Rapport d'activités 2014
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. Fin 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 $CNS/(C+V)^O$.

Enfin, 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, dès la deuxième année de leur formation une activité de projet importante. 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...).

Thèmes de recherche

Le laboratoire de cryptologie et de virologie opérationnelles a pour thème principal de recherche la sécurité informatique – essentiellement en virologie et en cryptologie – 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, sécurité des environnements embarqués : 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.

- Techniques de *data mining* et *big data* appliquées à la sécurité.

Composition du laboratoire

- Directeur du laboratoire (et officier de sécurité)

  Eric Filiol (Ing. - Ph D - HDR).
  Email : `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 et RSSI du laboratoire - Laval

  Richard Rey (Ing.)
  Email : `rey@esiea-ouest.fr`
  Sécurité réseau, sécurité radio et télécommunications, électronique.

- Adjoint du laboratoire - Paris

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

- Chercheurs permanents

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

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

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

  – Olivier Ferrand (Ing. et doctorant)
  Email : `olivier.ferrand@esiea-ouest.fr`
  Programmation sécurisée, sécurité système antivirale.

  – Nicolas Bodin
  Email : `bodin@esiea-ouest.fr`
  Stéganographie.

- Doctorants

  - Arnaud Bannier
    Email : bannier@esiea-ouest.fr
    Mathématiques discrètes, combinatoire, cryptologie.

  - Michel Dubois
    Email : dubois@esiea-ouest.fr
    Cryptographie symétrique.

  - Cécilia Gallais
    Email : gallais@esiea-ouest.fr
    Modélisation mathématique des cyberattaques

- Chercheurs associés

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

  - Kevin Gallienne (Ing.)
    Email : kevin.gallienne@esiea.fr
    Analyse malware, réseau, virologie.

  - Paul Irolla (Ing.)
    Email : irolla@esiea.fr

  - 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.

  - Clément Vincent (2A/3A)
    Email : vincent.clement@et.esiea.fr
    Cryptologie.

  - De Oliveira David (4A/5A)
    Email : david.deoliveira@et.esiea-ouest.fr
    Sécurité réseau.

  - Girardat Sébastien (3A/4A)
    Email : sebastien.girardat@et.esiea-ouest.fr
    Systèmes, reverse-engineering.

- Swaenepoel Guillaume (3A/4A)
  Email : `guillaume.swaenepoel@et.esiea-ouest.fr`
  Stéganographie.

- Ollivier Wilfried (3A/4A)
  Email : `wilfried.ollivier@et.esiea-ouest.fr`
  Stéganographie.

- Delisle Laure (2A/3A)
  Email : `delisle@et.esiea.fr`
  Algorithmique, cryptographie, big data.

- Amicelli Paul (3A/4A)
  Email : `paul.amicelli@et.esiea-ouest.fr`
  Algorithmique, sécurité Linux, virologie.

- Bertin Tristan (3A/4A)
  Email : `tristan.bertin@et.esiea-ouest.fr`
  Algorithmique, sécurité Windows, virologie.

- Thieuleux Jonathan (3A/4A)
  Email : `jonathan.thieuleux@et.esiea-ouest.fr`
  Algorithmique, sécurité Linux et embarqué, virologie.

- Pion Raphael (2A/3A)
  Email : `raphael.pion@et.esiea-ouest.fr`
  Algorithmique, sécurité Linux, virologie.

- Hernault Paul (2A/3A)
  Email : `paul.hernault@et.esiea-ouest.fr`
  Algorithmique, sécurité Windows, virologie.

- Siccardi Clément (2A/3A)
  Email : `clement.siccardi@et.esiea-ouest.fr`
  Algorithmique, sécurité Linux, virologie.

- Aubin Thomas (2A/3A)
  Email : `thomas.aubin@et.esiea-ouest.fr`
  Algorithmique, sécurité Windows, virologie.

