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

Rapport d'activité 2017

- § -

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.

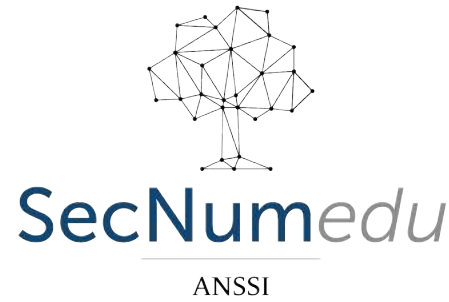
Du fait de cet héritage, l'activité de recherche du laboratoire s'inscrit dans la continuïté et conserve des liens forts non seulement avec le ministère de la Défense mais également avec les ministères de la Justice et de l'Intérieur. Cela concerne à la fois une partie des thématiques de recherche du 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 śecurité 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



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 cherche, 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 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. 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 asprects 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 scénarios terroristes. Initiée en 2016, à la suite de travaux du laboratoire, le but est d'analyser et d'imaginer les possibilités de scénario 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

- 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

  — Nicolas Bodin (Ph D)
  Email : `nicolas.bodin@esiea.fr`
  Stéganographie, matématiques discrètes.

  — 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.

- Doctorants

  — Arnaud Bannier (Ph D)
  Email : `arnaud.bannier@esiea.fr`
  Mathématiques discrètes, combinatoire, cryptologie.

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

  — Michel Dubois
  Email : `michel.dubois@esiea.fr`
  Cryptographie symétrique.

  — Cécilia Gallais
  Email : `cecilia.gallais@esiea.fr`
  Modélisation mathématique des cyberattaques

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

- Espoirs recherche.
  Dans le cadre de la promotion de la recherche auprès des étudiants, le laboratoire identifie chaque année des étudiants particulièrement prometteurs 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. Leur objectif est, souvent, après leur diplôme d'ingénieur, de préparer une thèse.

  — Béclair Louis (3A/4A)
  Programmation, Cryptographie, Data-Mining et analyse de données.

  — Bernard Hippolyte (4A/5A)
  Algorithmique, sécurité Windows, virologie.

— Beheshti Loïc (4A/5A)
Détection de malware Android, techniques d'apprentissage.

— Bimboutsa Koumba Worphy (4A/5A)
Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

— Champenois Godeleine (4A/5A)
Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

— Coddet Clément (4A/5A)
Stéganographie, réseau, programmation, calcul parallèle.

— Delong Maxence (3A/4A)
Algorithmique, calcul parallèle, cryptographie, réseau, programmation.

— Dey Alexandre (4A/5A) Détection de malware Android, techniques d'apprentissage.

— Fatou Olivier (4A/5A)
Algorithmique, calcul parallèle, cryptographie, réseau, programmation.

— Guédon Timothée (3A/4A)
Programmation, sécurité réseau.

— Hamza Bourrahim (4A/5A)
Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

— Hébert Antoine (3A/4A)
Programmation, Cryptographie

— Tom Houdayer (3A/4A)
Programmation, sécurité des bases de données.

— Lardier William (3A/4A)
Programmation, Cryptographie.

— Le Huitou Pierre-Aymeric (3A/4A)
Programmation, Data-Mining et analyse de données.

— Jeannaud Quentin (4A/5A)
Détection de malware Android, techniques d'apprentissage.

— Obame de Soumbou Mbwath Ralph Steevens (4A/5A)
Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

— Sido Marie-Kerguelen (4A/5A)
Détection de malware Android, techniques d'apprentissage.

— Suhart Clément (4A/5A)
Algorithmique, calcul parallèle, cryptographie.

— Toriello Lucas (3A/4A)
Programmation, Data-Mining et analyse de données.

— Varo Quentin (3A/4A)
Programmation, Cryptographie.

Thèses et stages

Thèses soutenues en 2017

- Thèse de Michel Dubois *Conception, développement et analyse de systèmes de fonctions booléennes décrivant les algorithmes de chiffrement et de déchiffrement de l'Advanced Encryption Standard*. École doctorale SMI de l'ENSAM. Soutenance le 24 juillet 2017.

