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

Rapport d'activité 2016

- § -

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 sera 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* (N&IS).

En 2012, le laboratoire fusionne avec le pôle SI&S (Sécurité de l'Information & des Systèmes) afin que le groupe puisse disposer d'un laboratoire plus conséquent dans la thématique sécurité. Avec le pôle SI&S, c'est également la seconde formation mastère spécialisé *Sécurité de l'Information et des Systèmes* ainsi que les formations badge en reverse engineering et en sécurité offensive, toutes deux sous la direction de Vincent Guyot, qui rejoignent le laboratoire $(C+V)^O$. Site officiel S&IS : `http://www.esiea.fr/formation-ingenieurs/master-securite-information-systemes`.

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 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.

SecNumedu

ANSSI

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, Mastères Spécialisés et Badges) 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 nos 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. Ce dernier pilote cette sensibilisation en particulier via son référent de Défense. 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, de *data mining*, *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 et référent de Défense - Laval

  Richard Rey (Ing.)
  Email : `richard.rey@esiea.fr`

Sécurité réseau, sécurité radio et télécommunications, électronique, guerre électronique, audits de sécurité, pentesting.

- Adjoint du laboratoire - Paris

  Vincent Guyot (Ing. - Ph D).
  Email : `vincent.guyot@esiea.fr`
  Sécurité cartes à puce, sécurité RFID, sécurité système, sécurité réseau.

- Chercheurs permanents

  — Damien Gros (Ph D)
  Email : `damien.gros@esiea.fr`
  Virologie, sécurité réseau et système.

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

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

- Doctorants

  — Arnaud Bannier
  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.

- Chercheurs associés

  — Alexandre Denjean
  Techniques de renseignement ouvert (OSINT) et d'ingéniérie sociale.

- 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.

  — Aubin Thomas (4A/5A)
  Algorithmique, sécurité Windows, virologie.

  — Beheshti Loïc (3A/4A)
  Détection de malware Android, techniques d'apprentissage.

  — Bimboutsa Koumba Worphy (3A/4A)
  Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

  — Champenois Godeleine (3A/4A)
  Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

  — Coddet Clément (3A/4A)
  Stéganographie, réseau, programmation, calcul parallèle.

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

  — Dey Alexandre (3A/4A) Détection de malware Android, techniques d'apprentissage.

  — Fatou Olivier (3A/4A)
  Algorithmique, calcul parallèle, cryptographie, réseau, programmation.

  — Hammani Sami (3A/4A)
  Détection de malware Android, techniques d'apprentissage.

  — Hamza Bourrahim (3A/4A)
  Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

  — Hernault Paul (4A/5A)
  Algorithmique, sécurité Windows, virologie.

  — Jeannaud Quentin (3A/4A)
  Détection de malware Android, techniques d'apprentissage.

— Meziani Hugo (4A/5A)
Algorithmique, sécurité Linux, virologie.

— Obame de Soumbou Mbwath Ralph Steevens (3A/4A)
Programmation, analyse d'image, techniques de reconnaissance, techniques d'apprentissage.

— Pion Raphael (4A/5A)
Algorithmique, sécurité Linux, virologie.

— Sido Marie-Kerguelen (3A/4A)
Détection de malware Android, techniques d'apprentissage.

— Suhart Clément (3A/4A)
Algorithmique, calcul parallèle, cryptographie.

Thèses et stages

Thèses en cours

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. Du fait des procédures administratives, la soutenance de plusieurs thèses a été décalée de six mois.

- Thèse de Michel Dubois. *Etude combinatoire de la mise en équations sur $GF(2)$ des algorithmes de chiffrements par bloc.* École doctorale ENSAM/SMI. Cette thèse a débuté en septembre 2010. Soutenance prévue en avril 2017.

- Thèse (CIFRE) de Cécilia Gallais. *Formalisation et modélisation algébriques des concepts de cyberattaque et d'infrastructure critique.* École doctorale ENSAM/SMI. Cette thèse a débuté en décembre 2013. Soutenance prévue avril 2017.

- Thèse d'Arnaud Bannier. *Analyse combinatoire des systèmes de chiffrement par bloc avec trappes.* École doctorale ENSAM/SMI. Cette thèse a débuté en décembre 2013. Soutenance prévue avril 2017.

- 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), Université Paris-sud, ED 419, Biosigne. Cette thèse a débuté en septembre 2014 dans le cadre du projet 3D NeuroSecure.

- 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. Cette thèse a débuté en septembre 2015.

- 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.