Thèses et stages

Thèses soutenues en 2013

- Thèse d'Eddy Deligne, soutenue le 31 mars 2014. Titre : *Hyperviseur de protection d'exécutables*, École doctorale de l'Ecole Polytechnique, mention très honorable. Thèse CIFRE/DCNS, Confidentiel Industrie.

  Composition du jury : Jean-Louis Lanet (Université de Limoges/XLIM, rapporteur), Vincent Nicomette (INSA Toulouse et LAAS/CNRS, rapporteur), François Déchelle (X94/Ph D, examinateur), Florent Chabaud (Ministère de la Défense/DGSIC, examinateur), Loïc Duflot (ANSSI, examinateur), Gilles Grimaud (Université Lille I, LIFL/CNRS, examinateur), Jean-Marc Steyaert (président, École Polytechnique), Éric Filiol (directeur de thèse, ESIEA).

Thèses en cours

- 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 décembre 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, Palaiseau. Cette thèse a débuté en septembre 2012. Soutenance prévue en novembre 2015.

- 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 septembre 2014.

- 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 2014.

- 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`.

Stages Master - Mastère et Ingénieur 2014 (cycle M)

- Baptiste David. *Développement de solutions antivirales en mode noyau sous Windows*. Stage de fin d'études d'ingénieur, ESIEA, 6 mois.

- Dorian Larget. *Programmation d'une application SMS Android sécurisée - Mise en place des procédures qualité*, Stage de fin d'études d'ingénieur, ESIEA, 6 mois.

- Valentin Hamon. *Mise en place d'une solution de gestion de terminaux mobiles sur DAVFI Android*, Stage de fin d'études d'ingénieur, ESIEA, 6 mois.

- Kévin Gallienne. *Implementation of Innovative Antiviral Techniques Based on Algebraic and Combinatorial Methods*. Stage fin d'études d'ingénieur, ENSEIRB - MATMECA, Bordeaux, 6 mois.

- Olivier Houssenbay. *Sécurité 802.1X*. Stage de fin d'études d'ingénieur, ESIEA, 6 mois.

- Thibaut Scherrer. *Sécurisation des couches basses du système d'exploitation DAVFI Android*. Stage de fin d'études d'ingénieur, ESIEA, 6 mois.

Stages 2014 (cycle L)

- Nicolas Aubry. *Intégration d'une plate-forme d'auto-enregistrement au portail ALCASAR*. Stage technique/MSc I ESIEA, 4 mois.

- Matthieu Breban. *Industrialisation d'un concentrateur VPN*. Stage technique/MSc I ESIEA, 4 mois.

- Nicolas Chauveau. *Radio-frequency Identification Security Analysis*. Stage technique/MSc I ESIEA, 4 mois.

- Jean-Baptiste Coulprit. *Réarchitecture du pare-feu d'ALCASAR pour un comportement dynamique*. Stage technique/MSc I ESIEA, 4 mois.

- Sebastiaan Groot (Pays-Bas). *Implementation around GostCrypt and SecureMail*. Stage de Bachelor of Science, Hogeschool van Amsterdam, durée 5 mois.

- Florent Mabriez. *Implémentation et tests d'un système de VoIp chiffrée pour Android*. Stage technique/MSc I ESIEA, 4 mois.

- Matthieu Paulais. *Développement et Industrialisation du market d'applications du projet DAVFI/Uhuru*. Stage technique/MSc I ESIEA, 4 mois.

- David de Oliveira. *Évaluation de plusieurs clients IPsec - Détermination d'une procédure de franchissement du portail captif ALCASAR par un tunnel IPsec*. Stage technique/MSc I ESIEA, 4 mois.

- Alexis Vernet. *Implémentation des syndromes treillis-code appliqués à la stéganographie*. Stage technique/MSc I ESIEA, 4 mois.

