Forum International de la Cybersécurité

ALLISTENE
l'alliance des sciences et technologies du numérique

PROGRAMME MASTERCLASS ALLISTENE 2022

cdefi
Conférence des Directeurs des Écoles Françaises d'Ingénieurs

cea

cnrs

IMPACT DIGITRUST

France Universités

Inria

Institut Mines-Télécom

L'Alliance Allistene

Allistene est l'alliance des sciences et technologies du numérique ; elle accompagne les mutations économiques et sociales liées à la diffusion des technologies numériques. L'alliance a pour but d'assurer une coordination des différents acteurs de la recherche dans les sciences et technologies du numérique, afin d'élaborer un programme cohérent et ambitieux de recherche et de développement technologique. Elle permet d'identifier des priorités scientifiques et technologiques communes et de renforcer les partenariats entre les opérateurs publics (universités, écoles, instituts), tout en créant de nouvelles synergies avec les entreprises.

L'alliance Allistene est dotée d'un groupe de travail (GT) « Cybersécurité », avec pour mission d'aider le Comité de Coordination à répondre aux différents enjeux relatifs à la cybersécurité :

- Prospective sur les thématiques de recherche en cybersécurité, en précisant les enjeux de recherche, les impacts applicatifs et les acteurs concernés de la communauté française ;
- Elaboration d'éléments programmatiques au niveau national et européen ;
- Veille en matière de cybersécurité et développement d'une stratégie collaborative, en interaction avec le CSF Industries de sécurité.

Ce GT rassemble des représentants des principaux EPST, de France Université, des écoles d'ingénieurs et du secteur privé.

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 7 juin 2022

11h à 11h30

Cryptographie reposant sur les réseaux euclidiens et finalistes du NIST

Adeline Roux-Langlois **/ CNRS**

La cryptographie permet par exemple de sécuriser nos communications, lors de transactions bancaires ou d'une connexion sur un site internet par exemple. Une partie des constructions cryptographiques utilisées aujourd'hui seraient possible à attaquer avec un ordinateur quantique suffisamment élaboré. Même si un tel ordinateur quantique n'existe pas encore, il est important d'anticiper sa possible construction et de préparer une transition vers des outils cryptographiques résistants aux attaques quantiques.
Parmi toutes les possibilités de constructions post-quantiques mises en avant par la compétition de standardisation post-quantique organisée par le NIST, la cryptographie reposant sur les réseaux euclidiens semble être la plus prometteuse. En effet, cinq des sept constructions finalistes reposent sur ce type d'hypothèses.
Dans cet exposé, je vais présenter la cryptographie reposant sur les réseaux euclidiens. Dans une première partie, je vais introduire les grands principes de cette branche de la cryptographie ainsi que les problèmes difficiles sur lesquels reposent la sécurité des constructions, puis je donnerais un aperçu du principe des constructions de chiffrement à clé publique et des signatures finalistes à la compétition du NIST.

Adeline Roux-Langlois est chargée de recherche au CNRS dans l'équipe CASPULE de l'IRISA à Rennes. Elle a obtenu sa thèse à l'ENS de Lyon en 2014 et a travaillé en post-doctorat à l'EPFL en Suisse. Ses recherches portent sur les fondements de la cryptographie reposant sur les réseaux euclidiens, elle travaille notamment sur la difficulté théorique des problèmes sous-jacents à la sécurité des constructions, et sur les constructions cryptographiques et leurs preuves de sécurité.

cnrs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 7 juin 2022

11h30 à 12h

Authentification biométrique : comment (ré)concilier sécurité, utilisabilité et respect de la vie privée ?

Estelle Cherrier **/ ENSICAEN / Laboratoire GREYC**

Lorsqu'on s'intéresse à l'authentification biométrique, il est aujourd'hui fondamental de considérer les trois aspects complémentaires suivants : la sécurité, l'utilisabilité et le respect de la vie privée (ou la protection des données). Ceci, afin d'éviter les dérives sécuritaires et de préserver les libertés individuelles. Ainsi, la sécurité apportée par la biométrie implique une confiance élevée dans l'identité revendiquée par l'utilisateur et permet le déploiement d'applications d'authentification forte pour accéder à de nombreux services numériques. Ces services sont accessibles via une authentification forte, soit dans le cadre régalien, soit dans un cadre commercial privé. L'utilisabilité permet, quant à elle, une réelle acceptation de la biométrie par le grand public — on peut citer la reconnaissance du visage ou de l'empreinte digitale par exemple —, en complément ou même parfois en remplacement de moyens plus traditionnels d'authentification tels que les codes PIN ou les mots de passe qui encombrent nos mémoires. Enfin, la protection des données biométriques constitue une protection essentielle des libertés individuelles, dans le sens où il s'agit de données personnelles sensibles selon la CNIL. Plus largement, la protection des données personnelles est mise en lumière depuis un an par l'entrée en vigueur du RGPD dans tous les pays membres de l'Union Européenne, les plaçant de fait au premier rang des pays soucieux de protéger les données de leurs citoyens.