Projets et Stages Master - Mastère et Ingénieur 2015 (cycle M)

- Paul Hernault *Pin Sandbox - Automated Analysis of Packed Binaries* et *OpenDavfi : antivirus de serveur mail pour traitement preventif des ransomware*, Stage technique/MSc I ESIEA, 4 mois (dont 2 en collaboration avec Polytecnico di Milano, Necst Lab, supervisé par Stefano Zanero).

- Raphaël Pion *Deéveloppement et amélioration d'Alcasar et migration vers la version 3.0*. Stage technique/MSc I ESIEA, 4 mois.

- Thomas Aubin et Paul Hernault. *Securité et confidentialité sous Windows 10*. Projet technique/MSc I ESIEA, 4 mois.

- Quentin Sallio, Christian Ipoli Felho, Kévin Combet, Hamza Essayegh. *Réalisation d'une plateforme CTF collaborative*. Projet technique/MSc I ESIEA, 4 mois.

- Julian Alcaraz Ordaz, Jeremy Kersale, Arnaud Lerailler. *Hacking RF*. Projet technique/MSc I ESIEA, 4 mois.

- Clément Siccardi et Bettyna Bourcier. *Réalisation de la cartographie logicielle d'ALCASAR. Réécriture des fonctions PHP dépréciées. Analyse des solutions de documentation collaboratives*. Projet technique/MSc I ESIEA, 4 mois.

- Hervé Froc, Vianney Lapouble, Adrien Burel. *Opendom'X : plateforme d'analyse de la sécurité d'objets connectés de type domotique*. Projet technique/MSc I ESIEA, 4 mois.

- Rodolphe Humeau, Alexis Lefrançois, Simon Gaulard. *Plateforme d'interception satellite*. Projet technique/MSc I ESIEA, 4 mois.

- Vincent Clément, Andy Da Silva Araujo et Antony Lor. *SDR : écoute radio et contrôle de drone*. Projet technique/MSc I ESIEA, 4 mois.

Projets et Stages 2015 (cycle L)

- Florian Berson, Clément Coddet, Olivier Fatou FATOU, Benjamin Laurent. *Recherche d'images JPEG modifiées sur Internet et le Deep/DarkWeb et récupération des modifications*. Projet technique/BSc, ESIEA, 3 mois.

- Herizou-Thé Godefroy, Dabo Pabegba Abdellatif Kouanda, Romain Pautonnier et Loys Boufflers. *Interception GSM par dispositif de type IMSI-Catcher*. Projet technique/BSc, ESIEA, 3 mois.

- Mickaël Charuel, Baptiste Dagnet. *Étude et conception d'une « cage optique laser »pour drones*. Projet technique/BSc, ESIEA, 3 mois.

- Kevin Guinet, Adrien Ruisseau. *Étude et réalisation démonstrateur permettant de mesurer et quantifier la puissance d'un pointeur laser*. Projet technique/BSc, ESIEA, 3 mois.

- Ralph Steevens Obame de Soumbou Mbwath, Worphy Bimboutsa Koumba, Hamza Bourrahim, Godeleine Champenois. *OpenFacetracker (système open source de détection et de reconnaissance faciale)*. Projet technique/BSc, ESIEA, 3 mois.

- Arnaud Piriou, Martin Praddaude. *Reverse Engineering sur Architecture x86*. Projet technique/BSc, ESIEA, 3 mois.

Publications du laboratoire

Livres et chapîtres d'ouvrages

- Éric Filiol. Contribution sous forme d'interviews pour le livre de Blaise Mao et Thomas Saintourens, « *Cyberfragiles - Enquête sur le danger de nos vies connectées* », éditions Tallandier, avril 2016.

Revues internationales à comité de lecture

- Michel Dubois et Éric Filiol. 3D Visualization Applied to PRBG and Cryptography. *Computer Science and Information Technology*, Vol. 4 (5), pp. 171 – 180, DOI : 10.13189/csit.2016.04050.

- Olivier Ferrand et Éric Filiol. Combinatorial Detection of Malware by IAT Discrimination. Special Issue on Knowledge-based System and Security, Prof. Roy Park Guest Editor, *Journal in Computer Virology and Hacking Techniques*, vol. 12, issue 3, pp. 131– 136 (DOI number 10.1007/s11416-015-0257-8), 2016.

- Jonathan Dechaux et Eric Filiol. Proactive Defense Against Malicious Documents. Formalization, Implementation and Case Studies. Special Issue on Knowledge-based System and Security, Prof. Roy Park Guest Editor, *Journal in Computer Virology and Hacking Techniques*, vol. 12, issue 3, pp. 191 – 202 (DOI number 10.1007/s11416-015-0259-6).