Publications du laboratoire

Revues internationales à comité de lecture

- Gregory Commin & Eric Filiol. Unrestricted Warfare vs Western Traditional Warfare : a Comparative Study. *Journal in Information Warfare*, accepté pour publication, parution en 2015, volume 14 numéro 1.
- Olivier Ferrand. How to detect the Cuckoo Sandbox and to Strengthen it ? *Journal in Computer Virology and Hacking Techniques*, accepté pour publication sous le numéro DOI 10.1007/s11416-014-0224-9, parution en 2015, volume 11.

- Eric Filiol. La realidad operacional de la ciberguerra y de los ciberataques : cómo paralizar un país". *La Vanguardia* Dossier 54, pp. 70-76, 11 décembre 2014 (version numérique également en anglais).

- Valentin Hamon. Android botnets for multi-targeted attacks. *Journal in Computer Virology and Hacking Techniques*, accepté pour publication sous le numéro DOI 10.1007/s11416-014-0216-9, parution en 2015, volume 11.

- Ashwin Kalbhor, Thomas Austin, Eric Filiol, Sébastien Josse & Mark Stamp. Dueling Hidden Markov Models for Virus Analysis. *Journal in Computer Virology and Hacking Techniques*, accepté pour publication sous le numéro DOI 10.1007/s11416-014-0232-9, parution en 2015, volume 11.

Conférences et articles invités (niveau international)

- Eric Filiol. *The Control of technology by nation states : Past, Present and Future - The Case of Cryptology and Information Security II*. RusCrypto'2014, Moscow, 25 – 28 Mars 2014, `http://www.ruscrypto.ru/accotiation/archive/rc2014/`

- Eric Filiol. *Pourquoi la lutte antivirale actuelle a échoué ?*. ITSecuday 2014, Genève, 16 mai 2014, `http://www.gri-portal.ch/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=92&cntnt01detailtemplate=dtplEVENTS&cntnt01returnid=116`

- Eric Filiol. *Le contrôle des technologies de l'information : un bien ou un mal ?*. $(ISC)^2$ Secure Events 2014, 16 octobre 2014, Paris.

Conférences et articles invités (niveau national)

- Éric Filiol. *Réseaux informatiques bancaires et de télésurveillance : quelques réflexions avec la vision de l'attaquant*. 24ème Forum ADITEL, Grenoble 18 et 19 octobre 2014 , `http://www.aditel-asso.fr/le-forum/le-forum-aditel.html`

- Jonathan Dechaux & Eric Filiol. *Un marché cyber sécurité français en structuration - Présentation et démonstrations du projet DAVFI*. Journée nationale des DSI du groupe Crédit Agricole sur le thème « Journée de veille : Une nouvelle dynamique réglementaire pour le

Crédit Agricole : Quels impacts sur la sécurité du Groupe ? », 4 juin 2014, Paris.

- Eric Filiol & Jeremy Zimmerman. *Liberté, justice, sécurité et défense*. Conférence donnée lors du Master « Affaires publiques » intitulé « *État et révolution numérique* », Sciences Po Paris, 11 février 2014.

Conférences internationales avec comité de sélection et actes

- Bhume Bhumiratana, Saran Chiwtanasuntorn et Eric Filiol. *Perseus on VoIP Protocols - Development and Implementation of VoIP Platforms*. IEEE - ECTI-CON, Thailand, 14-17 may 2014.

- Eric Filiol et Cécilia Gallais. *Critical Infrastructure : Where We Stand Today ?*. 9th International Conference On Cyber Warfare and Security (ICCWS'2014). Indiana, USA, 24-25 mars 2014, pp. 47–57, Academic Conferences and Publishing International Limited.

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).

- Eric Filiol. *Year in Crypto in Light of Snowden's Leaks (Past, Present and Future)*. PHDays 2014, Moscow, 21-22 may 2014, `http://2014.phdays.com/program/tech/`.
- Eric Filiol & Paul Irolla. *(In)Security of Mobile Banking*. 31st Chaos Computer Congress (31C3), Hamburg, 27-30 décembre 2014, `http://media.ccc.de/browse/congress/2014/31c3_-_6530_-_en_-_saal_6_-_201412272145_-_in_security_of_mobile_banking_-_ericfiliol_-_paul_irolla.html`.

