NLP-based Testing and Monitoring for Security Checking[⋆]

Andrey Sadovykh[1,6], Zujany Salazar[2], Wissam Mallouli[2], Ana R. Cavalli[2], Dragos Truscan[4], Eduard Paul Enoiu[3], Rosa Iglesias[5], and Olga Hendel[3]

[1]Softeam, France, andrey.sadovykh@softeam.fr
[2]Montimage EURL, France,
zujany.salazar,wissam.mallouli,ana.cavalli@montimage.com
[3]Mälardalen University, Sweden, eduard.paul.enoiu, olga.hendel@mdh.se
[4]Åbo Akademi University, Finland, dragos.truscan@abo.fi
[5]Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA), Spain, riglesias@ikerlan.es
[6]Innopolis University, Russia, a.sadovykh@innopolis.ru

Abstract. VeriDevOps aims at bringing together fast and cost-effective security verification through formal modelling and verification, as well as test generation, selection, execution and analysis capabilities to enable companies to deliver quality systems with confidence in a fast-paced DevOps environment. Security requirements are intended to be processed using NLP advanced algorithms in order to deliver formal specifications of security properties to be checked during development and operation of a system under test.

Keywords: Model-Driven Engineering · Cybersecurity · Test and validation · Runtime Analysis · Natural Language Processing.

1 The VeriDevOps Concept

Fig.1. depicts the overall concept of the VeriDevOps project. Given an existing system under continuous integration/delivery, security requirements[2] come in different forms. These can be standard requirements, such as those from ISA/IEC 62443 standard for control systems or description of vulnerabilities from common repositories, as well as reports from security experts. In all cases, these requirements should be immediately taken into account according to their severity and at all relevant levels. In this way, the protection mechanisms such as firewalls and intelligent traffic monitors may be the first to be re-configured in order to avoid an immediate danger and secure the system perimeter. Next, the design of the system should be examined in order to locate the root-cause of the potential security breach and identify the remediation methods on code level as a patch or upgrade, at the design level, as a major redesign.

The use of security requirements for protection and prevention suffers from limited automation support which is mostly limited to vulnerability scanners.

[⋆] H2020 VeriDevOps project: https://cordis.europa.eu/project/id/957212

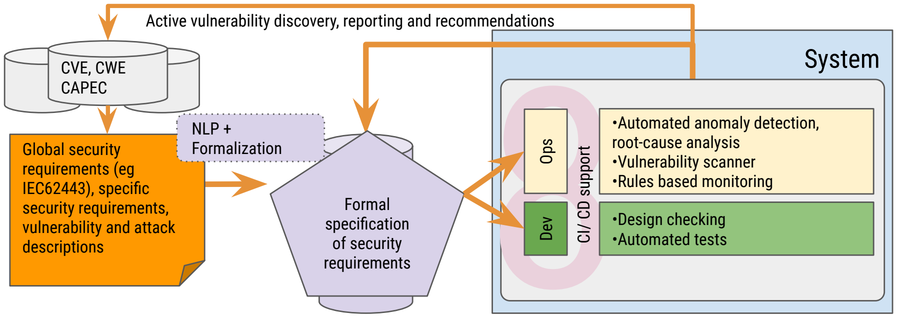
Active vulnerability discovery, reporting and recommendations
CVE, CWE
CAPEC
Global security requirements (eg IEC62443), specific security requirements, vulnerability and attack descriptions
NLP +
Formalization
Formal specification of security requirements
System
Ops
Dev
CI/ CD support
•Automated anomaly detection, root-cause analysis
•Vulnerability scanner
•Rules based monitoring
•Design checking
•Automated tests

Fig. 1. The VeriDevOps main concept

There is still a tremendous amount of manual work to configure protection means at operations level and locate and prevent the vulnerabilities at design level, beyond the use of tools for scanning the libraries and tool chains used during the implementation. Despite the large volume of academic research on software testing and verification, there are relatively few commercial and industry-strength tools for security testing that require formal specifications of the system. In addition, the formalization of requirements is still a very human-intensive activity; much information is informally exchanged among the engineers and due to this, most verification activities cannot be automated and need human intervention. We argue that this formalization of security requirements and the creation of environment and system models could increase the product quality, and make the development and operation more efficient and less costly.

Thus, the key challenge of the project is to automatically express and manage security requirements in an effective and unambiguous way (by formalizing them using NLP[1]), such that both engineers and stakeholders have a common understanding of their content. Once these security requirements are unambiguously specified and decomposed, one needs to verify the compliance of the realizations to required security behavior by formal verification and testing for both protection and prevention means. In order to save time and lower the effort for adjusting the prevention and protection mechanisms, VeriDevOps automates the specification and analysis of requirements with security relevance, testing of system realizations and the integration of these techniques and tools with current VeriDevops practices in industry.

References

1. V. Garousi, S. Bauer, and M. Felderer. NLP-assisted software testing: A systematic mapping of the literature. *Inf. Softw. Technol.*, 126:106321, 2020.
2. R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas. Systematic mapping study on security approaches in secure software engineering. *IEEE Access*, 9:19139–19160, 2021.