PhD Proposal
Quantitative analysis of software security against adaptive attacks

UGA Verimag – CEA List

March 28, 2024

In spite of the undeniable progress made in terms of secure code development and protection mechanisms, software security is still a major concern with an increasing number of CVEs assigned each year. This situation is mainly due to the amount of *vulnerability building blocks* available on a modern execution platform (code and hardware level vulnerabilities, side channels, etc.) and to the ability of attackers to *chain* such building blocks in order to launch complex attack scenarios, allowing to bypass protection mechanisms or to incrementally get the required capabilities.

To address these new threats, the next generation of vulnerability analysis tools will need both:

- to embed a powerful **adaptive attacker model**, able to dynamically deploy an optimal attack strategy when interacting with a target code, in order to gain the knowledge and capabilities required to break the expected security properties;
- to **measure and evaluate** the likelihood and dangerousness of complex attack scenarios.

This PhD proposal aims to progress in this direction by leveraging some recent works:

Robust reachability [2] allows to ensure that a vulnerability can be triggered in a controllable way with respect to a fixed set of program input supposed to be provided by an attacker. This notion can be expressed both in a qualitative way (is the vulnerability attacker controlled or not ?), through a quantitative viewpoint[1, 5] (how much is the vulnerability attacker controlled) or even by supplying a sufficient condition on uncontrolled inputs to make the attacker able to trigger the vulnerability[3].

DQMax#SAT [4] is a quantitative boolean problem allowing to encode a notion of adaptive attacker interacting with a target program by gaining knowledge through (legal or side channel) outputs and controlling the code execution by providing well-chosen inputs. Finding an optimal attack strategy in this context can be achieved by solving specific DQMax#SAT instances, either to maximize the probability of triggering a vulnerability, or to get information about some secret values.

Among the PhD contributions a prototype tool is expected to be developed in the BINSEC framework[1], together with a set of relevant benchmarks to evaluate the benefits of the proposed approach in security contexts.

Practical information:

- This PhD proposal is funded by the French Secureval project, within the PEPR Cybersécurité framework – the leading French initiative in cybersecurity research, aiming to develop techniques and tools for software vulnerabilities detection and analysis, to be used within certification processes. It will be co-hosted between the BINSEC team of CEA List (Paris Saclay) and Verimag (Grenoble).
- Supervisors:
  - Marius Bozga (CNRS/Verimag), Research Engineer at CNRS, research activities on formal methods for system design, `Marius.Bozga@univ-grenoble-alpes.fr`,

[1] `https://binsec.github.io/`

  - Sébastien Bardin (CEA List), Senior researcher and CEA Fellow, head of the BINary-level SECurity group and main designer of the BINSEC platform, `Sebastien.Bardin@cea.fr`,
  - Laurent Mounier (UGA/Verimag), Assistant Professor at UGA, research activities on code analysis techniques for security, `Laurent.Mounier@univ-grenoble-alpes.fr`.

- **How to apply:** send an email to the three advisors. This PhD is expected to start no later than autumn 2024, applications are welcome right now!

Verimag @ Université Grenoble Alpes. The PACS team of Verimag develops code analysis techniques and tools for software security. Current research areas concern code robustness against fault injections, the integration of security countermeasures into formally verified compilers and quantitative security analysis against adaptive attacks.

The BINSEC team @ CEA List and Université Paris-Saclay. The BINSEC team develops binary-level program analysis methods to help security investigation, especially reverse and vulnerability analysis. The team is part of CEA List, a major Research Technological Organization dedicated to Computer Science. CEA List is affiliated to Université Paris-Saclay, the leading research-oriented French university.

References

[1] Sébastien Bardin and Guillaume Girol. A quantitative flavour of robust reachability. *CoRR*, abs/2212.05244, 2022.

[2] Guillaume Girol, Benjamin Farinier, and Sébastien Bardin. Not all bugs are created equal, but robust reachability can tell the difference. In Alexandra Silva and K. Rustan M. Leino, editors, *Computer Aided Verification*, pages 669–693, Cham, 2021. Springer International Publishing.

[3] Yanis Sellami, Guillaume Girol, Frédéric Recoules, Damien Couroussé, and Sébastien Bardin. Inference of robust reachability constraints. *Proc. ACM Program. Lang.*, 8(POPL):2731–2760, 2024.

[4] Thomas Vigouroux, Marius Bozga, Cristian Ene, and Laurent Mounier. Function synthesis for maximizing model counting. In Rayna Dimitrova, Ori Lahav, and Sebastian Wolff, editors, *Verification, Model Checking, and Abstract Interpretation*, volume 14499 of *LNCS*, pages 258–279. Springer, 2024.

[5] Thomas Vigouroux, Cristian Ene, David Monniaux, Laurent Mounier, and Marie-Laure Potet. Baxmc: a CEGAR approach to max#sat. In Alberto Griggio and Neha Rungta, editors, *22nd Formal Methods in Computer-Aided Design,Trento, Italy*, pages 170–178. IEEE, 2022.