Estelle Cherrier est Maîtresse de conférences HDR depuis 2007 à l'Ecole Nationale Supérieure d'Ingénieurs de Caen, rattachée au laboratoire GREYC. Ses thématiques de recherche actuelles sont centrées sur les données : les données biométriques (leur sécurité, leur protection), la collecte de données respectueuse de la vie privée des utilisateurs, l'authentification sur smartphone, l'utilisabilité des applications d'authentification, l'évaluation des algorithmes de détection de communautés dans les multi-graphes.

France Universités

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 7 juin 2022

15h à 15h30

Attaques et Mécanismes de protection dans l'Apprentissage Fédéré

Vlad Nitu / **CNRS**

Grâce à l'apprentissage collaboratif (aussi appelé Apprentissage Fédéré), un grand nombre de dispositifs mobiles peuvent entraîner collectivement un modèle sur leurs données privées, sans envoyer les données brutes à des fournisseurs de services externes. À cette fin, les clients mettent à jour de manière itérative un modèle global en utilisant leurs données d'entraînement locales et n'envoient que ces mises à jour à un serveur central (appelée aussi serveur d'agrégation) qui orchestre le processus d'entraînement. L'apprentissage fédéré (FL) a été rapidement adopté dans de multiples domaines d'application émergents, tels que la prédiction du mot suivant dans le clavier Android, le domaine de la santé, les services bancaires, etc. Cependant, le protocole FL expose une surface d'attaque assez importante pour deux raisons principales. Premièrement, les clients Edge peuvent à la fois accéder aux paramètres du modèle et influencer leur valeur par le biais des mises à jour du modèle envoyées au serveur d'agrégation. Du côté du serveur, définissant à quoi ressemble une mise à jour malveillante et la manière de la distinguer des mises à jour bénignes n'est pas une tâche facile en raison de la faible interprétabilité des modèles ML. Deuxièmement, de multiples attaques ont démontré que, dans certaines conditions, les modèles ML peuvent être inversés de sorte qu'un attaquant peut potentiellement récupérer des informations sensibles sur les données d'entraînement. Dans cet exposé, nous discuterons des attaques les plus récentes sur la confidentialité et la robustesse de l'apprentissage fédéré, ainsi que des mécanismes de protection visant à remédier à ces vulnérabilités.

Vlad Nitu est un jeune chercheur (Chargé de Recherche) au Centre National de la Recherche Scientifique (CNRS), affecté au laboratoire LIRIS, à Lyon. Ses principaux intérêts de recherche sont la sécurité et l'efficacité énergétique de l'IA collaborative, ainsi que son applicabilité à de différents domaines tels que l'Industrie 4.0. Auparavant, Vlad était post-doc à l'École Polytechnique Fédérale de Lausanne, au sein du Laboratoire des Systèmes Distribuée. Vlad a obtenu son doctorat en 2018 à l'Université de Toulouse avec une thèse portant sur l'efficacité énergétique et la performance des datacenters cloud virtualisés. Il est le lauréat du prix Léopold Escande et du prix ASF/GDR pour les meilleures thèses de doctorat soutenues en 2018. Au cours de sa carrière, Vlad a également collaboré avec des entreprises big-tech (Facebook, IBM, Huawei, etc.) ou d'autres partenaires de recherche académique internationaux (ETH Zurich, George Washington University, Virginia Tech, etc.)

cnrs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 7 juin 2022

15h30 à 16h

KRAKEN: Un système de recommandation basé sur la connaissance, afin de donner un coup de pouce aux analystes dans l'exploration des données

Romain Brisse **/ Inria / Malizen**

Les systèmes de détection et de visualisation de logs sont aujourd'hui les outils les plus communément utilisés pour détecter et qualifier des attaques. L'analyste en sécurité est toujours au centre de ce processus et fait face à des problèmes importants, tels que l'hétérogénéité et la quantité de données à analyser. Malgré les solutions déjà en place, le travail est toujours plus difficile face à des attaquants de plus en plus nombreux et organisés. Des attaques peuvent être étalées sur plusieurs mois afin de les rendre difficiles à détecter, par exemple. C'est l'une des raisons pour lesquelles nous avons décidé de nous concentrer sur la facilitation du travail de l'analyste.
Notre objectif est de rendre la tâche des analystes plus simple et plus efficace en les aidant à sélectionner la prochaine étape de leur investigation en fonction de leurs découvertes récentes. Pour ce faire, nous présentons KRAKEN, un système de recommandation se reposant sur des connaissances expertes et le contexte de l'investigation pour faire des recommandations d'exploration pertinentes, sous la forme de champs à aller explorer. KRAKEN est développé dans le cadre d'une thèse et intégré au produit ZeroKit de la startup Malizen.

Nous avons implémenté une base de connaissances experte à l'aide des projets MITRE ATTA&CK et Elastic Common Schema, ainsi que deux processus de décision, l'un basé sur un principe de similarité et l'autre sur le Multi-Attribute Decision-Making. Nous avons ensuite réuni 7 experts afin de tester notre outil, intégré dans l'outil de chasse à la menace ZeroKit. Cette évaluation a été riche en retours et nous a permis d'estimer l'utilité que KRAKEN peut avoir pour un analyste en sécurité. L'évaluation reste cependant majoritairement qualitative. Dans un futur proche, nous allons conduire une évaluation plus complète sur une version de KRAKEN intégrant de nouveaux éléments : historique des recommandations, détails sur les motivations des recommandations, apprentissage, amélioration de l'IHM.

