences of failure have increased significantly.
- *As software becomes more complex*, it tends to contain more flaws, and as it becomes more networked and ubiquitous, its exposure to potential adversaries increases.
- *Software-intensive systems* are increasingly becoming viable financial and political targets for well-funded and well-motivated attackers, thus increasing the overall threat to these systems.



The continuous growth of vulnerabilities in software till 2006 and a very large number of discovered vulnerabilities in 2007 and 2008, based on three independent sources

Network security solutions are failing

The traditional way of protecting software by relying on network security solutions, that is merely trusting firewalls and anti-virus applications, will not hold in the long run. Security must be an inherent property of the software itself.

2009-12-10

Lack of security information for developers

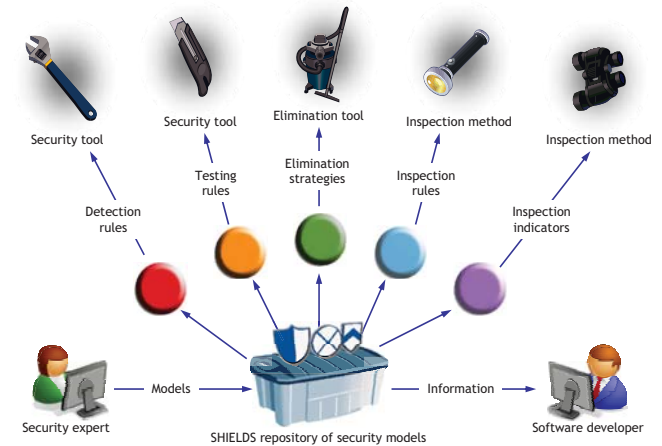
Typical vulnerability databases contain very general overviews of problems, information for risk assessment, solutions and tools explicitly conceived for users and system administrators; developers can only find limited support for discovering or eliminating vulnerabilities.

The objectives of SHIELDS

- *Bridge the gap between security experts and software developers* and thereby reduce the occurrence of security vulnerabilities.
- *Make it easier and faster for security experts to make information about identified security vulnerabilities known.*
- *Help individual developers to avoid or detect and remove security vulnerabilities* from directly within the development tools they use.
- *Increase awareness amongst developers* about known security vulnerabilities.
- *Help software development organisations to verify that they have successfully reduced security vulnerabilities* in their products.

The SHIELDS concept: Sharing knowledge about security

The fundamental concept behind SHIELDS is that there should be a *shared repository of security information* that can be used by software security tools and methods. Tools will access the repository to get information about security vulnerabilities and security activities and translate them into their internal format.



The structure of SHIELDS

The SHIELDS certification programmes

The project will develop two certification programmes called *SHIELDS Compliant*, for tools that use the SHIELDS repository services in a compatible and appropriate manner, and *SHIELDS Verified*, for certifying that software has been checked for vulnerabilities during development.