Feature Stories - Cutting the costs of secure, evolving software

Software-based systems are increasingly security-critical and are often used for much longer than their intended lifespan. Enabling software to evolve to meet new requirements, usage models and threats while remaining secure is a huge and costly challenge, but one that EU-funded researchers are addressing with a radical new approach to software development, verification and deployment.

Have you just downloaded a new app on your smartphone? Did you notice the tickbox that said 'Update automatically'? There are many reasons to update the software, from adding new features to fixing security bugs that could make you a victim of hackers. But sometimes newly downloaded features introduce new security vulnerabilities. That, in essence, is the problem of traditional approaches to software development and deployment - a trade-off between security and flexibility.

'You have secure software, for example. You ship it to the customer and then you need to update it, perhaps to add features to stay ahead of the competition. If you need to start from scratch every time and verify all code - even if only a small part of it has changed - you face considerable time and financial costs,' explains Fabio Massacci, a professor of computer science at the University of Trento in Italy.

Prof. Massacci, who coordinated the SecureChange (1) project - which addressed precisely this problem - points to web browsers as common examples of regularly updated software with strict security requirements.

An analysis conducted by the SecureChange team, spanning five years and six major version updates of the open source Firefox browser, found that only around one third of the software code changed from one version to the next. In addition, a significant number of vulnerabilities were inherited by each new version from its predecessor, a phenomenon common to other browsers like Chrome and IE. The need for quick updates means there is less time to do testing and verification. But is it possible to test only the new parts and maintain the security and integrity of the entire system?

Supported by EUR 5.1 million in research funding from the European Commission, the SecureChange researchers have developed the methodology, techniques and tools to make the entire software lifecycle - from requirements engineering, through design, development, testing and verification, to deployment and updating - more efficient, more flexible, more secure and far less costly in terms of time and money.

Change - a first-class citizen

'Our main idea was to consider change itself as a first-class citizen, using evolution rules for the software to make sure that each change respects the desired security properties. In this way, you automatically know that any modification satisfies your
desired properties,' Prof. Massacci says.

Their approach focused on the so-called ‘delta’ - the difference between the old and the new release of the software. A range of innovative tools enable developers and test engineers to work in a synchronised way and automatically identify only those pieces of code that need to be tested along with those verified properties that are preserved from one version to the next.

'Test engineers can quickly and easily identify which tests are needed, what is new and what is obsolete, thereby avoiding the need to re-test millions of lines of code that have not changed and enabling them to focus their efforts on what is really new and hence potentially more risky,' Prof. Massacci explains.

When it comes to development, the SecureChange team's approach to engineering processes focused on orchestrating changes to the software in a granular fashion, rather than integrating directly, so modifications to one element of the software do not necessarily impact other elements.

Significantly, this approach scales from small software programmes to large-scale critical systems with millions of elements. That potential was highlighted by the SecureChange researchers in a series of prototype implementations built around real-world case studies and involving several industrial partners.

With Thales in France, the team looked at how their tools and approach could improve and speed up the incorporation of new features to an air traffic management system that required changes in organisational and operational processes.

With Telefónica in Spain, the researchers implemented prototype technology on security-critical features of home networks, enabling the network to dynamically configure and reconfigure itself in a secure way to allow for the incorporation of new devices, such as a friend bringing over a smartphone.

With French digital security company Gemalto, the researchers implemented the system with smartcards and tokens, such as those used to pay for public transport and other services, enabling the software to be securely updated.

'Take a Visa or Mastercard for example. It would be convenient if you could also use that as a smartcard to use the railway, but at the moment that is impossible because it would take too long and be too expensive for a third party, such as the railway company, to go through the process of verifying any changes they make to the software on the card. We have shown that with our approach such features are possible to implement easily and quickly, and we have proven it not just in theory but also, for the first time, in practical applications,' Prof. Massacci says.

Commercial plans and spin-offs

The SecureChange industrial partners are exploiting some of the project results internally, the SecureChange coordinator says. A tool called EvoTest, developed by French partner SmartTesting, is now in commercial production, for example, while other tools have been made available as open source software. The project also contributed to the foundation of a spin-off company, QE LaB Business Services, from the University of Innsbruck and the Centre for Academic Spin-Offs Tyrol, Austria.

Meanwhile, open source community development on some of the technology is going to continue for a component called EMF-IncQuery, which has been proposed to the Eclipse Foundation.

The biggest upshot of the SecureChange approach, if adopted widely by the software development community, would be a dramatic reduction in the time-to-market of new software and software versions, and a considerable reduction in the cost of software testing and verification.
Currently, software testing accounts for around half of software pre-release costs and as much as 70% of post-release expenses, while almost 6 in 10 software development projects do not achieve their desired functionality and more than 8 in 10 are not completed on time.

'Not only would the risk of errors and security vulnerabilities be reduced, but companies would be able to release software much quicker, enabling them to rapidly seize market opportunities,' Prof. Massacci notes.

SecureChange received research funding under the Future and Emerging Technologies (FET) part of the European Union’s Seventh Framework Programme (FP7).

(1) 'Security engineering for lifelong evolvable systems'

Useful links:

- FET
- 'Security engineering for lifelong evolvable systems' website
- SecureChange project factsheet on CORDIS

Related information

| Projects | SecureChange - Security Engineering for lifelong Evolvable Systems |

Subjects

- Electronics and Microelectronics
- Information Processing and Information Systems
- Social sciences and humanities
- Telecommunications

Last updated on 2012-08-14
Retrieved on 2019-06-16

© European Union, 2019