Workshop on Information Security and Social Media
Call for Papers

蒋方婷：2020XXX034 | 文雅：2020XXX035 | 周雨婷：2020XXX060

May 18, 2021

Title	Short-Title	Only-for-Homework	Accept-Chinese-Submission
Workshop on Information Security and Social Media	ISSM	False	True

1 Overview

In decades past, the rapid development in the field of internet technology has brought the bloom of online social media. The Internet's first-generation(Web 1.0) consisted of static pages instead of dynamic HTML. The second-generation (Web 2.0) encouraged people to share information and interact with each other by posting and retweeting user-generated content in virtual communities. The rapid development of Web 2.0 brought the bloom of online social media and allowed many new social networking sites to flourish such as Facebook, Twitter, Sina Weibo, and others. Online social media replace traditional media as an established trend.

With the continuous development of artificial intelligence, big data, cloud computing, and other technologies, the editing methods of information are also changing with each passing day. On the one hand, online social media which provide a wealth of raw data invaluable to researchers are with these characteristics, large user scale, rapid information dissemination, and wide range of influence. The large user scale of social media provides a wealth of raw data invaluable to researchers. It presents a challenge to researchers to analyze the noisy data collected from such information. On the other hand, modifying the digital image, audio, and video data become simple and interesting, but it also brings many security issues. Information security is the intersection of multimedia intelligent information processing and cyberspace security, and they have received extensive attention in recent years.

The Workshop on Information Security and Social Media focus on recent advances and address existing challenges in security, privacy, cryptography of information and Image, audio and video processing. processing technologies. It provides great opportunities for participants to share, interact and learn from each other, and thus inspires cross-field social networks research. The objective of this workshop is to provide general guidelines on the current and future trends in information security and social media technologies.

2 Topics of Interest

- Natural Language Processing :

- Dialog Systems
- Information extraction and Text mining
- Linguistic Theories, Cognitive Modeling, and Psycholinguistics
- Machine Translation
- NLP deep learning
- Textual Inference and all Areas of Semantics

- Cloud security
- Mobile security and privacy
- Secure and Privacy-Preserving Computation and Data Processing
- Security and Privacy of Blockchain
- ...

- Image, audio and video processing :

- Information Hiding Technology:
  - Numeric steganography in semantic and structural terms
  - Robust copyright identification using watermarks and fingerprints
  - The copyright protection of fragile digital watermark
  - Steganography and steganalysis(including image, audio, and video)
  - Multimedia watermarking
  - Signal Processing in the Encrypted Domain
- Fake multimedia forensics and anti-forensics
- Multimedia information tampering:
  - Deepfake multimedia detection
- ...

- Online Social Meida and Online Social Network :

- Measurement, analysis, and modeling of networked users' behavior in Online Social Network
- Named Entity Recognition and Keyword extraction
- Speech recognition, synthesis, and speaker identification
- Sentiment analysis and classification
- Event extraction and semantic role labeling

- Dynamics of trends, information and opinion diffusion in Online Social Network
- Complex-network analysis of OSNs
- Information Retrieval
- Social robot detection
- Sensitive information identification
- Public opinion monitoring
- ...

- Security :

- Web security and privacy:
  - Multi-source target website page extraction
  - Phishing site detection
- Secure and Privacy-Preserving Computation and Data Processing
- ...

- Privacy :

- Machine learning and privacy
- Information leakage, data correlation, and abstract attacks on privacy
- Privacy technologies and mechanisms
- Anonymous
- ...

- Cryptography

- ...

3 Important Dates

Submission Deadline : **June 25, 2021 23:59:59 UTC+8**
Notification Due : **July 12, 2021**
workshop time : **July 19, 2021**

4 Paper Submission

Authors are invited to submit papers to the email address **847582804@qq.com** by **June 25, 2021 23:59:59 UTC+8**. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated for this conference.

5 Paper Formatting

All submissions must obey the following formatting requirements.

