FRAMEWORK SECURE SOFTWARE

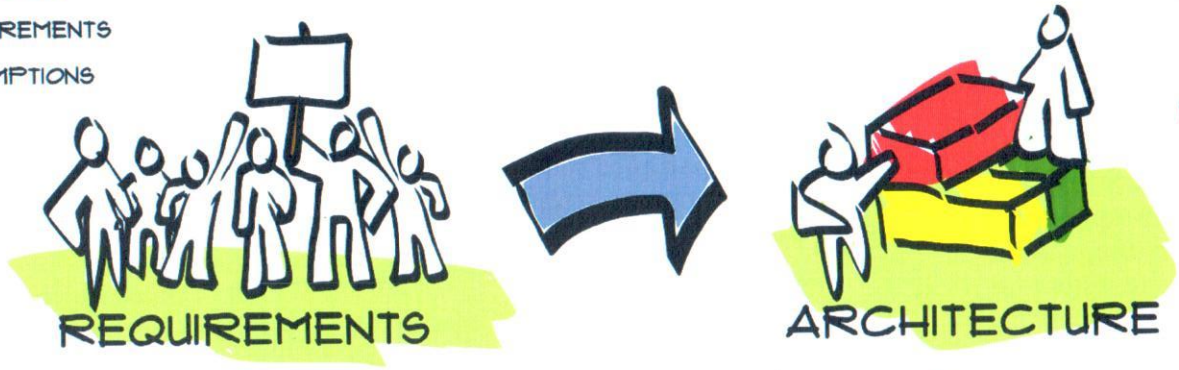
Secure Software Foundation

CONTEXT

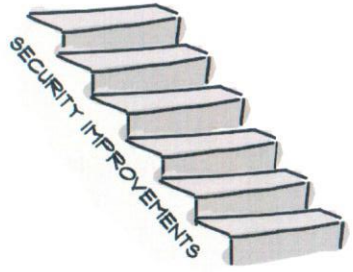
- FUNCTIONS AND ENVIRONMENT
- APPLICATION ASSETS
- SECURITY REQUIREMENTS
- SECURITY ASSUMPTIONS

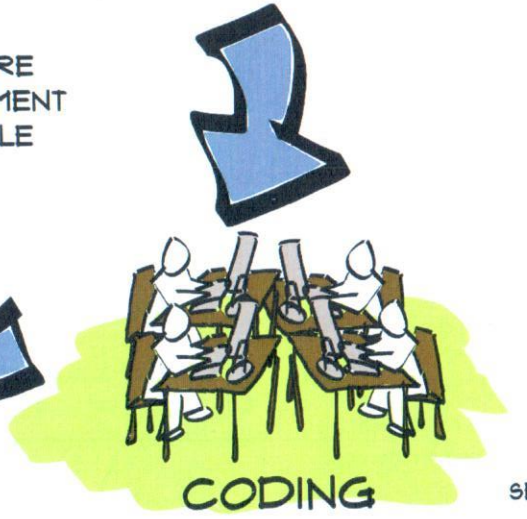
THREATS

- FUNCTIONAL THREATS
- ARCHITECTURAL THREATS
  - ARCHITECTURE INVENTORY
  - THREAT LIBRARY
- MITIGATIONS



SOFTWARE DEVELOPMENT LIFECYCLE





VERIFICATION

- VERIFICATION METHOD
  - CODE REVIEW
  - PENETRATION TEST
  - VULNERABILITY SCAN
  - FUZZING
  - ABUSE TESTS
- VERIFICATION PROCESS

IMPLEMENTATION

- SECURE CODING PRINCIPLES
- SECURE CODING STANDARD
- CODE AUDIT

Framework Secure Software

The Framework Secure Software defines a standard to help to improve secure software development:

- For *development teams*, the framework helps to implement secure software development practices.
- For *auditors*, the framework gives criteria to evaluate the security of software.
- For *purchasers*, the secure software certificate makes the software's security properties visible.

Goals of the Framework

100% security is impossible, but the framework can evaluate if security is sufficiently implemented.

The framework:

- covers all phases of the SDLC
- fits all software development methodologies
- is applicable to a wide range of software applications
- bridges the gap between non-technical requirements and technical implementation
- makes it possible to issue the secure software certificate.

How does it Work?

The framework is divided into four phases:

Context
In the context phase, the security requirements and security assumptions are determined. The context defines what `secure' means for the software system. Using a systematic method, it is possible to check for missing security requirements.

Threats
Based on the above context, potential security problems (threats) are identified. Threats originate from the application's behavior, its architecture and its implementation. For every threat, a countermeasure (mitigation) is created. Because threats are gathered systematically using a threat library, missing threats can be detected.

Implementation
The use of a secure coding standard helps to prevent security issues at the implementation level. A systematic code audit can check if the software is securely implemented.

Verification
For every mitigation, a verification is described. During development, these verifications provide feedback to the development team. The evaluation of these verifications gives an extra assurance that the mitigations are securely implemented.

Secure Software Foundation

The Secure Software Foundation is the trustee of the Framework Secure Software.
The objective of the Secure Software Foundation is to publish, further develop, and monitor the quality of the Framework Secure Software for assessing the security of software and certification criteria with which the parties can demonstrate that their software complies with the framework.

In addition the Secure Software Foundation will support other initiatives and ideas that help to increase software security.

The framework is available under an open license; this is indicative of the open nature of this initiative. The Secure Software Foundation intends to issue Secure Software Certificates for software following a positive audit advice from an auditor accredited by the foundation. For more information about the Secure Software Foundation and to download the framework: www.securesoftwarefoundation.org

Initiators
The Framework Secure Software was created by iComply and the Security Academy. The Security Academy is the largest provider and developer of information security education programs in The Netherlands. iComply specializes in developing and executing security improvement projects for software development organizations. More information: www.securityacademy.nl, www.icomply.nl.
The program has been substantially supported by the Dutch Ministry of Economic affairs and ECP. ECP is a neutral platform formed by private companies, governmental and social organizations. Its goal is to strengthen the use of ICT in the Dutch society. More information: www.ecp.nl.