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

Rapport d'activité 2015

- § -

ESIEA

Axe Confiance Numérique et Sécurité

Table des matières

Rapport d'activités 2015
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) sur le plan réglementaire 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 2016 (dossier initié en 2015), 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 $CNS/(C+V)^O$.

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 de recherche réels (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 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 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 socíété 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).

- Carte à puce, RFID, NFC, 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* et *big data* appliquées à la sécurité et au renseignement.

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, audits de sécurité.

- 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

  – Laurent Beaudoin (Ing. - Ph D)
  Email : `laurent.beaudoin@esiea.fr`
  Algorithmique, cartographie, imagerie.

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

  – Jonathan Dechaux (Ing. - Ph D)
  Email : `jonathan.dechaux@esiea.fr`
  Sécurité des applications - Programmation et développement sécurisés.

  – Olivier Ferrand (Ing. et doctorant)

Email : olivier.ferrand@esiea.fr
Programmation sécurisée, sécurité système antivirale.

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

- Doctorants

  – Arnaud Bannier
  Email : arnaud.bannier@esiea.fr
  Mathématiques discrètes, combinatoire, cryptologie.

  – 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

  – Baptiste David (Ing.)
  Email : bdavid@esiea.fr
  Virologie, cryptographie, algorithmique, développement noyau Windows.

  – 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.

  – Amicelli Paul (4A/5A)
  Email : paul.amicelli@et.esiea.fr
  Algorithmique, sécurité Linux, virologie.

  – Aubin Thomas (3A/4A)

Email : thomas.aubin@et.esiea.fr
Algorithmique, sécurité Windows, virologie.

– Bertin Tristan (4A/5A)
Email : tristan.bertin@et.esiea.fr
Algorithmique, sécurité Windows, virologie.

– Bonduelle Lucie (2A/3A)
Email : lucie.bonduelle@et.esiea.fr
Algorithmique, calcul parallèle, cryptographie.

– Bouteiller Jordan (3A/4A)
Email : jordan.bouteiller@et.esiea.fr
Sécurité NFC.

– Coddet Clément (2A/3A)
Email : clement.codet@et.esiea.fr
Stéganographie.

– Delong Maxence (2A/3A)
Email : maxence.delong@et.esiea.fr
Algorithmique, calcul parallèle, cryptographie.

– Demme Tanguy (3A/4A)
Email : tanguy.demme@et.esiea.fr
Tracking, géoréférencement automatique de cible sous-marine.

– De Soete Quentin (2A/3A)
Email : quentin.desoete@et.esiea.fr
Sécurité réseau.

– Fourcade Pierre-Ange (2A/3A)
Email : fourcade@et.esiea.fr
Sécurité réseau.

– Gattolin Nicolas (2A/3A)
Email : nicolas.gattolin@et.esiea.fr
Sécurité réseau.

– Girardat Sébastien (4A/5A)
Email : sebastien.girardat@et.esiea.fr
Systèmes, reverse-engineering.

– Gobillot Thomas (3A/4A)
Email : thomas.gobillot@et.esiea.fr
Sécurité NFC.

- Hernault Paul (3A/4A)
  Email : `paul.hernault@et.esiea.fr`
  Algorithmique, sécurité Windows, virologie.

- Meziani Hugo (3A/4A)
  Email : `hugo.meziani@et.esiea.fr`
  Algorithmique, sécurité Linux, virologie.

- Ollivier Wilfried (4A/5A)
  Email : `wilfried.ollivier@et.esiea.fr`
  Stéganographie.

- Pion Raphael (3A/4A)
  Email : `raphael.pion@et.esiea.fr`
  Algorithmique, sécurité Linux, virologie.

- Siccardi Clément (3A/4A)
  Email : `clement.siccardi@et.esiea.fr`
  Algorithmique, sécurité Linux, virologie.

- Suhart Clément (2A/3A)
  Email : `clement.suhart@et.esiea.fr`
  Algorithmique, calcul parallèle, cryptographie.

- Swaenepoel Guillaume (4A/5A)
  Email : `guillaume.swaenepoel@et.esiea.fr`
  Stéganographie.

- Thieuleux Jonathan (4A/5A)
  Email : `jonathan.thieuleux@et.esiea.fr`
  Algorithmique, sécurité Linux et embarqué, virologie.

- Ventuzelo Patrick (3A/4A)
  Email : `patrick.ventuzelo@et.esiea.fr`
  Sécurité NFC.

