CfP: CSF 2021

Submitted by Anonymous on Thu, 07/30/2020 - 2:00pm

CALL FOR PAPERS

34th IEEE Computer Security Foundations Symposium (CSF 2021)

June 21-25, 2021, Dubrovnik, Croatia | https://www.ieee-security.org/TC/CSF2021/

The Computer Security Foundations Symposium is an annual conference for researchers in computer security. CSF seeks papers on foundational aspects of computer security, such as formal security models, relationships between security properties and defenses, principled techniques and tools for design and analysis of security mechanisms, as well as their application to practice. While CSF welcomes submissions beyond the topics listed below, the main focus of CSF is foundational security and privacy.

Submission Server
Submit papers at https://csf2021.sec.uni-stuttgart.de/

Topics
New results in security and privacy are welcome. We also encourage challenge/vision papers, which may describe open questions and raise fundamental concerns about security and privacy. Possible topics for all papers include, but are not limited to:

- access control
- accountability
- anonymity
- attack models
- authentication
- blockchains and smart contracts
- cloud security
- cryptography
- data provenance
- data and system integrity
- database security
- decidability and complexity
- decision theory
- distributed systems security
- electronic voting

- embedded systems security
- forensics
- formal methods and verification
- hardware-based security
- information flow control
- intrusion detection
- language-based security
- mobile security
- network security
- privacy
- security and privacy aspects of machine learning
- security and privacy for the Internet of Things
- security architecture
- security metrics
- security policies
- security protocols
- software security
- socio-technical security
- trust management
- usable security
- web security

SoK papers: Systematization of Knowledge Papers
CSF'21 solicits systematization of knowledge (SoK) papers in foundational security and privacy research. These papers systematize, re-formulate, or evaluate existing work in one established and significant research topic. Such papers must provide new insights. Survey papers without new insights are not appropriate. Submissions will be distinguished by the prefix "SoK:" in the title and a checkbox on the submission form. Accepted papers will be presented at the symposium and included in the proceedings.

Special Sessions
This year, we strongly encourage papers in three foundational areas of research we would like to promote at CSF:

MACHINE LEARNING MEETS SECURITY AND PRIVACY (Session Chair: Suman Jana). Machine learning has revolutionized computer science. However, machine learning algorithms have been applied to problem domains as black boxes and offer little guarantees in terms of fairness and transparency of the results and privacy of the dataset, We invite submissions on foundational work in this area. Topics include security, privacy, and fairness issues of machine learning algorithms, reasoning techniques necessary to justify safety of its autonomous decisions, and techniques for protecting the privacy of the dataset.

BLOCKCHAIN and SMART CONTRACT (Session Chair: Aggelos Kiayias). Many challenges arise with the rapid development of the blockchain technology and its main application: smart contract. The need for formal foundations for the security and privacy of blockchains and smart contracts. We invite submissions on foundational work in this area. Topics include security and privacy issues, analysis and verification of existing solutions, design of new systems, broader foundational issues such as how blockchain mechanisms fit into larger distributed ecosystems and foundational security aspects of applications built on top of blockchain mechanisms, new programming languages for smart contracts, and formal analysis of smart contracts.

APPLIED CRYPTOGRAPHY (Session Chair: Ran Canetti). Cryptography is at the heart of many security- and privacy-critical systems. As such it is an integral part of the field of security and privacy. While modern cryptography is built on firm theoretical foundations, new applications frequently need new cryptographic solutions, new security definitions, models, and proof techniques and tools. We invite submissions in this area. Topics include, but are not limited to, the design and analysis of cryptographic protocols, new cryptographic frameworks and proof techniques, including composability as well as automated, tool-supported analysis and verification of cryptographic primitives and protocols.

These papers will be reviewed under the supervision of the special session chairs. They will be presented at the conference, and will appear in the CSF proceedings, without any distinction from the other papers.