Revues nationales à comité de lecture

- Thomas Aubin, Baptiste David, Éric Filiol et Paul Hernault. Windows 10 - Confidentialité et sécurité de vos données. *Journal de la Sécurité Informatique MISC*, numéro 86, pp. 70–77, juillet-août 2016.

- Michel Dubois et Éric Filiol. Visualisation 3D appliquée au PRBG et à la cryptographie. *Journal de la Sécurité Informatique MISC*, numéro 83, pp. 74–82, janvier-février 2016.

- Hugo Meziani et Raphaël Pion. Détecter l ?interception des flux web chiffrés. *Journal de la Sécurité Informatique MISC*, HS 13, pp. 70–83, juillet 2016.

Conférences et articles invités (niveau international)

- Eric Filiol. *Techniques d'extraction de connaissances (data mining, big data) : définitions et enjeux*. Master class, Forum International de la Cybercriminalité (FIC) 2016, 25 janvier 2016, Lille.

- Richard Rey. *Imputabilité des connexions internet en entreprise : problématiques techniques et réglementaires. Retour d'expérience sur le projet libre ALCASAR*. Master class, Forum International de la Cybercriminalité (FIC) 2016, 25 janvier 2016, Lille.

- Éric Filiol. *Débat/échange autour de la sensibilisation et la formation en cybersécurité*, Assises Francophones de la Cybersécurité, 2-3 novembre 2016, Antananarivo, Madagascar, `https://www.auf.org/media/filer_public/72/f0/72f0b988-dbe9-48e8-97f8-8ea80888a371/programme_et_liste_des_participants_2016_10_28.pdf`

- Éric Filiol. *Souveraineté, indépendance, autonomie numérique : quelle marge de manoeuvre ?* Journées cybersécurité organisées par l'AUF dans le cadre du Projet de renforcement de la cybersécurité dans l'espace scientifique francophone, 27 et 28 juillet 2016, Tunis, Tunisie.

Conférences et articles invités (niveau national)

- Éric Filiol. *Vers une police 3.0 - Horizons et perspectives à l'horizon 2025*. Expert contributeur à la 27ème Session Nationale « Sécurité et Justice »2015 - 2016, Groupe de diagnostic stratégique (GDS) numéro 3, Institut National des Hautes Études de Sécurité et de Justice. Disponible sur `https://www.inhesj.fr/sites/default/files/fichiers_site/les_publications/les_travaux_des_auditeurs/gds3.pdf`

- Richard Rey. *Cybersécurité : La vulnérabilité des réseaux industriels*. Séminaire « Usine du futur », Nantes, 8 novembre 2016, `http://www.captronic.fr/Les-objets-connectes-au-service-de-l-Industrie-du-futur.html`

- Éric Filiol. *Défense Opérationnelle du Territoire (DOT) : de la sphère physique au domaine cyber. Pourquoi la réserve est indispensable ?*. Colloque « Une nouvelle réserve pour de nouvelles menaces », Journée Nationale du Réserviste 2016, 21, avril 2016, Laval, France

- Éric Filiol. *Etes-vous à l'abri d'une attaque informatique ?*. Atelier-débat, Universités des Entrepreneurs Mayennais organisée par le MEDEF, Laval, 7 juillet 2016.

- Éric Filiol. *IoT : Comment gérer la sécurité des objets connectés* (Exemples d ?attaques sur objets connectés : enjeux et risques d'aujourd'hui. Focus sur le milieu bancaire/de l'assurance). Journée de veille SSI du des directeurs du groupe Crédit Agricole - SA, 29 juin 2016, Montrouge.

- Éric Filiol. *Les enjeux du contrôle de la technologie de l'information*, Assemblée Générale du club d'entreprises de haute Mayenne, 24 mars 2016, Mayenne.

Conférences internationales avec comité de sélection et actes

- Baptiste David, Éric Filiol, Kévin Gallienne et Olivier Ferrand. *Heuristic and Proactive IAT/EAT-based Detection Module of Unknown Malware*. 15^{th} European Conference on Cyber Warfare and Security (ECCWS) 2016, Bundeswehr University, Munich, Germany, July 2016, $7-8^{th}$, ACPI, pp. 84–93.

- Michel Dubois et Éric Filiol. *3D Visualization Applied to PRBGs and Cryptography*. 11^{th} International Conference on Cyber Warfare and Security (ICCWS) 2016, Boston, March 17-18th, 2016, ACPI, pp. 371–381. ICCWS 2016 Best PhD Paper Award.

