

Dr.-Ing. Aurore Fass

Tenure-Track Faculty at CISPA

✉ [fass@cispa.de](mailto:fass@cispa.de)  
[aurore54f.github.io](https://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

- 2023– **Tenure-Track Faculty**, *CISPA Helmholtz Center for Information Security*, Germany.
- 2021–2023 **Visiting Assistant Professor**, *Stanford University*, U.S.
  - Host: [Zakir Durumeric](#)
- 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

- 2024 **Noteworthy Reviewer Recognition**, *EuroS&P*.
- 2023 **Top Reviewer Award**, *ACSAC*.

- 2023 **Top Reviewer Award**, *ACM CCS*.
- 2022 **Top Reviewer Award**, *ACM CCS*.
- 2022 **PC Member Honorable Mention**, *TheWebConf*.
- 2021 **Inspiring Career Recognition**, 1 of 3 invited alumni (out of 2,300 alumni) for the 30<sup>th</sup> 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

Dominic Troppmann, **Aurore Fass**, and Cristian-Alexandru Staicu. **Typed and Confused: Studying the Unexpected Dangers of Gradual Typing**. In *IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2024. Code repository: <https://zenodo.org/records/13760256>.

Acceptance rate: 26% (155 / 587 full research papers).

Giovanni Apruzzese, **Aurore Fass**, and Fabio Pierazzi. **When Adversarial Perturbations meet Concept Drift: an Exploratory Analysis on ML-NIDS**. In *ACM AISec (CCS Workshop on Artificial Intelligence and Security)*, 2024. Code repository: <https://github.com/hihey54/aisec24>.

Acceptance rate: 25% (18 / 72 full research papers).

Shubham Agarwal, **Aurore Fass**, and Ben Stock. **Peeking through the window: Fingerprinting Browser Extensions through Page-Visible Execution Traces and Interactions**. In *ACM CCS*, 2024. Code repository: <https://github.com/raider-ext/raider>.

Acceptance rate: 18% (129 / 710 full research papers, Cycle A).

\* Sheryl Hsu, Manda Tran, and **Aurore Fass**. **What is in the Chrome Web Store? Investigating Security-Noteworthy Browser Extensions**. In *ACM AsiaCCS*, 2024. Media coverage: <https://aurore54f.github.io/papers/hsu2024cws.media>.

Acceptance rate: 22% (65 / 301 full research papers).

Liz Izhikevich, Manda Tran, Michalis Kallitsis, **Aurore Fass**, and Zakir Durumeric. **Cloud Watching: Understanding Attacks Against Cloud-Hosted Services**. In *ACM Internet Measurement Conference (IMC)*, 2023.

Acceptance rate: 25% (52 / 208 full research papers).

\* 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.

Acceptance rate: 26% (56 / 212 full research papers).

\* **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>.

Acceptance rate: 23% (131 / 564 full research papers, May cycle).

Marvin Moog, Markus Demmel, Michael Backes, and **Aurore Fass**. **Statically Detecting JavaScript Obfuscation and Minification Techniques in the Wild**. In *IEEE/IFIP Dependable Systems and Networks (DSN)*, 2021. Code repository:

<https://github.com/MarM15/js-transformations>.

Acceptance rate: 16% (48 / 295 full research papers).

\* **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>.

Acceptance rate: 14% (32 / 225 full research papers, February cycle).

**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>.

Acceptance rate: 23% (60 / 266 full research papers).

**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>.

Acceptance rate: 32% (18 / 56 full research papers).

The publications are listed in reverse-chronological order. I marked the four most important ones with an \*.

---

## Community Services

<b>Organizing Role</b>	<b>USENIX Security Artifact Evaluation Committee Co-Chair 2025, ACM CCS Workshop General Co-Chair 2024, Associate Editor</b> of the ACM Transactions on Security and Privacy (TOPS) 2024, MADWeb (workshop co-located with NDSS) 2024 & 2023 <b>PC Co-Chair</b> and MADWeb 2025– <b>Steering Committee</b>
<b>PC Member</b>	USENIX Security 2025 & 2024, ACM CCS 2025–2021, IEEE EuroS&P 2024 & 2023, ACSAC 2024 & 2023, IEEE S&P 2023, TheWebConf 2023 & 2022, ARES 2023 & 2022, SecWeb 2024–2021
<b>Doctoral Committee</b>	Romain Fouquet (Ph.D., Computer Science, Université de Lille, May 2023)
<b>Project Proposal</b>	Reviewed projects for several European funding organizations (2023)
<b>Artifact Committee</b>	USENIX Security 2021, ACSAC 2018
<b>External Reviewer</b>	IEEE S&P 2024, TWEB 2024, ESORICS 2023, ICCCN 2023, NDSS 2022–2020, USENIX Security 2022–2020, IEEE EuroS&P 2019, ACSAC 2019 & 2018, ACM CCS 2018
<b>Misc</b>	IMC Travel Grants 2023, CISPA Faculty Hiring Committee 2021

