PARIS,
LE 22 JANVIER 2019

COMMUNIQUÉ DE PRESSE

Le CEA présente ses solutions de sécurité pour l'internet des objets au Forum international de la cybersécurité

En réponse à la multiplication des cybermenaces dans le monde numérique, le CEA conduit un programme de recherches en cybersécurité tant pour ses propres besoins qu'en réponse aux besoins opérationnels des acteurs du domaine. Dans ce cadre, l'organisme développe des technologies destinées à renforcer la cybersécurité des systèmes et de leurs composants. Quatre d'entre elle seront présentées au Forum international de la cybersécurité (stand F11), les 22 et 23 janvier 2019 à Lille.

Des objets de la vie quotidienne (smartphone, montres connectées…) aux grandes infrastructures de transport (aéroport, trains à grande vitesse…), le numérique occupe une place de plus en plus importante dans notre vie. Les logiciels pilotent et produisent de nombreuses données sur les états des systèmes et de leurs interactions. Ces systèmes sont devenus des cibles privilégiées pour qui voudrait les compromettre à des fins stratégiques, criminelles ou de vandalisme. Ainsi, pour les particuliers comme pour les entreprises, la confidentialité et l'intégrité des données, la sécurité et la fiabilité des logiciels informatiques et des composants électroniques qui les exploitent sont devenues des sujets essentiels de la transition numérique que vit notre société.

Le CEA présente, au Forum international de la cybersécurité (22 et 23 janvier 2019, Lille, sante F11), quatre des technologies qu'il développe dans ce domaine. Celles-ci sont issues des recherches de l'institut CEA-List, labellisé Carnot, spécialisé dans les systèmes numériques intelligents.

Quatre technologies CEA au Forum FIC2019

Sécuriser les logiciels critiques

La sécurité de fonctions logicielles critiques est un élément clé de confiance dans les systèmes informatiques. Comment peut-on passer cette confiance à l'échelle à la fois des menaces, et de la vague de numérisation actuellement en cours ? L'automatisation et les raisonnements mathématiques avancés améliorent la sécurité des produits informatiques en permettant de vérifier de façon plus exhaustive l'absence de vulnérabilité dans les produits.

frama C
Software Analyzers

En s'appuyant sur des techniques de raisonnement automatisé, les outils de la plateforme Frama-C, développés par le CEA, permettent d'appuyer l'évaluation

CONTACTS PRESSE

François Legrand
francois.legrand@cea.fr
Tél. : 01 64 50 20 11

www.cea.fr
@CEA_Recherche

PARIS,
LE 22 JANVIER 2019

COMMUNIQUÉ DE PRESSE

de sécurité des composants logiciels exposés, et de fournir des garanties exhaustives d'absence des failles les plus dangereuses. Leur mise en œuvre permet, d'ores et déjà, d'établir des différenciateurs qualitatifs, reconnus internationalement, de systèmes numériques de pointe.

- *La technologie Frama-C s'adresse aux développeurs d'applications critiques dotés de forts objectifs de sécurité. La démonstration intéressera en particulier les développeurs de produits ou les entreprises ayant une vraie sensibilité sur le développement de produits sûrs et sécurisés.*

Détecter et contrer les attaques ciblant un réseau industriel IoT sans-fil

L'évolution actuelle des réseaux de communication tend vers un accroissement de leur complexité, de leur criticité, et du caractère massif de leur déploiement. Il est nécessaire d'en définir des mécanismes de protection tant préventifs que réactifs destinés à se complémenter l'un l'autre.

Les équipes du CEA développent et transfèrent des solutions de sécurité réseaux réactives et efficaces. Ces dernières doivent être en mesure de détecter des attaques connues et inconnues, et d'y réagir rapidement et de manière appropriée, en particulier dans des topologies IoT.

- *La technologie s'adresse en particulier aux opérateurs d'infrastructures ou développant des produits intégrés dans des systèmes industriels*

Renforcer la sécurité des systèmes embarqués IoT contre les attaques physiques

Les attaques par canaux auxiliaires (ou attaques physiques)[1] représentent une menace spécifique pour la sécurité des systèmes embarqués (composants électroniques des véhicules autonomes par exemple, ou même cartes bancaires à puces). Jusqu'à récemment, ces attaques ne pouvaient être pratiquées que par des laboratoires spécialisés en évaluation sécuritaire et disposant d'équipements onéreux et de compétences bien spécifiques ; mais l'évolution des matériels facilite leur mise en œuvre.

Face à ces nouveaux risques d'attaque physiques à bas coût des technologies logicielles ont été développées afin de renforcer la sécurité de composants existants

CONTACTS PRESSE

François Legrand
francois.legrand@cea.fr
Tél. : 01 64 50 20 11

www.cea.fr
@CEA_Recherche

[1]Les attaques par canaux auxiliaires (ou « side channel attacks ») sont des attaques très particulières, qui utilisent les propriétés physiques d'un composant ou d'un microprocesseur pendant le processus de chiffrement pour attaquer les clés servant à sécuriser la transmission de l'information et s'en emparer.