- Éric Filiol et Cécilia Gallais. *Combinatorial Optimization of Operational (cyber) Attacks Against Large-scale Critical Infrastructures - The Vertex Cover Approach*. 11^{th} International Conference on Cyber Warfare and Security (ICCWS) 2016, Boston, March 17-18th, 2016, ACPI, pp. 129–138.

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).

- Thomas Aubin et Paul Hernault. *Windows 10 - Security and Privacy*. Nuit du Hack, 2 juillet 2016, Parc Eurodisney, Marne la Vallée.

- Wilfried Ollivier. *Cloisonner pour mieux partager*. Conférence Pas Sage en Seine, Hacker Space festival, 3 juillet 2016, `http://data.passageenseine.org/2016/mp4/PSESHSF-2016%20-%20Wilfried%20OLLIVIER%20-%20Cloisonner%20pour%20mieux%20partager.mp4`

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.

- Richard Rey. *Réseau informatique : la surveillance à la portée de PME*. Journal SécuritéOff, 30 novembre 2016, `http://www.securiteoff.com/surveiller-facilement-son-reseau/`

- Killian Colleu. *Comment contourner un dispositif de filtrage réseau avec Tor)*. Journal SécuritéOff, 28 novembre 2016, `http://www.securiteoff.com/comment-contourner-un-dispositif-de-filtrage-reseau-avec-tor/`

- Éric Filiol. *Cyberguerre ou l'escroquerie marketing*. Journal SécuritéOff, 14 novembre 2016, `http://www.securiteoff.com/cyberguerre-ou-lescroquerie-marketing/`

- Antoine Quélard et Adrien Luyé. *Les ransomware : comment ça marche*, Journal SécuritéOff, 11 novembre 2016, `http://www.securiteoff.com/cryptoransomwares-ca-marche/`

- Éric Filiol. *Windows est pour nous une boite noire que connait très bien la NSA*, Journal SécuritéOff, 24 octobre 2016, `http://www.securiteoff.com/eric-filiol-windows-boite-noire-connait-tres-bien-nsa/`

- Jean Carette. *Un plan de reprise d'activité (PRA) adapté au PME*, Journal SécuritéOff, 10 oct. 2016, `http://www.securiteoff.com/plan-de-reprise-dactivite-pra-adapte-aux-pme/`

- Julian Alcaraz et Arnaud Lerailler. *La radio-logicielle : quels dangers pour la sécurité des objets connectés ?*, Journal SécuritéOff, 5 octobre 2016, `http://www.securiteoff.com/radio-logicielle-dangers-securite-objets-connectes/`

- Raphaël Pion et Hugo Meziani. *CheckMyHTTPS : un module de détection d'Interception de flux WEB chiffrés 1ère partie*, Magazine Programmez !, numéro 199, septembre 2016, `http://www.programmez.com/magazine/article/checkmyhttps-un-module-de-detection-dinterception-de-flux-web-chiffres-1ere-partie`

- Raphaël Pion et Hugo Meziani. *CheckMyHTTPS : un module de détection d'Interception de flux WEB chiffrés 1ère partie*, Magazine Programmez !, numéro 200, octobre 2016, `http://www.programmez.com/magazine/article/checkmyhttps-un-module-de-detection-dinterception-de-flux-web-chiffres-2e-partie`

- Alexandre Denjean. *Lutte contre le cyberterrorisme : l'ingénieur ou le hacker ?*, Journal SécuritéOff, 25 juillet 2016, `http://www.securiteoff.com/cyberterrorisme/`

- David de Oliveira. *Avast : un espion dans votre PC ?*, Journal SécuritéOff, 1er juillet 2016, `http://www.securiteoff.com/avast-un-espion-dans-votre-pc/`

- Wilfried Ollivier. *Maîtriser le BYOD ou le télétravail en entreprise*, Journal SécuritéOff, 25 juin 2016, `http://www.securiteoff.com/le-byod-et-le-teletravail/`

- Antoine Quélard et Adrien Luyé. *Décryptement d'un ransomware de type Teslacrypt 2.0*, Journal SécuritéOff, 16 juin 2016, `http://www.securiteoff.com/retour-dexperience-ransomware-de-type-teslacrypt-2-0/`

- Alexandre Denjean. *Journalistes RFI tués au Mali : la remise en cause de la version officielle (via l'OSINT)*, Journal SécuritéOff, 2 mai 2016, `http://www.securiteoff.com/exclusif-quand-les-techniques-osint-jettent-doute-sur-les-theses-officielles/`