  Composition du jury : Professeur Maroun Chamoun (ESIB, Université Saint-Joseph, Liban - Rapporteur), professeur Radu State (SnT, Université du Luxembourg, rapporteur), Dr. Robert Erra (Epita, examinateur), Dr. Eric Jaeger (Ministère de la Défense/DGSIC, examinateur), professeur Jean-Marc Steyaert (président, École Polytechnique), Éric Filiol (directeur de thèse, ESIEA).

- Thèse d'Arnaud Bannier *Combinatorial Analysis of Block Ciphers With Trapdoors*. École doctorale SMI de l'ENSAM. Soutenance le 29 septembre 2017.

  Composition du jury : Professeur Kenny Paterson (Royal Holloway, University of London, UK - Rapporteur), professeur Massimiliano Sala (University of Trento, Italy, rapporteur), professeur Anne Canteaut (INRIA, examinateur), professeur Alexei Zhukov (Bauman - Moscow State University, Russie, examinateur), Jean-Marc Steyaert (président, École Polytechnique), Éric Filiol (directeur de thèse, ESIEA).

- Thèse de Cécilia Gallais *Formalization and Algebraic and Combinatorial Analysis of Generalized Attack Scenarios*. École doctorale SMI de l'ENSAM. Soutenance le 18 décembre 2017.

  Composition du jury : Professeur Maroun Chamoun (ESIB, Université Saint-Joseph, Liban - Rapporteur), professeur Thomas Engel (Université du Luxembourg, rapporteur), professeur Antonella Santone (University of Molise, Italie, examinateur), Dr. Johann Barbier (Evoluttion XY, CTO, examinateur), Jean-Marc Steyaert (président, École Polytechnique), Éric Filiol (directeur de thèse, ESIEA).

Thèses en cours

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

- 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 prévue pour fin 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 fin 2018.

- 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. Cette thèse a débuté en décembre 2016.

Stages Master - Mastère et Ingénieur 2017 (cycle M)

- Antoine Bouvard, *Création d'une procédure d'analyse de serveurs Active Directory*. Stage de fin d'études d'ingénieur, MSc II ESIEA, 6 mois. Maître de stage : R. Rey.

- Clément Coddet. *Réalisation d'un audit de sécurité et développement d'outils d'audit*. Projet technique/MSc I ESIEA, 4 mois. Maître de stage : R. Rey.

- Maxence Delong, *Développement de la plateforme-Internet Health de scan massif*. Stage technique/MSc I ESIEA, 4 mois (dont 2 en collaboration avec *Universita degli studi del Sannio*, Italie co-supervisé par Aaron Visaggio). Maître de stage : E. Filiol.

- Hamza Essayegh, *Développement d'une méthodologie et d'outils d'audits de sécurité d'objetc connectés*. Stage de fin d'études d'ingénieur, MSc II ESIEA, 6 mois. Maître de stage : R. Rey.

- Olivier Fatou. *Réalisation d'un audit de sécurité et développement d'outils d'audit*. Projet technique/MSc I ESIEA, 4 mois. Maître de stage : R. Rey.

- Nicolas Job. Évaluation de la sécurité réelle du protocole d'anonymisation Tor et mesure de l'impact réel des contraintes de routage sur la qualité et la prédictabilité de ce dernier. Stage Expert en Sécurité des Systèmes d'Information (ESSI) de l'ANSSI, stage 6 mois. Maître de stage : E. Filiol

- Vincent Lorion, *Missions d'audits de sécurite de systèmes d'information d'entreprises*. Stage de fin d'études d'ingénieur, MSc II ESIEA, 6 mois. Maître de stage : R. Rey.

- Clément Suhart. *Réalisation d'un audit de sécurité et développement d'outils d'audit*. Stage technique/MSc I ESIEA, 4 mois. Maître de stage : R. Rey.

Stages 2017 (cycle L)

- Louis Béclair. *Développements cryptographiques dans le cadre du projet GostCrypt*. Stage BSc, ESIEA, 2 mois. Maître de stage : E. Filiol

- Antoine Hébert. *Développements cryptographiques dans le cadre du projet GostCrypt*. Stage BSc, ESIEA, 2 mois. Maître de stage : E. Filiol.

