Antoine Delignat-Lavaud

Personal Information

Born in 1987, French citizenship Email: antdl@microsoft.com
Work Address: Microsoft Research Cambridge, 21 Station Road, CB1 2FB Cambridge, UK
`http://antoine.delignat-lavaud.fr`

Education

2012-2015: PhD candidate at INRIA Paris (accredited by ENS Paris) under the supervision of Karthikeyan Bhargavan (team PROSECCO), on formal verification of Web applications.

2009-2011: Parisian Master of Research in Computer Science, *magna cum laude*.

2008-2009: Admitted at ENS Cachan.
Bachelor of mathematics; Bachelor of Computer Science, *magna cum laude*.

2005-2008: *Classe préparatoire* in Mathematics, *Lycée Camille Jullian*, Bordeaux.

2005: *Baccalauréat* (Advanced Levels), *magna cum laude*.

Journal Articles

Discovering Concrete Attacks on Website Authorization by Formal Analysis (with C. Bansal, K. Bhargavan and S. Maffeis), in *Journal of Computer Security, special issue on Web Application Security - Web @ 25*, IOS Press, 2014

Conference Publications

Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation, (with C. Fournet, M. Kohlweiss, B. Parno) in *37th IEEE Symposium on Security and Privacy*, 2016.

Dependent Types and Multi-Monadic Effects in F*, (with N. Swamy, C. Hritcu, C. Keller, A. Rastogi, S. Forest, K. Bhargavan, C. Fournet, P.-Y. Strub, M. Kohlweiss, J.-K. Zinzindohoue, S. Zanella-Béguelin) in *43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 2016.

A Messy State of the Union: Taming the Composite State Machines of TLS, (with B. Beurdouche, K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, J. K. Zinzindohoue) in *36th IEEE Symposium on Security and Privacy*, 2015.

Network-based Origin Confusion Attacks against HTTPS Virtual Hosting, (with K. Bhargavan) in *24th International Conference on World Wide Web*, 2015.

Verified Contributive Channel Bindings for Compound Authentication (with K. Bhargavan, A. Pironti), in *22nd Network and Distributed System Security Symposium*, 2015.

Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS (with K. Bhargavan, C. Fournet, A. Pironti and P. Y. Strub), in *35th IEEE Symposium on Security and Privacy*, 2014.

Web PKI: Closing the Gap between Guidelines and Practices (with M. Abadí, A. Birrell, I. Mironov, T. Wobber and Y. Xie), in *21st Annual Network and Distributed System Security Symposium*, 2014.

Language-Based Defenses Against Untrusted Browser Origins (with K. Bhargavan and S. Maffeis), in *22nd USENIX Security Symposium*, 2013.

Keys to the Cloud: Formal Analysis and Concrete Attacks on Encrypted Web Storage (with C. Bansal, K. Bhargavan and S. Maffeis), in *2nd Conference on Principles of Security and Trust*, 2013.

Workshop Papers

AFlexTLS: A Tool for Testing TLS Implementations, (with K. Bhargavan, B. Beurdouche, N. Kobeissi, A. Pironti) in *9th Usenix Workshop on Offensive Technologies*, 2015.

Web-based Attacks on Host-Proof Encrypted Storage (with K. Bhargavan), in *6th USENIX Workshop on Offensive Technologies*, 2012

Dissemination

The BEAST Wins Again: Why TLS Keeps Failing to Protect HTTP
Briefing at *Black Hat USA*, 2014.

Transport Layer Security Session Hash and Extended Master Secret Extension
RFC 7627, IETF Internet Standards, 2015.

Internships

Microsoft Research, *Cambridge, England* **Summer 2014**

With Cedric Fournet, on an anonymous credentials system derived from the Web PKI using the Pinocchio verified computation scheme.

Microsoft Research, *Mountain View, United States* **Summer 2013**

With Ted Wobber, on the specification and enforcement of security policies to X.509 certificates and other aspects of the PKI.

Boston College, *Boston, United States* **Summer 2010**

With Howard Straubing, on a new automaton model for forest algebras and its applications to algebraic characterizations of unranked tree languages and tree automaton minimization.

Teaching

École Polytechnique, *Palaiseau, France* **2013-2015**

Teaching assistant for courses INF311 (Introduction to Computer Science), INF431 (Algorithms and Programming), INF321 (Principles of Programming Languages), and INF442 (Big Data).

Lycée Carnot, *Paris, France* **2010-2011**

Introduction to programming with Maple (second year preparatory class).

Software Projects

F* Language: a new higher order, effectful programming language designed with program verification in mind. The F* type-checker aims to prove that programs meet their specifications by discharging proof obligations to an SMT solver. My contributions to F* are mostly related to the translation of F* programs to OCaml and JavaScript. `https://www.fstar-lang.org`

miTLS Project: a verified reference implementation of the TLS protocol and X.509 PKI, with tools for protocol fuzzing and prototyping. In the process of being ported from F7 and F# to F* and OCaml. My contributions to miTLS are on extension support, elliptic curve cipher suites, TLS version 1.3, and everything related to the PKI. `http://www.mitls.org`

Defensive JavaScript (DJS): a language subset of JavaScript enforced by typing. I implemented the DJS type inference and the translation of DJS to applied pi-calculus, as well as a DJS cryptographic library. This tool also supports translating a subset of PHP to pi-calculus for modeling the server-side behavior of applications. `http://www.defensivejs.com`

Awards

Best Paper Award, *9th Usenix Workshop on Offensive Technologies*, 2015.

Distinguished Paper Award, *36th IEEE Symposium on Security and Privacy*, 2015.

Security Impact

Google Chrome: CVE-2014-3166, CVE-2013-6628, CVE-2013-6659, CVE-2013-2853

Firefox: CVE-2014-1570, CVE-2014-1569, CVE-2014-1568, CVE-2014-1490, CVE-2012-4196

OpenSSL: CVE-2015-0205, CVE-2015-0204, CVE-2014-3572

Java: CVE-2014-6457, CVE-2014-6593

Safari: CVE-2014-1295

Computer Skills

I am familiar with most softwares used by academics, including :

- Symbolic and numerical computing: Maple, Matlab, GAP
- Programming languages: C/C++, OCaml/F#, ASM, Java, Prolog, Haskell, Perl, Ruby, Python, PHP, JavaScript, SQL ...
- Publishing: LaTeX, HTML/CSS, Adobe Creative Suite

Languages

French: native speaker; English: fluent; German: intermediate level.

Other activities

Advanced pianist specialized in the romantic era and Russian composers.
Secretary of an association to promote the works of Simon Segal, a Russian-born painter of the School of Paris. Participated in the organization of exhibitions in France and Poland.