- Hamza Bourrahim et Godeleine Champenois. *Reconnaissance faciale pour la sécurité : quelles solutions techniques ?*, Journal SécuritéOff, 25 avril 2016, `http://www.securiteoff.com/reconnaissance-faciale-securite-solutions-techniques/`

- Paul Irolla. *User tracking et Facebook : l'heure de la surveillance globale*, Journal SécuritéOff, 19 avril 2016, `http://www.securiteoff.com/user-tracking-facebook-lere-de-surveillance-globale/`

- Raphaël Pion et Hugo Meziani. *Comment intercepter des flux web chiffrés*, Journal SécuritéOff, 18 avril 2016, `http://www.securiteoff.com/interception-des-flux-web-chiffres/`

- Éric Filiol. *Les entreprises françaises : une cible facile pour les pirates*, Journal SécuritéOff, 23 mars 2016, `http://www.securiteoff.com/les-entreprises-sont-des-cibles-faciles/`

- Raphaël Pion et Hugo Meziani. *Détection d'une interception des flux Web chiffrés sous Firefox*, Journal SécuritéOff, 3 mars 2016, `http://www.securiteoff.com/detection-dune-interception-flux-web-chiffres-firefox/`

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.

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.

- Paul Irolla et Éric Filiol. *Glassbox : Dynamic Analysis Platform for Malware Android Applications on Real devices*. Arxiv preprint on arXiv.org, number 1609.04718, `http://arxiv.org/abs/1609.04718`

- Michel Dubois et Éric Filiol. *Hacking of the AES with Boolean Functions*. Arxiv preprint on arXiv.org, number 1609.03734, `https://arxiv.org/abs/1609.03734`

- Arnaud Bannier, Nicolas Bodin et Éric Filiol. *Automatic Search for a Maximum Probability Differential Characteristic in a Substitution-Permutation Network*. IACR Preprint 2016/652. This paper is the extended and revised version of the paper presented at HICSS-48, `http://eprint.iacr.org/2016/652`

- Arnaud Bannier, Nicolas Bodin et Éric Filiol. *Partition-based Trapdoor Ciphers*. IACR Preprint 2016/493, `http://eprint.iacr.org/2016/493`

Prix, qualifications et récompenses

- Michel Dubois & Éric Filiol. *Best PhD paper Award*, International Conference in Computer Warfare and Security ICCWS'2016.

- Ralph Steevens Obame de Soumbou Mbwath, Worphy Bimboutsa Koumba, Hamza Bourrahim, Godeleine Champenois. OpenFacetracker (système open source de détection et de reconnaissance faciale). Prix jury de la « Student Demo Cup »(Open source Summit), https://blog.econocom.com/blog/la-student-demo-cup-2016-recompense-4-projets-innovants/

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

Pour l'année 2016 la médiatisation des travaux du laboratoire a été, encore une fois, particulièrement riche et intense tant pour la presse écrite, qu'audio-visuelle et Internet, en France et à l'étranger. Pour 2016, comme pour 2014, ce sont plusieurs centaines de « points presse » identifiés pour le laboratoire (France et étranger)

Les principaux sont :

- Éric Filiol. Interview pour le site/webtv Maddyness « *#Cybersécurité : vers un marche de la confiance* ». 5 décembre 2016, https://www.maddyness.com/business/2016/12/05/cybersecurite-en-route-vers-un-marche-de-la-confiance/

- Éric Filiol et Paul Hernault. Interview et démonstrations dans l'émission Cash Investigation « *Marchés publics - Le grand dérapage* ». France 2, 18 octobre 2016, 20 :55.

- Courrier de la Mayenne. *Le compteur Linky, un espion à la maison ? L'ESIEA-OUEST prépare la parade*, 13 octobre 2016.

- Éric Filiol. Interview France Inter « *Lutte anti-terroriste : les nouveaux cerveaux du renseignement français* ». Émission Secrets d'Info du 6 octobre 2016, https://www.franceinter.fr/societe/secrets-d-info

- Éric Filiol. Collaboration avec le Journal Sud-Ouest pour une série de 5 articles dans le cadre de la série « *Un été Sud-ouest* »sur la protection de la vie privée. Articles du 28 juillet 2016 (http://www.sudouest.fr/2016/07/28/les-ecrits-en-disent-bien-plus-que-ce-que-l-on-croit-2449470-4803.php), du 4 aout 2016 (http://www.sudouest.fr/2016/08/04/le-compteur-linky-un-indic-dans-la-maison-2456568-4585.php), du 11 aout 2016 (http://www.collegegujan.fr/sites/technopc/img/nouvelles/photosendisentlong.pdf?captchatexte=773edd0405fa42f428c795237651f42e), du 18 aout 2016 (http://www.collegegujan.fr/sites/technopc/img/nouvelles/naviguezenpaix.pdf?captchatexte=773edd0405fa42f428c795237651f42e) et du 25 aout 2016 (http://www.sudouest.fr/2016/08/25/a-la-recherche-d-un-quart-d-heure-de-vie-privee-2478206-4585.php).