Actuellement doctorant CIFRE entre Malizen et Inria, Romain Brisse est membre de l'équipe CIDR (commune à Inria, CentraleSupélec, CNRS et Univ. Rennes 1). Ses travaux se concentrent sur l'utilisation des systèmes de recommandation dans l'investigation d'incidents de sécurité.

Inria

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 7 juin 2022

16h00 à 16h30

Etude sur les abus du DNS (Domain Name System)

Maciej Korczyński **/ Grenoble INP / Grenoble Alpes Cybersecurity Institute / KOR Labs**

L'abus du système de noms de domaine (DNS) est toute activité qui utilise les noms de domaine ou le protocole DNS pour mener des activités nuisibles ou illégales. Les activités malveillantes sur le DNS sont un problème fréquent et grave depuis des années, affectant la sécurité en ligne, causant des dommages aux utilisateurs et aux tiers et minant la confiance dans l'internet. L'étude a évalué la portée, l'ampleur et l'impact de l'abus du DNS et a fourni des éléments pour d'éventuelles mesures politiques. À cette fin, les contractants ont effectué des mesures techniques axées sur la santé des écosystèmes DNS et ont interrogé des experts et des parties prenantes au moyen de questionnaires, d'entretiens approfondis et d'ateliers impliquant un large éventail d'acteurs (registres, bureaux d'enregistrement, fournisseurs d'hébergement, fournisseurs d'infrastructure DNS) et de parties intéressées dans le domaine de la protection des consommateurs, des droits de propriété intellectuelle, de la cybersécurité et des politiques publiques. L'étude propose un ensemble de recommandations dans le domaine de la prévention, de la détection et de l'atténuation de l'abus de DNS adressées aux opérateurs DNS (registres TLD, bureaux d'enregistrement, revendeurs et fournisseurs d'hébergement, en fonction de leur rôle dans la chaîne DNS) mais aussi aux institutions et organes de coordination internationaux, nationaux et européens. L'étude recommande également des actions dans le domaine des métadonnées DNS, du WHOIS et des informations de contact, du signalement des abus, de la protection des opérations DNS, de la sensibilisation, du renforcement des connaissances et de la collaboration en matière d'atténuation au niveau de l'UE.

Maciej est maître de conférences en réseaux informatiques et cybersécurité à Grenoble INP et co-fondateur de KOR Labs. Ses principaux intérêts tournent autour des mesures passives et actives à grande échelle pour la cybersécurité, avec un accent sur le DNS. Depuis 2015, il a co-écrit plus de 30 articles de recherche sur l'abus de noms de domaine, les vulnérabilités DNS, les mesures de réputation DNS, les incitations économiques pour améliorer la sécurité de l'écosystème DNS, l'usurpation d'adresse IP, les attaques DDoS, les botnets et les notifications de vulnérabilité.

cdefi
Conférence des Directeurs des Écoles Françaises d'Ingénieurs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 7 juin 2022

16h30 à 17h

Développement rigoureux des architectures sécurisées : approches orientées objective et menaces de sécurité

Brahim HAMID **/ IRIT/ Université Toulouse Jean-Jaurès**

Les experts en sécurité, les praticiens et les chercheurs de différentes organisations internationales, associations et universités ont convenu que pour la sécurité, "ce n'est pas seulement le code". Les vulnérabilités de sécurité logicielle les plus populaires et les plus connues sont liées à des problèmes de conception. L'existence de menaces de sécurité dans les conceptions de logiciels peut avoir un impact significatif sur leur fonctionnement sûr et fiable. En conséquence, il existe des défis concernant les moyens d'identifier, d'analyser et de se préparer aux menaces, d'atténuer les vulnérabilités et de minimiser l'impact et les conséquences des faiblesses engendrées. Notre travail vise à relever ces défis en développant une approche intégrée pour spécifier, détecter et traiter les menaces de sécurité durant la phase de conception de l'architecture logicielle dans un effort d'intégration de la sécurité. Cet objectif peut aider les concepteurs de systèmes à retravailler leurs conceptions pour éliminer ou atténuer les menaces identifiées et/ou pour aider à sélectionner des contrôles de sécurité et de fiabilité appropriés pour garantir le fonctionnement sûr, sécurisé et fiable de leurs systèmes. Des notions telles que les modèles, les propriétés, les patrons, l'analyse et les évaluations expérimentales peuvent aider au développement de systèmes sécurisés bien conçus, correctement modélisés, correctement documentés et bien compris. L'idée générale de l'approche est de : (1) spécifier les menaces comme des propriétés du système modélisé dans un langage de spécification indépendant de la technologie ; (2) exprimer les conditions qui révèlent ces menaces dans un langage approprié avec un support d'outil automatisé pour la détection des menaces par la vérification de modèles ; et (3) suggérer un ensemble de politiques de sécurité pour se protéger contre les menaces détectées. Les menaces formalisées et les politiques de sécurité sont ensuite fournies sous forme de bibliothèques de modèles formels. De plus, nous avons défini une approche similaire pour gérer les exigences de sécurité du point de vue positif comme des objectifs de sécurité. Nous utilisons l'ingénierie dirigée par les modèles (IDM) et des techniques formelles pour la mise en œuvre de l'approche. Pour valider notre travail, nous explorons un ensemble de menaces représentatives issues de catégories basées sur la classification STRIDE de Microsoft et des objectifs issues de catégories basées sur la classification CIAA dans le contexte d'une architecture logicielle sécurisés basée sur des composants.

