Laboratoire de cryptologie et de virologie opérationnelles
$(C+V)^O$

Rapport d'activité 2018

- § -

ESIEA

Axe Confiance Numérique et Sécurité

Table des matières

Axe Confiance Numérique et Sécurité/laboratoire $(C+V)^O$

Présentation du laboratoire et de l'axe de recherche

Le laboratoire de cryptologie et de virologie opérationnelles $(C+V)^O$ est présent à l'ESIEA Laval depuis juillet 2007. Il a d'abord fonctionné en collaboration avec le laboratoire de virologie et de cryptologie de l'École Supérieure et d'Application des Transmissions (ESAT) de Rennes (période juillet 2007 - mai 2008), puis ce laboratoire a accueilli définitivement la ressource ESAT (son directeur de laboratoire et une dizaine de chercheurs associés) fin juin 2008. La période 2007 - 2008 a donc constitué une phase de transition. Les activités de recherche courantes ont été faites au nom des deux laboratoires pour cette période, néanmoins avec une nette prééminence du laboratoire lavallois.

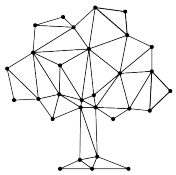
Du fait de cet héritage, l'activité de recherche du laboratoire s'inscrit dans la continuïté et conserve des liens forts non seulement avec le ministère de la Défense mais également avec les ministères de la Justice et de l'Intérieur. Cela concerne à la fois une partie des thématiques de recherche du laboratoire, la création et le maintien d'un environnement sécurisé pour mener l'activité de recherche dans le respect des principales réglementations en la matière (sécurisation des locaux, habilitation des personnels, audits).

La sécurisation du laboratoire (phase I) en conformité avec la réglementation a été finalisée en 2011 avec pour principal changement, le passage sous tutelle exclusive du ministère de la Défense. Le laboratoire a désormais la capacité de mener des travaux classifiés dans le respect des réglementations existantes. Il dispose également d'un réseau informatique dédié, hautement sécurisé. Courant 2017 (dossier initié en 2015, validé en 2016), compte tenu de l'évolution de la réglementation (circulaire interministérielle $N°$ 3415/SGDSN/AISTfPST du 7 novembre 2012), le laboratoire est passé sous tutelle administrative de la DGSI et opérationnelle des ministères de la Défense et de l'Intérieur. En 2013, les deux premières thèses classifiées ou confidentielles ont été soutenues.

Depuis fin 2011, le laboratoire assure l'organisation et la direction scientifique du mastère spécialisé international (en langue anglaise) *Network & Information Security* (MS N&IS).

En 2014, dans le cadre de la réorganisation de la recherche, le laboratoire pilote l'un des deux axes de recherche du groupe ESIEA dénommé « *Confiance Numérique et Sécurité* ». Le laboratoire prend alors pour acronyme $CNS/(C+V)^O$.

Depuis 2015, le laboratoire pilote, anime et gère, en plus du MS N&IS, le parcours sécurité de l'ESIEA qui se répartit de la deuxième année à la 4ème année pour tous les étudiants et permet une spécialisation en 5ème année dans le domaine ce la cybersécurité (site officiel : `www.esiea.fr/parcours-securite`). Les deux formations, parcours sécurité ingénieur option cybersécurité et le mastère S&IS ont recu le label *SecNumEdu* de l'*Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) le 24 janvier 2017. Depuis 2016, le laboratoire est rattaché



SecNumedu

ANSSI

à l'école doctorale SMI d'Arts & Métiers - ParisTech (ENSAM), l'école doctorale de l'École Polytechnique à laquelle était rattachée le laboratoire historiquement ayant été dissoute, suite à la réforme des universités.

Le laboratoire $CNS/(C+V)^O$ s'ouvre très tôt dans la formation aux étudiants curieux et volontaires. Le laboratoire pilote le dispositif « Espoir Recherche », il met en avant la formation par la recherche. En effet, les formations de l'ESIEA (Diplôme d'Ingénieur, MS N&IS) se veulent opérationnelles et les étudiants ont une activité de projets importante et ce, dès la deuxième année de leur formation. Lorsque ces projets sont en connexion directe avec des activités de recherche du laboratoire $CNS/(C+V)^O$, l'émulation générée par les enjeux permet d'envisager de nombreuses innovations pédagogiques et d'associer les étudiants à des problèmes réels de recherche et développement (contrats, expertises, recherches en cours, formations spécialisées à la carte...).

Enfin, le laboratoire vise, notamment via la recherche, à développer l'esprit citoyen et l'esprit de défense auprès de ses chercheurs et étudiants. Les questions d'Éthique, de réglementation et de défense des valeurs démocratiques et citoyennes sont une préoccupation majeure et constante au sein du laboratoire. Le but est de donner à nos étudiants non seulement une formation scientifique solide mais également une formation morale forte.

Thèmes de recherche

Le laboratoire de cryptologie et de virologie opérationnelles a pour thème principal de recherche la sécurité informatique dans le domaine de la lutte informatique défensive avec applications opérationnelles à la lutte informatique offensive.

Privilégiant à la fois l'approche théorique — pour maintenir une compétence académique élevée — et une recherche appliquée inspirée de problèmes concrets (issus du monde gouvernemental mais également du monde industriel) — l'objectif principal est non seulement de comprendre les attaques informatiques actuelles, mais également et surtout, de prévoir et d'inventer les attaques futures en considérant un champ informationel élargi. Cette démarche pro-active permet d'anticiper la menace (domaine défensif) et, dans un contexte d'évolution de la doctrine française, de se doter d'un arsenal technique dans le domaine offensif (domaine étatique), le maître mot dans les deux domaines étant la capacité opérationnelle.

Cette vision et les compétences qui en découlent sont de nature à également intéresser fortement les entreprises, qui sont, dans un contexte de complexité croissante des systèmes d'information d'une part, et de forte concurrence industrielle d'autre part, de plus en plus soumises aux attaques informatiques et informationnelles, en particulier ciblées.