Thèses et stages

Thèses soutenues en 2015

- Thèse de Jonathan Dechaux *Formalisation du concept de logiciel antivirus et conception d'une méthologie et de techniques d'évaluation des techniques antivirales.* École doctorale École Polytechnique, mention très honorable.

  Composition du jury : Olivier Festor (Télécom Nancy - INRIA, rapporteur), Radu State

(Université du Luxembourg, rapporteur), Johann Barbier (ARX Arcéo, Ph D, examinateur), Eddy Deligne (Ministère de la Défense/DGA-MI, examinateur), Jean-Marc Steyaert (président, École Polytechnique), Éric Filiol (directeur de thèse, ESIEA).

Thèses en cours

- Thèse de Loïca Avanthey. *Mosaïquage de données 3D obtenues par des drones hétérogènes à l'interface air/eau*. École doctorale Sup Télécom ParisTech. Cette thèse a débuté en septembre 2010 (bourse DGA). Soutenance prévue au premier semestre 2016.

- Thèse de Michel Dubois. *Etude combinatoire de la mise en équations sur $GF(2)$ des algorithmes de chiffrements par bloc*. École doctorale École Polytechnique, Palaiseau. Cette thèse a débuté en septembre 2010. Soutenance prévue en mars/avril 2016.

- Thèse de Olivier Ferrand *Techniques combinatoires de détection de malware*. École doctorale École Polytechnique, Palaiseau. Cette thèse a débuté en septembre 2012. Soutenance prévue juin 2016.

- Thèse (CIFRE) de Cécilia Gallais. *Formalisation et modélisation algébriques des concepts de cyberattaque et d'infrastructure critique*. École doctorale École Polytechnique, Palaiseau. Cette thèse a débuté en décembre 2013. Soutenance prévue décembre 2016.

- Thèse d'Arnaud Bannier. *Analyse combinatoire des systèmes de chiffrement par bloc avec trappes*. École doctorale École Polytechnique, Palaiseau. Cette thèse a débuté en décembre 2013. Soutenance prévue décembre 2016.

- Thèse de SOLAT Siamak. *La sécurité des applications sous NFC*. Thèse UMPC - LIP6 dirigée par Guy Pujolle et co-dirigée par Pascal Urien et Vincent Guyot, `http://www.lip6.fr/actualite/personnes-fiche.php?ident=D1543`.

- 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.

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

- Paul Amicelli *Projet Gostxboard : librairie anti-keylogger pour Windows 7, 8 et 10*, Stage technique/MSc I ESIEA, 4 mois.

- Matthias Astourne, Irvin Boyer, Killian Colleu et Raherimanana Tamby. *Dispositifs de contournement de systèmes de filtrage réseau*. Projet technique/MSc I ESIEA, 4 mois.

- Tristan Bertin. *Impléntation d'algorithmes cryptographiques dans la suite GostCrypt*. Stage technique/MSc I ESIEA, 4 mois.

- Florian Brouillet, Jean Carette, Alexandre Despots & Ollivier Wilfried. *CLÉS : Container Logiciel Étanche et Sécurisé*. Projet technique/MSc I ESIEA, 4 mois

- Étienne Chauve, Clément Michel, Vincent Lorion & Thomas Signeux. *Plate-forme d'interception satellite*. Projet technique/MSc I ESIEA, 4 mois

- Marc-Antoine Crue, Édouard Cortes, Floriane Fontaine & Louis-Julien GO. *Domotique : sécurité et respect de la vie privée*. Projet technique/MSc I ESIEA, 4 mois

- David De Oliveira *Création d'un module pédagogique d'audits de Sécurité des Systèmes d'Information (SSI)*, Stage de fin d'études d'ingénieur, ESIEA, 6 mois.

- Audrey Gilet, Adrien Luyé, Antoine Quélard & Mickaël Salomez. *Cage optique pour drone de surveillance*. Projet technique/MSc I ESIEA, 4 mois

- Sébastien Girardat. *Conception et implémentation d'un framework de scan et d'exploration automatiques et distribués du réseau Internet à grande échelle*, Stage technique/MSc I ESIEA, 4 mois.

- Guillaume Swaenepoel *Conception et implémentation d'une nouvelle interface sécurisée en Qt pour la suite GostCrypt*. Stage technique/MSc I ESIEA, 4 mois.