Brahim HAMID est professeur d'informatique à l'Université de Toulouse Jean-Jaurès, Toulouse, France, et il a été membre de l'équipe IRIT-ARGOS de 2019 à aujourd'hui. Il travaille sur la sécurité, la sûreté de fonctionnement, les architectures logicielles, la formalisation, la vérification et la validation. Il travaille sur le développement d'outils pour modéliser et analyser les architectures logicielles sécurisées. Pour le contacter : brahim.hamid@irit.fr

France Universités

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 8 juin, 2022

11h à 11h30

Référentiel de vulnérabilités et d'attaques pour l'IdO

Anna Felkner **/ NASK** et Gregory Blanc **/ Télécom Sud Paris**

L'objectif du projet VARIoT (Vulnerability and Attack Repository for IoT) est de créer un service fournissant des informations exploitables sur les objets IoT que l'on puisse traiter manuellement ou automatique, afin d'en assurer la sécurité. Les données pertinentes seront mises à disposition via le portail européen de données (EDP, data.europa.eu) ainsi que via d'autres interfaces telles que la plateforme MISP, et les flux quotidiens de remédiation de Shadowserver. Le projet VARIoT est co-financé par l'outil de financement CEF (Connecting Europe Facility) de l'Union Européenne et par le programme du Ministère Polonais des Sciences et de l'Education Supérieure.
Les principaux résultats du projet sont 1) une base de données sur les vulnérabilités des objets IoT et leurs codes d'exploitation, 2) les mécanismes de corrélation des divers types d'information, 3) un moteur de recherche sur les informations de vulnérabilités, 4) des catalogues de types d'objets IoT et les codes malveillants (malware) associés, 5) des campagnes de scan Internet identifiant les objets IoT vulnérables et publiquement accessibles, 6) un système de détection d'anomalies réseaux des objets IoT, 7) des documents de type Internet Draft décrivant les données ouvertes du projet et leur implémentation dans MISP, et 8) des statistiques agrégées et anonymisées sur les objets IoT infectés et vulnérables.

Anna Felkner est la coordinatrice du projet VARIoT. Elle est professeure assistant et responsable du département « Information Security Methods » au NASK PIB (centre de recherche et développement du « Research and Academic Computer Network »). Ses intérêts de recherche couvrent le contrôle d'accès, la modélisation de la confiance, l'analyse de risques et la gestion de vulnérabilités, les cadres de confiance, la gestion nationale de la cybersécurité et la coopération dans un contexte de cybersécurité. Elle est titulaire d'un doctorat en technologie de l'information de l'université de technologie de Varsovie. Elle a participé à de nombreux projets de recherche nationaux et à financement européen, a co-écrit plus d'une quarantaine de publications et est intervenue dans de nombreuses conférences.

Gregory Blanc est responsable du lot 4 sur l'analyse comportementale des objets IoT et des codes malveillants. Il est maître de conférences à Télécom Sud Paris et en charge de la spécialisation de fin de cursus ingénieur en Sécurité des Systèmes et des Réseaux (SSR). Titulaire d'un doctorat du NAIST (Japon), ses intérêts couvrent la détection d'intrusion, la migration d'attaques, la virtualisation réseau, et les interactions entre IA et cybersécurité.

Institut Mines-Télécom

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 8 juin 2022

11h30 à 12h

La sécurité des protocoles de communications de l'IoT - Exemple du BLE

Romain Cayre **/ Apsys Lab / LAAS-CNRS** et Vincent Nicomette **/ INSA Toulouse / LAAS-CNRS**

Le protocole Bluetooth Low Energy (BLE) s'est imposé comme l'un des protocoles de communication sans fil les plus populaires pour l'Internet des Objets (IoT). Malheureusement, diverses attaques visant le protocole ou ses implémentations ont été publiées récemment, illustrant à la fois l'intérêt croissant pour cette technologie mais aussi sa fragilité du point de vue de la sécurité. Cette présentation vise à présenter un panorama des attaques les plus connues ciblant ce protocole, mais aussi une nouvelle attaque, nommée InjectaBLE, permettant d'injecter du trafic malveillant dans une connexion établie, ce qui restait jusqu'à présent un défi technique. La vulnérabilité exploitée étant inhérente à la spécification du protocole, elle touche de fait l'ensemble des connexions BLE, indépendamment des équipements utilisés, la rendant particulièrement critique. Dans cette présentation, nous décrivons les fondements théoriques de l'attaque, son implémentation en pratique et quelques exemples de scénarios d'attaques.

Romain Cayre est doctorant CIFRE, dans le cadre d'une collaboration entre Apsys.Lab et le LAAS-CNRS. Il est membre de l'équipe TSF (Tolérance aux Fautes et Sûreté de Fonctionnement Informatique). Ses travaux de thèse portent sur la sécurité des protocoles de communication de l'IoT, à la fois d'un point de vue offensif et défensif. Il est également l'auteur de plusieurs outils et preuves de concept en source libre, tels que Mirage, InjectaBLE et RadioSploit (https://github.com/RCayre).