- Paper bodies (all content before references and appendices) must be between three(3) and four(4) single–spaced pages, including figures and tables, followed by as many pages as necessary for references and optional appendices. Papers whose pre-reference content is longer than 4 pages will not be reviewed.
- Reviewers are not required to read any appendices or consider them in their review. Authors should thus ensure that the core paper is complete and self-contained. For example, if the appendix provides details of a proof or experiment, the body should summarize the key result.
- The paper body must include some statement about ethical considerations. This could be simply the sentence "This work does not raise any ethical issues" , or where relevant (for example, but not exclusively, a paper involving human subjects), the discussion may be more detailed.

- If submitting to the experience-track, authors should indicate as such in the submission form and paper title.

- The conference use manuscript templates provided by IEEE eXpress Conference Publishing. You can get it in https://www.ieee.org/conferences/publishing/templates.html

Your goal as an author is to produce a clearly readable submission within the above constraints. Authors are strongly discouraged from violating the formatting requirements with the aim of including additional material: submissions that violate the formatting requirements may not be reviewed. You can visually inspect a page-by-page report of your paper format using the same tool as the submission system via a separate online form.

After the submission deadline, we will use the same tool to check the conformance of papers. The format checking tool uses heuristics and can make mistakes. The chairs will manually inspect and possibly reject those papers with evident format violations.

Please make sure that your submitted paper satisfies the following:

- You must provide an abstract, and it should be of no more than 200 words.

- You must submit papers in PDF (Portable Document Format) and ensure that they are compatible with Adobe Acrobat (English version). Other formats, including Postscript, will not be accepted. Avoid using non-standard fonts. The PC must be able to display and print your submission exactly as we receive it using only standard tools and printers, so we strongly suggest that you use only standard fonts that are embedded in the PDF file.

- You should ensure that the paper prints well on black-and-white printers, not color printers. Pay particular attention to figures and graphs in the paper to ensure that they are legible without color. Explicitly using grayscale colors will provide best control over how graphs and figures will print on black-and-white printers.

- You should ensure that labels and symbols used in graphs and figures are legible, including the font sizes of tick marks, axis labels, legends, etc.
- You should limit the file size to less than 15 MB. Contact the chairs if you have a file larger than 15 MB.

6 Paper Anonymity

All submitted papers will be judged based on their quality and relevance through **double-blind** reviewing, where the identities of the authors are withheld from the reviewers. As an author, you are required to make a good-faith effort to preserve the anonymity of your submission, while at the same time allowing the reader to fully grasp the context of related past work, including your own. Common sense and careful writing will go a long way towards preserving anonymity. Minimally, please take the following steps when preparing your submission:

- Remove the names and affiliations of authors from the title page. For experience-track papers, it is OK (but not necessary) to reveal company or system names but NOT author names; this applies to both the title block and the main body of the paper.
- Remove acknowledgment of identifying names and funding sources.
- Use care in naming your files. Source file names (e.g., "Alice-n-Bob.dvi") are often embedded in the final output as readily accessible comments.
- Use care in referring to related work, particularly your own. Do not omit references to provide anonymity, as this leaves the reviewer unable to grasp the context. Instead, reference your past work in the third person, just as you would any other piece of related work by another author.
- Do not embed pointers to external sources (e.g., public GitHub repositories) that leak author identity or affiliation.

In addition to submitting an anonymized paper, double-blind reviewing requires that both authors and reviewers take care while reviewing is happening:

- Authors are welcome to release their paper in a non-peer-reviewed location, but you should not broadcast information about the publication widely. For example, do not post it to large mailing lists or social media forums where members would easily encounter it, and do not do general press releases. Authors are also welcome to talk about their work (as work-in-progress) at local institutions. In either case, authors should be aware of members who might encounter the work and avoid sharing the work in a way that a member would encounter it.

- Members and other reviewers are expected to not actively attempt to deanonymize papers. In either case, if there is a breach of double-blind reviewing, the author and the reviewer should report it to the chairs.

7 Paper Acceptance

The Workshop on Information Security and Social Media will notify authors of acceptance/rejection decisions by July 12, 2021. Authors of accepted papers should Prepare to Share ideas with other Authors one week later after notification.