Le CEA et Thales lancent une innovation de rupture en cybersécurité pour sécuriser les codes cryptographiques

Paris, le 9 mars 2017

Dans le cadre de leur laboratoire commun FormalLab, Thales et le CEA présentent une solution inédite pour garantir la sécurité des codes cryptographiques. Véritable rupture technologique, l'innovation réside dans la vérification formelle[1] de composants de librairies sécurisés pour le chiffrement des communications sensibles.

La cybersécurité, ou sécurité informatique, constitue l'un des enjeux majeurs des sociétés numériques, à la croisée de la conception, des techniques de vérification, et des enjeux de certification. Le List, institut de CEA Tech, a développé depuis de nombreuses années une forte expertise dans le domaine de l'analyse et de la vérification formelle de logiciels. Ses technologies innovantes ont trouvé leurs applications dans les secteurs de l'énergie et de l'aéronautique, et plus récemment de l'automobile et du naval.

FormalLab : l'atout des méthodes formelles

Au travers du laboratoire commun FormalLab, créé en juin 2015, Thales et le CEA ont pour objectif de traiter des enjeux de confiance numérique en se basant sur des approches formelles. Basées sur des techniques avancées de raisonnement mathématique, ces solutions sont considérées comme une alternative prometteuse aux techniques de vérification classiques de type « test », qui par définition peuvent comporter des failles. Si elles nécessitent une expertise des techniques de spécification et d'analyse, les solutions formelles présentent un atout majeur : elles fournissent des garanties très fortes sur les comportements attendus des logiciels. Elles permettent, en particulier, de démontrer l'absence de certaines classes de vulnérabilités de sécurité, fermant ainsi la porte à de nombreux types de cyberattaques.

L'analyse formelle de code au service de la cybersécurité

Les logiciels de communication chiffrée sous-tendent une large partie des échanges numériques actuels. Tout défaut dans ces logiciels peut mener à une cyberattaque dont l'impact serait majeur. Ainsi la faille *Heartbleed*, découverte en 2014, a instantanément impacté la sécurité de 17 % des serveurs sécurisés d'Internet. Les équipes de Thales et du CEA se sont attelées au problème de la cybersécurité des codes de communication chiffrée : grâce à la plateforme d'analyse de code Frama-C[2], elles ont spécifié un cahier des charges de sécurité et validé formellement la conformité du code de communication à ces exigences.

---

[1] La vérification formelle met en œuvre des techniques mathématiques pour démontrer qu'un système se conforme aux propriétés qui en sont attendues.

[2] www.frama-c.com

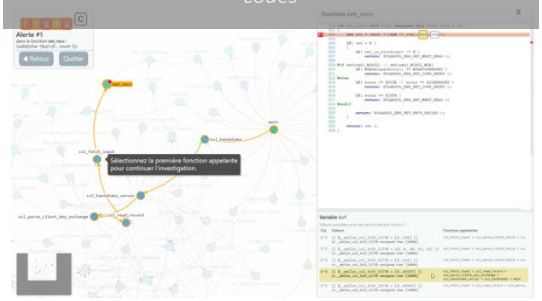
« A l'heure du cloud computing et de l'interconnexion généralisée des systèmes d'information, même les plus critiques comme ceux du secteur de la Défense, la conception périmétrique de la cybersécurité a vécu. Nul ne peut plus croire désormais que la sécurité de l'information numérique se confond avec la sécurité du réseau. Chez Thales, nous sommes convaincus que l'avenir est aux solutions nativement sécurisées dans lesquelles la cyber-sécurité est prise en compte à tous les niveaux : l'architecture globale, le réseau, bien sûr, mais aussi et surtout le logiciel, tout particulièrement les modules applicatifs liés aux communications et au cryptage des données. Dans ce domaine, les travaux de FormalLab rompent avec les pratiques de cybersécurité conventionnelles pour faire face à une cyber-menace en perpétuelle évolution.» témoigne Marko Erman, Directeur technique et innovation de Thales.