Les principaux thèmes de recherche sont les suivants :

- Cryptologie symétrique. Dans ce type de cryptologie, l'émetteur et le destinataire partagent

une même clef secrète. Cette dernière doit donc être mise en place préalablement à la communication. Elle est utilisée principalement pour réaliser la confidentialité de volumes inportants d'information durant leur stockage, leur transmission et leur traitement. Les principaux sous-thèmes traités au laboratoire sont :

(a) Étude combinatoire des primitives cryptographiques en vue de la caractérisation de faiblesses pouvant être exploitées dans la cryptanalyse (attaque) de systèmes de chiffrement.

(b) Conception et évaluation de systèmes de chiffrement symétriques.

(c) Conception de systèmes cryptographiques **avec trappes** (introduction de faiblesses mathématiques indétectables permettant une cryptanalyse moins complexe pour quiconque a la connaissance de la trappe).

(d) Cryptanalyse de systèmes symétriques fondée sur la vision combinatoire de ces systèmes.

(e) Techniques de reconstruction d'algorithmes inconnus à partir des éléments interceptés (messages codés, messages chiffrés).

- Analyse et conception de systèmes stéganographiques. Les données chiffrées ayant un profil statistique particulièrement caractéristique, un attaquant peut, par conséquent, facilement identifier un échange de données chiffrées. Il est donc capital dans certains contextes de cacher l'existence même (stockage, échange) de ces dernières. C'est le rôle de la stéganographie (dissimulation du canal).
- Virologie informatique :

  (a) Caractérisation formelle des techniques virales (connues et inconnues).

  (b) Étude et conception de nouvelles technologies virales. L'objectif est de comprendre comment fonctionnent les principales techniques virales et comment ces dernières sont susceptibles d'évoluer. Le principe général est que toute défense est illusoire si elle ne se nourrit pas de la connaissance et de la vision de l'attaquant dont la principale démarche est l'innovation et l'inventivité. À ce titre la prospection et l'évaluation de techniques de conception de codes malveillants, de la théorie à la pratique — dans le strict respect de la réglementation en vigueur et en liaison avec les services compétents de l'État — est indispensable.

  (c) Formalisation et conception de techniques antivirales. Analyse automatique de malwares, par exemple, en utilisant la notion de distance d'information ou des techniques d'analyse combinatoire. Une autre idée importante est de changer la *granularité* de la comparaison, en passant au niveau des fonctions (ou des blocs d'instructions) nous obtenons de bien meilleurs résultats.

  (d) Mathématiques et cryptographie malicieuse (utilisation du potentiel mathématique et cryptographique dans les techniques virales et utilisation des codes viraux à des fins de cryptanalyse).

  (e) Analyse et évaluation des logiciels antivirus.

- Analyse et étude techniques du concept de guerre informatique. Si les concepts « théoriques » de la guerre informatique commencent à émerger — essentiellement chez les historiens, les sociologues et spécialistes en relations internationnales — il n'existe pratiquement aucune recherche, du moins connue à ce jour, sur les concepts opérationnels touchant à la préparation, la planification et la conduite de « cyberattaques ». Le laboratoire étudie sur

une base technique et opérationnelle les différents scénarii qui peuvent être mis en œuvre par les attaquants que ce soit à un niveau local (simple infrasctructure de type société ou installation critique) ou à un niveau plus large (région, territoire, pays). Cette connaissance peut être en particulier très utile aux entreprises qui sont les cibles privilégiées de ce type d'attaques.

- Sécurité réseau (défensif et offensif). Cybersurveillance (innovation dans le domaine des SOC/SIEMG). Nouvelles méthologie d'audit. Collecte et gestion des traces. Un des aspects primordiaux est la prise en compte des défis techniques tout en garantissant la protection de la vie privée et la confidentialité des données.
- Carte à puce, RFID, NFC, HackRF et analyse de trains binaires, sécurité des environnements embarqués et des objets connectés : développement d'applications et de protocoles sécurisés. Ces environnements extrêmement contraints (en terme de ressources et de puissance) nécessitent une déclinaison spécifique des méthodes, fonctionnalités et outils de la sécurité. En outre, l'évolution des attaques montre que ces dernières se déplacent de plus en plus de la couche logicielle vers la couche physique (firmware et électronique). Il est donc important de développer et de maintenir une compétence dans ce domaine.
- Techniques d'OSINT, d'extraction de connaissances (*data mining, machine learning, big data...*), algorithmique et combinatoire des structures complexes, appliquées à la sécurité et au renseignement.
- Sécurité des infrastructures critiques. Analyse pro-active de scénarii terroristes. Initiée en 2016, à la suite de travaux du laboratoire, le but est d'analyser et d'imaginer les possibilités de scénarii terroristes possibles en fonction du type de cibles (infrastructures critiques, cibles molles) en combinant l'expérience opérationnelle (et en particulier la MRT) avec les outils prédictifs dans le domaine de l'analyse de données et des techniques d'extraction de connaissances.

Composition du laboratoire

La composition du laboratoire au 31 décembre 2018 est la suivante.

- Directeur du laboratoire (et officier de sécurité)

  Eric Filiol (Ing. - Ph D - HDR).
  Email : `eric.filiol@esiea.fr`
  Site web : `http://sites.google.com/site/ericfiliol/`
  Blog : `http://cvo-lab.blogspot.com/`
  Tél : +33(0)2 43 59 46 09
  Fax : +33(0)2 43 59 46 02

- Adjoint, RSSI du laboratoire

  Richard Rey (Ingénieur de recherche)
  Email : `richard.rey@esiea.fr`
  Sécurité réseau, sécurité radio et télécommunications, électronique, guerre électronique, audits de sécurité, pentesting.

- Personnels permanents

  — Jean-Pierre Aubin - Technicien de recherche (MS N&IS)
  Email : `jean-pierre.aubin@esiea.fr`
  Sécurité des applications - Programmation et développement sécurisés, sécurité réseau, audits de sécurité.

- Chercheurs associés

  — Paul Irolla
  Email : `paul.irolla@esiea.fr`
  Virologie, sécurité des applications et environnements mobiles, combinatoire.

