Announcement and Call for Papers USENIX

2010 Workshop on Collaborative Methods for Security and Privacy (CollSec '10)

Sponsored by USENIX, the Advanced Computing Systems Association, and Deutsche Telekom

http://www.usenix.org/collsec10

August 10, 2010 **Washington, DC**

CollSec '10 will be co-located with the 19th USENIX Security Symposium, which will take place August 11–13, 2010.

Important Dates

Submissions due: *May 5, 2010, 11:59 p.m. PDT*
Notification of acceptance: *June 10, 2010*
Final paper files due: *June 30, 2010*

Workshop Organizers

Program Co-Chairs

Nadav Aharony, *MIT Media Lab*
Yaniv Altshuler, *Technion*
Yuval Elovici, *Ben-Gurion University of the Negev and Deutsche Telekom Laboratories at Ben-Gurion University*

Program Committee

Sahin Albayrak, *Technical University of Berlin*
Nikita Borisov, *University of Illinois at Urbana-Champaign*
Armin Cremers, *University of Bonn*
Shlomi Dolev, *Ben-Gurion University of the Negev*
Murat Kantarcioglu, *University of Texas at Dallas*
Bernhard Loehlein, *Deutsche Telekom*
Arie Matsliah, *Centrum Wiskunde & Informatica*
David Reed, *MIT Media Lab*
Pierangela Samarati, *Università degli Studi di Milano*
Jean-Pierre Seifert, *Technical University of Berlin and Deutsche Telekom Laboratories*
Ronen Vaisenberg, *University of California, Irvine*
Gill Zussman, *Columbia University*

Overview

The complexity and sophistication of security threats are expected to increase further in the near future. Existing security solutions might soon become useless in the face of attacks that will most likely be launched from many computers at once (for example, the use of large botnets). An appropriate answer to such threats should rely on collaborative methods that harness the collective strength of many independent units. When it comes to defending against a given threat, different end-units as well as entire networks are essentially performing the same work redundantly. As a result, the need to share knowledge (for accelerating detection and response to new attacks and threats) and resources (increasing efficiency and reducing resources consumption) becomes clear.

The workshop aims to bring to the forefront innovative approaches that involve the use of collaborative methods for privacy and security. While the workshop will touch on themes that are at the heart of the USENIX Security Symposium, discussion will focus on the boundary between collaborative algorithms and swarm intelligence and the implementation domains of networking, privacy, and security.

Co-located with the 19th USENIX Security Symposium in Washington, DC, CollSec '10 will be a one-day event on Tuesday, August 10, 2010. Accepted papers will be published electronically. Attendance at the workshop will be open to the public. The workshop will feature an award for the best paper.

Workshop Topics

Proposed topics for the workshop include but are not limited to the following:

- Collaborative detection of distributed network attacks
- Peer-to-peer–based security mechanisms
- Adversarial abuse of collaborative security mechanisms
- Anti-epidemic network vaccination
- Efficient implementation of security and privacy algorithms through sharing knowledge and resources
- Increasing energy efficiency through collaboration in network security
- Use of low complexity property testing methods by decentralized security agents
- Collaboration in future Internet security and privacy layers
- Novel collaborative network architectures for increased security and privacy
- Trust and authentication in collaborative environments
- Collaboration-aware network protocols: security and privacy aspects
- Collaborative privacy management: access controls and permissions
- Decentralized, trusted third-party approaches and methods
- Intrusion detection in collaborative and cloud computing environments
- Security configuration based on social context groups (social firewall, authentication protocols, etc.)
- Security algorithms inspired by human social-cooperation interactions
- Providing security and privacy for social overlay networks
- Configuring security protocol parameters based on social and cooperative information

Submission Instructions

Papers are due by May 5, 2010, at 11:59 p.m. PDT. All submissions should be made online via the Web submission form on the CollSec '10 Call for Papers Web site, http://www.usenix.org/collsec10/cfp. Submissions should be finished, complete papers.

Prospective authors are invited to submit original, unpublished research papers that are not being considered in another forum. We will welcome works in progress, in addition to well established works.

Your submission may be in the form of:

- A short position paper of up to 4 proceedings pages in length.
- A full-length technical paper of up to 12 proceedings pages in length.

Page limits include the bibliography and any appendices.

Papers should be typeset in two-column format, using a 10-point Times Roman font on 12-point leading in a text block of 6.5" by 9", as is customary for USENIX papers.

Papers will be evaluated in terms of their relevance to the workshop's topics, novelty, and scientific contribution, in addition to their potential for encouraging discussion and exchange of ideas during the workshop itself.

Please note: At least one author per paper must attend the workshop to present the accepted paper.

Submissions are single-blind; authors should include their names and affiliations as part of their submissions. Submissions must be in PDF format. Note that LaTeX users can use the "dvipdf" command to convert a DVI file into PDF format. Please ensure that your submission can be opened using Adobe Acrobat 4.0.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX CollSec '10 Web site; rejected submissions will be permanently treated as confidential.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy at http://www.usenix.org/submissionspolicy. Questions? Contact your program co-chairs, collsec10chairs@usenix.org (use "[CollSec '10]" in the subject of your email), or the USENIX office, submissionspolicy@usenix.org.

All papers will be available online to registered attendees before the workshop. If your accepted paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop, August 10, 2010.

Specific questions about submissions may be sent to the program co-chairs at collsec10chairs@usenix.org (use "[CollSec '10]" in the subject of your email).