« Les questions de confiance numérique, et en particulier de cybersécurité, figurent au cœur des programmes du List. Ses équipes conçoivent les nouvelles générations d'outils de sécurisation logicielle, en s'appuyant sur des bases mathématiques ancrées dans la dynamique de Paris Saclay, et fortes d'expériences reconnues internationalement. Au sein du FormalLab, dans une collaboration rapprochée avec les ingénieurs Thales, elles œuvrent pour identifier les besoins industriels, déterminer les valeurs ajoutées, et mener l'innovation depuis les levées de verrous jusqu'au transfert aux unités opérationnelles. Le CEA contribue ainsi aux avancées technologiques de l'écosystème cybersécurité Français.» conclut Philippe Watteau, Directeur du List.

Le CEA et Thales au #techday#cealist

Le **14 mars 2017**, les industriels pourront découvrir l'approche d'analyse de sécurité de code basée sur **Frama-C** développée dans le cadre du laboratoire commun **Thales CEA, FormalLab** : son application à la vérification d'un code cryptographique sera visible dans l'espace **Cybersécurité.**

Frama-C : la plateforme d'analyse de sécurité des codes



A propos du CEA

Le CEA est un organisme public de recherche qui intervient dans quatre domaines : la défense et la sécurité, les énergies décarbonées (nucléaire et renouvelables), la recherche technologique pour l'industrie et la recherche fondamentale. S'appuyant sur une capacité d'expertise reconnue, le CEA participe à la mise en place de projets de collaboration avec de nombreux partenaires académiques et industriels. Fort de ses 16 000 chercheurs et collaborateurs, il est un acteur majeur de l'espace européen de la recherche et exerce une présence croissante à l'international. Pour en savoir plus : www.cea.fr

Le List, institut de CEA Tech, le pôle de recherche technologique du CEA, focalise ses recherches sur les systèmes numériques intelligents. Porteurs d'enjeux économiques et sociétaux majeurs, ses programmes de R&D sont centrés sur le manufacturing avancé, les systèmes cyberphysiques, la data intelligence et les technologies pour le patient numérique. En développant des technologies de pointe, le List contribue à la compétitivité industrielle de ses partenaires par l'innovation et le transfert technologique. La qualité de sa recherche partenariale a valu au List d'être labellisé Institut Carnot dès 2006. Pour en savoir plus : www-list.cea.fr

A propos de Thales

Thales est un leader mondial des hautes technologies pour les marchés de l'Aérospatial, du Transport, de la Défense et de la Sécurité. Fort de 64 000 collaborateurs dans 56 pays, Thales a réalisé en 2016 un chiffre d'affaires de 14,9 milliards d'euros. Avec plus de 25 000 ingénieurs et chercheurs, Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services pour répondre aux besoins de sécurité les plus complexes. Son implantation internationale exceptionnelle lui permet d'agir au plus près de ses clients partout dans le monde.

La recherche, source d'innovation, est inscrite dans l'ADN du Groupe. Thales a consacré en 2016 743 millions d'euros à la Recherche & Développement autofinancée. L'innovation chez Thales c'est : un portefeuille de 16 500 brevets, des centres de R&D dans 19 pays, 20 laboratoires communs créés dans le monde avec des instituts de recherche, 50 accords-cadres conclus avec des universités et des centres de recherche publics en Asie, aux Etats-Unis et en Europe. www.thalesgroup.com

Contacts Presse

CEA : Guillaume Milot | guillaume.milot @cea.fr | 01 64 50 14 88

Thales : Dorothée Bonneil | dorothee.bonneil@thalesgroup.com | 01 57 77 90 89

Constance Arnoux | constance.arnoux@thalesgroup.com | 01 57 77 91 58

Thales est un leader mondial des hautes technologies pour les marchés de l'Aérospatial, du Transport, de la Défense et de la Sécurité. Fort de 64 000 collaborateurs dans 56 pays, Thales a réalisé en 2016 un chiffre d'affaires de 14,9 milliards d'euros. Avec plus de 25 000 ingénieurs et chercheurs, Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services pour répondre aux besoins de sécurité les plus complexes. Son implantation internationale exceptionnelle lui permet d'agir au plus près de ses clients partout dans le monde.