- Tom Houdayer. *Analyse comparative de performances de bases de données et la base de données Brucaria du CEA*. Stage BSc, ESIEA, 2 mois. Maître de stage : R. Rey.

- William Lardier. *Développements cryptographiques dans le cadre du projet GostCrypt*. Stage BSc, ESIEA, 2 mois. Maître de stage : E. Filiol.

Publications du laboratoire

Livres et chapîtres d'ouvrages

- Arnaud Bannier et Eric Filiol. « *Partition-based Trapdoor Ciphers* ». InTech editions. September 2017, ISBN :978-953-51-3386-5 (Print)/ISBN :978-953-51-3385-8 (Online).

- Eric Filiol, Baptiste David et Paul Irolla. « *Les virus informatiques* ». Chapitre des Techniques de l'Ingénieur [H5440], octobre 2017 (version augmentée et actualisée de la version de 2007).

- Eric Filiol. « *Proactive Detection of Unknown Malware* ». Chapter in Book "*Computer Security*", Jaydip Sen editor, Intech editions, ISBN 978-953-51-3346-9, Print ISBN 978-953-51-3345-2.

Revues internationales à comité de lecture

- Baptiste David, Éric Filiol & Kévin Gallienne. « Structural Analysis of Binary Executable Headers for Malware Detection Optimization ». *Journal in Computer Virology and Hacking Techniques*, volume 13, Issue 2, pp. 87–93.

- Éric Filiol & Cécilia Gallais. « Combinatorial Optimization of Operational (Cyber) Attacks against Large-scale Critical Infrastructure - The Vertex Cover Approach ». *International Journal in Cyber Warfare and Terrorism*, vol. 7, issue 3, pp. 29–43, June/July 2017.

- Éric Filiol & Cécilia Gallais. « Critical Infrastructure : Where we Stand Today - A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure ». *Journal of Information Warfare*, Volume 16, Issue 1, pp. 64–87, 2017.

- Arnaud Bannier & Nicolas Bodin, « A new drawing for simple Venn diagrams based on algebraic construction ». Journal of Computational Geometry, vol. 8, nr. 1, pp. 153–173.

Conférences et articles invités (niveau national)

- Éric Filiol. « *Espionnage et cybercriminalité en entreprises : risques et enjeux* ». Société EPTICA, Boulogne-Billancourt, 4 mai 2017.

- Éric Filiol. « *La cybercriminalité à l'heure de la révolution numérique* ». Conférence Shanghai Accueil, 12 avril 2017, Shanghai.

- Éric Filiol. « *Espionnage et cybercriminalité en entreprises : risques et enjeux* ». Présentation devant le Groupe Axians - Vinci Énergies Infrastructures Télécoms. 30 mars 2017, château des Guermantes, Guermantes.

- Éric Filiol. « *Cyber-sécurité : la déstabilisation, la désinformation de l'entreprise, la manipulation à l'international ; menaces et acteurs à considérer dans nos relations d'affaires* ». Club Sarthe International, CCI du Mans - Sarthe, 30 janvier 2017.

- Richard Rey. « *Sensibilisation sécutité auprès de développeurs et d'administrateurs réseaux* ». Société ARTIC, Lisieux, 15 mars 2017.

Conférences internationales avec comité de sélection et actes

- Joanna Moubarak, Éric Filiol & Maroun Chamoun. « *Comparative Analysis of Blockchain Technologies and the TOR Network : Two Faces of the same Reality ?* »IEEE-CSNet 2017, Rio de Janeiro, Brazil, October 18-20th, 2017.

- Joanna Moubarak, Maroun Chamoun & Éric Filiol. « *Comparative Study of Recent MEA Malware Phylogeny* ». 2nd International Conference on Computer and Communication Systems (ICCCS'2017), July 11th-14t, 2017, Krakow, Poland. IEEE Proceedings, pp. 16–20. Prix de la meilleure présentation.

- Joanna Moubarak, Maroun Chamoun & Éric Filiol. « *Middle East Malware Evolution* ». 23rd international Scientific Conference of LAAS, April 6th - 7th, 2017, Beyrouth, Lebanon.

