

# List of publications

Olivier Levillain

## International peer-reviewed journals

- [1] Loïc Duflot, Olivier Levillain, and Benjamin Morin. ACPI: Design Principles and Concerns. In *Trusted Computing, Second International Conference, Trust 2009, Oxford, UK*, pages 14–28, April 2009.
- [2] Olivier Levillain, Arnaud Ébalard, Benjamin Morin, and Hervé Debar. One Year of SSL Internet Measurement. In *28th Annual Computer Security Applications Conference, ACSAC 2012, Orlando, FL, USA*, pages 11–20, December 2012.
- [3] Olivier Levillain, Hervé Debar, and Benjamin Morin. Parsifal: Writing efficient and robust binary parsers, quickly. In *2013 International Conference on Risks and Security of Internet and Systems (CRiSIS), La Rochelle, France, October 23-25, 2013*, pages 1–6, 2013.
- [4] Éric Jaeger and Olivier Levillain. Mind Your Language(s): A Discussion about Languages and Security. In *35. IEEE Security and Privacy Workshops, SPW 2014, San Jose, CA, USA*, pages 140–151, May 2014.
- [5] Olivier Levillain. Parsifal: A Pragmatic Solution to the Binary Parsing Problems. In *35. IEEE Security and Privacy Workshops, SPW 2014, San Jose, CA, USA*, pages 191–197, May 2014.
- [6] Olivier Levillain, Baptiste Gourdin, and Hervé Debar. TLS Record Protocol: Security Analysis and Defense-in-depth Countermeasures for HTTPS. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, Singapore*, pages 225–236, April 2015.
- [7] Florian Maury, Jean-René Reinhard, Olivier Levillain, and Henri Gilbert. Format Oracles on OpenPGP. In *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA*, pages 220–236, April 2015.
- [8] Guillaume Endignoux, Olivier Levillain, and Jean-Yves Migeon. Caradoc: a pragmatic approach to PDF parsing and validation. In *37. IEEE Security and Privacy Workshops, SPW 2016, San Jose, CA, USA*, pages 126–139, May 2016.

## Other publications

- [1] Loïc Duflot, Olivier Levillain, Benjamin Morin, and Olivier Grumelard. Getting into the SMRAM: SMM Reloaded. In *CanSecWest Applied Security Conference, CanSecWest 2009, Vancouver, Canada*, 2009.
- [2] Loïc Duflot and Olivier Levillain. ACPI et routine de traitement de la SMI : des limites à l'informatique de confiance ? In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France, June 3-5, 2009*, pages 131–167, 2009.
- [3] Yves-Alexis Perez, Loïc Duflot, Olivier Levillain, and Guillaume Valadon. Quelques éléments en matière de sécurité des cartes réseau. In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, pages 213–235, June 2010.
- [4] Loïc Duflot, Olivier Levillain, Benjamin Morin, and Olivier Grumelard. System Management Mode Design and Security Issues. In *IT Defense 2010, Brühl, Germany*, February 2010.
- [5] Loïc Duflot, Olivier Grumelard, Olivier Levillain, and Benjamin Morin. On the Limits of Hypervisor- and Virtual Machine Monitor-Based Isolation. In Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security - Foundations and Practice*, chapter 16, pages 349–366. Springer, 2010.
- [6] Loïc Duflot, Olivier Grumelard, Olivier Levillain, and Benjamin Morin. ACPI and SMI handlers: some limits to Trusted Computing. *Journal in Computer Virology*, 6(4):353–374, 2010.

- [7] Pierre Chifflier, Loïc Dufлот, Olivier Levillain, Fernand Lone Sang, Arnauld Michelizza, Benjamin Morin, and Yves-Alexis Perez. Sécurité et architecture PC : l'impossible confiance ? *Multi-System & Internet Security Cookbook (MISC)*, 58:18–47, November 2011.
- [8] Loïc Dufлот, Olivier Levillain, and Alix Caznave. Chiffrement de supports: principe, intérêts et limites. *Sécurité de l'information*, 11:6–8, March 2011.
- [9] Olivier Levillain. SSL/TLS : état des lieux et recommandations. In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, pages 3–42, June 2012.
- [10] Olivier Levillain. Parsifal : écriture rapide de *parsers* robustes et efficaces. In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication SSTIC, Rennes, France*, June 2013.
- [11] Olivier Levillain and Benjamin Morin, editors. *Proceedings of Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, June 2013.
- [12] Olivier Levillain. Parsifal : une solution pour écrire rapidement des *parsers* binaires robustes et efficaces. In *25. Journées francophones des langages applicatifs, Fréjus, France*, pages 193–194, January 2014.
- [13] Olivier Levillain and Benjamin Morin, editors. *Proceedings of Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, June 2014.
- [14] Olivier Levillain. SSL/TLS, 3 ans plus tard. In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, pages 227–273, June 2015.
- [15] Olivier Levillain and Benjamin Morin, editors. *Proceedings of Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, June 2015.
- [16] Éric Jaeger and Olivier Levillain. Un FizzBuzz pour le cyber. In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, pages 445–450, June 2016.
- [17] Olivier Levillain, Benjamin Morin, and Frédéric Tronel, editors. *Proceedings of Symposium sur la Sécurité des Technologies de l'Information et de la Communication, SSTIC, Rennes, France*, June 2016.

