Towards secure product development – The Secure Development Lifecycle

Marjo Hanhikoski
Centria UAS
ISSUES-project funded by Interreg Aurora

In an ever-changing world, where people are becoming more and more aware of cyber security, information security and data privacy and where the threat landscape is changing and developing, organizations and societies demand and need increasingly high-quality and secure services and products. Information security has become one of the product's quality factors and competitive advantages. (Finnish Transport and Communications Agency Traficom 2018, 7, 10.) The Secure Development Lifecycle (SDL) framework is a way to meet these requirements.

The SDL is a perspective used in product development, where information security is considered at every stage of the product's lifecycle, from definition to decommissioning (Finnish Transport and Communications Agency Traficom 2018). Thus, the framework expands the product development process with security aspects. Originally, the SDL focused on software development and Microsoft is considered to be its pioneer, but the framework can be smoothly applied in all kinds of product development processes (Dorsey 2020; The Security Development Lifecycle (SDL) Explained 2016). The SDL model depends on the organization, but as a result of the research it was found that the lifecycle can be generally divided into the following phases: definition, planning, implementation, testing, deployment, maintenance and decommissioning. In addition, the lifecycle model includes several activities that support it, which are not actually included in the SDL, such as the organization's information security policy (Gupta et al. 2007; Finnish Transport and Communications Agency Traficom 2018).

In the definition phase, in addition to the product's normal requirement definition, the product's information security requirements are defined. These requirements contain the security measures needed by the product, which can be used to protect the product's data and functions from harmful actors or other adversities. In order to make the right solutions, product supplier must have a clear understanding of the product's intended use and environment, as well as the coming structure. When defining security requirements, it is necessary to consider known threats, the regulations and requirements of product's industry, and to make use of a ready existing experience from cases that may have occurred in the past. In addition, it is important to maintain and update requirements throughout the product's lifecycle. (Finnish Transport and Communications Agency Traficom 2018, 7, 14–15; Microsoft 2023.)

In the design phase, the structure of the product is finally planned. When designing the structure, product supplier should follow the principles of secure design, which include e.g. minimization of the attack surface, defence in depth, simplicity of the structure, secure by default and fail securely (Finnish Traffic and Communications Agency 2018 Traficom, 19–26; OWASP Foundation 2006). According to the OWASP top 10 list, insecure design was the fourth most common cause of application security risks in 2021 (OWASP Foundation 2021). During the planning phase, threat modeling of the product should also be carried out, which can be used to identify current and future threats to the product and to assess the product's security. Threat modeling is recommended to be implemented as early as possible in the product's lifecycle, but the threat modeling must be developed, maintained, and updated throughout the product's lifecycle. (Drake 2024; Finnish Transport and Communications Agency Traficom 2018, 16; Microsoft 2023.)

In the implementation phase, the product is implemented in accordance with the defined requirements and design (Microsoft 2023). In the implementation, the threat modeling done for the product is taken into account and the threats detected in it are removed or mitigated (Lipner 2004). In secure implementation, general and industry specific best practices, standards, and recommendations for implementing a secure product are considered, such as secure coding best practices (Gupta et al. 2007, 24; Lipner 2004). Secure implementation must also consider the functions that support it, such as the security of developing tools and the development environment and the competence of personnel (Gupta et al. 2007, 24; Finnish Transport and Communications Agency Traficom 2018, 12, 27). The goal of the implementation phase is to ensure that the product corresponds to the plans and that the functions and features work as planned (Dorsey 2020). To ensure this product supplier should carry out e.g., code reviews and static analyzes during the implementation phase (Gupta et al. 2007, 24; Finnish Transport and Communications Agency Traficom 2018, 27–28).

The testing phase overlaps with the implementation phase because preliminary testing of the product is already carried out during the implementation phase. In the testing phase, it is tested that the planned security functions work as expected, the product meets its requirements and whether there are any security aspects left in the product that have not been considered. At the same time, it is verified whether any new vulnerabilities have appeared in the implementation that should be addressed. (Gupta et al. 2007, 24.) All necessary testing must be carried out for the product, such as penetration testing and vulnerability testing etc. (Finnish Transport and Communications Agency Traficom 2018, 30–34). The tests product supplier carry out for the product must be planned, implemented, analyzed, and documented (Scarfone et al. 2008, 13). Finally, the product is subjected to final acceptance testing before its official deployment. Acceptance testing should be carried out by a testing team independent of the development team or by a third party. (Finnish Transport and Communications Agency Traficom 2018, 30; Microsoft 2023.) The goal of the testing phase is to verify that the product is ready for to be delivered for customers (Dorsey 2020; Lipner 2004).