  — Alexandre Triffault
  Email : `alexandre.triffault@esiea.fr`
  Sécurité physique et des contrôles d'acc'es, hacking.

- Doctorants

  — Baptiste David
  Email : `baptiste.david@esiea.fr`
  Virologie, programation système noyau (Windows), reverse-engineering.

  — Maxence Delong
  Email : `maxence.delong@esiea.fr`
  Sécurité réseau, OSINT, algorithmique.

  — Joanna Moubarak
  Université Saint-Joseph, Beyrouth, Liban
  Virologie, technologie blockchain.

- Espoirs recherche.
  Dans le cadre de la promotion de la recherche auprès des étudiants, le laboratoire identifie chaque année des étudiants particulièrement prometteurs ou motivés tant sur le plan scientifique que du point de vue des dispositions pour la recherche.
  Ces étudiants font l'objet, durant toute leur présence en scolarité, d'un encadrement spécifique et adapté, en plus du cursus obligatoire. Leur objectif est, souvent, après leur diplôme d'ingénieur, de préparer une thèse.

  — Bachelot Dorian (3A)
  Sécurité électronique, reverse-engineering matériel.

  — Barbier Alexandre (4A)
  Cryptographie symétrique, analyse cryptographique.

  — Béclair Louis (5A)
  Programmation, Cryptographie, Data-Mining et analyse de données.

— Cisterna Nicolas (2A)
Sécurité de l'information, programmation, cryptographie.

— De Faria Katarina (4A)
Sécurité des systèmes, systèmes SCADA, CyberRange (Stormshield).

— Dugué Clovis (3A)
Programmation, sécurité système Linux.

— Échard Lucas (4A)
CyberRange (Stronmshield), cybersurveillance et technologie SOC

— Grondin Matthieu (2A)
Cryptographie symétrique, analyse cryptographique.

— Ito Armand (4A)
Programmation et sécurité UEFI.

— KETOBIAKOU Pierre (4A)
Cryptographie symétrique, analyse cryptographique.

— Lardier William (5A)
Programmation, Cryptographie, Data-Mining et analyse de données.

— Maillard Pierre-François (4A)
Programmation et sécurité UEFI.

— Plumerault François (3A)
Virologie, programmation système, UEFI.

— Poujade Florian (2A)
Cryptographie symétrique, analyse cryptographique.

— Rakotondrajao Fabien (4A)
Sécurité des systèmes, hacking, cybersécurité opérationnelle.

— Sprenger Solène (4A)
Programmation et sécurité UEFI.

Thèses et stages

Thèses soutenues en 2018

- Thèse de Paul Irolla. *Formalisation et application des réseaux de neurones à la sécurisation d'Android et d'applications mobiles 3D*. Thèse co-dirigée avec Jean-Philippe Deslys (CEA/DSV) dans le cadre du projet 3D NeuroSecure. Université Paris-sud, ED 419, Biosigne. Soutenance le 19 décembre 2018.

  Composition du jury : Professeur Antonella Santone (University of Molise, Italie - Rapporteur), Professeur Ludovic Apvrille (Telecom ParisTech, Paris - Rapporteur), Professeur Maroun Chamoun (ESIB, Université Saint-Joseph, Liban - examinateur), Dr Akka Zemmari (Laboratoire Bordelais de Recherche en Informatique [LaBRI], Bordeaux - Examinateur), professeur Jean-Philippe Deslys (CEA/DSV, Paris - Directeur de thèse), Éric Filiol (ESIEA, co-directeur de thèse).

Thèses en cours

Depuis 2016, le laboratoire est rattaché à l'école doctorale SMI d'Arts & Métiers - ParisTech (ENSAM) (directrice Anne Bouteville).

- Thèse de Maxence Delong. *Analyse, conception et implémentation d'un nouveau protocole de communication anonyme reposant sur la stéganographie*. École doctorale ENSAM/SMI. Cette thèse a débuté en octobre 2018.

- Thèse de Joanna Moubarak. *Formalisation et implémentation de nouvelles techniques virales informatiques*. Co-direction avec le professeur Maroun Chamoun, Faculté d'Ingénierie de l'Université Saint-Joseph, Beyrouth, Liban. Soutenance prévue pour l'été 2019.

- Thèse de Baptiste David. *Évaluation des mécanismes de sécurité de Windows NG (7, 8 et 10) et conception, mise en œuvre de techniques et outils de durcissement*. École doctorale ENSAM/SMI. Soutenance prévue pour fin 2019.

Stages Master - Mastère et Ingénieur 2018 (cycle M)

- Mohamad Ayache (Liban). *Development of Security Audit Tools*. Projet Mastère Spécialisé N&IS ESIEA, 6 mois. Maître de stage : R. Rey.

- Fabien Bouchain, *Réalisation d'audit de sécurité en entreprises et développement d'outils d'audit*. Stage de fin d'études d'ingénieur, MSc II ESIEA, 6 mois. Maître de stage : R. Rey.

- Godeleine Champenois. *Réalisation d'audit de sécurité en entreprises et développement d'outils d'audit orienté OSINT*. Projet technique/MSc II ESIEA, 6 mois. Maître de stage : R. Rey.

- Cédric Delaunay, *Implémentation sécurisée de l'algorithme de chiffrement Grasshopper sur carte FPGA et analyse de résistance aux attaques DPA*. Stage d'assistant-ingénieur, MSc I ENSTA Bretagne (voie IETA), 4 mois. Maître de stage : E. Filiol.

- Maxence Delong, *Surveillance interne et sécurité du réseau TOR*. Stage MSc II ESIEA, 6 mois. Maître de stage : E. Filiol.

- Abhilash Hota (Inde). *Deep learning and Machine Learning techniques Applied to Security*. Projet Mastère Spécialisé N&IS ESIEA, 6 mois. Maîtres de stage : E. Filiol et Paul Irolla.

- Eliot Rabaud. *Réalisation d'audit de sécurité en entreprises et développement d'outils d'audit*. Projet technique/MSc II ESIEA, 6 mois. Maître de stage : R. Rey.