- Jonathan Thieuleux. *Implementation d'algorithmes de chiffrement symétriques addtionnels dans le noyau Linux*. Stage technique/MSc I ESIEA, 4 mois.

Projets et Stages 2015 (cycle L)

- Clément Siccardi et Raphaël Pion. *Étude de la sécurité et de la stabilité d'applications Linux par fuzzing*. Projets technique/BSc, ESIEA, 3 mois.

- Lucie Bonduelle, Maxence Delong, Damien Di Gianni & Maxime Henry. *Construction, mise en œuvre, administration et exploitation d'un supercalculateur SGI sous OpenBSD*. Projet technique/BSc, ESIEA, 3 mois.

- Hamza Essayegh, Alexandre Laurent, Vincent Le Fournis & Hugo Meziani. *RFID et sécurité : démonstration de défauts d'implémentation*. Projet technique/BSc, ESIEA, 3 mois.

Publications du laboratoire

Livres et chapîtres d'ouvrages

- Éric Filiol. Texte de l'audition devant la commission parlementaire « *Sécurité numérique et risques : enjeux et chances pour les entreprises* ». Rapport 2541 (Assemblée Nationale)/271 (Sénat) de l'Office Parlementaire d'Évaluation des Choix Scientifiques et Technologiques (OPECST), tome II, pp. 181–188, 2 février 2015. Disponible sur `http://www.senat.fr/rap/r14-271-2/r14-271-21.pdf`

- Éric Filiol & Grégory Commins. *Unrestricted Warfare versus Western Traditional Warfare : A Comparative Study*. In : Leading Issues in Information Warfare and Security Research, Volume 2, pp. 73–89, Julie Ryan Editor, Academic Publishing International Ltd, ISBN 978-1-908272-08-9, 2015.

Revues internationales à comité de lecture

- Gregory Commin & Eric Filiol. Unrestricted Warfare vs Western Traditional Warfare : a Comparative Study. *Journal in Information Warfare*, volume 14, numéro 1, pp. 14–23.

- Olivier Ferrand. How to detect the Cuckoo Sandbox and to Strengthen it ? *Journal in Computer Virology and Hacking Techniques*, volume 11, numéro 1, pp. 51–58.

- Valentin Hamon. Android botnets for multi-targeted attacks. *Journal in Computer Virology and Hacking Techniques*, volume 11, numéro 4, pp. 193–202.

- Ashwin Kalbhor, Thomas Austin, Eric Filiol, Sébastien Josse & Mark Stamp. Dueling Hidden Markov Models for Virus Analysis. *Journal in Computer Virology and Hacking Techniques*, volume 11, numéro 2, pp. 103–118.

Revues nationales à comité de lecture

- Éric Filiol. *Comment vraiment paralyser un pays à l'aide du cyber*. Les Cahiers de la Revue de Défense Nationale, « Penser autrement », 10 juin 2015, pp. 103–110, `http://fr.calameo.com/read/00055811533cd3636d191`

Conférences et articles invités (niveau international)

- Eric Filiol. *The Control of technology by nation states : Past, Present and Future - Intelligence versus Forensics Aspects*. C0c0n 2015 (CyOps Con), International Cyber Security and Policing Conference 2015, Kochi, India, August 20th-21st, 2015, `http://is-ra.org/c0c0n/2015/uploads/speakers/c0c0n2015_keynote_day2.pdf`.

- Eric Filiol. *Quelles solutions innovantes en matière de chiffrement et en cryptologie*. Master class, FIC 2015, 20 janvier 2015, Lille.

Conférences et articles invités (niveau national)

- Éric Filiol. *La problématique du contrôle des technologies de l'information*. Keynote Conférence DEVOXX, 8 au 10 avril 2015, Paris, `https://www.parleys.com/tutorial/keynote-de-lequipe-devoxx-france`.

- Éric Filiol. *Le contrôle des technologies de l'information : enjeux cachés*. Conférence régionale des Commissaires aux Comptes, Laval, 6 décembre 2015, Lactopole, Laval.

- Éric Filiol. *Les enjeux du contrôle des technologies de l'information*. Conférence annuelle des clubs Rotary du district 1650, 14 mars 2015, Mayenne.

Conférences internationales avec comité de sélection et actes

- Éric Filiol and Cécilia Gallais. *How Internal and External Dependencies can Affect Infrastructure's Security*. 14^{th} European Conference on Cyber Warfare and Security ECCWS-15, Hatfield, UK, July 2-3rd, 2015. In : Proceedings of the 14^{th} European Conference on Cyber Warfare and Security, pp. 363–372, Academic Conferences & Publishing International.

