SBA-K1
Combinatorial Security Testing

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Centre K1

Type of project: strategic project

SECURE SOFTWARE THROUGH COMBINATORIAL SECURITY TESTING

SBA RESEARCH AND NIST ARE WORKING ON NEW METHODS THAT CAN DRAMATICALLY IMPROVE SOFTWARE SECURITY.

Combinatorial testing in security is a strategic project of SBA Research in the COMET program. **Numerous successful applications in the areas of cross-site scripting (XSS), SQL injection and Linux kernel testing have already demonstrated the enormous potential of this basic research. Now another important milestone has been reached.**

SBA Research sees itself as one of the most basic research institutions in the field of information security. As a superficially rather dry-looking field of research with traditionally less audience appeal, the applied discrete mathematics for information security could, in cooperation with Adobe and NIST, demonstrate once again the valuable contributions of this research to improving security in complex software projects.

Classical measures to improve the security of complex software projects primarily include so-called penetration tests and static and dynamic code analyses. Put simply, combinatorial security testing offers a new and additional way with a completely different approach. This has the potential to find bugs or vulnerabilities that are virtually undetectable by classical methods in this form.

Impact and effects

Our ambitious research collaboration between the COMET MaTRIS research group of **SBA Research** (Area 4 of SBA-K1, Dimitris Simos, Ludwig Kampel, Manuel Leithner, Bernhard Garn), **NIST** (Rick Kuhn, Raghu Kacker) and **Adobe** (Riley Smith, Darryl Jarman, Jared Bellows, Gabe Gosney) led to concrete successes in which potential vulnerabilities were found through

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Version 01/2019

combinatorial testing that could not be identified previously in extensive testing. This approach is now also implemented at COMET corporate partners.

"The successful use of Combinatorial Testing at a major manufacturer like Adobe shows us what is still possible in this area", says Michael Kofler, CTO of **Cyan Security**, "an application with our own products, which have already been continuously improved in recent years through intensive cooperation with SBA Research, can now provide us with another USP".

Similar to Michael Hollauf of **Meisterlabs**: "Through our long-standing cooperation with SBA Research, we have already been able to integrate numerous new security functions into our products and solidly integrate security into our software development processes. However, SBA Research's strategic research approach to combinatorial testing represents a potential quantum leap that is unique internationally."

Georg Lindsberger, CEO of **XiTrust**, is also convinced: "This success at Adobe shows us that there is also top international research in Austria, which additionally provides Austrian companies such as XiTrust with concrete benefits. We are already looking forward to applying the newly developed combinatorial security test sets to important components of our own solution, such as the TLS protocol (Note: Encrypted Internet Transport Protocol), to ensure that our solutions are of significantly higher quality than the industry standard. For companies that develop security solutions themselves, this is a significant market advantage made possible by working with SBA Research."

COMET in an international context

As part of COMET, SBA Research has been working for several years with the American standards institute NIST (National Institute of Standards and Technology) on new fields of application for combinatorial testing in the field of information security.

"Combinatorial security testing is becoming a valuable tool that all quality-affine software companies can use to find unknown vulnerabilities that are difficult to locate using traditional methods," says Dr. Dimitris Simos, head of the working group at SBA Research, describing the broad potential application environment, "but NIST is particularly interested in using this technology in high-risk areas where software failure can lead to disasters, such as in aviation or in autonomous or semi-autonomous vehicles. *Combinatorial Security Testing* represents a milestone in software security research".

Dr. Edgar Weippl, scientific director of SBA Research and overall research director of SBA-K1, points out the enormous future potential of this research work, in which the COMET Center is internationally leading: "In my opinion, the successes of recent years, in which we were able to prove a number of previously undiscovered security problems in various software products through the application of combinatorial testing, are only the beginning. Our researchers are already working on concepts to apply this powerful tool to AI environments. With this we want to reach a next milestone, namely, to address Explainable AI in a new way".

Explainable AI is currently the most important topic in the field of AI research. Understanding why and how an AI system came to a specific decision is a major open research question that is essential in a wide variety of potential applications. Mechanisms have to be created to enable a human readable and comprehensible comprehensibility of AI decisions. Here, however, research is still in its infancy.

This basic research of the future will also be supported by the SBA-K1 corporate partners. Michael Kofler of Cyan Security: "As Europe's leading 'white label' provider of data privacy, high-end mobile radio solutions and easy security products, AI is of course also on our agenda, and in the first products we are already working on implementations together with SBA Research. Therefore, we fully support the efforts to find new solutions for the problem area Explainable AI".

Project coordination
Dr. Dimitris Simos
Team lead MATRIS
SBA Research

T +43 (1) 505 36 88
dsimos@sba-research.org

SBA-K1
SBA Research gGmbH
Floragasse 7
1040 Vienna
www.sba-research.org

Project partner

- SBA Research gGmbH, AT
- TU Graz, AT

- cyan Security Group GmbH, AT
- MeisterLabs GmbH, DE

- XiTrust Secure Technologies GmbH, AT

This success story was provided by the consortium leader/centre management and by the mentioned project partners for the purpose of being published on the FFG website. Further information on COMET: www.ffg.at/comet

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at