Publications du laboratoire

Livres et chapîtres d'ouvrages

- Éric Filiol. « *Les risques concernant l'usage des algorithmes dits prédictifs dans le domaine sensible de la Justice* ». Chapitre dans le volume 60 des Archives de Philosophie du Droit sous la direction de Mme Sylvie Lebreton-Derrien, pp. 147–152, éditions Dalloz, novembre 2018.

Revues internationales à comité de lecture

- Paul Irolla & Alexandre Dey. « The Duplication Issue in the Drebin Dataset ». *Journal in Computer Virology and Hacking Techniques*, volume 14, Issue 3, pp. 245–249, août 2018.

Revues nationales à comité de lecture

- Éric Filiol. La réalité du contexte cyber - Menaces, risques et enjeux. *Revues Risques - Les Cahiers de l'Assurance*, numéro 113, pp. 35–42, juillet-août 2016.

Conférences et articles invités (niveau national)

- Éric Filiol. « *Risques liés à l'utilisation des algorithmes dans le domaine sensible de la Justice* ». Colloque sur la Justice prédictive - Risques et avenir d'une justice virtuelle, 6 avril 2018, Laval `https://justice2018.sciencesconf.org`

- Éric Filiol. « *Vol de données et état de l'art dans la gestion opérationnelle et sécurisée des mots de passe* ». Conférence Lenovo, 25 janvier 2018, Hotel Banke, Paris.

Conférences internationales avec comité de sélection et actes

- Alexandre Dey, Loïc Beheshti et Marie-Kerguelen Sido. « *Health State of Google Play Store : Finding Malware in Large Sets of Applications from the Android Market* »4th International Conference on Information System, Security and Privacy (ICSSP'18)/2nd International

Workshop on FORmal Methods in Security Engineering (ForSE) 2017, Funcha, Madeira, Portugal, 22-24 January 2017. ScitePress 2018, pp. 538-544, ISBN 978-989-758-282-0.

- Éric Filiol, Maxence Delong et Nicolas Job. « *Statistical and combinatorial Analysis of the TOR Routing Protocol - Structural Weaknesses Identified in the TOR Network* ». 4th International Conference on Information System, Security and Privacy (ICSSP'18)/2nd International Workshop on FORmal Methods in Security Engineering (ForSE) 2017, Funcha, Madeira, Portugal, 22-24 January 2018. ScitePress 2018, pp. 507-516, ISBN 978-989-758-282-0.
- Maxence Delong, Éric Filiol, Clément Coddet, Olivier Fatou & Clément Suhart. « *Technical and OSINT Analysis of the TOR Foundation* », 13rd International Conference on Cyber Warfare and Security (ICCWS) 2018, National Defense University, Washington DC, USA, March 8-9th, 2018. Academic Conference Publishing International, Jim S Chen & John S. Hurley eds, pp. 164–173, 2018, ISBN 978-1-5108-5963-0.

- Joanna Moubarak, Éric Filiol & Maroun Chamoun. « *On Blockchain Security and Relevant Attacks* ». IEEE-Menacomm, Jounieh, Lebanon, 18-20th April 2018. IEEE 2018, pp. 1-6, ISBN 978-1-5386-1254-5.

- Joanna Moubarak, Éric Filiol & Maroun Chamoun. « *Developping a k-ary Malware Using Blockchain* ». IEEE/IFIP Network Operations and Management Symposium (NOMS'2018), Taipei, Taïwan, 23-27th April 2018. IEEE 2018, pp. 1-5, ISBN 978-1-5386-3416-5.

Conférences internationales avec comité de sélection sans actes

Les présentations (slides) et les vidéos de ces interventions sont disponibles sur le site des conférences correspondantes (en général l'année suivante).

- Éric Filiol. « *Black InfoOps Approach to Evaluate Critical Infrastructure Security* ». InfoSecurity Europe 2018, Geek Street, 7 June 2018, London, `https://www.infosecurityeurope.com/en/Sessions/62467/Black-Info-Ops-Approach-to-Evaluate-Critical-Infrastructure-Security`

- Baptiste David. « *Vulnerability in Compilers Leads to perfect Stealth Backdoor - Part I* ». 11th International Conference on Cybersecurity, Data Privacy and Hacking (C0c0n XI), Kochi, India, 5-6 October 2018, `https://is-ra.org/c0c0n/2018/speakers/agenda`.

- François Plumerault. « *New Hook Method : From the State-of-the-art to a More Efficient One.* ». 11th International Conference on Cybersecurity, Data Privacy and Hacking (C0c0n XI), Kochi, India, 5-6 October 2018, `https://is-ra.org/c0c0n/2018/speakers/agenda`. Le code source est disponible sur `https://github.com/fplu/Safe_Hook`

- Baptiste David. « *Vulnerability in Compilers Leads to perfect Stealth Backdoor - Part II* ». International Hacking Conference Zero NIGHTS 2018, 20-21 November 2018, Saint-Pétersbourg, Russie, `https://2018.zeronights.ru/en/reports/vulnerability-in-compiler-leads-to--stealth-backdoor-in-software/`

- Alexandre Triffault. *Bank Headquarters : Physical Intrusion*. Conférence RTFM - Cybersécurité - Project SIGSEGV1 (RTFM.re), Paris, 6 décembre 2018. Vidéo disponible sur `https://www.youtube.com/watch?v=6bIUnkL820s`

Articles de vulgarisation - Presse technique

Le laboratoire favorise le transfert de connaissances au moyen d'articles techniques et de vulgarisation. Les espoirs-recherche, étudiants ingénieurs de dernière année, sont fortement incités à rédiger de tels articles pour démontrer leur capacité à expliquer clairement des sujets complexes.