- Baptiste David. *Hacking humans for military Intelligence*. International Cyber Security and Policing Conference C0c0n, 22-23 août 2014, Kochi, Inde, `http://is-ra.org/c0c0n/2014/speakers`.

- Éric Filiol et Thibaut Scherrer. *Securing Cities with CCTV ? Not so Sure - A Urban Guerilla Perspective*. La nuit du Hack (NDH'2013), June 22nd 23rd, 2013, Paris.

- Éric Filiol. *The Control of Technology by Nation State : Past, Present and Future - The Case of Cryptology and Information Security*. Hacking in Paris (HIP) 2013, June 20th, 2013, Paris.

Conférences nationales avec comité de sélection sans actes

- Éric Filiol. *E-santé et sécurité - Perspectives et enjeux*. Techno-conférence santé, Laval, 22 février 2014.

- Antoine Gademer, Loïca Avanthey, Laurent Beaudoin, Michel Roux et Jean-Paul Rudant. *Micro-charges utiles dédiées à l'acquisition de données par drone pour l'étude des zones naturelles* (poster). Colloque scientifique francophone Drones et moyens légers aéroportés d'observation, Montpellier, 2014, `http://drone.teledetection.fr`

- Laurent Beaudoin, Antoine Gademer, Loïca Avanthey, Bruno Riéra et Jean-Paul Rudant. *Faucon Noir : retour d'expérience sur une étude de la biodiversité par drone* (poster). Colloque scientifique francophone Drones et moyens légers aéroportés d'observation, Montpellier, 2014, `http://drone.teledetection.fr`

- Michel Dubois. *Sécurité et intégrité des dispositifs de santé mobile et des objets connectés en santé*. Conférence Atelier « Informatique et santé », 7 novembre 2014, Paris, `http://www.adij.fr/2014/10/16/conference-atelier-informatique-et-sante/`
- Michel Dubois. *Cloud et sécurité : comment sécuriser la donnée de bout en bout ?*. FIC 2014, Lille, 21-22 janvier 2014, `http://www.forum-fic.com/2014/fr/speaker/dubois-michel/`

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.

- Nicolas Aubry. *Accès à un réseau : pourquoi les entreprises doivent utiliser l'authentification par SMS*. Journal SécuritéOff, 7 novembre 2014,
`http://www.securiteoff.com/acces-reseau-les-atouts-lauthentification-sms/`

- Nicolas Chauveau. *Accès aux bureaux : pourquoi les entreprises doivent se méfier des badges d'accès*. Journal SécuritéOff, 3 octobre 2014,
`http://www.securiteoff.com/contact-nfc-technologie-pratique-precautions-simposent/`

- Jean-Baptiste Coulprit. *Le pare-feu devient dynamique : quels apports pour la sécurité ?*, Journal SécuritéOff, 2 septembre 2014,
`http://www.securiteoff.com/pare-feu-devient-dynamique-quels-apports-securite/`

- Jean-Baptiste Coulprit. *Le pare-feu devient dynamique : quels apports pour la sécurité ? (Partie II)*, Journal SécuritéOff, 2 octobre 2014,
`http://www.securiteoff.com/pare-feu-devient-dynamique-quels-apports-securite-suite/`

- Valentin Hamon. *Espionnage : la NSA a-t-elle infiltré le jeu Angry Birds ?*, Journal SécuritéOff, 12 mars 2014,
`http://www.securiteoff.com/nsa-angry-birds-la-verite-donnee-par-le-code-lui-meme/`

- Dorian Larget. *Espionnage économique : accédez facilement aux données privées des smartphones !*, Journal SécuritéOff, 6 février 2014,
`http://www.securiteoff.com/les-smartphones-des-mines-dor-pour-lespionnage-economique/`

- Thibaut Scherrer. *« Paranormal iPhonity » : attention aux contrefaçons d'Apple*, Journal SécuritéOff, 6 février 2014,
`http://www.securiteoff.com/paranormal-iphonity-un-smartphone-dapple-victime-dun-virus/`

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 de plus en plus pour publier des versions étendues de travaux présentés dans des conférences avec comité de sélection.