- Arnaud Bannier, Nicolas Bodin & Éric Filiol. *Automatic Search for a Maximum Probability Differential Characteristic in a SPN*. HICSS 2015, Software technology, Cybersecurity and Software Assurance Track, Hawai, January 5-8th, 2015. Prix du meilleur papier 2015, catégorie *(*Software Technology).

- Laurent Beaudoin, Loïca Avanthey, Antoine Gademer, Michel Roux & Jean-Paul Rudant. *Dedicated payloads for low altitude remote sensing in natural environments*. ISPRS Geospatial Week 2015, 28 Septembre - 3 Octobre 2015, La Grande Motte, France. Actes disponibles in : *International Society for Photogrammetry and Remote Sensing archives (ISPRS)*, Volume XL-3/W3, `http://www.int-arch-photogramm-remote-sens-spatial-inf-sci.net/XL-3-W3/index.html`

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).

- Paul Amicelli & Baptiste David. *How to Secure the Keyboard Chain*. Conférence DefCon 23, 6 - 9 août, 2015, Las Vegas. Vidéo sur `https://www.youtube.com/watch?v=W5B-zjaDzfU`

- Paul Amicelli & Baptiste David. *How to Secure the Keyboard Chain II*. C0c0n 2015 (CyOps Con), International Cyber Security and Policing Conference 2015, Kochi, India, August 20th-21st, 2015.

- Paul Irolla. *(In)Security of Mobile Banking ... and of other Apps*. C0c0n 2015 (CyOps Con), International Cyber Security and Policing Conference 2015, Kochi, India, August 20th-21st,

2015.

- Éric Filiol & Paul Irolla. *(In)Security of Mobile Banking. The Asian Area.* Black Hat Asia 2015, Singapore, 26 et 27 Mars 2015, `https://www.blackhat.com/asia-15/archives.html#Filiol`.

- Hugo Meziani & Raphaël Pion. *CheckMyHttps*, 32ème Chaos Computer Congress (32C3), Hambourg, 26 décembre 2015, vidéo sur `https://media.ccc.de/v/32c3-7559-lightning_talks_day_3#video` (index 1 :14 :09).

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.

- Guillaume Swaenepoel & Wilfried Ollivier. *La stéganographie ou l'art de bien cacher les données (partie 1).* Journal SécuritéOff, 1er janvier 2015, `http://www.securiteoff.com/la-steganographie-ou-lart-de-bien-cacher-des-donnees-partie-1/`

- Guillaume Swaenepoel & Wilfried Ollivier. *La stéganographie ou l'art de bien cacher les données (partie 2).* Journal SécuritéOff, 1er février 2015, `http://www.securiteoff.com/la-steganographie-ou-lart-de-bien-cacher-des-donnees-partie-2/`

- David De Oliveira. *AVAST : un espion dans votre PC.* Journal SécuritéOff, 1er mars 2015, `http://www.securiteoff.com/avast-un-espion-dans-votre-pc/`

- Éric Filiol. *The reality of cyberwar : how to paralyze the USA really*, Journal SécuritéOff, 29 avril 2015, `http://www.securiteoff.com/reality-of-cyberwar-how-to-paralyze-the-usa-really/`

- Éric Filiol. *Les juges ignorent la notion de donnée*, Journal SécuritéOff, 10 mai 2015, `http://www.securiteoff.com/les-juges-ignorent-la-notion-de-donnees/`

- Floriane Fontaine. *Domotique : la fuite de donnnées*, Journal SécuritéOff, 1er juin 2015, `http://www.securiteoff.com/domotique-la-fuite-des-donnees/`

- Wilfried Ollivier. *Le BYOD et le télétravail*, Journal SécuritéOff, 5 juin 2015, `http://www.securiteoff.com/le-byod-et-le-teletravail/`

- Raphaël Pion & Clément Siccardi. *Linux est-il plus stable et sécurisé que Windows (partie I) ?*, Journal SécuritéOff, 6 juin 2015, `http://www.securiteoff.com/linux-est-il-plus-stable-et-securise/`