- Maxence Delong & Éric Filiol. *Accéder à ses données selon le RGPD : les bons, les brutes et les truands*. Journal SécuritéOff, 18 juin 2018, `https://www.securiteoff.com/acceder-a-ses-donnees-selon-le-rgpd-les-bons-les-brutes-et-les-truands`

- Éric Filiol. *Usurpation d'identité 3.0 - Les évolutions à prévoir*, Journal SécuritéOff, 22 juin 2018, `https://www.securiteoff.com/usurpation-didentite-3-0-les-evolutions-a-prevoir`

- Romain Garnier. *Vers une meilleure sécurité pour les objets connectés*. Journal SécuritéOff, 2 juillet 2018, `https://www.securiteoff.com/vers-une-meilleure-securite-pour-les-objets-connectes/`

Articles en *Open Access*

La publication en *Open Access* devient une tendance lourde, en particulier dans le monde anglo-saxon. Sans sacrifier ni la qualité ni la rigueur scientifique, elle permet de mettre rapidement et gratuitement à disposition de la communauté académique internationale des résultats de recherche théoriques et/ou appliqués aboutis. La publication sur des blogs techniques est également un moyen efficace et immédiat de toucher une communauté spécifique.

Cette forme de publication (en particulier le site `arxiv.org`, géré et maintenu par l'Université de Cornell) bénéficie d'une très large audience (beaucoup plus large que les revues scientifiques traditionnelles). Les chercheurs l'utilisent très souvent pour publier des versions étendues de travaux présentés dans des conférences avec comité de sélection. De plus en plus, il est demandé lors de la soumission à ces dernières, de déposer simultanément un preprint sur ce type de sites.

- Joanna Moubarak, Éric Filiol & Maroun Chamoun. *Developping a K-ary Malware Using Blockchain*. Available on arXiv.org, number 1804.01488, `https://arxiv.org/abs/1804.01488`

- Maxence Delong, Éric Filiol, Clément Coddet, Olivier Fatour & Clément Suhard. *OSINT Analysis of the TOR Foundation*. Available on arXiv.org, number 1803.05201, `https://arxiv.org/abs/1803.05201`

- Baptiste David. *How a simple bug in ML compiler could be exploited for backdoors ?*. Arxiv preprint on Arxiv.org, number 1811.10851, `https://arxiv.org/abs/1811.10851`

- Amir Afianian, Salman Niksefat, Babak Sadeghiyan & David Baptiste . *Malware Dynamic Analysis Evasion Techniques : A Survey*. Arxiv preprint on Arxiv.org, number 1811.01190, `https://arxiv.org/abs/1811.01190`

Prix, qualifications et récompenses

- Jean-Pierre Aubin et Richard Rey ont obtenu la certification *Stormshield Network Administrator Instructor*, sous les références 99V30CSNAI73627 et 99V30CSNAI28077 et ce pour une durée de trois ans.

Le laboratoire $(C+V)^O$ dans la presse

Pour l'année 2018 la médiatisation des travaux du laboratoire a été, s'est poursuivie sur un rythme quasi-identique à celui de 2017, que ce soit pour la presse écrite ou audio-visuelle ainsi qu'Internet, en France et à l'étranger. De très nombreux « points presse » ont été ainsi identifiés pour le laboratoire (France et étranger). Faute de place, il n'est plus possible de le répertorier tous.

Les principaux sont :

- Éric Filiol. Interview Journal Society. « *L'affaire Quennedey* ». Article de Pierre Boisson & Thomas Pitrel. *Society*, numéro 96, pp. 42-48, décembre 2018. - Janvier 2019.

- Éric Filiol. Interview Journal Sud Ouest. « *Les nouveaux espions venus du froid* ». 29 octobre 2018, Article de Yann Saint-Sernin, `https://www.sudouest.fr/2018/10/26/les-nouveaux-espions-venus-du-froid-5515226-4803.php`

- Éric Filiol. Interview France Culture. « *La fin des revues : la révolution de papier* ». Émission La méthode scientifique. Jeudi 11 octobre 2018, `https://www.franceculture.fr/emissions/la-methode-scientifique/la-methode-scientifique-du-jeudi-11-octobre-2018`

- Interview et démonstrations dans le magazine Révélations, ayant pour thème « Travail, vie privée, sommes-nous sous surveillance ? »RMC Story, 17 septembre 2018, 20h50, `http://www.numero23.fr/programmes/revelations/travail-vie-privee-sommes-nous-sous-surveillance/`

- Éric Filiol. « *Un autre regard sur les revues prédatrices* ». Interview Pour la Science, 13 août 2018, `https://www.pourlascience.fr/sd/science-societe/un-autre-regard-sur-les-re-`

vues-predatrices-entretien-avec-eric-filiol-14530.php

- Éric Filiol. « *Alerte au business de la fausse science* », 20 juillet 2018, Journal le Monde, https://www.lemonde.fr/sciences/article/2018/07/19/alerte-mondiale-a-la-fausse-science_5333374_1650684.html

- Éric Filiol. Interview France Info. « *Dark web : cet "internet parallèle" ne peut pas être arrêté ni interdit car "c'est un réseau collaboratif mondial"* », Edition du journal de 15h10, 16 juin 2018, https://www.francetvinfo.fr/economie/transports/trafic/dark-web-cet-internet-parallele-ne-peut-pas-etre-arrete-ni-interdit-car-c-est-un-reseau-collaboratif-mondial_2805035.html

- Journal Danois Version 2. *Når bagdøren ligger i matematikken*, 16 janvier 2018, article de Jakob Møllerhøj, https://www.version2.dk/artikel/naar-bagdoeren-ligger-matematikken-1084046

- Journal Danois Version 2. *Har den kryptering, vi allesammen bruger, en bagdør ?* article de Jakob Møllerhøj, 18 janvier 2018, https://www.version2.dk/artikel/har-kryptering-vi-allesammen-bruger-bagdoer-1084078

Merci également à Sud-Ouest, Intelligence Online, L'Informaticien, Numérama, Pirate Informatique, RT France, Radio France International... et à tous ceux qui involontairement auraient été oubliés mais qui ont contribué très activement à faire connaître les activités de notre laboratoire.