- Arnaud Bannier, Johann Barbier, Eric Filiol & Pierre Castel. *A Corollary of the Hamada and Ohmori's Theorem on Group Law over BIBD*. Arxiv preprint on `arXiv.org`, number 1401.1700.`http://arxiv.org/abs/1401.1700`

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

Pour l'année 2014 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 2014, ce sont plus de 1000 « points presse » identifiés pour le laboratoire, avec une proportion accrue à l'étranger. Des projets comme DAVFI, MMP et Stégobox ont généré, à eux seuls, un nombre important de communications presse.

Les principaux sont :

- Eric Filiol. *Mépriser les hackers est une erreur stratégique*. Interview Ragemag, 7 mars 2014, `http://ragemag.fr/filiol-hackers-erreur-strategique-69732/`

- Eric Filiol. *Orange aurait-il pu éviter un tel piratage ?*, Europe1.fr, 7 mai 2014, `http://www.europe1.fr/high-tech/orange-aurait-il-pu-eviter-un-tel-piratage-2114865`

- Eric Filiol, invité de l'émission *Tout peut changer - Comment échapper aux nouvelles arnaques*, Émission-débat FR3, 19 mai 2014, `http://www.france3.fr/emission/tout-peut-changer/diffusion-du-19-05-2014-20h45`.

- Le monde du renseignement/Intelligence Online, numéro 715, 2 juillet 2014, pp. 4 & 8.

- Eric Filiol. *Insécurité numérique : mal inévitable ou formidable opportunité ?*. Article Magazine Sécurité Off, Septembre 2014, `http://www.securiteoff.com/insecurite-numerique-mal-inevitable-formidable-opportunite/`

- Magazine Zone Interdite. *Vie privée : pourquoi nous sommes tous concernés*. M6, 28 septembre 2014, 20 :50, `http://www.m6.fr/emission-zone_interdite/28-09-2014-vie_privee_en_danger_pourquoi_nous_sommes_tous_concernes/`

- Eric Filiol, participation au débat *L'armée redéploie ses troupes*, C dans l'air, FR5, 22 octobre 2014, 17 :45,

http://www.france5.fr/emissions/c-dans-l-air/diffusions/22-10-2014_272101

- Magazine Vox Pop. *Faut-il avoir peur des investissements chinois ?*. Arte, 26 octobre 2014, 2015.
  http://www.arte.tv/guide/fr/051476-027/vox-pop

- Interview de Richard Rey. *Comment les entreprises peuvent surveiller les accès à leur réseau avec ALCASAR*, 4 novembre 2014, Journal SécuritéOff,
  http://www.securiteoff.com/lcen-projet-alcasar-au-service-pme/

- Magazine « À Bon Entendeur ». *Réseaux Wifi : gare aux pirates*. Radio Télévision Suisse 1, 18 novembre 2014,
  http://www.rts.ch/emissions/abe/6205697-reseaux-wifi-gare-aux-pirates.html.