- Arnaud Bannier & Éric Filiol. « One *construction of a backdoored AES-like block cipher and how to break it* ». RusKrypto 2017, Moscow, March, 21st - 24th, 2017.

- Paul Irolla & Éric Filiol. « *Glassbox : Dynamic Analysis Platform for Android Malware Applications on Real Devices* ». 1st International Workshop on FORmal Methods in Security Engineering (ForSE) 2017, Porto, Portugal, February 21st- 23rd, 2017.

- Arnaud Bannier & Éric Filiol. « *Mathematical Backdoors in Symmetric Encryption Systems - Proposal for a Backdoored AES-like Block Cipher* ». 1st International Workshop on FORmal Methods in Security Engineering (ForSE) 2017, Porto, Portugal, February 21st-23rd, 2017.

- Michel Dubois & Éric Filiol. « *Hacking of the AES with Boolean Functions* ». 1st Internatio-

nal Workshop on FORmal Methods in Security Engineering (ForSE) 2017, Porto, Portugal, February 21st- 23rd, 2017.

- Nicolas Bodin, Éric Filiol, Clément Coddet & Olivier Fatou. « *Intelligence Gathering by Comparison of JPEG images and Their Thumbnails* », 12th International Conference on Cyber Warfare and Security (ICCWS) 2017, Wright State University & the Center for Cyberspace Research, Air Force Institute of Technology, Dayton, USA, March 2nd & 3th, 2017, pp. 48–56, Academic Conference Publishing International.

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).

- Arnaud Bannier. & Éric Filiol. « *By-design Backdooring of Encryption System - Can We Trust Foreign Encryption Algorithms ?* ». Black Hat Europe 2017, London, December 4th-7th, 2017.

- Baptiste David. « *Shall We Play a Game : How to Fool Antivirus Software* ». 15ème Nuit du Hack, Eurodisney, Marne-la-Vallée, 24 juin 2017.

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.

- Paul Amicelli. *Comment fonctionnent les keyloggers*. Journal SécuritéOff, 19 mars 2017, `https://www.securiteoff.com/comment-fonctionnent-les-keyloggers/`

- Thomas Aubin et Paul Hernault. *Voitures connectées : les différentes failles (partie 2)*, Journal SécuritéOff, 19 mars 2017, `https://www.securiteoff.com/voitures-connectees-differentes-failles-partie-2/`

- Adrien Luyé et Antoine Quélard. Vidéo-protection : comment éviter de tout stocker et de tout traiter. Journal SécuritéOff, 20 avril 2017, `https://www.securiteoff.com/videoprotection-eviter-de-stocker-de-traiter/`

- Tom Houdayer. *Attaque homographique sur les noms de domaine internationalisés*. Journal SécuritéOff, 5 juin 2017, `https://www.securiteoff.com/attaque-homographique-noms-de-domaine-internationalises/`

- Romain Garnier et Lucas Toriello. *La sécurité des systèmes RFID : études de cas*, Journal SécuritéOff, 9 juin 2017, `https://www.securiteoff.com/securite-systemes-rfid-etude-de-cas/`

- Alexandre Dey. *Google et le 40 000 apps malveillantes*. Journal SécuritéOff, 6 juillet 2017, https://www.securiteoff.com/play-store-de-google-plus-de-40-000-applications-malveillantes/

- Éric Filiol (interview) *Peut-on encore faire confiance à TOR ?*, Journal SécuritéOff, 5 septembre 2017, https://www.securiteoff.com/on-faire-confiance-a-tor/

- Éric Filiol. *Premiers retours sur l'analyse du réseau TOR*. Journal SécuritéOff, 14 septembre 2017, https://www.securiteoff.com/premiers-retours-lanalyse-reseau-tor/

- Éric Filiol. *Windows est pour nous une boite noire que connait très bien la NSA*, Journal SécuritéOff, 24 aout 2017, https://www.securiteoff.com/eric-filiol-windows-boite-noire-connait-tres-bien-nsa/

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.

