Secure Software Development

Nowadays more systems and products are connected and therefore exposed to security risks, there is an increased need for understanding security requirements and for product developers to design secure systems and implement countermeasures that meets these challenges.

Security requirements that are considered late in the development process usually result in costly and complicated “emergency” solutions to be able to meet the requirements, but it may still may not result in a good or maintainable security design.

Instead it is important to identify and analyze the security requirements early in the process, and ensure that the system architecture, design and implementation supports these requirements and that this design is robust and maintainable over time. This can only be done in an environment were the developers understand IT security were the development environment support such development.

atsec offers training and consultant services in secure software development. To the advantages for our customers we are not software developers, but we have have extensive developer experience of security products as well as much experience in the evaluation of security products.

Secure Software Development

- Adherence to security principles in all development phases
- Security as basic principle for software architecture and design
- Secure coding

It essentially covers the following five areas:

Defining security requirements

Before a product is to be developed, not only the security functionality, but also the security requirements must be known. This includes not only the security functionality, but also security properties and ability to withstand attacks customers may expect in their operational environment. This means we should have a comprehensive set of and well-defined security requirements, covering all relevant security aspects. The security requirements should then be trackable through the entire process, from design and architecture to implementation and testing of the product or the system. atsec can assist you in ensuring that the requirements are complete, unambiguous, testable and consistent.

Secure development environment

The next step is to consider the security of the development environment, which includes physical protection of the local workstation as well as other components such as networks and servers. It is also important to look at the tools and techniques used in the development environment, including aspects such as secure repositories, change control, configuration handling, version handling, life cycle processes and code reviews. atsec offers assistance in developing processes for secure software development, tailored for the development model in use from classical waterfall models to high iteration development models. Development environments that are hosted in-hose or cloud-based, etc. atsec can help you in establishing a secure lifecycle process, configuration management, build processes and processes for flaw remediation.

Secure architecture and design

The products’s security requirements architecture and design should not only implement the security requirements, but also reduce the risk for example by reducing the attack surfaces and allow easy product maintenance and patching.
Such a design will not only be more robust to attacks, but also be easier to maintain and therefore more stable over time. At the end the maintenance cost of such a well-designed product is much lower over time. atsec offers not only training in secure architecture and design, but also assistance in analyzing the design and help in finding the right

design decisions. atsec can help you establishing an architecture that by using defense in depth, layering and encapsulation that increase the security robustness of the product. atsec can also guide you on design and implementation issues issues like least privilege, input validation, use of central security services, and error and exception handling.

Implementation

When implementing the security architecture and design it is important not only to avoid programming errors, but also to be able to maintain the code over time. More than half of the development cost goes into the software maintenance. atsec has much experience in security implementation and in the evaluations of security products and can especially help in areas, such as using crypto libraries, key generation and random number generators.

Security Testing

There are two types of security testing.

- Functional testing that is done to demonstrate that the security functionality behaves as specified.
- Penetration testing that is used to detect vulnerabilities or flaws and may range from simple port scans to developing specific security exploits. Penetration testing is usually considered part of penetration testing.

Other types of tests are usually not security testing, but could be functional test, performance test, unit test, integration test or simply code coverage test, to ensure that all the code has been tested.

Many of these tests may be done as automatic tests, which is a way convenient to detect bugs or unwanted behaviour during development when the product changes.

While the security functional testing can be done as part of other tests it is important that the tests are actually testing the security behavior, i.e. negative tests and that the testing is done under conditions that are consistent from a security point of view.

From our Common Criteria evaluations atsec has a lot of experience from security functional testing as well as independent evaluator testing. We can share this experience with our customer.

Vulnerability Assessment

Usually vulnerability assessments are done by 3rd parties, such as a penetration testing or security evaluation. However, it is important that the developer also perform both some active search for vulnerabilities, does some penetration testing and has vulnerability management processes to deal with security flaws that are detected after the product has been released. Such flaw remediation processes should include (for customers) secure release processes of vulnerabilities and fixes.

atsec has extensive experience in different ways for the vulnerability search, vulnerability assessment, and the flaw remediation processes and can guide developers finding the best approaches.

Training

To provide your development team the best possible start to develop secure products, atsec offers tailored educations in secure software development in general as well as in each specific area.

Other services offered by atsec

Secure software development is one of many security services we offer. For more information on what other services atsec offers, please visit: www.atsec.-com

For more information on how we can help you or other questions about secure software development, please contact us on: info-se@atsec.com

atsec information security

atsec information security was founded in 2000 and is an independent, standards based security consultant and security company based in Danderyd, Stockholm. We also operate internationally, in Germany, the US, China and Italy and we have performed many successful projects with different companies and authorities. Our more than 80 employees have extensive international experience and technical expertise within the areas of information security and IT security.

www.atsec.com
info-se@atsec.com