- Raphaël Pion & Clément Siccardi. *Linux est-il plus stable et sécurisé que Windows (partie II) ?*, Journal SécuritéOff, 10 juin 2015,

http://www.securiteoff.com/linux-est-il-plus-stable-et-securise-2/

- Raphaël Pion & Hugo Meziani. *Comment intercepter des flux Web chiffrés*, Journal SécuritéOff, 5 juillet 2015, http://www.securiteoff.com/interception-des-flux-web-chiffres/

- Thomas Aubin & Paul Hernault. *Voitures connectées : les différentes failles (partie I)*, Journal SécuritéOff, 11 juillet 2015, http://www.securiteoff.com/les-failles-des-voitures-connectees-partie-1/

- Thomas Aubin & Paul Hernault. *Voitures connectées : les différentes failles (partie II)*, Journal SécuritéOff, 11 juillet 2015, http://www.securiteoff.com/voitures-connectees-2-2/

- Paul Amicelli. *Comment fonctionnent les keyloggers*, Journal SécuritéOff, 12 juillet 2015, http://www.securiteoff.com/comment-fonctionnent-les-keyloggers-2/

- Killian Colleu. *Comment contourner un filtrage réseau avec TOR*, Journal SécuritéOff, 12 juillet 2015, http://www.securiteoff.com/comment-contourner-un-dispositif-de-filtrage-reseau-avec-tor/

- Paul Irolla. *Applications bancaires : une sécurité baclée (partie I)*, Journal SécuritéOff, 30 octobre 2015, http://www.securiteoff.com/applications-bancaires-une-securite-baclee-12/

- Vincent Lorion. *Un projet de plateforme d'interception satellitaire*, Journal SécuritéOff, 2 novembre 2015, http://www.securiteoff.com/un-projet-de-plate-forme-dinterception-satellitaire/

- Paul Irolla. *Applications bancaires : une sécurité baclée (partie II)*, Journal SécuritéOff, 2 novembre 2015, http://www.securiteoff.com/applications-bancaires-une-securite-baclee-22/

- Adrien Luyé & Antoine Quélard. *Vidéprotection : comment éviter de tout stocker et de tout traiter.*, Journal SécuritéOff, 24 novembre 2015, http://www.securiteoff.com/videoprotection-eviter-de-stocker-de-traiter/

- Paul Irolla. *Le danger d'une cartographie mondiale des points d'accès Wifi*, Journal SécuritéOff, 27 novembre 2015, http://www.securiteoff.com/dangers-dune-cartographie-mondiale-points-dacces-wi-fi/

Prix, qualifications et récompenses

- Arnaud Bannier, Nicolas Bodin & Éric Filiol. Prix du meilleur papier 2015, catégorie *(*Software Technology), conférence HICSS 2015 (rang A), Hawaï, janvier 2015, http://www.hicss.org/#!hicss48highlights/c2002 et https://drive.google.com/file/d/0B6BlkqAoxXq1eTIzUF96VDdCNGM/view

- Nicolas Bodin. Qualification Maître de Conférence, numéro 15227275970, section 27, CNU, campagne 2015, 31 janvier 2015.

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

Pour l'année 2015 la médiatisation des travaux du laboratoire a été particulièrement riche et intense tant pour la presse écrite, qu'audio-visuelle et Internet, en France et à l'étranger. Pour 2015, comme pour 2014, ce sont plus de 1000 « points presse » identifiés pour le laboratoire, avec une forte progression à l'étranger.

Les principaux sont :

- Éric Filiol. Magazine *On est plus des pigeons*. Interview sur la sécurité du cloud, 2 février 2015, 20 :50, `http://www.france4.fr/emissions/on-n-est-plus-des-pigeons/enquete/le-cloud-est-il-bien-securise_298559`

- Éric Filiol. Magazine M6 *66 minutes*, interview et démos sur les risques liés au téléphones portables, 3 mai 2015, 17 :15.

- Éric Filiol, interview *Cyberguerre et souveraineté*, Agence Info Libre, 28 juillet 2015, `http://www.agenceinfolibre.fr/eric-filiol-cyberguerre-et-souverainete/`.