Vincent Nicomette est enseignant à l'INSA de Toulouse et chercheur dans l'équipe Tolérance aux Fautes et Sûreté de Fonctionnement Informatique du LAAS-CNRS. Ces principaux travaux de recherche concernent la sécurité des couches basses du logiciel, la sécurité des systèmes embarqués critiques et la sécurité des communications, en particulier celles de l'IoT.

cdefi
Conférence des Directeurs des Écoles Françaises d'Ingénieurs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 8 juin 2022

12h à 13h

Tout votre code nous appartient : une histoire d'utilisateurs antagonistes

Grégoire Menguy et Sébastien Bardin **/ CEA**

Les programmes peuvent intégrer des informations précieuses comme des algorithmes propriétaires ou des clés cryptographiques. Des attaquants peuvent tenter de les extraire pour porter atteinte à la propriété intellectuelle ou contourner les protections légitimes du programme. Ces situations sont modélisées dans le scénario Man-At-The-End (MATE), où un utilisateur privilégié est lui-même l'attaquant et essaie d'extraire des informations secrètes du programme en ayant recours à un large panel d'attaques (reverse du code, simulation, réécriture, etc.). L'obfuscation de code permet de répondre à ce défi en transformant un programme P en un programme équivalent P' plus complexe à comprendre ou modifier (en temps ou en argent). Face à cela, des méthodes dites de désobfuscation tentent de récupérer un code proche de l'original à partir de sa version obfusquée pour aider la rétro-ingénierie. L'obfuscation et la désobfuscation ont donc des objectifs opposés. À l'image d'autres domaines en cybersécurité, il est nécessaire de bien connaître les attaques et protections existantes ainsi que leurs évolutions afin de protéger de manière efficace la propriété intellectuelle contenue dans un programme. Dans cette présentation, nous présenterons le contexte MATE et exposerons rapidement les approches d'obfuscation et déobfuscation usuelles, puis nous présenterons les dernières avancées du domaine, notamment les méthodes dites de déobfuscation symboliques et les méthodes en boîte noire.

Grégoire Menguy est ingénieur spécialisé en cybersécurité et certifié ESSI par l'ANSSI. Il est actuellement doctorant au CEA LIST dans l'équipe Binsec, sous la direction de Sébastien Bardin, où ses recherches se concentrent sur l'utilisation des méthodes d'intelligence artificielle et de machine learning pour la rétro-ingénierie et la désobfuscation.

Sébastien Bardin est chercheur au CEA LIST, où il a fondé et dirige le groupe BINSEC dédié à l'analyse formelle de programmes exécutables pour la sécurité – avec notamment des applications en termes d'analyse de vulnérabilités, reverse et déobfuscation ou encore protection de code. Sébastien s'est notamment intéressé aux techniques de déobfuscation symbolique, à leur mise en œuvre efficace et à la conception de protections dédiées, et plus récemment aux approches boite noire pour le reverse de code. Ces travaux ont été présentés dans les meilleurs conférences internationales académiques (S&P, CCS) et industrielles (Black Hat). Sébastien est Docteur en Informatique de l'ENS Cachan, ACM Senior Member et Fellow du CEA

cea

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 8 juin 2022

15h à 15h30

L'IA data-centric pour stopper les attaques ciblant les données

Belkacem Teibi **/ Inria / Daspren** et Mathieu Thiery **/ Inria / Daspren**

Aujourd'hui, la première cible des cyberattaques est la donnée. Des ransomware de plus en plus sophistiqués en font tous les jours la démonstration. Les solutions de protection existantes, basées massivement sur l'analyse de binaires ou de leur comportement, sont continuellement mises en difficulté par les nouvelles menaces inconnues. Leur stratégie de défense est donc insuffisante. Un point est constamment négligé : la donnée elle-même. En effet les ransomware ont pour but premier d'altérer les données pour que celles-ci soient inexploitables, pourtant très peu de solutions les prennent en considération, ou alors en utilisant des techniques encore trop rudimentaires. Une réponse à cette problématique s'impose : l'intelligence artificielle centrée sur les données.

Belkacem Teibi est responsable du développement stratégique de Daspren. Ingénieur R&D en sécurité informatique avec une expérience dans l'industrialisation et le transfert de l'innovation au sein Inria. Belkacem est aussi diplômé d'un Executive MBA à Rennes School Business.

Mathieu THIERY est responsable du développement technique de Daspren. Docteur en sécurité et protection de la vie privée, Mathieu a précédemment travaillé dans une start-up sur le développement d'un driver noyau cryptographique.

Inria

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 8 juin 2022

15h30 à 16h

HEIR – Une plate-forme globale de sécurité pour les environnements médicaux

Michalis Smyrlis **/ SPHYNX** et Hervé Debar **/ Institut Mines Télécom**

HEIR (Grant Agreement 883275 – heir2020.eu) est un projet de recherche et d'innovation de la Commission Européenne qui a pour but de développer une plate-forme d'identification des vulnérabilités et de gestion du risque tant au niveau local (hôpital, centre médical) qu'au niveau national (régulateurs et autorités). Les capacités de la plate-forme HEIR en termes d'analyse de la menace incluent des fonctions de Machine Learning pour identifier les menaces les plus répandues dans les systèmes médicaux connectés. Les informations sur la menace sont agrégées sous forme d'un vecteur et d'une valeur de risque, le Risk Assessment of Medical Applications (RAMA). Le RAMA mesure le niveau de risque de chaque objet de santé et permet une analyse détaillée du risque dans les environnements médicaux.

