

Dr.-Ing. Aurore Fass

Visiting Assistant Professor at Stanford University
Research Group Leader at CISP

✉ aurore@cs.stanford.edu
aurore54f.github.io



Research Overview

My research work revolves around designing practical approaches to protect the security and privacy of Web users. I build systems to proactively detect malicious JavaScript code and suspicious browser extensions. I analyze data to understand how people spend time on the Web, and I want to use the resulting perspective to prioritize defense strategies.

Scientific Career

- 2021–2023 **Visiting Assistant Professor**, *Stanford University*, U.S.
 - Host: [Zakir Durumeric](#)
- 2021–2023 **Research Group Leader**, *CISPA Helmholtz Center for Information Security*, Germany.
- 2021 **Postdoctoral Researcher**, *CISPA Helmholtz Center for Information Security*, Germany.
- 2017–2021 **Ph.D. Student**, *Saarland University & CISPA Helmholtz Center for Information Security*, Germany.
 - Ph.D. thesis: *Studying JavaScript Security Through Static Analysis*
 - Advisors: [Michael Backes](#) and [Ben Stock](#)

Education

- 2014–2017 **Grande École** (similar to a Master Degree), *TELECOM Nancy*, France, valedictorian.
Major: Telecommunication, Network, and Security
 - Master thesis: German Federal Office for Information Security (BSI), Germany
Automated clustering of JS samples for the detection of malware contained in obfuscated code
 - Industrial project: French Ministry of Defense, France
Implemented an Xposed module to monitor Android devices; group of 4 persons (6 months)
 - Internship: Fraunhofer IOSB, Germany
Implemented a passive asset detection system (8 weeks)
- 2012–2014 **Preparation for the highly competitive nationwide entrance examination to the French Grandes Écoles**, France.
Major: Mathematics, Physics, and Computer Science
- 2012 **High school graduation**, France, graduated with distinction (“mention très bien”), European section.
Major: Mathematics, Physics & Chemistry, Biology, and German

Awards and Honors

- 2022 **Top Reviewer Award**, *ACM CCS*.
- 2022 **PC members – Honorable mentions**, *TheWebConf*.

- 2021 **Inspiring Career**, 1 of 3 invited alumni (out of 2,300 alumni) for the 30th anniversary of the French Grande École TELECOM Nancy, Remote.
- 2019–2022 **Program of Excellence**, Saarland University, Germany.
- 2017 **Valedictorian**, French Grande École TELECOM Nancy, France.
- 2016 **Best Student Recognition Event**, IBM, UK.

Publications

Kimberly Ruth, **Aurore Fass**, Jonathan J. Azose, Mark Pearson, Emma Thomas, Caitlin Sadowski, and Zakir Durumeric. **A World Wide View of Browsing the World Wide Web**. In *ACM Internet Measurement Conference (IMC)*, 2022.

Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock. **DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale**. In *ACM CCS*, 2021. Code repository: <https://github.com/Aurore54F/DoubleX>.

Marvin Moog, Markus Demmel, Michael Backes, and **Aurore Fass**. **Statically Detecting JavaScript Obfuscation and Minification Techniques in the Wild**. In *Dependable Systems and Networks (DSN)*, 2021. Code repository: <https://github.com/MarM15/js-transformations>.

Aurore Fass, Michael Backes, and Ben Stock. **HIDENOSEEK: Camouflaging Malicious JavaScript in Benign ASTs**. In *ACM CCS*, 2019. Code repository: <https://github.com/Aurore54F/HideNoSeek>.

Aurore Fass, Michael Backes, and Ben Stock. **JSTAP: A Static Pre-Filter for Malicious JavaScript Detection**. In *ACSAC*, 2019. Code repository: <https://github.com/Aurore54F/JStap>.

Aurore Fass, Robert P. Krawczyk, Michael Backes, and Ben Stock. **JAST: Fully Syntactic Detection of Malicious (Obfuscated) JavaScript**. In *DIMVA*, 2018. Code repository: <https://github.com/Aurore54F/JaSt>.

