

Mohammad M. Ahmadpanah

Information Security Researcher, Postdoc at KTH

 [smahmadpanah.github.io](https://github.com/smahmadpanah)

 smmah@kth.se

 [smahmadpanah](https://www.linkedin.com/in/smahmadpanah)

Profile

Information security researcher with 12+ years of experience in language-based security, holding a PhD from Chalmers and postdoctoral experience at KTH. I build practical tools and formal models, including static/dynamic program analysis, data minimization, sandboxing, and information-flow models, to secure web-driven software, IoT platforms, browser extensions, and LLM applications. My research has uncovered critical vulnerabilities in platforms like Zapier and IFTTT with 30M users, earning bug bounties in 2020 and 2023, as well as privacy violations in 212 Chrome extensions affecting up to 3.6M users.

Research Experience

- **KTH Royal Institute of Technology**, *Postdoctoral Researcher* 1/2025 – present
 - **DiffSec**: Differential static analysis that identifies the security findings impacted by a code change, implemented in CodeQL and Joern; over 97% precision and recall on labeled dataset, and 93% fewer reported alerts.
 - **Server-side JavaScript Sandboxing**: Found sandbox breakouts in IFTTT and helped it migrate to a secure sandbox; studied migrations from vm2 in GitHub repositories; built Fiberglass, a secure sandbox with barriers for transparent host-guest sharing.
 - **Prototype Pollution**: Formal definitions of pollution freedom and gadget freedom over a core JavaScript model.
 - **LLM App Security**: Co-organizing a PhD reading course on prompt injection, contextual integrity, and information-flow security.
- **Chalmers University of Technology**, *PhD and Postdoctoral Researcher* 9/2019 – 12/2024
 - **CodeX**: Static contextual flow tracking for extensions using CodeQL, detecting 212 Chrome extensions as privacy-violating.
 - **SandTrap**: Found critical vulnerabilities in IFTTT, Zapier, and Node-RED; built a Node.js vm-based sandbox enforcing fine-grained access control.
 - **LazyTAP**: On-demand data minimization for IoT JavaScript apps via lazy computation, 95% over IFTTT and 38% over SoTA.
- **Amirkabir University of Technology**, *Graduate Researcher* 3/2015 – 9/2019
 - Research projects on Information-flow security and hyperproperties: abstract interpretation (PhD); secure multi-execution for timing-sensitive noninterference (MSc); Program-Dependence-Graph-based program rewriting tool for noninterference (BSc).

Industry and Consulting Experience

- **KNSecure**, *Security Consultant and Protection Profiles Designer* 6/2018 – 7/2019
 - Designed security protection profiles for software, web, and mobile apps, and security architectures for banking solutions.
- **Kolah Sefid Bug Bounty Platform**, *Web Security Consultant and Technical Referee* 9/2018 – 7/2019
 - Technical referee for the first national bug-bounty platform, similar to HackerOne.
- **Amirkabir CERT Lab**, *Web Security Tester, Developer, and Instructor* 5-8/2015, 9/2018 – 7/2019
 - Assessed web applications for security vulnerabilities, applied security tooling, and taught CEH courses.

Technical Skills

- **Program analysis**: data-flow and information-flow analysis, type systems, runtime monitoring; CodeQL, Joern, Jelly.
- **Web and JavaScript security**: sandboxing, browser-extension and IoT platform security and privacy, threat modeling, vulnerability assessment, secure coding; Burp Suite, Nessus, Acunetix, Invicti, Kali CEH tools.
- **Formal verification**: Rocq, Lean, Promela/Spin, Maude-NPA.
- **Languages**: JavaScript/Node.js, Java, C, Haskell, Racket, OCaml, Shell.

Selected Publications

- **DiffSec: Differential Static Analysis for Change-Impacted Security Findings**, Lu, Tang, Ahmadpanah, Balliu, *Under review*.
- **A Roadmap for Server-Side JavaScript Sandboxing**, Hedin, Ahmadpanah, Rezk, Sabelfeld, *Under review*.
- **A Theory of Prototype Pollution**, Ahmadpanah, Sands, Balliu, *In progress*.
- **CodeX: Contextual Flow Tracking for Browser Extensions**, Ahmadpanah, Gobbi, Hedin, Kinder, Sabelfeld, [CODASPY 2025](#).
- **LazyTAP: On-Demand Data Minimization for Trigger-Action Applications**, Ahmadpanah, Hedin, Sabelfeld, [S&P 2023](#).
- **SandTrap: Securing JavaScript-driven Trigger-Action Platforms**, Ahmadpanah, Hedin, Balliu, Olsson, Sabelfeld, [USENIX 2021](#).
- Also: [EuroS&P 2021](#), [Protocols, Strands, and Logic 2021](#); PhD thesis 2024; full list on [Google Scholar](#).

Education

- **PhD, Information Security**, Chalmers University of Technology, Supervisors: Andrei Sabelfeld, Daniel Hedin 9/2019 – 8/2024
- **MSc, Information Security**, Amirkabir University of Technology (1st place) 9/2015 – 9/2017
- **BSc, Software Engineering**, Amirkabir University of Technology (top 10%) 9/2011 – 9/2015

Teaching, Service, and Honors

- **Talks and visits**: invited talks at **ETH Zurich**, **Inria**, Chalmers, KTH, Sharif (2023 – 2025); research visits at **Google Zurich** (2024) and Mälardalen University (2022); **CSF'20**, **CSF'23**, **FOSAD'22**, **SWITS'22**, **ShiftLeft'24**, **ShiftLeft'25**.
- **Teaching**: Formal Methods (lecturer, KTH, 2026); Research Course in Programming Languages and Formal Methods (lecturer, KTH, 2026); Language-Based Security (guest lecture and teaching assistant, KTH, 2025 – 2026); Computer Security (teaching assistant, KTH, 2025); Language-Based Security, Programming Language Technology, Finite Automata and Formal Languages (teaching assistant, Chalmers, 2019 – 2024); Advanced Programming (course responsible, Amirkabir, 2018; top 3% of 830 lecturers).
- **Supervision**: PhD co-supervision (KTH, 1/2025 – present); MSc co-supervision (KTH, 1/2025 – 7/2026); MSc supervision (Chalmers, 2022 – 2023).
- **PC member**: **EuroS&P'27**, **ASIACCS'27**, **NordSec'26**, **SecDev'26**, **PST'26**, **PLAS'24**, **FCS'24**; **AEC**: **TACAS'25**. *External reviewer*: **CCS**, **USENIX Security**, **S&P**, **CSF**, **EuroS&P**, **WWW**, **MADWeb** (2019 – 2026).
- **Honors**: Adlerbert Foundation scholarship 2021 – 2024; Chalmers–KTH–Aarhus educational CTF organization team (2021 – 2025).