Proceedings will be published by the IEEE Computer Society Press and will be available at the symposium. Some small number of papers will be selected by the PC as "Distinguished Papers".

Important Dates AoE (UTC-12h)

Spring cycle:

- May 8th: paper submission deadline
- July 10th: author notification

Fall cycle:

- Oct 2nd: paper submission deadline
- Dec 7th: author notification

Winter cycle:

- Early Feb: paper submission deadline
- Mid April: author notification

Paper Submission Instructions
Submitted papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with published proceedings.

Papers must be submitted using the two-column IEEE Proceedings style available for various document preparation systems at the IEEE Conference Publishing

Services page. All papers should be at most 12 pages long, not counting bibliography and well-marked appendices. Anonymized supplementary material such as proof scripts can be uploaded as a tar ball on the submission site. Committee members are not required to read appendices, and so the paper must be intelligible without them.

Papers failing to adhere to any of the instructions above will be rejected without consideration of their merits.

Papers intended for one of the special sessions should select the "Applied Cryptography", "Blockchain and smart contract", "Machine learning meets security and privacy" option, as appropriate.

At least one coauthor of each accepted paper is required to attend CSF to present the paper. In the event of difficulty in obtaining visas for travel, exceptions can be made and will be discussed on a case-by-case basis.

Review process

CSF'21 will employ a light form of double-blind reviewing. Submitted papers must (a) omit any reference to the authors' names or the names of their institutions, and (b) reference the authors' own related work in the third person (e.g., not "We build on our previous work ..." but rather "We build on the work of ..."). Nothing should be done in the name of anonymity that weakens the submission or makes the job of reviewing the paper more difficult (e.g., important background references should not be omitted or anonymized). The author information will be revealed to the reviewers after reviews are submitted. Please see our frequently asked questions (FAQ) that address many common concerns. When in doubt, contact the program chairs.

Decisions

The outcome of the review process can be one of the following three: accept, reject, major revision. In rare occasions, accepted papers are shepherded for minor modifications.

Major revisions

Papers with "major revision" decision must be re-submitted within the following two cycles, accompanied by a writeup explaining how the revision meets reviewers' revision requirements. These papers will be reviewed by the same reviewers as those for the initial submission. These papers do not have to be anonymized, they should in fact contain the authors' names and affiliations. They may use 16 pages in the usual IEEE template. But the 16 pages should contain everything, in particular bibliography and appendix (if any). In other words, revisions should be prepared as if they were camera-ready papers. For additional material authors may point to technical reports or supply additional material when submitting the paper. Reviewers are, however, not obliged to read this material.

Authors should submit their revision as a new paper (rather than updating the previous submission) and mark it as "major revision". For major revision papers the submission system will ask authors to provide additional information in a textbox, such as the cycle and the submission number of the previous submission.

The possible decisions for such resubmitted revised papers are the following: accept (possibly with shepherding) or reject, i.e., a major revision decision is excluded.

Like all papers, major revision papers can be withdrawn from the conference at any time.

Major revision papers not re-submitted within the following two cycles will be considered new submissions, reviewed by serving PC members. A writeup explaining how the revision meets previous reviewers' revision requirements is optional. The layout of these papers has to follow the guidelines for regular submissions, in particular, for these papers the limit of 12 pages applies.

Resubmissions of rejected papers

Rejected papers can be re-submitted at any time. If a rejected paper is re-submitted within 11 months of the last deadline they were submitted to (e.g., rejected submissions to Oct. 2019 is resubmitted to May 2020 deadline), reviews and a writeup explaining how the current submission addresses concerns in the reviews must be submitted as supplementary material. The paper will be desk-rejected by the PC chairs if previous reviews or the explanation is missing. We may use a different set of reviewers for re-submissions. All resubmissions of rejected papers can optionally submit reviews from previous submissions and a writeup explaining how the current submission addresses concerns in the reviews as supplementary material.

CfP: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2021) ?

Calls for Papers