Productions logicielles

L'année 2018 a vu la poursuite et/ou la clôture des projets initiés les années précédentes avec leur montée en puissance pour certains d'entre eux. Quelques nouveaux projets ont vu le jour. La mise à disposition d'outils libres, ouverts et aboutis – dans le respect des réglementations existantes – est une volonté forte du laboratoire. Le nombre de téléchargements (plusieurs centaines de milliers au total) témoigne de la validité de cette démarche. La plupart de ces productions logicielles sont validées, le plus souvent, par des publications scientifiques internationales.

Seuls les nouveaux projets ou ceux ayant évolué en 2018 sont mentionnés ici.

- Richard Rey. Projet *Soft'IA* : avatar d'analyse d'identité numérique (travail sur une V1 dont la publication est planifiée pour août 2019).

- Richard Rey. Projet *OpenSOC* : SOC semi-automatique à collecteurs déportés pour la cybersurveillance des PME/ETI (travail sur une V1 dont la publication est planifiée pour août 2019).

- Éric Filiol. Projet *BACKDOOR*. Conception d'algorithmes de chiffrement avec backdoor mathématique. En 2018 un second algorithme de chiffrement par flot, baptisé SEA-1, a été conçu, implémenté et testé. D'une taille de clef de 162 bits, il sera rendu public en mars 2019 lors d'une conférence internationale.

- Baptiste David. CVE-2018-8232 (juillet 2018). Vulnérabilité dans le compilateur ML de Microsoft, permettant d'introduire une porte dérobée dans un code source au moment de la compilation. Ces travaux ont été présentés lors des conférences *C0c0n XI* en Inde et *Zero-Nights 2018* à Saint-Pétersbourg. `https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8232`

- Richard Rey. *Projet ALCASAR* (*Application Libre Pour le Contrôle d'Accès Sécurisé Au Réseau*). ALCASAR (`http://www.alcasar.net`) est un projet libre et indépendant, sous li-

cence GPL V3, de portail captif initié en 2008 par Richard REY et Franck BOUIJOUX. Il authentifie, impute et protège les accès à Internet des usagers indépendamment des équipements connectés. En France, il permet aux responsables d'un réseau de consultation Internet de répondre aux obligations légales. Intégrant des fonctions de filtrage, il répond aux besoins des organismes accueillant des mineurs.
Ce projet est conforme aux aspects juridiques et techniques suivants :
— Directive européenne 2006/24/CE sur la conservation des données.
— Loi française Numéro 2004-575 pour la confiance dans l'économie numérique (consolidée 19/05/2011).
— Décrêt français 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.
— Journalisation conforme aux préconisations de la CNIL et du CERTA (CERTA-2008-INF-005).
— Intégration des recommandations ANSSI (audit de sécurité et CSPN-2009/04).
Ce projet est déployé au sein de plusieurs ministères français et étrangers. Il est exploité par plusieurs centaines d'entreprises et de collectivités. À l'ESIEA, il est utilisé comme support pédagogique pour les cours « sécurité réseau » du mastère N&IS. Au laboratoire, il est le support opérationnel de plusieurs sujets d'étude et de recherche (projets PAIR, PSI, E.R, stages mastère).
  - En 2018, ont été publiées une version majeure (V3.3) et trois versions mineures (3.3.1, 3.3.2 et 3.3.3).

- Éric Filiol. Projet *GostCrypt*. Ce projet initié en décembre 2013 consiste en un fork du logiciel TrueCrypt intégrant des système de chiffrement non issus de la sphère anglo-saxonne (ANZUS et UKUSA) pour lesquels on peut raisonnablement avoir un déficit de confiance (en particulier depuis les révélations de Snowden qui ont démontré une volonté très aggressive des USA de contrôler la cryptographie dans le monde). Le premier algorithme

choisi est l'algorithme GOST. Une équipe ouverte et internationale a été créée pour piloter ce projet. Un second algorithme, *Grasshopper* `http://cvo-lab.blogspot.fr/2015/01/the-new-gost-standard-from-russian.html` a été implémenté fin 2015 dans la version 1.3 (sortie début 2016).
Depuis 2016, le projet a adopté un statut plus R&D car le laboratoire n'a pas les ressources nécessaires pour maintenir un tel projet au plan industriel (recherche et correction des vulnérabilités en particulier). Actuellement, le projet GostCrypt se veut plus un laboratoire pour tester de nouveaux algorithmes de chiffrement, de nouveaux protocoles de gestion de clefs. En 2017 et 2018, l'effort a été de revoir entièrement l'interface graphique (source de problèmes lors de la compilation selon les plateformes, existence de vulnérabilités, problème de licence) et de produire une interface portable multi-OS. Le code a été considérablement nettoyé et totalement commenté. Des tests intensifs d'analyse de code (statique et dynamique) ont été menés. Il en résulte un code simplifié, durci et sécurisé. Le code Grasshopper a été amélioré en termes de vitesse de chiffrement. Des fonctions de sécurité logicielles et utilisateurs ont été ajoutées à la suite. Enfin, la version UEFI de Gostcrypt a été initiée durant l'automne 2018 ce qui devrait permettre, en autres avantages, d'offrir le chiffrement de partitions systèmes pour Linux.
La sortie de la suite en version 2.0 est prévue pour le printemps 2019 avec une refonte totale du site web. La refonte totale du code, en particulier de l'interface graphique, a permis d'abandonner la licence — trop restrictive — de Truecrypt pour celle plus ouverte de la GPLv3.
Site officiel : `https://www.gostcrypt.org`