- Éric Filiol. Interview dans le journal El Pais, *Cuando los virus adoraban a Apple*, 16 février 2016, http://tecnologia.elpais.com/tecnologia/2016/02/14/actualidad/1455487219_496751.html

- Richard Rey. *Quel enseignement pour la cyber-sécurité ?*, tribune de janvier 2016 pour Le Figaro, reprise le 9 février 2016 sur http://www.informatiquenews.fr/quel-enseignement-pour-la-cyber-securite-richard-rey-esiea-44578

- Richard Rey. *Le cursus pour devenir un pro de la cyber-sécurité*, 25 janvier 2016, `http://www.challenges.fr/`

- Zataz, *CheckMyHTTPS, l'anti interception Man in the Middle SSL/TLS*, 17 mars 2016, `http://www.zataz.com/checkmyhttps-lanti-interception-ssltls/#axzz434wYfHMt`

- Marc jacob. *CheckMyHTTPS » : un logiciel qui vérifie que vos connexions WEB sécurisées ne sont pas interceptées*, Global Security Mag, avril 2016, `http://www.globalsecuritymag.fr/Des-etudiants-de-l-ESIEA-inventent,20160426,61634.html`

Merci également à Ouest France, L'Informaticien, Cultures Sciences, Le journal des entreprises, 01net, PubliNews, Release Capital, Zataz, L'Informaticien, Usbek et Rica, Challenges, Undernews... 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 2016 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 2015 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).

- Nouvelles fonctionnalités 2016.
  - Deux déploiements d'ALCASAR décidés dans les services de l'état :
    — l'ensemble des commissariats de police via la PSSI du Ministère de l'Intérieur,
    — l'ensemble des préfectures et sous-préfectures par décision du « *Service Interministériel Départemental des Systèmes d'Information et de Communication* »(SIDSIC).

    C'est la future version 3.1 qui est mise en avant. En effet, celle-ci intégrera des fonctionnalités demandées par ces ministères.
  - Migration vers *Mageia* 5.0.
  - Interception HTTPS.
  - Filtrage optionnel des nœuds TOR.
  - Cartographie et réécriture des fonctions PHP prévues d'être dépréciées.
  - Migration vers le codage de caractères UTF8 (php + mariadb + radius).
  - Traitement d'un bug apparaissant lors de la traversée d'un tunnel IPSEC. Le problème est résolu pour les tunnels créés par des *appliances* industriels (Stormshield + Arkoon + Netasq). Le problème persiste pour certaines tunnels particuliers (investigation en cours)

- 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).

  En 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 2016, l'effort a été de revoir entièrement l'interface graphique (source de problèmes lors de la compilation selon les plateformes, existence de vulnérabilités) et de produire une interface portable

multi-OS en langage Qt (courant 2017).
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 dans le site de Laval.

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

- Richard Rey. Poursuite du développement de la plate-forme de réception satellite libre. Cette plateforme peut être visitée dans 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.

- Paul Irolla. Projet *Glassbox*. Il s'agit du premier système d'analyse dynamique de malware Android sur machine réelle. Cela est une contremesure à l'évasion des machines virtuelles, protection que de nombreuses familles de malwares mettent en place actuellement. Glassbox est capable de collecter les appels Java, les appels système ainsi que le contenu des communications en clair et chiffrées. C'est un matériau de base pour la détection de malwares par apprentissage automatique. Glassbox ne requiert aucune interaction manuelle : il installe et teste automatiquement les applications. Le système Glassbox est capable d'exécuter en moyenne 13,52 % de nouveaux blocs de base par rapports aux outils de référence.
  Dans le cadre de ce projet, une base de données, dénommée *AndroCoverage* a été créée. Il s'agit d'une base de données couplée à des outils pour l'évaluation des méthodes de tests automatiques d'applications Android. Cela permet de mesurer la couverture de code moyenne sur une base de données de 100 applications provenant de F-Droid. Le but de ce projet est d'établir une base commune entre scientifiques afin d'évaluer objectivement les outils et méthodes de test automatique.