Community Services

- PC Co-Chair** **MADWeb 2023** (co-located with NDSS)
- PC Member** S&P 2023, EuroS&P 2023, TheWebConf 2023 & 2022, ACM CCS 2022 & 2021, ARES 2022, SecWeb 2022 & 2021
- Artifact Committee** USENIX Security 2021, ACSAC 2018
- External Reviewer** NDSS 2022–2020, USENIX Security 2022–2020, EuroS&P 2019, ACSAC 2019 & 2018, ACM CCS 2018
- Hiring Committee** CISP faculty hiring committee 2021

Teaching

- WS 2020–2021 **Lecturer at TELECOM Nancy** (Université de Lorraine, France)
- Browser Extensions: Architecture and Security Consideration (lectures and practicals for MSc students)
- WS 2019–2020 **Seminar: Joint Advances in Web Security**
- Browser Extensions: Security and Vulnerabilities

- Overview of Malicious JavaScript Detection Techniques and Attacks

WS 2018–2019 **Seminar: Joint Advances in Web Security**

- Overview of Malicious JavaScript Detection Techniques
- Cryptojacking: Definition, Detection, and Dimensions

Student Advising and Mentoring

Ph.D. Students

- Winter 2022– **Liz Izhikevich** – *Internet Scanning*, with Zakir Durumeric, Stanford University
- Fall 2021– **Kimberly Ruth** – *Browsing Behavior*, with Zakir Durumeric, Stanford University
- Fall 2021– **Shubham Agarwal** – *Browser Extension Security*, CISP

Master Students

- Fall 2022– **Manda Tran** – *Browser Extension Security*, Stanford University

Bachelor Students

- Spring 2022– **Sheryl Hsu** – *Browser Extension Security*, Stanford University

Alumni

- 2022 **Mark Tran** (BSc student) – *Browser Extension Fingerprinting*
Basheerah Abdus-Shakur (BSc student) – *Vulnerability Patching*, with Zakir Durumeric
Vrushank Gunjur (BSc student) – *Over-Privileged Extensions*
Nahum Maru (BSc student) – *Browser Extension Crawler*
Fengchen (Maggie) Gong (MSc student → Princeton Ph.D.) – *Fingerprinting*
- 2021 **Liana Patel** (Ph.D. student) – *Web Crawler*, with Zakir Durumeric
Luca Pistor & Nathan Bhak (BSc students) – *Exam Software Security*
Paul Szymanski (BSc thesis) – *A Study of State-of-the-Art Call Graph Creation Approaches for JavaScript*, with Cristian-Alexandru Staicu
- 2020 **Anne Christin Deutschen & Luc Seyler** (BSc students) – *Browser Extension Vulnerability*, with Dolière Francis Somé
- 2019–2020 **Marvin Moog & Markus Demmel** (BSc students) – *Analysis of JavaScript Obfuscation Techniques* → DSN 2021
- 2019 **Maximilian Zöllner & Niklas Kempf** (BSc students) – *Intelligent Fuzzing System for JavaScript*
- 2018 **Nils Glörfeld** (BSc student) – *Malicious JavaScript Deobfuscation*
Dennis Salzmann (BSc student) – *Malicious JavaScript Detection*

Selected Talks

DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

- Jul 2022 **Berkeley Security Seminar**. Berkeley, CA, U.S.
- May 2022 **RuhrSec**. Bochum, Germany (extended version).
- Apr 2022 **Stanford Computer Forum** – Security Workshop. Stanford, CA, U.S.

Nov 2021 [Stanford Security Lunch](#). Stanford, CA, U.S.

[Studying JavaScript Security Through Static Analysis](#)

Mar 2022 Palo Alto Networks (CA, U.S.). Remote (extended version).

Jun 2021 Spirals Webinar at Inria Lille (France). Remote.

[Statically Analyzing Malicious JavaScript in the Wild](#)

Mar 2021 Webinar at LORIA (France). Remote.

Dec 2020 BINSEC Webinar at CEA (France). Remote.

[HIDENoSEEK: Camouflaging Malicious JavaScript in Benign ASTs](#)

May 2020 [RuhrSec](#) (Germany). Remote (extended version).

Mar 2019 Grande Region Security and Reliability Day (GRSRD). Nancy, France.

Feb 2019 [MADWeb](#). San Diego, CA, U.S.

[JAST: Fully Syntactic Detection of Malicious \(Obfuscated\) JavaScript](#)

Nov 2018 [Blackhoodie](#). Berlin, Germany.

Jun 2018 Malware Meeting at LORIA. Nancy, France.

Mar 2018 Grande Region Security and Reliability Day (GRSRD). Saarbrücken, Germany.

[Publicly Available Software](#)

[DOUBLEX](#) Static browser extension analyzer: detection of suspicious external data flows

[HIDENoSEEK](#) Static analyzer to detect syntactic clones in JavaScript inputs

[JSTAP](#) Static and modular malicious JavaScript detector

[JAST](#) Static malicious JavaScript detector

[Additional Skills – Languages](#)

French Mother tongue

English Trilingual proficiency *TOEIC score: 910 (2014); living in the U.S. since 2021*

German Trilingual proficiency *C1 Certificate (2016); lived in Germany 2017–2021*