- Éric Filiol. Interview NoLimitSecu du 16 aout 2015 sur le projet GostCrypt, `http://www.nolimitsecu.fr/gostcrypt/`

- Éric Filiol. Interview et démonstrations de cyber attaques dans l'émission Infrarouge « *On nous écoute : Cyberguerre, l'arme fatale* », France 2, 22 septembre 2015, 22 :30, `http://www.france2.fr/emissions/infrarouge/diffusions/22-09-2015_341460`

- Éric Filiol. Interview et démonstrations dans l'émission Envoyé Spécial « *Comment les djihadistes communiquent-ils entre eux ?* », France 2, 3 décembre 2015, 21 :30, `http://www.francetvinfo.fr/replay-magazine/france-2/envoye-special/video-envoye-special-comment-les-djihadistes-communiquent-ils-entre-eux_1204377.html`

- Éric Filiol, participation au débat « *Terrorisme, État d'urgence, où sont les solutions ? Journaliste, renseignement, stratégiste, hacker* ». Chaîne Thinkerview, 3 décembre 2015, `https://www.youtube.com/watch?v=fmgxfvbAMK8`

- Portail de l'Intelligence économique, `http://www.portail-ie.fr/article/1190/La-cryptologie-au-21e-siecle-vers-de-nouveaux-enjeux-de-souverainete-nationale`, 27 mars 2015.

Merci également à Ouest France, 20Minutes.fr (plusieurs interviews et articles), Le journal Le Monde (plusieurs interviews et articles), Dagens Naeringsliv (DN), Sciences & Avenir, Science & Vie Junior, Capital, L'Express, Usine-digitale.fr, Reuters, Digital News Asia, Deutschland Radio, Mediapart, L'Informaticien, La Croix, Metronews, Usbek et Rica, Challenges... 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 2015 a vu la poursuite et/ou la clôture des projets initiés depuis 2011 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) dans les domaines suivants :
  ◦ Nouvelles fonctionnalités 2015.
    ◇ Évolution du système hôte vers Mageia V4.1.
    ◇ Amélioration du dispositif de filtrage :
      – Ajout d'une liste blanche.

  - Traitement différencié des noms de domaine, des URLs et des adresses IP.
  - Filtrage de l'accès au réseau TOR.
  - Import massif par fichiers (CERT, CALID, listes étrangères).
  - Activation/désactivation par utilisateur.
- ◇ Mise à jour d'ALCASAR possible via SSH.
- ◇ Ajout des statistiques d'utilisation de la bande passante.

- 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 prévue début 2016).
  Site officiel : `https://www.gostcrypt.org`

- Richard Rey et Jonathan Dechaux. Création d'une plate-forme d'analyse de sécurité des objets Domotiques. 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. Création d'une plate-forme HackRF. Cette plateforme peut être visitée dans le site de Laval.

- Richard Rey. Création d'une 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.
  Le projet Checkmyhttps a été présenté au Chaos Communication Congress en décembre 2015, un des rendez-vous incontournables du monde de la sécurité qui réunit chaque année plus de 8.000 participants de la scène hacker internationale. Il s'agit d'une extension à installer sur votre navigateur web Firefox. Ce projet a déjà été bien accueilli par cette communauté de spécialistes dans le domaine, `https://checkmyhttps.net`
- Paul Irolla. Plate-forme d'analyse statique et dynamique des applications Android (plateforme non publique à ce jour, seuls les résultats le sont). Présentée au 31C3 à Hambourg en décembre 2014. Les vulnérabilités trouvées pour la phase I de l'étude (applications bancaires mobiles) ont été communiquées aux banques concernées (BNP Paribas, JP Morgan, Commerz Bank, banques asiatiques...). Les résultats seront publiés une fois les vulnérabilités identifiées corrigées. Les outils suivants ont été développés en 2015 :
  - Outil *Egide* : programme d'analyse statique d'application Android.
  - Outil *Panoptes* : programme d'interception et d'analyse des communications réseaux d'applications Android.

  - Outil *Tarentula* : web crawler massif d'applications Android.
  - Outil *Smart monkey* : programme de tests automatiques des fonctionnalités d'applications Android.

  Une convention de collaboration avec une grande banque française est en cours de finalisaiton pour signature en 2016.

- Paul Amicelli & Baptiste David. Projet Gostxboard. *GostxBoard is a beta module developed to improve Windows's security, by protecting the system from a wide range of keyloggers. The module consists of a kernel mode driver and an API which can be used by developpers to improve the security of their applications*, `https://bitbucket.org/WhiteKernel/gostxboard`

Activités scientifiques diverses

Domaine institutionnel

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

- 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.

- Éric Filiol. Groupe de travail/conférence *Protecting online privacy by enhancing IT security and strengthening EU IT capabilities*, the European Parliament and the Luxembourg Presidency, 8-9 Déecembre 2015, Parlement Européen, Bruxelles,
- Éric Filiol. Expertise technique judiciaire pour le SRPJ et la cour d'Appel/TGI de Montpellier (affaire d'assassinat). Décembre 2014 - mars 2015. Cette expertise a associé des espoirs-recherche 4A et 5A.