Michalis Smyrlis est le Chief Software Engineer de SPHYNX TECHNOLOGY SOLUTIONS AG. Ses centres d'intérêt se focalisent sur la sécurité du logiciel, la protection des données personnelles, l'analyse de risque et l'analyse de donnes massives. Expert dans le développement de cybersécurité, il a contribué à de nombreux projets européens sur l'analyse de données et les plates-formes de cybersécurité. Sa recherche se focalise sur l'analyse de risque pour les systèmes cyber utilisant des méthodes hybrides et continues.

Hervé Debar est professeur, directeur de la recherche et des formations doctorales à Télécom SudParis, une école de l'Institut Mines-Télécom. Il travaille dans le domaine de la cybersécurité depuis plus de 30 ans, tant dans le secteur privé que dans la recherche académique. Ces domaines de recherche couvrent la détection d'intrusions, la corrélation d'alertes, la remédiation et la lutte contre les attaques cyber.

Institut Mines-Télécom

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 8 juin 2022

16h à 16h30

Injection de fautes par laser dans un microcontrôleur

Jean-Luc Danger **/ Télécom Paris**

Cet exposé présente comment un microcontrôleur 32 bits (MCU) peut être mis en défaut par injection de fautes par laser (LFI). La faute peut alors être exploitée pour dévoiler les secrets du logiciel exécuté par le MCU et de l'architecture du dispositif. Des expériences ont été menées sur un processeur ARM Cortex M0+ avec un MCU SAMD21. La première opération de génération de fautes consiste à localiser les points de vulnérabilité dans l'architecture du MCU, de la mémoire Flash jusqu'au pipeline d'exécution du processeur en passant par le bus interne et le cache. Il est notamment montré que les fautes peuvent être créées le long de ce chemin et sont particulièrement faciles à générer sur le buffer de l'interface Flash. Le modèle de faute peut être soit un « saut d'instruction » équivalent à un remplacement par une instruction NOP, soit un « rejeu d'instruction » où l'instruction courante est rejouée et la nouvelle instruction n'est pas exécutée. L'étude présente également l'impact de la largeur d'impulsion du laser et de la puissance du laser. Elle montre qu'il est possible d'injecter des fautes multiples en augmentant la largeur d'impulsion. Deux contre-mesures logicielles permettant soit d'être résiliente soit de détecter le type de faute « saut d'instruction » sont présentées. L'une repose sur la duplication du code, l'autre sur l'utilisation d'une instruction sensible.

Jean-Luc Danger est professeur à Télécom Paris. Il est responsable de l'équipe de recherche SSH dont les thèmes de recherche sont la sécurité/sûreté des systèmes embarqués, les architectures configurables, l'implémentation d'algorithmes complexes dans des ASICs ou des FPGAs. Jean-Luc est l'auteur de plus de 250 publications scientifiques, 25 brevets, a encadré 18 thèses et co-fondé la société Secure-IC.

Institut Mines-Télécom

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE: 8 juin 2022

16h30 à 17h

Traçage par empreintes de navigateur : passé, présent et évolutions futures

Pierre Laperdrix **/ CNRS**

Les empreintes de navigateur, ou "browser fingerprinting" en anglais, ont beaucoup évolué depuis leurs débuts en 2010. Grâce à un script qui collecte des données depuis un navigateur web, une société peut apprendre beaucoup d'informations sur un individu, son terminal et la configuration utilisée. Plusieurs études ont montré que les empreintes de navigateur représentent une menace réelle pour la vie privée des utilisateurs car elles peuvent remplacer les cookies pour retracer des historiques de navigation.
Dans cette présentation, nous donnerons un aperçu de la recherche effectuée dans le domaine du fingerprinting en expliquant comment cette technique fonctionne, comment elle est utilisée aujourd'hui avant de se pencher sur son futur.

Pierre Laperdrix est actuellement chargé de recherche au CNRS dans l'équipe Spirals du laboratoire CRIStAL à Lille. Auparavant, il était chercheur postdoctoral dans le laboratoire PragSec de l'université de Stony Brook et, ensuite, dans le Secure Web Applications Group à Cispa. Ses sujets de recherche couvrent principalement la sécurité et le respect de la vie privée sur Internet. L'un des objectifs de ses recherche est de comprendre ce qui se passe sur le web afin de concevoir des contre-mesures pour mieux protéger les utilisateurs en ligne.

cnrs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 9 juin 2022

10h à 11h

Sûrs et sécurisés : de la sûreté de fonctionnement à la détection des intrusions orientée processus dans les systèmes industriels.

