Florian MAURY
11, rue de la destinée
95800 Cergy, France
+33 6 87 41 49 60
florian.maury-cv@x-cli.eu

Network and Protocol Security Specialist

#Adaptative #Curious #TeamPlayer #Communicative

Professional Experience

Mar 2013 – Mar 2018 — **Network and Protocol Security Specialist & Teacher** — ANSSI, Paris, France

Author of protocol security studies on DNS, OpenPGP, U2F, HTTP/2, Certificate Transparency, and Signal/Whatsapp/OMEMO.
Teacher (≈ 70 hours per year) of the "Applied Information Security", "DNS security", "Development of secured web applications" courses.
Developer in Python, PHP, Ocaml, Go and Rust.
Responsible of a public contract for the development of a fuzzing platform.

Mar 2012 – Jan 2013 — **Security Auditor & Teacher** — HSC, Paris, France

Security evaluations of a dozen of web applications using blackbox, graybox and whitebox methodologies. Co-authored a course on Public Key Infrastructures (PKI).

Jul 2010 – Feb 2012 — Resumption of studies to specialize in Information Security. Please see the Education section.

Jun 2009 – Jun 2010 — **System and Software Architect** — Neximus, Paris, France

Design and realization of stackable appliances for second-factor authentication using mobile phones.

Sep 2008 – May 2009 — **System Administrator** — Pixmania, Paris, France

Administration of hundreds of mostly Debian servers.
Refactoring of the DNS and email infrastructure.

Jan 2006 – Aug 2008 — **Web Application Developer** — Celsius Online, Paris, France

Development of web applications in PHP, Actionscript and Javascript.

Sep 2003 – Dec 2005 — Various system administrator jobs for the French educational system.

Education (initial training)

2010 – 2012 — **Master's degree in Information Security** — Limoges University, France

Auditor during the two-year period. Degree obtained in 2014 through VAE (a procedure to grant degrees based on work experience).

2003 — ***Licence* in Computer Science** — Limoges University, France

A French *licence* is roughly equivalent to a Bacherlor's degree.

Education (continuous training)

2016	Electromagnetic Security (TEMPEST) A one-week Crash course on TEMPEST, to better grasp the risks related to electromagnetic fields.	ANSSI
2016	Physical and Logical Security of device components A one-week crash course on secure element security.	ANSSI
2016	The Linux Programming Interface A two-week course on all the topics covered in Mickael Kerrisk's book and more (cgroups and namespaces).	Mickael Kerrisk
2015	Cryptography A five-week course on cryptography related topics, covering symmetric and asymmetric algorithms, modes, cryptanalysis, and usages (TLS, IPsec, etc.).	ANSSI
2015	Implementing Cisco MPLS Traffic Engineering A one-week crash course on MPLS implementation on CISCO networks to improve network usage and select "routes" based on constraints.	CISCO
2014	CISCO SP-Edge A one-week crash course on using CISCO devices on the edge of operator networks (L3VPN, L2VPN, iBGP, eBGP, IPv6, 6PE, etc.).	CISCO
2012	Web Application Security Certification (GWEB) A one-week course on web application security, covering server-side and client-side aspects.	SANS
2012	Network Penetration Testing Certification (GPEN) A one-week course on network penetration testing, covering methodology and tools.	SANS

Hobbies

Plays mostly support roles in multiplayer online games such as Overwatch or Paragon.

Plays lots of boardgames, with a preference for "german" games involving strategy, accounting and opportunism.

Appreciates vlogs of people moving to a foreign country and telling their stories and adventures.

Enjoys kick-biking and nordic walking.

Is probably not a profitable Netflix client.