- Richard Rey et Jean-Pierre Aubin. Poursuite du développement de la plate-forme d'analyse de sécurité des objets Domotiques (OpenDom'X). Ce démonstrateur de domotique met en relief les risques liés aux transferts de données personnelles. Le fait d'avoir une multitude d'objets connectés facilite la vie de chacun, mais multiplie également les risques de voir ces données récupérées et utilisées à notre insu. C'est l'objectif principal de ce projet : démontrer, sensibiliser et proposer une solution sécurisée. Cette plateforme peut être visitée sur le site de Laval. En 2017, le co-développement se poursuit avec la société DIGITEMIS avec la création d'une méthodologie d'audit d'objets connectés. En 2018, la première version de la méthodologie d'analyse de sécurité d'objets connectés a été finalisée.
  Au-delà de la mise en œuvre de la quasi-totalité des protocoles filaires et radio permettant aux objets de communiquer, cette plate-forme est exploitée pour élaborer une méthodologie d'évaluation de la sécurité d'objets connectés et de leur conformité au RGPD (éthique). Dans le cadre du contrat entre le laboratoire et l'entreprise Digitemis, plusieurs étudiants ont pu éprouver et améliorer cette méthodologie pour analyser des dizaines d'objets connectés liés au domaine de la domotique et de l'E-santé.
  Avec le soutien de la fondation MAIF, l'objectif a été de créer un référentiel de labellisation des objets connectés via un indice de confiance (notes de A à D). Ce référentiel est baptisé IOTRUST. Les résultats de ces analyses ainsi qu'un guide des bonnes pratiques sont désormais disponibles sur Internet :
  - ◇ `https://www.fondation-maif.fr/pageArticle.php?rub=1&id=407`
  - ◇ `https://www.iotru.st/`
  - ◇ `https://www.fondation-maif.fr/up/pj/20180612_BBU_Guide-bonnes-pratiques-V7_WEB.pdf`
  - ◇ `https://www.fondation-maif.fr/up/pj/20180622_BBU_Rfrentiel-V2_WEB.pdf`

- Richard Rey. Poursuite du développement de la plate-forme HackRF. Cette plateforme peut être visitée sur le site de Laval.

- Richard Rey. Poursuite du développement de la plate-forme de réception satellite libre. Cette plateforme peut être visitée sur le site de Laval.

- Richard Rey. Projet *Checkmyhttps* ou comment vérifier que vos connexions WEB sécurisées (https) ne sont ni déchiffrées, ni écoutées, ni modifiées. Il s'agit d'une extension à installer sur le navigateur web Firefox. Ce projet a déjà été très bien accueilli par cette communauté de spécialistes dans le domaine, `https://checkmyhttps.net`. En 2016 ce projet a fait l'objet d'une seconde version, de tests intensifs et d'une importante médiatisation.
  Les évolutions de 2018 sont les suivantes :
  - ◇ Publication d'une version majeure (V5.0) exploitant la nouvelle API « *Webextension* ».
  - ◇ Publication d'un module Python (en attendant que l'API soit complétée des fonctions nous intéressant). Cette version est ainsi exploitable sur 3 navigateurs (Firefox, Chrome et Edge).
  - ◇ Publication d'une version mineure intégrant la notion de proxy d'entreprise (V5.1).

- Éric Filiol, Maxence Delong. Projet *Internet Health*.

  Ce projet a pour but d'effectuer en quasi temps réel un scan de ports, services et vulnérabilités sur l'ensemble des machines directement reliées à Internet et sur TOR. Le projet permet également d'effectuer une analyse des métadonnées des images hébergées sur le site (comparaison images/miniatures et extraction de métadonnées pertinentes, et en particulier la restauration des images dans leur version initiale quand elles ont été modifiées). Une analyse du réseau Tor est également effectuée, avec une approche statistique, et pratique en environnement de laboratoire. Le but final est de pouvoir avoir une idée de l'état de santé d'Internet en temps réel, et d'analyser la fiabilité du réseau TOR, son évolution vis-à-vis de certains critères. La plateforme est en cours de déploiement opérationnel sous forme d'une war-room pour une analyse et utilisation en temps quasi-réel.

  Les évolutions et temps forts 2018 pour ce projet sont les suivants :
  - ◇ Développement d'un crawler/scraper permettant de collecter des éléments, données sensibles de manière sécurisée et légale. En particulier la collecte ou la détention de certains contenus (par exemple liés à la pédopornographie) sont illégales. Dans un contexte d'aide à l'enquête et la recherche liée au réseau TOR, nous avons conçu une plateforme de collecte sécurisée et compatible avec la loi permettant l'analyse de contenus et l'identification de personnes sans détenir ces contenus. La remontée de ces contenus se fait

directement vers les forces de police habilitées. Le détail de cette plateforme fera l'objet d'une conférence en juillet 2019.

Activités scientifiques diverses

Domaine institutionnel

Le laboratoire est engagé fortement dans le soutien (à titre gracieux) des différents organismes régaliens de l'État. Outre le fait d'inculquer à nos jeunes (chercheurs, étudiants) la notion de service au profit de leur pays, elle permet ġalement de se confronter à des cas critiques et opérationnels qui peuvent faire ensuite, sous forme démarquée, l'objet d'une valorisation au sein des différentes actions de formation en sécurité.

- Fabien Bouchain, Éliot Rabaud (sous la conduite de Richard Rey), séance de sensibilisation à la cybersécurité (open data, transformation numérique, sécurité informatique...) au profit des « chefs d'État »de la Mayenne (préfet, sous-préfets, commissaires...), 22 juin 2018, Laval.

- Éric Filiol. Conférence sur les enjeux du numérique dans les territoires ruraux organisée par Mrs les députés Yannick Favennec (Mayenne) et Philippe Gosselin (Manche) et avec la participation de la société Orange, `https://www.ouest-france.fr/pays-de-la-loire/laval-53000/ernee-un-forum-sur-les-enjeux-du-numerique-5792272`

Participation à des jurys de thèse ou de concours

- Examinateur de la thèse de Roberto Cimino, *Differential attacks using alternative operations and block cipher design*, University of Trento, soutenue le 6 mars 2018.

Participation à des comités de programmes

Le laboratoire a participé à aux comités de programme suivants :
- ICCWS 2018, ECCWS 2018, ForSE 2018.
- VII Conferencia International de Engeniera I^{n}NGENIO, Medellin, Colombie.

Activités de revue d'articles (*peer-reviewing*)

L'activité de *peer-reviewing*, pour 2016, s'est effectuée au profit des revues et conférences suivantes :
- International Workshop on FORmal methods for Security Engineering (ForSE 2018) (É. Filiol, membre du board)
- *Revista Antioqueña de las Ciencas Computacionales Y la Ingeniería de Software* (É. Filiol, membre du board).
- ECCWS 2018, ICCWS 2018.