PARIS,
LE 22 JANVIER 2019

COMMUNIQUÉ DE PRESSE

et complexifier, voire rendre impossible le travail des attaquants C'est le cas de Cogito, développé par le CEA.

Le démonstrateur met en évidence la nécessité de se protéger contre ces attaques physiques et les contre-mesures proposées, par exemple grâce au principe du polymorphisme de code qui apporte de la variabilité comportementale au composant à protéger, sans dénaturer la fonction originale du composant.

- *La démonstration intéressera en particulier les développeurs de produits et les industriels souhaitant déployer des produits IoT sécurisés à partir de composants génériques*

Renforcer la confidentialité des données vis à vis du RGPD[2]

Les nouvelles technologies de chiffrement ouvrent de nouvelles voies de sécurisation de données dans le cloud permettant de renforcer la protection de la vie privée et du secret industriel face à la cybercriminalité

Cingulata, une technologie développée par le CEA, permet de créer des applications de traitement et d'analyse de données sur des serveurs distants non sécurisés, tout en préservant leur confidentialité sur l'ensemble du processus de la collecte à l'utilisation. Les données sont chiffrées à leur création, puis manipulées uniquement sous forme chiffrée, et le résultat des opérations n'est accessible qu'au processeur de la clef de déchiffrement. Avec l'arrivée de la nouvelle règlementation européenne sur la protection des données personnelles (RGPD), Cingulata offre une solution attractive pour garantir la vie privée des utilisateurs sur leurs données critiques tout en permettant la poursuite d'applications existantes voire le développement de nouveaux services bénéficiant de cette technologie.

- *La démonstration intéressera toutes les sociétés travaillant avec des données sensibles et désireuses d'utiliser la puissance de calcul du cloud pour le traitement de ces données tout en respectant les nouvelles règlementations*

Masterclass : "Cybersecurity for IoT[3] : Verify your Software Today !"

Les objets et services connectés, ou Internet des Objets, qui prennent une place croissante dans nos sociétés, posent de nouveaux problèmes de sécurité. Des technologies de vérification existent déjà, permettant d'assurer la fiabilité et la sécurité des logiciels de l'Internet des Objets. La plateforme d'analyse logicielle Frama-C, développée par le CEA et Inria, peut notamment être est utilisée avec

CONTACTS PRESSE

François Legrand
francois.legrand@cea.fr
Tél. : 01 64 50 20 11

www.cea.fr
@CEA_Recherche

[2] Règlement général sur la protection des données
[3] Internet Of Things (internet des objets).

PARIS,
LE 22 JANVIER 2019

COMMUNIQUÉ DE PRESSE

succès utilisée notamment sur le code C de Contiki, un système d'exploitation open source de l'internet des Objets, pour détecter des erreurs ou vérifier leur absence.

- *Mardi 22 janvier 2019 de 12h à 12h45, avec Allan Blanchard (Inria) et Nikolai Kosmatov (CEA List)*

Les recherches du CEA en cybersécurité

Les équipes du CEA conduisent des recherches en cybersécurité principalement dans les domaines la sécurité des systèmes industriels, la sécurité physique ainsi que la sécurité logicielle. Les projets de recherche vont de l'analyse de la menace et des risques associés à l'évaluation de solutions de confiance sur des plateformes dédiées, avec un investissement important sur le développement de solutions technologiques innovantes. Celles-ci font aujourd'hui l'objet de partenariats et de transferts industriels pour en faire des produits de cybersécurité destinés à remplir des fonctions non couvertes à ce jour.

Les activités du CEA en cybersécurité s'adressent en priorité aux fabricants de composants et systèmes, aux développeurs de logiciels et fournisseurs de services de sécurité, aux constructeurs et opérateurs d'infrastructures critiques, aux industriels (transport, aéronautique, énergie) ainsi qu'aux organismes publics.

Retrouvez les équipes du CEA sur le stand F11 du Forum international de la cybersécurité

Le Forum International de la Cybersécurité s'inscrit dans une démarche de réflexions et d'échanges visant à promouvoir une vision européenne de la cybersécurité. Dans la continuité du marché unique numérique et du projet de règlement sur la protection des données personnelles, le FIC est l'évènement européen de référence réunissant tous les acteurs de la confiance numérique.

https://www.forum-fic.com/

La sécurisation des données de santé est un des enjeux de la R&D en cybersécurité (DR)

CONTACTS PRESSE

François Legrand
francois.legrand@cea.fr
Tél. : 01 64 50 20 11

www.cea.fr
@CEA_Recherche