During the deployment phase, it must be ensured that the product is put into use securely and that it is used appropriately. Consequently, it must be ensured that the user of the product has been comprehensively instructed on the secure deployment, operation, maintenance and decommissioning of the product. It is the duty of the product supplier to provide adequate guidance on the product, to inform and take care of addressing vulnerabilities that have occurred during deployment and the necessary countermeasures. (Finnish Transport and Communications Agency Traficom 2018, 35–37.) Implementing and maintaining product's security is not a single process, but a continuous process that lasts throughout the product's lifecycle (Otieno et al. 2023, 62).

Developing a completely secure product is impossible (Dorsey 2020; Finnish Transport and Communications Agency Traficom 2018, 36). Consequently, sufficient resources, both financial and time and personnel resources, must be invested in the SDL process (Kanniah and Mahrin 2016, 3025–3027). The SDL process must also be continuously developed and improved to respond to future security threats as well. The application of the framework improves the security and quality of the product, but also the quality of the work and creates conditions for the continuity of business operations (Finnish Transport and Communications Agency Traficom 2018, 7, 10). According to Gupta et al.'s study, security measures implemented afterwards are not long-lasting, comprehensive, and cost-effective solutions (Gupta et al. 2007, 22). Therefore, the product's security should be seen as its primary feature and not just a secondary one.

REFERENCES

Dorsey, V. 2020. *The 6 stages of a holistic hardware security development lifecycle.* BNP Media. Available at: https://www.securitymagazine.com/articles/93938-the-6-stages-of-a-holistic-hardware-security-development-lifecycle. Retrieved February 27, 2024.

Drake, V. 2024. *Threat Modeling*. OWASP Foundation. Available at: https://owasp.org/www-community/Threat_Modeling#. Retrieved January 18, 2024.

Finnish Transport and Communications Agency Traficom. 2018. *Turvallinen tuotekehitys: Kohti hyväksyntää.* Helsinki. Available at: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf. Retrieved January 17, 2024.

Gupta, A. K., Chandrashekhar, U., Sabnis, S. V. & Bastry, F. A. 2007. Building Secure Products and Solutions. *Bell Labs Technical Journal*, 12(3), 21–38. Available at: https://doi.org/10.1002/bltj.20247. Retrieved February 27, 2024.

Kanniah, S. L. & Mahrin, M. N. 2016. A Review on Factors Influencing Implementation of Secure Software Development Practices. *International Journal of Computer and Systems Engineering*, 10(8), 3022–3029. Available at: https://doi.org/10.5281/zenodo.1127256. Retrieved February 29, 2024.

Lipner, S. 2004. *The trustworthy computing security development lifecycle*. Institute of Electrical and Electronics Engineers. Available at: https://doi.org/10.1109/CSAC.2004.41. Retrieved February 27, 2024.

Microsoft. 2023. *Microsoft Security Development Lifecycle (SDL).* Available at: https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle?source=recommendations#design. Retrieved January 18, 2024.

Otieno, M., Odera, D., Ounza, J. E. 2023. Theory and practice in secure software development lifecy-cle: A comprehensive survey. *World Journal of Advanced Research and Reviews*, 18(3), 53–78. Available at: https://doi.org/10.30574/wjarr.2023.18.3.0944. Retrieved March 1, 2024.

OWASP Foundation. 2006. *Development Guide: Security by Design Principles.* Updated 3.8.2016. Available at: https://wiki.owasp.org/index.php/Security_by_Design_Principles. Retrieved January 18, 2024.

OWASP Foundation. 2021. *OWASP Top 10:2021.* Available at: https://owasp.org/Top10/. Retrieved January 29, 2024.

Scarfone, K., Souppaya, M., Cody A. & Orebaugh, A. 2008. *Technical Guide to Information Security Testing and Assessment*. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-115. Retrieved March 1, 2024.

The Security Development Lifecycle (SDL) Explained. 2016. Exida. Available at: https://www.youtube.com/watch?v=mRe3vLBpCJI. Retrieved January 17, 2024.