Intel Security Conference (iSecCon) 2022 Call for Papers

Conference Dates: Oct 13-14, 2022

Venue: Westside Commons

Address: 801 NE 34th Ave, Hillsboro, OR 97124

Theme:

Innovate. Elevate. Accelerate.

Delivering Exceptional End-to-End Security Solutions

This prestigious in-person conference aims to bring together esteemed speakers from Intel, industry, government, and academia to share knowledge and cutting-edge ideas about security and related topics. This is an excellent opportunity to engage with and hear from security experts and leaders across the industry, as well as influence the future directions of Intel products. The conference will be open to Intel engineers as well as some customers and partners. All talks will be delivered in English.

TOPICS:

The conference committee gives preference to presentations with practical demonstrations.

iSecCon will have multiple tracks. In the submission form, please indicate the track relevant to your presentation.

- **Hardware Security**
- **Firmware/Software Security**
- **Security Tools and Processes**
- **Other**

Example topics associated with these tracks include, but not limited to (in alphabetical order):

- AI and Machine Learning Security
- Applied Cryptography
- Cloud Computing Security
- Confidential Computing
- Defensive Security
- Edge/IOT Security
- Emerging Threats Security
- End-to-End Security
- Offensive Security
- Physical Attacks
- Platform Security
- Privacy

- Regulation and Compliance Security
- Reverse Engineering
- Secure Development Lifecycle
- Supply Chain Security

SUBMISSION GUIDELINES and TERMS:

- Authors will submit their abstracts to EasyChair—a third party public conference management site—and should not disclose confidential information that they and/or their employers are not ready to share with the public.
- Submissions may only be entered by researchers or speakers. (No submissions from PR firms or marketing representatives.) Submissions will not be accepted from any author that appears on a U.S. Government list of sanctioned entities or individuals.
- No product or vendor-related pitches will be accepted. If your presentation involves advertisement of products or services or is deemed to be a work of plagiarism, your submission will be rejected.
- Submissions must clearly detail the concepts, ideas, findings, and solutions that the speaker plans to present.
- Multiple proposals may be submitted by the same individual, but each proposal must be submitted via a separate submission form.
- Intel follows the common industry practice of Coordinated Vulnerability Disclosure (CVD) for reported security vulnerabilities on launched products. CVD is intended to reduce adversary advantage while a security vulnerability is being evaluated and mitigated. In addition to practicing inbound CVD in partnership with external security researchers, Intel also coordinates outbound vulnerability disclosure with industry partners and other external stakeholders as appropriate, so that all affected parties are disclosing in unison for an optimal defensive position.
- For any submission regarding a security vulnerability, that security vulnerability must have been reported to the affected vendor(s) and publicly disclosed by those vendor(s) before the conference (October 13-14, 2022), and any embargo that is in place must be noted on the submission form.
- If you have discovered a potential security vulnerability in an Intel product, and have not already disclosed it to Intel, please contact the Intel Product Security Incident Response Team (PSIRT) at secure@intel.com. For more information on reporting potential security vulnerabilities to Intel, please see the Intel Vulnerability Handling Guidelines found on the Intel Security Center.
- Intel employees that encounter a potential security vulnerability in a non-Intel product, where Intel products are not affected, are still required to report the issue to the Intel PSIRT. The Intel PSIRT will work with you to report the issue to the affected vendor.
- If you are not an Intel employee and have encountered an undisclosed potential security vulnerability in a non-Intel product then please contact the vendor of that product to file a report
- Submissions that highlight Intel-relevant security research, tools, and vulnerabilities will be given priority.
- Submitters will be contacted directly by review board members if there are questions regarding their submissions.
- Selections are made at Intel's sole discretion.
- Intel reserves the right to rescind an accepted submission without reason and strives to communicate any rescissions as early as possible.

- Selected speakers grant Intel permission to post pictures/bios and to record, reproduce, distribute, advertise and show a speaker's presentation including but not limited to intel.com, conference proceedings and materials, audio, video, printed and/or electronic ads, fliers, mailers, etc.
- Please note that in the event that an in-person conference is not feasible, selected speakers will be expected to present virtually or have recordings of their talks available for the conference by Sep. 30, 2022.

TALK DURATION:

Each speaker will be allotted a **40-minute** presentation time slot and 10 additional minutes for Q&A.

SPEAKER BENEFITS:

Travel Reimbursement:

- Economy-class, round-trip airfare for one Speaker per team; cap of $1,000 domestic/$1,300 international USD
- $ 100 per diem for up to 3 days.

Accommodations:

- One hotel room for two nights (Oct 13 and 14) for one Speaker

- Speaker dinner with iSecCon speakers and select Intel security leaders as a token of appreciation from Intel.

KEY DATES (*Terms & Dates are subject to change)*:

Abstract submission opens	May 18, 2022
Abstract submission deadline	Jun. 24, 2022
Speaker Notification	Jul. 20, 2022
Confirmation from speakers	Jul. 29, 2022
Speaker collateral submitted to Intel (pics, bios, NDA and Personal Material Release forms)	Aug. 5, 2022
First presentation submitted for legal/VRL review (internal)	Sep. 9, 2022
Final presentations ready and submitted for conference	Sep. 30, 2022
iSecCon'22	**Oct. 13-14, 2022**

CFP REVIEW BOARD MEMBERS:

The iSecCon Review Board is comprised of credible and distinguished security professionals and thought leaders throughout various areas of the security community at Intel.

Name	Designation at Intel
Alyssa Milburn	Offensive Security Researcher
Antonio Martin	Principal Engineer, University Research Manager
Brent Thomas	Sr. Principal Engineer, Security Assurance & Governance
Bruce Monroe	Principal Engineer, Lead Engineer Intel PSIRT
Burzin Daruwala	Director, Offensive Security Research and Product Red Teaming
Chris Holt	Bug Bounty Program Manager
Jonathan K Valamehr	Principal Engineer, Security Assurance and Cryptography
Matthew D Wood	Principal Engineer, Software and Technology Group
Neer Roggel	Offensive Security Researcher
Richard Chow	Principal Engineer, Univ. Collaborations Office
Ronald Perez	Intel Fellow, Chief Security Architect

Please contact security.conference@intel.com if you have questions.

Cheers,

iSecCon Organizing Committee