Stéphane Mocanu **/ Inria CTRL-A**

Cette présentation propose une vision de la cybersécurité des systèmes industriels combinant les aspects sûreté et sécurité. Nous positionnons le problème de la détection des intrusions orientée par rapport aux approches normatives concernant la sûreté des systèmes industriels. Les attaques dites "orientées processus" ciblent directement les propriétés de sûreté du processus physique contrôlé. Ces attaques sont souvent « furtives » dans le sens où elles ne vont pas violer les spécifications des protocoles de communication mais vont plutôt forcer des valeurs des variables du processus afin de mènes le procédé physique dans un état dangereux. Par conséquent, les techniques de détection d'intrusions doivent intégrer les propriétés de sûreté du procédé physique afin de détecter les commandes malveillantes. Dans cette présentation nous évoquons l'état de l'art de la détection des intrusions orientée processus, quelques résultats récents les verrous et les limites de l'approche.

Stéphane Mocanu a obtenu un Doctorat en Automatique en 1999 à Grenoble-INP. Il est Maître de Conférences à Grenoble-INP et au Laboratoire d'Informatique de Grenoble (LIG, UMR 5217 CNRS/G-INP/UGA) dans l'équipe commune Inria CTRL-A. Il a commencé la recherche sur la cybersécurité des systèmes industriels en 2012. Il est responsable d'une plateforme expérimentale pour les tests de pénétration et la recherche des vulnérabilités des systèmes industriels. (http://lig-g-ics.imag.fr/).

cdefi
Conférence des Directeurs des Écoles Françaises d'Ingénieurs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 9 juin 2022

11h à 11h30

Sécurité 6G adaptée au contexte : le rôle de la couche physique

CHORTI Arsenia **/ ETIS / UMR8051 / CYU / ENSEA / CNRS**

La qualité de la sécurité (QoSec) est envisagée comme un cadre flexible pour les futurs réseaux avec des exigences non fonctionnelles très diverses (délais, consommation d'énergie, connectivité massive / évolutivité, puissance de calcul, etc.). Parallèlement, l'intégration des communications et de la détection (sensing), ainsi que de l'intelligence artificielle embarquée, peuvent fournir les bases de l'élaboration de protocoles de sécurité autonomes et adaptatifs. À l'image du paradigme des réseaux à services différenciés (DiffServ), différents niveaux de sécurité pourraient être conceptualisés, s'éloignant ainsi des contrôles de sécurité statiques, actuellement pris en compte dans les architectures de sécurité à confiance zéro (zero-trust). En 6G, nous envisageons des contrôles de sécurité autonomes et adaptatifs, orchestrés par un plan de sécurité vertical en coordination avec un plan sémantique vertical, appelé sécurité 6G contextuelle. C'est dans ce cadre que nous envisageons l'incorporation de schémas de sécurité de la couche physique (PLS) dans les protocoles de sécurité 6G, introduisant pour la première fois des contrôles de sécurité à toutes les couches. Dans cet exposé, nous discuterons de la manière dont la sécurité de la couche physique (PLS), naturellement adaptative, s'inscrit dans le cadre de la QoSec ; nous proposerons ensuite une route pour son incorporation dans la 6G, en tirant parti de l'adaptation des paramètres de transmission aux hypothèses de sécurité sous-jacentes. Enfin, nous présenterons des exemples l'authentification et de génération de clés secrètes (SKG) basées sur les empreintes RF dans des données réels et nous discuterons de la possibilité d'une détection légère et distribuée des anomalies au niveau de la couche matérielle pour les réseaux à grande échelle de l'Internet des objets (IoT), composés de dispositifs contraints.

Arsenia (Ersi) Chorti est professeur à l'École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), co-directrice du groupe Information, Communications et Imagerie (ICI) du laboratoire ETIS UMR 8051 et chercheuse invitée aux universités de Princeton et d'Essex ainsi que le Barkhausen Institut. Ses recherches couvrent les domaines des communications sans fil et de la sécurité des systèmes sans fil pour la 5G et la 6G, avec un accent particulier sur la sécurité de la couche physique. Elle est membre senior de l'IEEE, membre de l'IEEE INGR on Security, du Pole Competitive Systematic et du Jury de Meilleure Thèse de GdR ISIS. Depuis octobre 2021, elle préside le groupe de réflexion (focus group) de l'IEEE sur la sécurité de la couche physique.

cdefi
Conférence des Directeurs des Écoles Françaises d'Ingénieurs

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 9 juin 2022

11h30 à 12h

Réduire à zéro les attaques de type zero-day grâce à un modèle de comportement cohérent des programmes