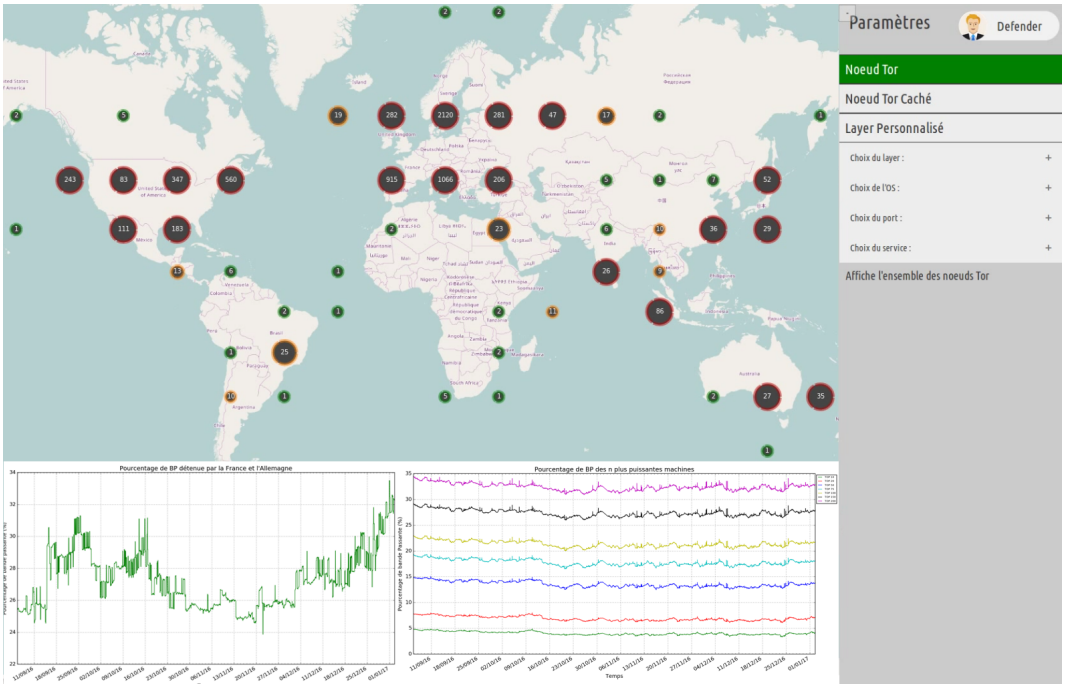
- Hugo Meziani. *ExitNodesAnalyzer*. Outil en python qui prend en paramètre une adresse IP et détermine si elle est, ou a été (depuis 2010) nœud de sortie sur TOR. Disponible sur `https://github.com/HugoMeziani/ExitNodesAnalyzer/`

- Éric Filiol et Paul Hernault. Projet *OpenDAVFI*. Reposant sur les travaux menés pour le projet DAVFI, le projet OpenDAVFI reprend un premier module dédié au traitement proactif des codes malveillants contenus dans les documents bureautiques (Microsoft Office, Libre Office, PDF...) et ne particulier les ransomware.

Cet outil et le code écrit sont totalement différents de ceux du projet DAVFI (voir aspects légaux concernant le projet DAVFI). Il se présente sous la forme d'un filtre au niveau du serveur de mail (MTA) et fonctionne sous forme de service. Postfix fait appel au service dès qu'un mail a besoin d'être analysé. Le module peut servir comme serveur mail de transition (conseillé). Il suffit pour cela de monter un serveur postfix en amont du serveur de mail ou ce module OpenDAVFI est déployé. On configure ensuite Postfix pour qu'il fonctionne en mode relai et délivre les mails au serveur de mail original après traitement (invisible donc, pour le serveur de mail original). La phase de test a confirmé l'efficacité de cet outil à contrer proactivement et systématiquement les ransomware inconnus (comparaison avec les résultats du site `www.virustotal.com`). Cet outil, qui sera rendu officiel en mars 2017, est libre comme tous les futurs produits OpenDavFi.

- Éric Filiol, Cément Coddet, Maxence Delong, Olivier Fatou et Clément Suhard. Projet *Internet Health*.

Ce projet à 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 métadonées 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.



