



# ACM CODASPY 2018

## 4th ACM International Workshop on Security and Privacy Analytics (IWSPA 2018)

Tempe, AZ, March 21, 2018

Co-located with 8<sup>th</sup> ACM CODASPY 2018 (Website: [CODASPY 2018](http://codaspy.org))

Website: <http://capex.cs.uh.edu/?q=content/4th-international-workshop-security-and-privacy-analytics-2018>

This is the fourth workshop in the series of workshops on Security and Privacy Analytics. Increasingly, sophisticated techniques from machine learning, data mining, statistics and natural language processing are being applied to challenges in security and privacy fields. However, experts from these areas have had no medium in the past where they can meet and exchange ideas so that strong collaborations can emerge, and cross-fertilization of these areas can occur. Moreover, current courses and curricula in security do not sufficiently emphasize background in these areas and students in security and privacy are not emerging with deep knowledge of these topics. Hence, we propose to continue the workshop that we started in the year 2015 to address the research and development efforts in which analytical techniques from machine learning, data mining, natural language processing and statistics are applied to solve security and privacy challenges (“security and privacy analytics”). Submissions of papers related to methodology, design, techniques and new directions for security and privacy that make significant use of machine learning, data mining, statistics or natural language processing are welcome. Furthermore, submissions on educational topics and systems in the field of security analytics are also highly encouraged. For more information about the workshop: <http://capex.cs.uh.edu/?q=content/4th-international-workshop-security-and-privacy-analytics-2018>

The workshop will focus on, but is not limited to, the following areas:

- ✓ Natural Language Processing for Security/Privacy;
- ✓ Data Mining techniques for Security/Privacy;
- ✓ Machine Learning for Security/Privacy;
- ✓ Statistics for Security/Privacy;
- ✓ Inference Control;
- ✓ Privacy-preserving data mining;
- ✓ Security of Machine learning;
- ✓ Security of Data Mining;
- ✓ Security of Natural Language Processing;
- ✓ Case studies;
- ✓ Educational topics and courses

The workshop is planned for one day, March 21, 2018, on the last day of the conference. All submissions must describe original research, not published nor currently under review for another workshop, conference, or journal.

All papers must be submitted electronically via the EasyChair system:

<https://easychair.org/conferences/?conf=iwspa18>

Papers must be at most 10 pages (12 pages in total) in length in double-column ACM format excluding bibliography and appendices. Submission implies the willingness of at least one author to attend the workshop and present the paper. Accepted papers will be included in the ACM Digital Library. The presenter must register for the workshop before the deadline for author registration. The accepted papers will be compiled in the workshop proceedings as either a regular paper within 11 pages or a short paper within 7 pages. A limited number of high quality submissions may be selected for publication in a special issue of a journal. Reduced registration fees will be provided to selected participants through an NSF grant.

We also plan to organize a **Shared Task Competition** for IWSPA'18. Details coming soon on the IWSPA'18 website!

### • Organizing Committee

- ✓ **Wenyaw Chan** (University of Texas-HSC at Houston)
- ✓ **Ping Chen** (University of Massachusetts-Boston)
- ✓ **Lila Ghemri** (Texas Southern University)
- ✓ **Stephen Huang** (University of Houston)
- ✓ **Ernst Leiss** (University of Houston)
- ✓ **Carlos Ordóñez** (University of Houston)
- ✓ **Rakesh Verma** (University of Houston)

### • Steering Committee

- ✓ **George Cybenko** (Dartmouth College)
- ✓ **Carl Landwehr** (George Washington)
- ✓ **Ravi Sandhu** (University of Texas, San Antonio)
- ✓ **Rakesh Verma** (University of Houston)

### • Technical Program Committee

- ✓ **Ali Ghorbani** (University of New Brunswick)
- ✓ **Omid Madani** (Cisco)
- ✓ **David Marchette** (NSWC)
- ✓ **Michael Rusinowitch** (LORIA - INRIA Nancy Grand-Est)
- ✓ **Haining Wang** (University of Delaware)
- ✓ **Roland Yap** (National University of Singapore)
- ✓ More to be added

### • Important Dates

- ✓ **Paper Submission Deadline:** December 8, 2017, 11.59pm anywhere on earth
- ✓ **Acceptance Notification:** January 3, 2018
- ✓ **Camera Ready Submission Deadline:** TBA

### • For more information:

- ✓ Contact: Stephen Huang at [s\\_huang@cs.uh.edu](mailto:s_huang@cs.uh.edu) or Rakesh Verma at [rverma@uh.edu](mailto:rverma@uh.edu)