Guest editors:

Sal Stolfo, Columbia University (sal@cs.columbia.edu)
Gene Tsudik, UC Irvine (gts@ics.uci.edu)

Please email the guest editors with a brief description of the article you plan to submit by 15 Oct. 2009.

Final submissions due 15 Nov. 2009

Privacy-Preserving Sharing of Sensitive Information (PPSSI) is motivated by the increasing need for organizations or people who don't fully trust each other to share sensitive information.

Many types of organizations must often collect, analyze, and disseminate data rapidly and accurately without exposing sensitive information to wrong or untrusted parties. For example, census-takers collect private data with the understanding that it won't be released in a form traceable to the individual who provided it. Companies might be willing to divulge sensitive financial data to organizations that release only aggregate data for an industry sector. A hospital might share patient information with a state health agency but only to allow the latter to determine the number (and not the identities) of uninsured patients. While statistical methods for protecting data have been in use for decades, they're not foolproof and they generally involve a trusted third party to produce privacy-preserving statistical digests.

More recently, techniques employing secure multi-party function evaluation, encrypted keywords, and private information retrieval have been studied and, in a few cases, deployed, However there are no practical tools and technologies to guarantee data privacy, especially, whenever organizations have certain common goals and require exchanges of data. To this end, the objective of PPSSI technology is to enable multiple entities to cooperate and share information without exposing more than what is necessary to complete a common task.

Potential submission topics include (but are not limited to) the following:

IEEE
SECURITY&PRIVACY

Call for Papers:

Privacy-Preserving Sharing of Sensitive Information

For submission information and author guidelines, please visit www.computer.org/security/author.htm

- PPSSI requirements and policy enforcement; prospective policies governing PPSSI, including formal models and policy languages as well as trust models.
- Data "cleaning" and obfuscation techniques.
- Cryptographic protocols; innovative constructs, their performance and implementation issues, for example, private information retrieval, searching over encrypted data and private set operations.
- Data management; storage and data management issues arising in PPSSI settings.
- Secure hardware; architectures and technologies in support of PPSSI

In general, we welcome articles that address innovative conceptual, implementation, and experimental results relevant to PPSSI. Articles addressing requirements, especially from potential users of PPSSI technology, are encouraged as well. Articles describing products or narrow/specific applications as well as largely theoretical articles are discouraged.

www.computer.org/security/cfp.htm

Submissions will be subject to the peer-review methodology for refereed papers. Articles should be 6,000 words, maximum, with a maximum of 15 references. Articles should be understandable to a broad audience of people interested in security and privacy. The writing should be down to earth, practical, and original. Authors should not assume that the audience will have specialized experience in a particular subfield. All accepted articles will be edited according to the IEEE Computer Society style guide.

To submit a manuscript, please log on to Manuscript Central (https://mc.manuscriptcentral.com/cs-ieee) to create or access an account, which you can use to log on to *S&P*'s Author Center and upload your submission.