# ARTUR JANC

**Mischief management. Also, a substantial amount of mischief design and development.**

contact@arturjanc.com   arturjanc.com   @arturjanc   github.com/arturjanc   linkedin.com/in/arturjanc

## EXPERIENCE

### Senior Staff Information Security Engineer

**Google** October 2019 – ongoing

- Lead a team of 10 engineers responsible for designing and deploying application security defenses against common web vulnerabilities.
- Work with product teams at Google, browser vendors, and standards bodies (W3C) to ship web isolation and anti-injection mechanisms.

### Staff Information Security Engineer

**Google** October 2016 – October 2019

- Managed a team responsible for deploying Content Security Policy to 250+ applications / 70% of external Google traffic.
- Owned infrastructure to support deployments of web security features, including server-side libraries and data collection systems.
- Designed major elements of web defenses against Spectre, including Fetch Metadata Request Headers and Cross-Origin Opener Policy.

### Senior Information Security Engineer

**Google** March 2014 – October 2016

- Established and managed a team of 5 security engineers focusing on proactive security improvements and mitigating common bug classes.
- Panel member of the Google Vulnerability Reward Program; decided reward amounts for 3,000+ bug reports from external researchers.

### Information Security Engineer

**Google** October 2010 – March 2014

- Conducted security reviews for 100+ product launches. Ran pentests and offensive exercises, including research into novel attack classes.
- Created security documentation and interactive education resources.
- Started a cross-team effort to protect Google against XSS bugs.

### Software Engineer

**Sacramento Press** February 2009 – October 2010

- First non-founder technical employee; developed and maintained the Sacramento Press web application. Owned frontend development.
- Supported production and office networks with 10+ Linux servers, OS X server and workstations; set up network monitoring (Nagios).

### Founder

**Lingro** June 2006 – February 2009

- Took Lingro from initial concept through incorporation and public release; secured a seed round. Sold tools as SaaS to Pearson Education.
- Designed and implemented server and database architecture (Django, MySQL). Responsible for majority of backend and frontend development, including UI, engagement tools, and developer APIs.

## EDUCATION

### Graduate coursework (non-degree)

**Stanford University, MS&E** 2011–2012

Completed courses in international security, investment science and marketing.

### M.Sc. in Computer Science

**Worcester Polytechnic Institute** 2009

Thesis: Network performance evaluation in the web browser sandbox

Teaching assistant in the CS department

### B.Sc. in Computer Science

**WPI** 2003–2007   GPA: 3.86

Project: Virtutopia: Design of a Massively Scalable Distributed Virtual Environment

### B.Sc. in Electrical Engineering

**WPI** 2003–2007

Project: Web-based interface to an FPGA-based True Random Number Generator

Software QA intern at EMC Corporation

## SELECT TALKS

### How the web became a scary place, and how we can fix it

**USENIX Security** 2019

A review of the origins of major security threats to the web platform and the ongoing efforts to mitigate them.

### Securing web apps with modern platform features

**Google I/O** 2019

An introduction to new web security mechanisms: CSP3, Trusted Types, Fetch Metadata and Cross-Origin Opener Policy.

### Rootkits in your web application

**28th Chaos Communication Congress**

An explanation of the impact of XSS bugs and analysis of application-specific ways to obtain malicious script persistence.

**More talks:** arturjanc.com/talks

# SKILLS

- **Full-stack developer** with a strong background in system design, frontend and backend languages & frameworks, databases and UI/UX.
  - Good knowledge of Python, Java, JavaScript and shell scripting.
  - Excellent command of web technologies (HTML, CSS, JS, including client-side frameworks), web browsers and web design patterns.
  - Experience in system administration (Linux, OS X) and networking.

- **10+ years of security experience**, including application security and infrastructure security; closely familiar with vulnerability trends.
  - Excellent knowledge of application security best practices, both offensive (pentesting, red teams) and defensive (secure design, SDL).
  - In-depth grasp of core security processes: audits, bug bounties and vulnerability disclosure, remediation, incident response.
  - Track record of innovative security and privacy-focused research.

- **Leadership**: 5+ years of people management, 7+ years as team lead.
  - End-to-end ownership of software engineering projects of diverse scopes, from idea/design to implementation and maintenance.
  - Project management of major Google and industry-wide efforts.
  - Expert communicator (including executive communications), speaker, presenter and tech writer for industry and academic audiences.

# SELECT PUBLICATIONS

## Academic research

- A. Janc K.Kotowicz; L. Weichselbaum, R. Clapis (2020). “Information Leaks via Safari’s Intelligent Tracking Prevention”. In: *arXiv:2001.07421*.
- L. Weichselbaum M. Spagnuolo; S. Lekies, A. Janc (2016). “CSP is dead, long live CSP! On the insecurity of whitelists and the future of Content Security Policy”. In: *Proceedings of ACM CCS 2016*.
- L. Olejnik C. Castelluccia, A. Janc (2012). “Why Johnny can’t browse in peace: On the uniqueness of web browsing history patterns”. In: *Proceedings of 5th HotPETs Workshop*.
- A. Janc, L Olejnik (2010). “Web browser history detection as a real-world privacy threat”. In: *ESORICS*, pp. 215–231.
- A. Janc, L. Olejnik (2010). “Feasibility and real-world implications of web browser history detection”. In: *Proceedings of W2SP*.

## Position papers & standards notes

- A. Janc C. Reis, A. van Kesteren (2019). *Cross-Origin Opener Policy and Cross-Origin Embedder Policy explained.*
- A. Janc, M. West (2018). *Spilling the Beans Across Origins. A primer on web attacks via cross-origin information leaks and speculative execution.*
- A. Janc (2017). *Why the web needs finer-grained origins.*.
- A. Janc, M. Zalewski (2013). *Technical analysis of client identification mechanisms.*

## Tutorials & developer documentation

- A. Janc, M. Spagnuolo, L. Weichselbaum, and D. Ross (2016). *Google Security Blog: Reshaping web defenses with strict Content Security Policy*
- A. Janc, L. Weichselbaum (2016). *Strict Content Security Policy*
- A. Janc, J. Munoz (2014). *Google Security: Cross-site scripting*

# SELECT PROJECTS

**Lingro dictionary** https://lingro.com

Lingro is an interactive dictionary and set of web-based tools for language learners. Launched as a startup project in college, over the past decade it translated 3.5 million words for over 200 thousand users.

*Built with a LAMPy stack using Django.*

**XSS game** https://xss-game.appspot.com

One of the first popular games to teach developers how to exploit and avoid cross-site scripting, used in many security courses.

*Built on Google App Engine (Python).*

**Light Sensor demos** arturjanc.com/ls

A set of exploits showing how attackers can use the browser’s light sensor API to leak sensitive application data. Resulted in changes to the AmbientLightSensor specification and implementations.

*Built with JavaScript and custom SVG filters.*

**More projects:** arturjanc.com/projects

# AWARDS, ETC.

Google Cloud **Feats of Engineering Award** for adoption of Content Security Policy.

Google **ISE Summit Awards** for advances in web security and the adoption of CSP.

**WPI Salisbury Award** for top senior graduating with *greatest faithfulness and excellence* in Computer Science.

1st place in **WPI CEI Business Plan Competition** for Lingro.

**WPI Neil Sullivan Scholarship** for *most meritorious junior* majoring in Computer Science.

1st place in **WPI Henry Strage Innovation Awards** for the prototype of Lingro.

Member of WPI chapters of TBP, IEEE-HKN, and UPE honor societies.