Byron Hawkins **/ Inria / Introspicion**

Selon une analyse du MIT, 66 vulnérabilités zero-day ont été identifiées en 2021, contre 37 en 2020. Certaines peuvent être valorisée à plus de 1 million de dollars. Les attaquants ont investi des millions de dollars par an dans l'acquisition de vulnérabilités zero-day et les dommages causés par les attaques se chiffrent en milliards de dollars. Tous les types d'acteurs sont visés, des très grandes entreprises aux petites et moyennes entreprises, en passant par les institutions et les particuliers. Ces attaques exploitent diverses vulnérabilités logicielles engendrées par la complexité croissante de logiciels qui s'immiscent toujours plus profondément dans nos systèmes. La prévention de ces vulnérabilités nécessiterait des ressources astronomiques. La sécurité réactive est donc privilégiée, mais les attaques avancées ne sont pas nécessairement visibles de l'extérieur des applications ciblées tandis que les mécanismes de surveillance actuels ne sont pas en mesure d'évaluer avec précision le comportement interne des dites applications.
Face à ce constat, les solutions logicielles d'Introspicion permette une analyse rapide et précise des exécutions binaires. Nous proposons deux approches : (1) l'introspicion réactive assimilable à une EDR, surveille et signale en permanence les anomalies éventuelles en fonction d'un profil de comportement logiciel déterminé par une analyse préliminaire ; (2) l'introspicion proactive vise à étendre la découverte de vulnérabilités hors ligne en se basant sur un modèle des chemins d'exécution normaux et un modèle des flux de données.
Un défi résultant de cette approche est la quantité de données à gérer. Une réalisation purement logicielle ne serait pas assez efficace. C'est pourquoi nos solutions s'appuient sur des modules de traçage CPU (Intel PT, ARM CoreSight) qui permettent d'observer tous les détails d'un thread ou d'un chemin d'exécution avec un coût (taux de ralentissement) inférieur à 1% pour un logiciel typique.

Byron Hawkins a obtenu en 2017 une thèse de l'Université de Californie qui apporte une contribution à la détection d'attaques de type zero-day. En parallèle, il a développé des innovations en cybersécurité dans le cadre de stages chez Google (fuzzing guidé sous Dr. Memory) et Microsoft (chiffrement des pointeurs sensibles sous Visual Studio). Il a ensuite rejoint Inria et s'y est intéressé aux algorithmes de graphes et à la compression de traces d'exécution de logiciels. Depuis 1 an, il cherche à transférer ces différents apports et est ainsi accueilli par l'Inria Startup Studio pour maturer le projet et travailler son intégration dans l'écosystème cyber français.

Inria

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 9 juin 2022

15h à 15h30

Nijta: une solution d'anonymisation de la voix pour protéger la vie privée des locuteurs

Brij Mohan Lal Srivastava **/ Inria**

La définition actuelle d'un business model centré sur le client est incomplète sans des composants de traitement automatique de la parole qui visent à répondre efficacement aux besoins des clients. Cependant, le déploiement de ces composants entraîne une collecte de données vocales à grande échelle, contenant potentiellement des informations privées, sensibles et identifiant personnellement les locuteurs.
Les lois européennes sur la protection de la vie privée telles que le RGPD exigent l'anonymisation des données et la suppression des informations biométriques des données vocales collectées. Nous relevons ce défi en fournissant une plate-forme d'anonymisation vocale robuste et sécurisée, Nijta, qui supprime rapidement les informations identifiant les locuteurs de leurs données vocales.
Le processus d'anonymisation accorde un large accès à ces données aux organisations, tout en leur permettant d'interagir avec leurs clients, en confiance, conformément au RGPD. De plus, il améliore l'utilisabilité des données clients pour optimiser les principaux composants métier tels que les systèmes de transcription vocale, conduisant à une extraction plus précise des métadonnées de la voix, par exemple les préférences des clients, les émotions, etc.

Brij Mohan Lal Srivastava est le porteur du projet Nijta à Inria Startup Studio situé à Lille. Auparavant, lors de sa thèse à Inria Lille et Nancy, il a travaillé avec les équipes Magnet et Multispeech pour étudier le sujet de la vie privée dans le traitement de la parole. Avec ses collaborateurs Nathalie Vauquier et Seyed Ahmed Hosseini, il travaille actuellement à la création d'une startup pour fournir un service commercial d'anonymisation de la voix aux centres d'appels et aux médias.

Inria

ALLISTENE
l'alliance des sciences et technologies du numérique

DATE : 9 juin 2022

15h30 à 16h

La résilience de la cryptographie post-quantique aux attaques physiques

Mikael Carmona **/ CEA**

La transition de la cryptographie classique à la cryptographie post-quantique est lancée. Les premiers crypto systèmes standardisés par le NIST seront connus en 2022 et des produits intégrant cette nouvelle cryptographie sont déjà sur le marché. Le processus de standardisation du NIST a éprouvé la résistance de ces nouveaux crypto systèmes aux attaques quantiques, qu'en est-il de leur résilience aux attaques physiques ? Dans cet exposé, nous présenterons le panorama des crypto systèmes post-quantiques sélectionnés par le NIST ainsi que les vulnérabilités identifiées aux attaques physiques. Un focus particulier sera proposé sur les schémas SIKE et HQC dont des vulnérabilités aux attaques physiques ont été révélés par le CEA-Leti et publiés à des congrès internationaux dont la 3ième conférence PQC organisée par le NIST en 2021.

Mikael Carmona est ingénieur diplômé de l'INPG (2007), agrégé de mathématiques (2007) et docteur diplômé de l'INPG en traitement du signal (2011). Ingénieur-Chercheur au CEA-Leti de 2011 à 2015 sur la thématique des réseaux de capteurs et du digital twin des structures, il co-fonde la start-up Morphosense en tant que CTO dans lequel il contribue à l'établissement et l'exécution des roadmaps Technologiques et Opérationnelles. En 2021, il intègre le service Cybersécurité du CEA Leti sur le domaine de la cryptographie post-quantique et des générateurs de nombres aléatoires. Il est à ce jour Chef du Laboratoire Sécurité des Composants.

cea

ALLISTENE

l'alliance des sciences
et technologies du numérique