Animations scientifiques

En 2018, le laboratoire a été sollicité et impliqué dans de nombreuses opérations d'animations scientifiques en Pays de la Loire mais également au plan national et international. Chaque fois qu'il était possible, le laboratoire a impliqué très activement nos meilleurs étudiants. Les principales sont les suivantes :

- Baptiste David & François. *Reverse-Engineering under Windows 10 with Malware Analysis*. Training Conférence C0c0n XI, Kochi, Inde. 3-4 octobre 2018, `https://is-ra.org/c0c0n/2018/workshop/pre-conference-workshop/`

- Richard Rey. *Organisation de OpenESIEA* à Laval (manifestation autour du libre et des technologies liées au logiciel libre), 28 mars 2018. Cet événement a été organisé avec le concours d'étudiants.
  Site officiel : `https://www.esiea.fr/openesiea-virtualesiea-campu-laval/`

- Éric Filiol. Animation scientifique du week-end Ciné Philo consacré a l'intelligence artificielle, Cinéma le Vox, Mayenne. Les étudiants de l'ESIEA en collaboration avec des étudiants de la faculté de droit de Laval ont rédigé un dossier distribué lors de cet événement. `https://www.ouest-france.fr/pays-de-la-loire/mayenne-53100/mayenne-le-vox-consacre-son-week-end-l-intelligence-artificielle-6025291`

Responsabilités éditoriales

- Eric Filiol anime et dirige au titre d'éditeur en chef, le journal de recherche *Journal in Computer Virology and Hacking Techniques* publié par Springer, leader mondial de l'édition scientifique. Cette revue de recherche est la revue de référence dans le domaine de la virologie informatique et des technologies du hacking. Le board de ce journal réunit les meilleurs spécialistes mondiaux dans le domaine. La revue est indexée par les plus grandes bases scientifiques. Le volume 14 (quatre numéros) a été publié en 2018.

Contrats et transferts technologiques 2018

Contrats

Du fait de la sensibilité de certains contrats, et à la demande de certains industriels, les identités de ces derniers et la nature des travaux sont confidentielles. Ces résultats financiers (contrats facturés et payés) ont été vérifiés et validés par le commissaire aux comptes du groupe ESIEA.

- Contrat 3DNeuroSecure. Projet d'Investissement d'Avenir (PIA). Accepté en décembre 2014 (voir Section suivante). Durée quatre ans (2015 - 2019).

- Contrats d'audit de sécurité pour différentes sociétés (PME, ETI) : 10 contrats dans toute la France en 2018.

- Contrats d'audit de sécurité et d'analyse d'objets connectés et de produits de sécurité : 25 pour l'année 2018.

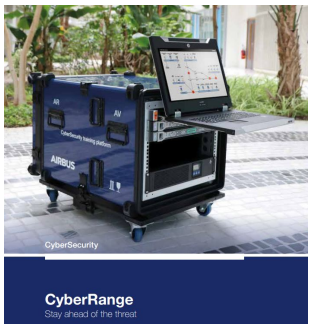
Projets industriels

Projet 3DNS `www.3dneurosecure.com`

- Projet *3DNeuroSecure* (Projet d'Investissement d'Avenir) accepté en décembre 2014. Consortium constitué de Neoxia (chef de file), CEA/DSV, CES/DAM, ESIEA/CNS/CVO, Tribun, Zayo, NVidia, Université de Reims-Champagne Ardennes. Début du projet le 1er janvier 2015. Durée 4,5 ans.
  Le projet 3D NeuroSecure porte sur le développement d'une solution collaborative sécurisée pour l'innovation thérapeutique, utilisant notamment l'exploitation d'images 3D (plateforme terapixel et très haut débit). Ce projet vise à exploiter des données issues d'images 3D de cerveaux entiers (taille de quelques Go par image) pour sélectionner et développer des molécules contre de nouvelles cibles thérapeutiques identifiées dans la maladie d'Alzheimer. Le laboratoire $(C+V)^O$ est responsable de la sécurisation de la plateforme et de tous les flux de données. Il bénéficie d'un financement lié aux Grands Projets d'Avenir. Le projet, fin 2018 et premier semestre 2019 entre dans sa phase de préindustrialisation.

Collaborations industrielles

- Collaboration avec la société Airbus sur le programme *CyberRange*. Le laboratoire exploite



CyberRange - `https://airbus-cyber-securite.com/fr/resource/cyberrange`

  CyberRange dans le cadre normal du cyber-entrainement en y associant activement les meilleurs de nos étudiants. De plus, certaines modifications sont apportées afin de pouvoir l'exploiter comme support à la pédagogie :
  ◇ réalisation de TP/TD système et réseau,

- ◇ exploitation distante par les ẃtudiants (cloisonnement VPN + VLAN),
- ◇ supervision au moyen d'une application mobile,
- ◇ évaluation du niveau de sécurisation d'un SI d'entreprise (qualification de la protection),
- ◇ Test unitaire de validation de sonde d'un SOC.

- Développement R&D en mode noyau Windows chez l'éditeur d'antivirus DrWeb, Saint-Pétersbourg. Dans le cadre de cette collaboration, Baptiste David a effectué un séjour doctoral de trois mois dans les locaux de cet éditeur. Il a notamment conçu et implémenté des contre-mesures contre *pa-fish*, des techniques de détection de VM basée sur `rdtsc` (utilisation de techniques bas niveau d'hyperviseurs type VT-X) et des méthodes de détection de scripts appliquées à powershell (machine learning, parser *perl* et *powershell* et utilisation d'AMSI dont il a amélioré la version d'origine).

- Collaboration avec la société NPP/Gamma dans le domaine de la sécurité cryptographique dans l'embarqué et la sécurité des composants électroniques, `https://www.nppgamma.ru/`

- Collaboration avec la société Heypster (`https://heypster.com`) qui développe un réseau social de type Facebook avec comme priorité et ligne de conduite la protection des données personnelles et le respect de la vie privée. Le laboratoire apporte son soutien scientifique dans le domaine de la sécurité.