Publications & Contributions

Jun 2018 Open source tool and Conference	DNS Single Point of Failure Detection using Transitive Availability Dependency Graph Analysis Sole author of a comprehensive study on DNS dependency, including the measurement of over four millions domain names.	Github SSTIC
May 2018 Press article and Open source tool	[fr] SMTP : la killer app de DNSSEC Sole author of an analysis of the threat landscape of SMTP-based emails when facing an active network attacker. This study also comprises a measurement of the DNSSEC, SPF, DKIM and DMARC deployment on domain names located under the .fr TLD. The measurement tool was published as FLOSS.	MISC
Jun 2017 Open source tool and Conference	PacketWeaver: a script filing and task sequencing framework for network audit purposes Co-author of a Python framework built with network audits in mind. Co-author of a talk to introduce the tool to the community.	Github SSTIC
Mar 2017 Press article	[fr] Chiffrement de messagerie quasi instantanée : à quel protocole se vouer ? Sole author of a presentation of the cryptography protocols Triple Diffie-Hellman (X3DH) and Double Ratchet, followed by a comparative analysis of OpenPGP, Off-the-record (OTR), Signal and XMMP/OMEMO.	MISC
Dec 2016 Conference	[fr] Certificate Transparency : des journaux publics en ajout seul pour améliorer la sécurité de TLS Sole author of a presentation of Certificate Transparency from the theoretical perspective as well as from the hands-on one. Certificate Transparency is a technology to help cope with issues in the trust system inherent to the Internet Public Key Infrastructure on which relies HTTPS.	NetSecure Day
Dec 2016 Open source tool	Certificate Transparency Add-Chain webservice Sole author of a webservice to submit X.509 certificate chains to the Certificate Transparency logs and download the resulting Signed Certificate Timestamps (SCT).	Github
Nov 2016 Press article	[fr] HTTP/2 : attention, peinture fraîche Sole author of an introdution to HTTP/2, a comparative analysis with its ancestor, and a discussion on the potential negative security impacts of HTTP/2 over the ecosystem.	MISC
Nov 2016 Open source tool	ATBTCT: AuTomated BitTorrent mirrors of Certificate Transparency Sole author of a toolset to collect certificate chains from Certificate Transparency, verify the tree integrity and republish them with using Bitorrent to improve bootstrapping time of a new mirror and help fighting split-view attacks.	Github
Nov 2016 Conference	[fr] Certificate Transparency : des journaux publics en ajout seul pour sécuriser TLS	Cert-IST

Publications & Contributions (continuation)

Nov 2016
Open source tool

Scapy HTTP/2 module — Github

Sole author of a HTTP/2 module for Scapy, a Python framework for crafting and parsing of binary network protocols. This module offers complete support of HTTP/2 and HPack.

Jul 2016
Press article

[fr] Souriez ! Les autorités de certificate sont filmées — MISC

Sole author of a popularized introduction to Certificate Transparency.

Jul 2016
Conference

[fr] Public Notary Transparency : des journaux publics en ajout seul et leurs usages avec TLS — JCSA

Jun 2016
Conference

A First Glance at the U2F Protocol — SSTIC

Co-author of a security analysis of the U2F second-factor authentication scheme.

Jun 2016
and Jun 2015
Public Report

Observatory of the Internet resiliency in France — ANSSI

Co-author of a public report on Internet resiliency in France. Author of the DNS and emails chapters and of the tools to collect DNS data for analysis.

May 2016
Podcast

[fr] Développement sécurisé d'applications web — NoLimitSecu

Participant of a Podcast on the secure development of web applications. Presentation of ANSSI "Secure Web Application Development" training course program and approach.

Nov 2015
Conference

The Traffic Amplifiers Great Hunt: Helping Network Operators To Bring Down DDoS Sources — RIPE meeting

Co-author of a talk presenting the results of the French initiative to help network operators to identify vulnerable devices that might be used to perform DDoS attacks.

Sep 2015
Press article

[fr] Décadence du DNS illustrée en trois attaques symptomatiques — MISC

Sole author of an article covering three recent DNS attacks and demonstrating that feature creep can also cripple network protocols.

May 2015
Conference

The Infinitely Delegating Name Servers attack — DNS-OARC

Presentation of a DNS attack causing increased traffic amplification for DDoS attacks, crashes or severe slowness to multiple DNS resolver implementations.

Feb 2015
Academic paper

Format Oracles on OpenPGP — ANSSI

Co-author of a group of attacks spanning multiple implementations of the OpenPGP standard enabling the recovery of cleartext messages from a new kind of padding oracles.

Jun 2014
Technical guidelines

[fr] Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine — ANSSI

Main author of ANSSI DNS technical guidelines on buying domain names and operating them.

Publications & Contributions (continuation)

Nov 2013
Conference

Blocking DNS messages is dangerous — DNS-OARC

Co-author of an attack enabling the poisoning of DNS caches in a matter of hours by leveraging the anti-DDoS RRL mechanism.

Sep 2012
Press article

[fr] DNSSEC à la rescousse de PKIX — MISC

Sole author of an article covering the use of DNS and DNSSEC to help cope with issues in the trust system inherent to the Internet Public Key Infrastructure on which relies HTTPS.