Merci également à Ouest France, 20Minutes.fr (plusieurs interviews et articles), Le journal Le Monde (plusieurs interviews et articles), Radio Télévision Suisse (plusieurs interviews), Le Nouvel Obs, Les Echos.fr, Sciences & Avenirs, Science & Vie Junior, Capital, Opex360.com, Zdnet.fr, L'Express, Mundo Estranho (Brésil), 01net. CNET.com, Vancouver Sun, The Province (Canada), Wired magazine, Thomson Reuters... 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 2014 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 2014 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 :
- Correction de bugs
  - Correction d'un trou de sécurité (EDB-ID : 34595 - OSVDB-ID : 111026)
  - Dans la page *Interception*, correction du comportement de boucle lorsqu'un utilisateur utilise le mot « *logout* » dans le champ url.
  - Correction du compteur temporel de session radius (merci à Olivier HOUSSENBAY).
  - Le fichier « *alcasar-services* » est désormais trié.
  - Nouvelle option graphique dans le fichier de configuation *Grub* pour correction des problèmes rencontrés avec les carte-mere *mini-itx-ATOM*.
- Nouvelles fonctionnalités.
  - Suppression des fonctionnalités *Firewall-eyes* et *AWstat* d'ACC.
  - L'attribut utilisateur « *Max_total-time* » est devenu « *authorized period after the first connection* ».
  - Création d'une sonde Netflow (module noyau).
  - Les statistiques complètes réseau peuvent être maintenant vues sous ACC (*nfsen*).
  - Le module de surveillance de ports (*nfsen* permet de consulter les statistiques réseau protocole par protocole.
  - Les fichiers d'imputabilité sont maintenant inclus dans une archive unique (hebdomadaire).
  - Le nom *Alcasar* inclut le nom de domaine (« *localdomain* » par défaut). Dans une version ultérieure, le nom de domaine société sera inclus également.

- Éric Filiol. *Librairie PERSEUS*.
  En 2014 : publication de l'application *SMSPerseus* pour le chiffrement des SMS sous Androïd en version 2.0, sur le repository Google et sur le Google Play (marché français pour des questions d'exportation). Cette version corrige les bugs de la version précédente et intègre de nouvelles fonctionnalités (intégration de la librairie GMP et OpenSSL, renforcement algorithmique, gestion sécurisée des clefs...).
  En collaboration avec l'université KMUTT de Thaïlande, une implémentation de VoIP protégée par *Perseus* a été mise au point, testée et validée (voir publications). La librairie *Perseus*

a fait d'autre part l'objet d'applications qui sont en phase d'exploitation. Le soutien industriel de la technologie *Perseus* est assuré par la société ARX Défense à Rennes.
Site officiel : `http://code.google.com/p/libperseus/`

- Michel Dubois. Productions logicielles liées à sa thèse : génération d'un nouveau système d'équations pour le mini-AES et l'AES, visualisation en 3D de fonctions booléennes..., `https://github.com/archoad`.

- 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.
Site officiel : `https://www.gostcrypt.org`

- Richard Rey et Jonathan Dechaux. Création d'une plate-forme d'analyse de sécurité des objets Domotiques. Ouverture en libre prévue en 2015.

- Richard Rey. Création d'une plate-forme de réception satellite libre. Ouverture en libre prévue en 2015.

- Richard Rey. Lancement d'une étude prospective relative à la gestion d'un agent VPN par un hyperviseur ou un gestionnaire de conteneur (CLÉS). Ouverture en libre prévue en 2016.

- Éric Filiol et Paul Irolla. Plate-forme d'analyse statique et dynamique des applications Android (plate-forme 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...). Les résultats seront publiés une fois les vulnérabilités identifiées corrigées.

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.

- Eric Filiol, Audition devant la commission parlementaire dédiée aux « Risques numériques » (Madame la députée Anne-Yvonne Le Dain et Monsieur le sénateur Bruno Sido), Sénat, Office parlementaire d'évaluation des choix scientifiques et technologiques, Direction de l'Initiative parlementaire et des Délégations, 2 avril 2014.
- Éric Filiol. Expertise judiciaire pour cour d'Appel/TGI de Paris (affaire terroriste). Février

2014.

- Éric Filiol. Expertise technique judiciaire pour le SRPJ et la cour d'Appel/TGI de Montpellier (affaire d'assassinat). Décembre 2014. Cette expertise a associé des espoirs-recherche 4A.

- Richard Rey. Présentation des risques liés aux technologies RFID aux gendarmes et policiers Ntech du département de la Mayenne. Mai 2014. Cette mini-formation a été en partie assurée par des espoirs-recherche.