Participation à des jurys de thèse ou de concours

- Rapporteur de la thèse de Samuel Marchal, *DNS and Semantic Analysis for Phishing Detection*, Université du Luxembourg, soutenue le 22 juin 2015.

- Membre du jury de concours de TSH (Technicien Supérieur Hospitalier) spécialité Techniques Biomédicales, centre hospitalier de Laval, 31 mars 2015.

- Membre du jury de concours de TSH, TH et OPQ, centre hospitalier de Laval, 26 juin 2015.

Participation à des comités de programmes

Le laboratoire a participé à aux comités de programme suivants :

- *Forum International de la Cybercriminalité* (FIC) 2015, Lille, janvier 2015.
- *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 2014, s'est effectuée au profit des revues et conférences suivantes :

- *IEEE Transactions on Computers* (É. Filiol).
- *Revista Antioqueña de las Ciencas Computacionales Y la Ingeniería de Software* (É. Filiol, membre du board).

Animations scientifiques

- Richard Rey. Organisation de OpenESIEA à Laval (manifestation autour du libre et des technologies liées au logiciel libre), mars 2015. Cet événement a été organisé avec le concours d'étudiants (Hervé Froc, Paul Hernault, Vincent Le Fournis, Hugo Meziani, Raphaël pion & Clément Siccardi),
  Site officiel : `http://www.esiea.fr/12-fevrier-openesiea-journee-dimmersion-campus-laval/`
- Ange Akanza, Robin Huet, Paul Planche & Clément Roulin (sous la direction de Richard rey). Organisation de *NDH for kids*, `https://nuitduhack.com/fr/ndhkids.html`, juin 2015.
- Richard Rey et étudiants 4A. Participation à la mise en réseau informatique (installation et configuration) du salon international *Laval-Virtual*, édition 2015.
- Richard Rey et étudiants 4A. Ateliers Sécurité Domotique et interception satellite. Nuit du Hack, juin 2015, Paris.
- Richard Rey et étudiants 4A. Organisation de deux workshops et d'une conférence lors du salon professionnel « *Sarthe-Le Mans-connexion* », Le Mans. 2 juillet 2015.
- Richard Rey. Conférence sur *La sécurité des données*, Clarté - Les matins du numérique, Laval, 30 avril 2015,
  `http://www.clarte.asso.fr/realite-virtuelle.php/Les-matins-du-numerique/`
- Richard Rey. Conférence sur *Les logiciels libres*, Clarté - Les matins du numérique, Laval, 26 novembre 2015,
  `http://www.clarte.asso.fr/realite-virtuelle.php/Les-matins-du-numerique/`
- Richard Rey et étudiants 4A. Sensibilisation des classes de 4ème et de 3ème du collège Alfred Jarry de Renazé aux risques d'Internet et des réseaux sociaux, 4 mai 2015.

- Richard Rey. *Quelle éthique dans le monde des objets connectés et du big data ?*, table ronde organisée par Grenoble École de Management dans le cadre du *GEN Digital Day*, `http://gem-digitalday.fr/schedule/track-2mb/`, 2 décembre 2015, Grenoble.

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 11 (quatre numéros) a été publié en 2015.

Contrats et transferts technologiques 2015

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 INFRASEC, Tevalis, Rennes (fin de projet 2016). Modélisation de scénario d'attaques généralisées contre des infrastructures critiques. Confidentiel.

- Contrat 3DNeuroSecure. Projet d'Investissement d'Avenir (PIA). Accepté en décembre 2014 (voir Section suivante). Durée trois ans (2015 - 2017).

- Contrats d'audit de sécurité pour différentes sociétés.

Projets industriels

Le laboratoire $(C+V)^O$, en 2015 a participé à et/ou piloté et créé plusieurs projets à finalité industrielle.

- Projet *InfraSec* avec ARX Défense et Tevalis. Modélisation de scénario d'attaques généralisées contre des infrastructures critiques. Ce projet a été labellisé par le pôle de compétitivité *Images & Réseaux*. Une version 1.0 a été livrée (lot 1) en 2014 et a été présentée en avant-première par Tevalis lors du FIC 2015 Ìa Lille.

- 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.
  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.