Le projet SecOPERA (Secure OPen source softwarE and hardwaRe Adaptable framework)

Virgile Prevosto*[1], Boussad Addad , and Pascal Bisson

[1]Laboratoire de Sûreté et de Sécurité des Logiciels (LSL) – CEA Tech List – Nano-Innov, Palaiseau, France

Résumé

SecOPERA 1 est un projet Horizon Europe, labellise en reponse à l'appel HORIZON-CL3-2021-CS-01. Il a demarre en janvier 2023, pour une duree de 3 ans. Il regroupe 13 partenaires de 7 pays, dont 3 partenaires français (CEA List, GreenCityzen, et le laboratoire ThereSIS du groupe Thales). Il est coordonne par l'Universite technique de Crète, le leader technique etant le centre de recherche ATHENA (Grèce).
Conformement aux objectifs de l'appel, le but de SecOPERA est de fournir une chaine d'outils permettant d'evaluer la securite de produits integrant des composants open-source, tant au niveau logiciel que materiel. Pour ce faire, le projet s'appuie en particulier sur des outils dejà relativement matures (TRL 4 ou plus) qui seront etendus et integres dans une meme plateforme durant le projet. La plateforme SecOPERA en tant que telle sera egalement validee au cours du projet par deux etudes de cas.

La première annee du projet a permis de fixer l'architecture de la plateforme, separee classiquement en un front-end permettant aux utilisateurs de gerer leurs projets, lancer des taches et visualiser des resultats ; un orchestrateur charge d'appeler les outils d'analyse individuels en fonction des taches demandees ; un depot offrant un ensemble de composants securises ; et les outils d'analyse eux-memes.

Le debut de l'evaluation de tout projet par la boite à outils de SecOPERA consistera à identifier ses dependances eventuelles, et à classer ses composants suivant la couche à laquelle ils appartiennent parmi les quatre couches identifiees par le projet : materiel, reseau, application, et cognitive (modèle de Machine Learning). L'analyse de chaque composant sera confiee à des classes d'outils differentes selon les couches en question. Les evaluations proprement dites incluront notamment une recherche de la presence de vulnerabilites, avec, entre autres, du fuzzing renforce avec l'IA, l'utilisation de techniques formelles de verification, et du pentesting. En outre, une phase d'adaptation du projet est prevue, avec en particulier un outil de debloating de code et des suggestions de remplacement de composants par des composants securises SecOPERA. Enfin, la plateforme devra integrer un mecanisme de suivi des evolutions des projets pour etre capable d'analyser les nouvelles versions au fur et à mesure des changements.

*Intervenant