Figure 1 – *Présentation des risques liés aux technologies RFID aux gendarmes et policiers Ntech du département de la Mayenne. Mai 2014*

- Richard Rey. Participation (pour avis) au comité de décision de la CCI de Nantes, pour le soutien financier d'une société d'audit en sécurité. Septembre 2014.

Organisation de conférences internationales

Le laboratoire a participé à l'organisation des conférences internationales suivantes :

- Vincent Guyot. Coorganisation du 28ème congrès DNAC (« De Nouvelles Architectures pour les Communications »), Paris, France, `http://www.dnac.org/DNAC/dnac2014/`

Participation à des comités de programmes

Le laboratoire a participé à aux comités de programme suivants :

- Forum International de la Cybercriminalité (FIC) 2014, Lille, janvier 2014 (Éric Filiol).

- DNAC 2014 (Vincent Guyot), Paris, novembre 2014.

- Conférence IEEE NoF 2014 (Vincent Guyot, *Technical Program Chair*), `http://www.network-of-the-future.org/`

- *International Workshop on Trust in Cloud Computing*, London, décembre 2014, `http://computing.derby.ac.uk/IWTCC2014`

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

L'activité de *peer-reviewing*, pour 2014, s'est effectuée au profit des revues et conférences suivantes :

- *Journal of Computer Engineering and Information Technology* (É. Filiol).

- *Journal of Systems and Software* (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). Février 2014.

- Richard Rey et étudiants 4A. Participation à la mise en réseau du salon international *Laval-Virtual*.

- Éric Filiol. Organisation du concours de hacking de la version DAVFI Android. Nuit du Hack, juin 2014, Paris.

- Richard Rey et étudiants 4A. Ateliers Sécurité RFID et Alcasar. Nuit du Hack, juin 2014, Paris.

- Richard Rey et étudiants 4A. Organisation de deux worshops et d'une conférence lors du salon professionnel « *Sarthe-Le Mans-connexion* », Le Mans. Juin 2014.

- Mise en œuvre de deux démonstrateurs (stéganographie et vulnérabilité des documents) pendant la fête de la science à Laval. Septembre 2014.

- Richard Rey et étudiants 4A. Organisation de deux workshops et d'une conférence lors d'un dîner du numérique organisé par la CCI de Vendée à la Roche/Yon. Novembre 2014.

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 10 (quatre numéros) a été publié en 2014.

Contrats et transferts technologiques 2013

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 DCNS - Encadrement thèse CIFFRE Eddy Deligne (fin).
- Contrat DAVFI (partie 3/3). Voir Section suivante.
- Contrat Stéganobox, ARX_Arcéo. Financement OSEO. Clôture du projet en novembre 2014.
- Contrat MMP (*Module Matériel Perseus*). Développement d'un module matériel transparent pour la protection des flux réseau. Financement OSEO. Clôture du projet en décembre 2014.
- 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.

Projets industriels

Le laboratoire $(C+V)^O$, en 2014 a participé à et/ou piloté et créé plusieurs projets à finalité industrielle. Ces projets, validés, sur le plan technique et labellisés, font actuellement l'objet de demandes de financements.

- Projet DAVFI (*Démonstrateur Anti Virus Français et International*). Proposé dans le cadre du « *Grand Emprunt* » (Appel à projet numéro 2 - Sécurité et résilience des réseaux) par un consortium constitué des sociétés *Nov-It* (`http://www.nov-it.fr/`) [chef de file], *Qosmos* (`http://www.qosmos.com/`), *Teclib* (`http://www.teclib.com/`) avec la participation technique et le soutien du directeur technique du projet *Honeynet.org*, ce projet vise à concevoir et à réaliser un antivirus français libre, ouvert, de confiance, adoptant des approches techniques totalement différentes de celles existantes, ces dernières ayant ont prouvé leurs limites.
  Cet antivirus existera sous deux versions, l'une, gratuite, pour le grand public, l'autre professionnelle (avec des services ajoutés, en particulier pour les Opérateurs d'Importance Vitale [OIV]). Le laboratoire $(C+V)^O$ était chargé de la conception et de la réalisation du moteur antiviral proprement dit pour les environnements Windows, Unix et Android.
  Ce projet a été labellisé par le pôle de compétitivité *System@tic* et a reçu le soutien de plusieurs organismes et entités : l'AFUL (*Association francophones des Utilisateurs de Logi-*