Activités scientifiques diverses

Domaine institutionnel

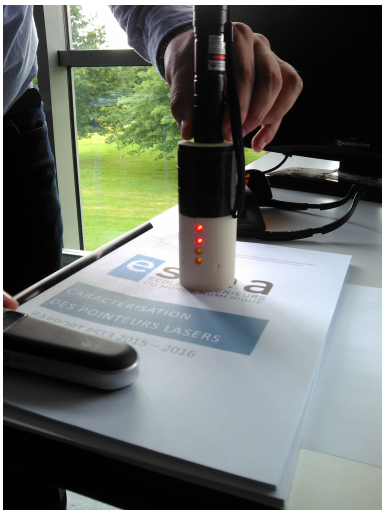
Le laboratoire est engagé fortement dans le soutien (à titre gracieux) des différents organismes régaliens de l'État. Outre le fait d'inculquer à nos jeunes (chercheurs, étudiants) la notion de service au profit de leur pays, elle permet également de se confronter à des cas critiques et opérationnels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

- Éric Filiol, Audition devant l'Institut des Hautes Études de la Sécurité et de la Justice, 27ème session nationale « *Sécurité et Justice* », groupe de diagnostic stratégique numéro 3, « *Vers une police 3.0, enjeux et perspectives à l'horizon 2025* », 2 décembre 2015.

- Richard Rey, Paul Hernault, Rapahël Pion. Présentation technique aux DSI des préfectures de l'ouest, 28 juin 2016. Les retombées suivantes sont constatées :
  — ALCASAR : validation du déploiement et désignation de la préfecture 53 comme référent national.
  — Sécurité Windows 10 : la DINSIC (*Direction Interministérielle Départementale des Systèmes d'Information et de Communication*) mandate la préfecture 53 pour se rapprocher de l'ESIEA suite à ses travaux dans le domaine, pour une participation au groupe de travail « postes de travail, harmonisation interministérielle et future migration Windows 10 ». Objectif : rendre le poste Windows 10 le plus muet possible tout en assurant les fonctionnalités demandées.

- Kévin Guinet (3A), Aurélien Ruisseau (3A), Richard Rey. Présentation au directeur départemental de la sécurité publique de la Mayenne, d'un dispositif de détection de lasers réalisé à l'occasion d'un Projet Scientifique et Technique 4A. Ce dispositif permet de qualifier les

infractions liées à l'utilisation des lasers. Les étudiants souhaitent maintenant améliorer leur création pour déboucher sur un second prototype plus élaboré et industrialisable.



- Thomas Aubin, Paul Hernault et Hugo Meziani. Investigation numérique suite à une demande d'aide de l'ESTACA en liaison avec les forces de l'ordre. L'enquête de police a ensuite permis, grâce aux éléments techniques fournis, à l'arrestation du coupable de l'attaque qui a avoué les faits. `http://www.20minutes.fr/nantes/1992779-20170110-laval-exclu-ecole-ingenieurs-avoir-detruit-90-ordinateurs`.

Participation à des comités de programmes

Le laboratoire a participé à aux comités de programme suivants :

- ICCWS 2016, ECCWS 2016, ARES/WMA 2016

- *International Workshop on Trust in Cloud Computing*, London, décembre 2015, `http://computing.derby.ac.uk/IWTCC2015/`

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)

- *SCIENCE CHINA Information Sciences* (A. Bannier)

- *Revista Antioqueña de las Ciencas Computacionales Y la Ingeniería de Software* (É. Filiol, membre du board).
- *International Workshop on Trust in Cloud Computing (IWTCC' 2016)* (É. Filiol, membre du board)

- *ARES 2016 - 11th International Conference on Availability, Reliability and Security* (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. Organisation d'un challenge de sécurité en conditions quasi-réelles dans le cadre du programme Erasmus. Le thème était celui de la lutte anti-terroriste. Le challenge, intitulé « *12 hours to save Amsterdam from a terrorist attack !* », consistait à empêcher, en temps limité, une attaque terroriste dans le centre d'Amsterdam. De l'analyse de scellés et de renseignements à la recherche sur le terrain, les équipes devaient identifier le lieu, la date et trouver les informations nécessaires à la réalisation de leur mission. Participation de Baptiste David et Paul Hernault pour le soutien technique.

Site web : `http://www.amsterdamuas.com/education/programmes/exchange-programmes/information-technology/international-security-summer-camp/international-security-summer-camp.html`

- Richard Rey. Organisation de OpenESIEA à Laval (manifestation autour du libre et des technologies liées au logiciel libre), mars 2016. Cet événement a été organisé avec le concours

d'étudiants.
Site officiel : `http://www.esiea.fr/12-fevrier-openesiea-journee-dimmersion-campus-laval/`

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 12 (quatre numéros) a été publié en 2016.

Contrats et transferts technologiques 2016

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).

- Contrat Calmwater. Implémentation d'algorithmes de détection de fuites d'eau et de contamination biologique dans des réseaux intelligents de distribution d'eau.

- Accord Cadre cyber piloté par CEIS. Sous-traitance.

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.