SECUBIC: Secured Binary Supply Chain

Michaël Marcozzi (porteur)
Université Paris-Saclay, CEA, List
Paris-Saclay, France
michael.marcozzi@cea.fr

Informations essentielles

Consortium

1) Université Paris-Saclay, CEA, List
   - Dr. Michaël Marcozzi (www.marcozzi.net)
   - Dr. Sébastien Bardin (sebastien.bardin.free.fr)
2) LORIA, CNRS
   - Pr. Jean-Yves Marion (members.loria.fr/JYMarion)
3) Telecom Paris
   - Pr. Stefano Zacchiroli (upsilon.cc/ zack)

Instrument de financement

Programme de Transfert au Campus Cyber (PTCC - ptcc.fr)
Appels à projets de recherche partenariale
Opéré par INRIA, financé par l'ANR (anr.fr)

Calendrier

Du 1 janvier 2025 au 31 décembre 2028

TRL

Le projet vise à développer un démonstrateur à TRL 3+

I. Contexte et problématiques

Un grand nombre des objets qui peuplent le quotidien personnel et professionnel (non seulement les ordinateurs et les téléphones, mais aussi les routeurs, robots, caméras de surveillance, etc.) sont fournis en étant équipés de code informatique au format binaire, chargé d'assurer leur pilotage. Dans les processus contemporains de développement logiciel, la réutilisation est une pratique massive et généralisée. Le développement d'un logiciel pilotant un objet quotidien peut ainsi avoir réutilisé jusqu'à des milliers de composants logiciels préexistants, dont le code était disponible de façon ouverte (open-source) sur Internet. Ceux-ci peuvent potentiellement implémenter des fonctions sensibles, comme la cryptographie, la gestion des données ou la communication à travers internet.

Une telle chaîne d'approvisionnement logicielle ouvre la porte à des attaques spécifiques contre les binaires inclus dans les objets du quotidien, comme l'exploitation de vulnérabilités connues dans des composants open-source obsolètes (attaque 1-day) ou comme l'injection à dessein de vulnérabilités dans le code de composants open-source sensibles (attaque backdoor), notamment par des développeurs malveillants de ceux-ci ou par le fabricant malveillant de l'objet.

II. Verrous scientifiques

Lorsque l'utilisateur d'un objet du quotidien veut s'assurer que le binaire qui le pilote n'est pas vulnérable à ce type d'attaques, il peut pour l'instant n'utiliser que des techniques génériques de détection de vulnérabilités sur l'entièreté du code binaire. Cela représente un effort considérable et il est donc hautement probable que nombre des vulnérabilités présentes ne puissent en réalité être détectées avec le temps et le budget disponibles.

Cela est d'autant plus frustrant qu'il s'agit ici de redécouvrir des vulnérabilités déjà publiquement connues (dans le cas des vulnérabilités 1-day, comme des CVE, dans les composants open-source du binaire) ou ayant conduit à des altérations notables du code originel de composants open-source (dans le cas de backdoors introduites par le fabricant malveillant de l'objet au sein d'un composant open-source sensible). Néanmoins, les composants open-source du binaire étant fondus dans la masse du code de celui-ci, leurs vulnérabilités connues et leurs altérations notables ne peuvent être aisément identifiées.

III. Pistes de recherche et méthodologies

Le projet vise donc dans un premier temps à rendre possible de manière large et fiable l'analyse de composition au niveau binaire, permettant ainsi d'extraire les composants open-source hors de la masse du code du binaire. Ensuite, il ambitionne d'adapter des techniques préexistantes d'analyse de vulnérabilités classiques et de backdoors, afin d'évaluer l'impact des vulnérabilités connues présentes sur la sécurité du binaire et de vérifier que les altérations détectées ne représentent pas des backdoors.

En ajoutant aux techniques génériques de détection des vulnérabilités au sein des binaires une approche dédiée pour les vulnérabilités liées à la chaîne d'approvisionnement logicielle, le projet ambitionne de rendre la neutralisation de ces vulnérabilités (ou leur exploitation, si l'on se place du point de vue d'un attaquant) exhaustive possible en un temps et un budget raisonnable.

Le projet, d'une durée de quatre ans, s'articulera autour de jalons annuels de développement, associés chacun à un évènement au Campus Cyber. Ces évènements permettront de faire rayonner les recherches effectuées vers l'écosystème académique et industriel français et européen, ainsi que d'accroître la formation de celui-ci aux thématiques du projet et à la cybersécurité.