## Invited talks

- [1] Éric Jaeger and Olivier Levillain. Langages et sécurité - généralités et cas des langages fonctionnels. In *24. Journées francophones des langages applicatifs, Aussois, France*, February 2013.
- [2] Éric Jaeger, Olivier Levillain, Damien Doligez, Christèle Faure, Thérèse Hardin, and Manuel Maarek. LaFoSec: Étude de la sécurité intrinsèque des langages fonctionnels. In *24. Journées francophones des langages applicatifs, Aussois, France*, February 2013.
- [3] Olivier Levillain. Mind Your Language(s): A Discussion about Languages and Security. In *High Integrity Software, Bristol, UK*, October 2014.

## Seminars

- [1] Olivier Levillain. SSL/TLS : état des lieux et recommandations. In *Séminaire CAMEL du LORIA, Nancy, France*, April 2012.
- [2] Éric Jaeger and Olivier Levillain. Langages de développement et sécurité - Mind your Language. In *Séminaire Performance et généricité au LRDE, Paris, France*, May 2013.
- [3] Olivier Levillain. Regards critiques sur SSL/TLS. In *Conférence ESSI, Paris, France*, September 2014.
- [4] Olivier Levillain, Éric Jaeger, and Pierre Chifflier. Mind your Language(s): Langages de développement et sécurité. In *Matinale de l'Innovation "Logiciel libre et Sécurité", Paris, France*, December 2014.
- [5] Olivier Levillain and Éric Jaeger. Mind your Language(s): Langages de développement et sécurité. In *Séminaire Méthodes formelles et langages pour le développement de logiciels fiables dans l'industrie, Paris, France*, April 2014.
- [6] Olivier Levillain. Some thoughts on SSL/TLS from a (nearly) 6-year PhD student. In *Séminaire EURECOM, Sophia Antipolis, France*, November 2015.

- [7] Olivier Levillain. Regards critiques sur SSL/TLS. In *Séminaire Sécurité du LORIA, Nancy, France*, December 2015.
- [8] Olivier Levillain. Regards critiques sur SSL/TLS. In *Journée Nouvelles Avancées en Sécurité des Systèmes d'Information, Toulouse, France*, January 2016.
- [9] Olivier Levillain. Regards critiques sur SSL/TLS. In *Séminaire sur la Confiance Numérique, Clermont-Ferrand, France*, April 2016.
- [10] Olivier Levillain. The real impact of obsolete cryptography, applied to SSL/TLS. In *École d'été Cyber In Bretagne, Rennes, France*, July 2016.

## Tools

- Parsifal** OCaml-based parsing framework (lead developer), 2011-2016
- Concerto** Set of tools to extract and analyse certificate chains (lead developer), 2014-2016
- Caradoc** Set of tools to extract, analyse and clean up PDF files (reviewer), 2015-2016

## Internships

- 2009** Yves-Marie Giraud. *Optimisation du chiffrement de disque pour la confidentialité et l'intégrité des données.*
- 2010** Gwenaél Saget. *Vulnérabilités et sécurisation des mécanismes de gestion de l'énergie.*
- 2011** Xavier Boudvin. *Mesures et analyse du protocole TLS côté serveur.*
- 2011** Cédric Bartholomey. *Sécurité des applications du Web 2.0.*
- 2012** Éric Voiselle. *Conception d'une plateforme de test HTTPS.*
- 2013** Anthony Albert. *Étude des formats de fichiers d'image.*
- 2015** Guillaume Endignoux. *Validation of PDF files at a structural level.*

## PhD jury

- 2014** Étienne Millon. *Analyse de sécurité de logiciels système par typage statique.* EDITE (école doctorale informatique, télécommunications et électronique) de Paris. *En qualité d'invité.*
- 2015** Yann Bachy. *Sécurité des équipements grand public connectés à Internet: évaluation des liens de communication.* MITT (école doctorale mathématiques, informatique, télécommunications de Toulouse).