ITEA 4

Project Results

SCRATCh

Security for SMEs in the IoT domain

The ITEA project SCRATCh (SeCuRe and Agile Connected things) aims to improve security in DevOps. Using their knowledge base, methodology and integrated tools, SMEs will have the opportunity to offer Internet of Things (IoT) devices in a safe, affordable manner.

Project origins

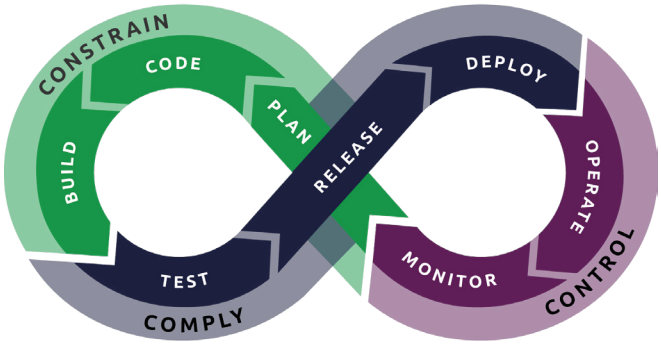
While 44% of SMEs plan to invest in resources related to IoT, only 20% plan to invest in cybersecurity. This awareness issue is compounded by a heterogenous landscape in which tools typically solve individual problems in a development cycle. A general lack of support for security in DevOps, including an integrated approach and practical guidelines, makes security a daunting prospect for SMEs with little in-house knowledge or budget.

SCRATCh has improved the DevOps process for SMEs by developing a toolkit, methodology and knowledge base. A set of interoperable tools provides an integrated approach to IoT, security and DevOps practices and is built on a common secure-by-design architecture. This includes the use of Secure Elements to provide guarantees on device identity, communication confidentiality, tamper resistance and evidence while collecting security metrics. Meanwhile, a SecDevOps-inspired process actively promotes the continuous deployment of incremental system upgrades based on real-world operational metrics, facilitating both security and reliability.

Technology applied

For SMEs that want to automate DevOps, the starting point is SCRATCh's Secure DevOps Knowledge Base, available online. This contains the IoT problems that they may face. Complementing this is the Secure DevOps Methodology, which includes guidelines to help SMEs find appropriate tools and working methods, a generic demonstrator, best practices for all DevOps phases and a software development kit (SDK) blueprint repository. The methodology is requirement-centric and expands the traditional DevOps loop according to the security principles of Constrain, Comply and Control. Constraint stages (planning, coding, building) involve limiting the design according to potential vulnerabilities. Compliance (testing, release, deployment) checks that these constraints are met during the automated process. Control (operations, monitoring) takes in new information, such as user patterns, to ensure that security remains in place and to feed the start of the loop for future developments.

The Secure DevOps Toolkit combines new and existing tools with a focus on plugging gaps in easily available tooling for SMEs (such as open source). In the deployment phase, for instance, no tools existed. 12 new tools have subsequently been developed across the DevOps chain and fall under the SCRATCh Toolkit architecture, available on GitHub. Tools from different vendors have been integrated and demonstrated in four use-cases: Retail (secure, continuous deployment of apps running on point-of-sale terminals, smart trolleys and electronic shelf labels), Police (redesign of an existing mobile surveillance platform for secure storage, streaming and provisioning), Smart Grids (anti-fraud algorithms, blockchain implementations and other security mechanisms) and Smart Machines (smart, secure connections between machines). This helps to address the off-putting issue of tool fragmentation for SMEs.



SCRATCh requirements-centric methodology for SecDevOps

Making the difference

With its 12 integrated tools and 13 product initiatives, SCRATCh is now demonstrating concrete improvements to security. ULMA, for instance, faced insecure ecosystem interfaces and exposed attack surfaces. Through SCRATCh's test case prioritisation, they

can now detect 90% of vulnerabilities/ failures by executing only 8% of test cases. By reducing the time to detect security issues by 280 minutes per 1000 test cases executions, their overall development costs have fallen by EUR 11,200 per month. Another success has been Irdeto's software for automatic zero-touch protection and AI-driven algorithms. This is the first (and only) obfuscation tool to use machine learning to automatically apply the most efficient code protection, requiring no interaction with or preparation of the code.

SCRATCh aims for a final market position as a complete, inexpensive provider of the methodology, modular architecture and toolset for the development of SecDevOps applications. Irdeto, for example, is currently negotiating a commercial license for the obfuscation tool and a keys & credentials service for 24/7 monitoring, incident and vulnerability management. Different paths to exploitation may include making tools freely available as open source, improving and expanding existing business models and applying existing tools in the new domain of security. The latter offers a parallel with SME end-users, which will now be able to expand into the IoT domain securely and affordably. As the number of connected devices grew by ~9% in 2021 despite the chip shortage, this is a good opportunity to establish a competitive position in a fast-emerging market.

In terms of wider impact, NVISO has developed the IoT Security Verification Standard (ISVS) within the OWASP (Open Web Application Security Project) non-profit foundation. This open standard contains 125 security requirements for IoT applications, which SMEs can choose from according to their needs. This has already received over 100 unique visitors per month, while more than 200 organisations have shown interest in SCRATCh via the online SecDevOps questionnaire or channels within the OWASP community. Alongside the project's 25 publications so far, these elements can serve as a springboard to future innovations. For example, the SCRATCh Toolkit could be the basis for a new ITEA project on device resilience. Much like the DevOps process itself, this will ensure that the project's results can continuously evolve.

Major project outcomes

Dissemination

- 10 public deliverables
- 2 whitepapers
- 14 academic publications and several presentations at conferences (SyberSA, INDIN, ICUMT, WEDMAIT, ICABME, ECCWS, CSADAA, IEEE IoT, USDAI - SAFECOMP, etc.)

Exploitation (so far)

SCRATCh Knowledge Base and open source tools:

- Available at https://github.com/SCRATCh-ITEA3/SCRATCh-Tools-Repo, a.o.:
- IOXY – MQTT intercepting proxy with multi-protocol and multi-broker support
- FirmwareCheck: automation of dynamic analysis of IoT firmware
- OTAlyzer: automated search for occurrences of predefined keywords in network capture files
- Deception Toolkit: inject lures into application traffic and conceal critical information

Commercial Products:

- Irdeto Trusted Software: code obfuscation tool using ML for code protection
- Irdeto Keys & Credentials Service: services around hardware rooted security foundations, trusted integrity and identity
- ULMA SPTool: test case prioritisation tool reducing testing costs

Standardisation

- Major contribution to IoT security verification standard OWASP-ISVS: Open standard of security requirements for Internet of Things applications

ITEA is the Eureka R&D&I Cluster on software innovation, enabling a large international community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. ITEA is part of the Eureka Clusters Programme (ECP).

https://itea4.org

SCRATCh

17005

Partners

Belgium

- NVISO
- SIRRIS

Germany

- consider it GmbH
- DFKI
- Diebold Nixdorf Systems GmbH
- NXP Semiconductors Germany GmbH
- OTARIS Interactive Services GmbH

Netherlands

- Almende BV
- AnyWi Technology BV
- Irdeto BV

Romania

- Beia Consult International

Spain

- HI Iberia Ingeniería y Proyectos
- Nimbeo
- Quantyca Software Solutions SL
- Quobis
- ULMA Embedded Solutions

Project start

September 2018

Project end

March 2022

Project leader

Andries Stam, Almende BV

Project email

andries@almende.org

Project website

https://scratch-itea3.eu/

ITEA 4

eureka