- Arnaud Bannier et Éric Filiol. *Mathematical Backdoors in Symmetric Encryption Systems - A Proposal for a Backdoored AES-like Block Cipher*. Arxiv preprint on Arxiv.org, number 1702.06475. arXiv.org, number 1702.06475, https://arxiv.org/abs/1702.06475

- Éric Filiol & Nicolas Job. *Preliminary Results on TOR Routing Protocol Statistical and Combinatorial Analysis*. Blog CVO-Lab, 4 septembre 2017, https://cvo-lab.blogspot.com/2017/09/preliminary-results-on-tor-routing.html. Les travaux ont été acceptés pour présentation lors de la conférence ForSE 2018.

- Éric Filiol & Nicolas Job. *List of TOR Relays for Optimal Correlation Attack*. Blog CVO-Lab, 16 octobre 2017, https://cvo-lab.blogspot.com/2017/10/list-of-tor-relays-for-optimal.html. Les travaux ont été acceptés pour présentation lors de la conférence ForSE 2018.

Prix, qualifications et récompenses

- Joanna Moubarak. *Best Presentation Award*, 2nd International Conference on Computer and Communication Systems (IEEE/ICCCS'2017), juillet 2017.

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

Pour l'année 2017 la médiatisation des travaux du laboratoire a été, encore une fois, riche et intense tant pour la presse écrite, qu'audio-visuelle et Internet, en France et à l'étranger. Ce sont plusieurs centaines de « points presse » identifiés pour le laboratoire (France et étranger). Faute de temps, il n'est plus possible de le répertorier tous.

Les principaux sont :

- Interview Radio France International. « Espionnage par objets connectés : Wikileaks révèle des documents de la CIA ». 9 Mars 2017, `http://www.rfi.fr/emission/20170309-espionnage-objets-connectes-wikileaks-revele-documents-cia`

- La Nouvelle République. « *Les pirates informatiques doivent être pris au sérieux* ». 18 mars 2017, `https://www.lanouvellerepublique.fr/actu/les-pirates-informatiques-doivent-etre-pris-au-serieux`

- Interview Mediapart. « Le virus WannaCry révèle les lacunes de la cybersécurité internationale », 22 mai 2017, `https://www.mediapart.fr/journal/international/220517/le-virus-wannacry-revele-les-lacunes-de-la-cybersecurite-mondiale/commentaires`

- Interview la Chaine Parlementaire. Émission « *Ca vous regarde. Cyberattaque : la guerre est déclarée* ». 30 juin 2017, 19 :30.

- Interview RFI. *Coding errors in 685 mobile-apps leave 180 million smartphone users vulnerable*, 10 novembre 2017, Radio France International. `http://en.rfi.fr/general/20171110-coding-errors-685-mobile-apps-leave-180-million-vulnerable`

- Éric Filiol. Interview 01net, « *Et si l ?algorithme de chiffrement le plus utilisé au monde avait une backdoor ?* », 01net, 19 décembre 2018, `http://www.01net.com/actualites/et-si-l-algorithme-de-chiffrement-le-plus-utilise-au-monde-avait-une-backdoor-1330455.html`

- Interview The Register. *We need to talk about mathematical backdoors in encryption algorithms*, The Register, 15 décembre 2017, `https://www.theregister.co.uk/2017/12/15/crypto_mathematical_backdoors/`

Merci également à Sud-Ouest, L'Informaticien, Numérama, Sciences et Vie Junior, Motherboard-VICE Magazine, Stylist Magazine, publihebdos.fr, developpez.com, Pirate Informatique... 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 2017 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 2017 sont mentionnés ici.

- 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 licence 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).
  - La version 3.1 a migré vers la version 3.2 avec quatre sous-versions. Nouvelles fonctionnalités 2017.
    - Migration vers *Mageia* 6.0 et Radius V3.
    - Rapport d'imputabilité « éthique »(les utilisateurs sont avertis de la consultation des journaux d'imputabilité : nom + motivation).
    - Compatibilité avec les infrastructures virtualisées *Vmware* ou *Proxmox*.
    - Formation du personnel (40) du ministère de l'Intérieur.

- 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). Des alternatives comme *Veracrypt* offrent ce suivi industriel. 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, 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. La sortie de la suite en version 2.0 est prévue pour l'automne 2018 avec une refonte totale du site web.
  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 (finalisation en 2018).

