

# Reducing Vulnerabilities in Software – A European Approach

Per Håkon Meland, Jostein Jensen and Lillian Røstad

{Per.H.Meland, Jostein.Jensen, Lillian.Rostad}@sintef.no

SINTEF ICT - Software Engineering, Safety and Security

N-7465 Trondheim, Norway

The number of discovered security vulnerabilities in software is constantly increasing; this can easily be confirmed by looking at the statistics from the *National Vulnerability Database* (NVD), the *US-CERT database* (CERT) or the *Open Source Vulnerability Database* (OSVDB). By looking at this data, it is also clear that the same types of vulnerabilities occur over and over again. It appears that developers continue to do the same mistakes. One may argue, that the core reasons for this is that information on vulnerabilities is not available to developers in a form conveniently accessible to them while they work on software design and development. Today's development methods tend to overlook security issues until near the end of development<sup>1</sup> and security tools are not well integrated into the development environment. Although there is an increasing desire amongst software developers, their customers, and society at large to avoid security vulnerabilities, the tools to help them do so are not available.

It is essential that security practices are operational and accepted by developers. It is pointed out by Apvrille and Pourzandi<sup>2</sup> that forcing too much theoretical information about ways to incorporate security is not very efficient, and Davis<sup>3</sup> gives examples of non-usable 700-page documents with security guidelines that exist within some organisations.

In 2006, a nationally funded project on software security called SODA (which stands for a *Security-Oriented Software Development Framework*) was started in Norway. The main goal for this project has been to put together a set of practical methods for creating secure software with a special focus on the early phases of the development lifecycle. The target group is the ordinary "developer-on-the-street", who is not primarily interested in (or knowledgeable about) security, but must focus on implementing as much functionality as possible before the deadline, and then patch whatever bugs there may be when it's time for the next release or hotfix<sup>4</sup>.

The work with SODA enabled cooperation with other European research groups within the same domain, which again lead to the formation of a consortium consisting of Universities, research institutes and security companies wanting to build software that is more resilient to attacks and that does not require constant maintenance and vigilance. The European

---

<sup>1</sup> M. Howard, Building More Secure Software with Improved Development Processes, in *IEEE Security & Privacy*, vol. 2, pp. 63-65, 2004.

<sup>2</sup> A. Apvrille and M. Pourzandi, Secure Software Development by Example, in *IEEE Security & Privacy*, vol. 3, pp. 10-17, 2005.

<sup>3</sup> N. Davis, Developing Secure Software, *The DoD Software Tech News*, vol. 8, pp. 3-7, 2005.

<sup>4</sup> Exemplified in J. D. Meier, "Web application security engineering," *Security & Privacy Magazine, IEEE*, vol. 4, pp. 16-24, 2006.

Commission has chosen to support a new collaborative project from this consortium within its seventh framework programme under the theme *ICT-2007.1.4: Secure dependable and trusted infrastructures*<sup>5</sup>. The name of this project is SHIELDS, and its main objective is to bridge the gap between security experts and software developers and thereby reduce the occurrence of security vulnerabilities. The project will:

- Make it easier and faster for security experts to make information about identified security vulnerabilities known to the developer community, in a form directly accessible via widely used design and development tools.
- Help individual developers to detect and remove security vulnerabilities from directly within the development tools they normally use.
- Increase awareness amongst developers about known security vulnerabilities.
- Help software development organisations to verify (internally and to their customers) that they have successfully reduced security vulnerabilities in their products.

The approach to achieve these overall objectives centres on developing and integrating leading edge research on formal security models and techniques for detection of security vulnerabilities made accessible by the project's *Security Vulnerabilities Repository Service* (SVRS). This internet-accessible service will provide a standardised way for security experts to represent and publish formalised vulnerability models that are easily accessible by development and security tools, providing the latest security information right at the fingertips of the developers. The project will:

- Devise models to be used in the SVRS for representation of classes of security vulnerabilities.
- Populate the SVRS with an initial set of vulnerability descriptions, sufficient to demonstrate the approach on a realistic set of case studies.

The SVRS will provide an open interface to allow different development tools to be interfaced to it, enabling tools to stay up-to-date with the latest security knowledge. A SHIELDS Compliant programme will be set up in the project to assist tool developers who want to interface their tools to the SVRS.

Globally the impact is long term since it would be difficult to suddenly rewrite all software being used; however, on some applications and systems being developed in Europe today the impact would be immediate. Likewise, the improved image of the companies adopting SHIELDS compliance rules, recommendations and tools will have positive economic effects, and increase end users' trust in their products, thereby improving their competitiveness.

The SODA project will run out 2007, and then overlap with SHIELDS which formally starts early 2008.

---

<sup>5</sup> See the CORDIS homepage, [http://cordis.europa.eu/fp7/ict/programme/challenge1\\_en.html](http://cordis.europa.eu/fp7/ict/programme/challenge1_en.html)