---

## Teaching

WS 2024–2025	<b>Guest Lecture at the University of Modena and Reggio Emilia</b> <ul style="list-style-type: none"><li>◦ Web Security &amp; Security of Browser Extensions (upcoming)</li></ul>
WS 2024–2025	<b>The Web Security Seminar</b>
SS 2024	<b>The Web Security Seminar</b>
WS 2023–2024	<b>The Web Security Seminar</b> <ul style="list-style-type: none"><li>◦ Malicious JavaScript Analysis</li><li>◦ Beyond Malicious Extensions: How can Extensions put User Security &amp; Privacy at Risk?</li><li>◦ User Browsing Behavior vs. Top Lists</li></ul>
WS 2020–2021	<b>Lecturer at TELECOM Nancy</b> (Université de Lorraine, France) <ul style="list-style-type: none"><li>◦ Browser Extensions: Architecture and Security Consideration (lectures and practicals for MSc students)</li></ul>
WS 2019–2020	<b>Seminar: Joint Advances in Web Security</b> <ul style="list-style-type: none"><li>◦ Browser Extensions: Security and Vulnerabilities</li><li>◦ Overview of Malicious JavaScript Detection Techniques and Attacks</li></ul>

- WS 2018–2019 **Seminar: Joint Advances in Web Security**
- Overview of Malicious JavaScript Detection Techniques
  - Cryptojacking: Definition, Detection, and Dimensions

---

## Advising and Mentoring

### Ph.D. Students

- Apr 2024– **Valentino Dalla Valle** – *Browser Extension Security* → *paper under submission*, Saarland University & CISP
- Dec 2023– **Dominic Troppmann** – *Type Checks* → *ASE 2024*, co-supervised with Cristian-Alexandru Staicu, Saarland University & CISP

### Research Assistant

- Dec 2024– **Laith Alhelwane** (MSc student) – *Browser Extension Security*, Saarland University

### Alumni

- 2023–2024 **Ben Rosenzweig** (BSc thesis) – *Machine Learning-Based Approach for Detecting Malicious Browser Extensions* → *paper under submission*, Saarland University
- 2022–2023 **Sheryl Hsu** (BSc student) – *Browser Extension Security* → *AsiaCCS 2024*, Stanford University  
**Manda Tran** (MSc student → Ph.D. student UCLA) – *Browser Extension Security* → *AsiaCCS 2024*, Stanford University  
**Liz Izhikevich** (Ph.D. student of Zakir Durumeric → Assistant Professor UCLA) – *Internet Scanning* → *IMC 2023*, Stanford University
- 2021–2023 **Shubham Agarwal** (Ph.D. student of Ben Stock) – *Browser Extension Security* → *CCS 2024*, Saarland University & CISP  
**Kimberly Ruth** (Ph.D. student of Zakir Durumeric) – *Web Browsing Behavior* → *IMC 2022* + *paper under submission*, Stanford University
- 2022 **Mark Tran** (BSc student) – *Browser Extension Fingerprinting*, Stanford University  
**Vrushank Gunjur** (BSc student) – *Over-Privileged Extensions*, Stanford University  
**Nahum Maru** (BSc student) – *Browser Extension Crawler*, Stanford University  
**Fengchen (Maggie) Gong** (MSc student → Ph.D. student Princeton) – *Fingerprinting*, Stanford University
- 2021 **Liana Patel** (Ph.D. student of Zakir Durumeric) – *Crawler*, Stanford University  
**Luca Pistor & Nathan Bhak** (BSc students) – *Exam Software Security*, Stanford University  
**Paul Szymanski** (BSc thesis) – *A Study of State-of-the-Art Call Graph Creation Approaches for JavaScript*, with Cristian-Alexandru Staicu, Saarland University & CISP
- 2020 **Anne Christin Deutschen & Luc Seyler** (BSc students) – *Browser Extension Vulnerability*, with Dolière Francis Somé, Saarland University & CISP
- 2019–2020 **Marvin Moog & Markus Demmel** (BSc students) – *Analysis of JavaScript Obfuscation Techniques* → *DSN 2021*, Saarland University & CISP
- 2019 **Maximilian Zöllner & Niklas Kempf** (BSc students) – *Intelligent Fuzzing System for JavaScript*, Saarland University & CISP
- 2018 **Nils Glörfeld** (BSc student) – *Malicious JavaScript Deobfuscation*, Saarland University & CISP  
**Dennis Salzmann** (BSc student) – *Malicious JavaScript Detection*, Saarland University & CISP

---

## Invited Talks

### Dos and Don'ts of Reviewing

- Nov 2024 Keynote at the Winter School, WinterHack 2024. Bochum, Germany.

## Browser Extension (In)Security

- Dec 2024 Spirals Seminar at Inria Lille (upcoming). Lille, France.  
Jun 2024 GDR Information Security. Rennes, France.

## DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

- Nov 2023 Workshop at INRIA. Paris, France.  
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

- Apr 2024 PEPR Cyber – Project DefMal Webinar (France). Remote (extended version).  
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

All the software I developed is publicly available on my GitHub account:

- [static-pdg-js](#) Static analysis of JavaScript code (AST, control & data flows, pointer analysis)  
[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  
[reimpl-cujo](#) Reimplementation of [Cujo](#), static malicious JavaScript detector  
[reimpl-zozzle](#) Reimplementation of [Zozzle](#), static malicious JavaScript detector

---

## Additional Skills – Languages

- French Mother tongue  
English Trilingual proficiency *TOEIC score: 910 (2014); lived in the U.S. 2021–2023*  
German Trilingual proficiency *C1 Certificate (2016); lived in Germany 2017–2021 & 2023 onwards*