- 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 2017 sont les suivantes :
  - ◇ Poursuite du développement (V4.3.0 du 09/11/2017).
  - ◇ Détection d'attaques homographiques (voir article de Tom Houdayer publié sur le site

SecuriteOff).
- ◇ Respect de la vie privée : publication d'une procédure pour que chacun puisse déployer son propre serveur *checkmyhttps*.
- ◇ Suite à la décision de la *Mozilla foundation* de migrer l'API de Firefox vers *WebEx*, *CheckMyHttps* n'est fonctionnelle que sur les versions « ESR »de Firefox. En attendant que cette nouvelle version de l'API permette à nouveau l'accès aux informations des certificats, nous développons une version incluant un appel externe (script python).

- 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 2017 pour ce projet sont les suivants :
- ◇ Création d'une interface graphique.
- ◇ Insertion d'une base de donnée SQL pour le stockage des résultats.
- ◇ Définition d'une architecture client-serveur.
- ◇ Extension du nombre de ports par scan.
- ◇ Possibilité de scan des nœuds du réseau TOR.
- ◇ Migration de l'environnement vers des conteneurs Dockers.
- ◇ Première campagne de scan sur 15M d'adresses IPv4.
- ◇ Définition d'une nouvelle architecture permettant le stockage des résultats de manière sécurisée ainsi que du scan à très haute vitesse sur des serveurs dédiés.
- ◇ Création d'une plateforme *Docker* pour l'émulation de l'architecture et la validation des codes avant déploiement.
- ◇ Modification et ajout d'une version de *ZMap* personnalisée.
- ◇ Benchmark des différentes bases de données NoSQL.
- ◇ Passage de la base de donnée SQL vers une base NoSQL (*MongoDB*) avec la mise en place d'un système de *sharding* et *réplica* (répartition de la charge et sauvegarde).
- ◇ Redéfinition du système de scan dorénavant fuseau horaire par fuseau horaire (pour le scanner lors d'une heure creuse assurant une plus grande précision des résultats).

◇ Création d'un bot de récolte d'information sur le réseau TOR.
◇ Récupération continu des consensus du réseau TOR afin d'en vérifier ses performances et son évolution.

Activités scientifiques diverses

Participation à des comités de programmes

Le laboratoire a participé à aux comités de programme suivants :
- ICCWS 2017, ECCWS 2017, ForSE 2017.
- Second edition of the Workshop on Malware Analysis, ARES 2017.

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 2017) (É. Filiol, membre du board)
- *Revista Antioqueña de las Ciencas Computacionales Y la Ingeniería de Software* (É. Filiol, membre du board).
- *ARES 2017 - Second edition of the Workshop on Malware Analysis* (É. Filiol).
- *Advances in Mathematics of Communications* (É. Filiol).

Animations scientifiques

En 2017, le laboratoire a été sollicité et impliqué dans de nombreuses opérations d'animations scientifiques en Pays de la Loire mais également au plan national. Chaque fois qu'il était possible, le laboratoire a impliqué très activement nos meilleurs étudiants. Il est impossible de les répertorier toutes ici mais les principales sont les suivantes :
- Éric Filiol. Formation Erasmus (Cyber Security Summer Camp). « Deep Forensics of Digital Data - An Intelligence Perspective. Juillet 2017, Laval.
- Richard Rey. Organisation de OpenESIEA à Laval (manifestation autour du libre et des technologies liées au logiciel libre), mars 2017. Cet événement a été organisé avec le concours d'étudiants.
  Site officiel : `https://www.esiea.fr/esiea-techdays-2017-projets-scientifiques-et-techniques-4a/`

- Éric Filiol. Conférence : « *se protéger, protéger son identité, ne pas mettre n'importe quoi sur la toile* « . J2A - Journées des doctorants de 2ème année de l'ED SMI/ENSAM, Amphithéatre Grégoire, CNAM, Paris, 20 juin 2017.

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 13 (quatre numéros) a été publié en 2017.

Contrats et transferts technologiques 2017

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 - 2018).

- Contrats d'audit de sécurité pour différentes sociétés (PME, ETI).

Projets industriels

- 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 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.

Collaborations industrielles

- 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 implémenté des systèmes de classification de malware protégés par des packers polymorphes.

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