ciels libres), le groupe thématique Logiciel Libre du pôle *System@tic* Paris-Région, l'APRIL (*Association pour la promotion et la défense du logiciel libre*), le ministère de l'Éducation Nationale (projet Éole), la Gendarmerie Nationale, la CGPME...
Le dḿonstrateur pour la version Android (smartphones et tablettes) a été livré en octobre 2013 pour commercialisation par la société Nov-It en avril 2014, après une phase d'industrialisation par cette dernière.

Le laboratoire $(C+V)^O$ a livré en septembre 2014 les versions Windows et Linux (cette dernière a été livrée après une courte phase d'industrialisation par Nov'IT, à la Gendarmerie Nationale pour équiper son parc informatique [près de 70 000 postes sous Linux et 18 000 postes sous Windows]). Cette livraison s'est accompagnée d'un transfert de propriété intellectuelle au profit de Nov'IT (compensation par la signature d'un accord de *royalties* entre NOV'IT et l'ESIEA) ainsi que d'une partie de l'équipe de développement. La livraison s'est faite dans le respect complet du cahier des charges initial et une réduction des coûts de 30 %.
Les tests réalisés lors du dernier semestre confirment (module 5.2) une capacité de détection des codes inconnus de plus de 98 % avec un taux de faux positifs négligeables (et nuls pour les fichiers critiques liés aux systèmes d'exploitation (module 1).

Le comité de clôture du 17 octobre 2014, présidé par la DGA (prescripteur et pilote technique) a validé la livraison par le laboratoire. La DGA a validé le travail sur le plan technique en janvier 2015. Un communiqué officiel de livraison a été publié le 1er octobre 2014 (`http://www.securiteoff.com/fin-bilan-du-projet-davfi`). Le laboratoire $(C+V)^O$ continue le développement autour du projet DAVFI dans le cadre des thèses d'Olivier Ferrand et Jonathan Dechaux.

Site officiel du projet : `http://www.davfi.fr`

- Projet MMP (*Module Matériel Perseus*). Ce projet a consisté à développer un module matériel miniature de la taille d'une clef USB, permettant de protéger automatiquement et de manière transparente, tous les flux sortants avec la technologie Perseus développée par le laboratoire.
  Ce module intégre de l'authentification forte, des fonctions de coffre-fort numérique, un système d'exploitation à faible empreinte, une pile de protocoles de type IPSec développée de zéro .... Ce projet a été labellisé par le pôle de compétitivité *Images & Réseaux*. Le contrat s'est achevé avec la réalisation d'une plateforme fonctionnelle complète (serveur, deux modules matériels, codes source...). Une première présentation sera faite lors du FIC 2015 à Lille par la société ARX Défense avec laquelle le laboratoire va travailler pour la phase II de ce projet (industrialisation et commercialisation).

- Projet *Steganobox* dans le cadre d'un consortium piloté par la société ARX Défense. (`http://www.arx-arceo.com/fr/accueil.php`). Ce projet consiste à développer des équipements réseaux dédiés à la détection de l'usage de la stéganographie. Ce projet a été labellisé par le pôle de compétitivité *Images & Réseaux*. Le contrat a été réalisé et livré en totalité en novembre 2014.

- Projet *InfraSec* avec ARX Défense et Tevalis. Modélisation de scénario d'attaques générali-

sées 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. Communication officielle début 2015.