

A Special Session on Engineering Security Requirements and Privacy Informatics

-The 2008 International Conference on Information Security and Assurance

This special session highlights two related problem areas: security requirements and privacy informatics. Both areas are important and the relationship between security and privacy is the subject of much discussion. This special session will explore both areas individually as well as their interconnections and potential conflicts.

Security requirements are often identified during the system life cycle. However, the requirements tend to be general specifications of the functions required, such as password protection, firewalls, and virus detection tools. Often the security requirements are developed independently of the rest of the requirements engineering activity and hence are not integrated into the mainstream of the requirements activities. As a result, security requirements that are specific to the system and that provide for protection of essential services and assets are often neglected.

Much of the study of requirements engineering research and practice has addressed the capabilities that the system will provide. So a lot of attention is given to the functionality of the system, from the user's perspective, but little attention is given to what the system should *not* do. A key problem is that, if security requirements are not effectively defined, the resulting system cannot be effectively evaluated for success or failure prior to implementation.

A philosophical debate about the notion of privacy has been going on for many years. Following the debate, a set of interesting issues are raised: What is privacy? What is the relationship between security and privacy? Why do we need protect data privacy? How to achieve privacy? The goal of the special session is to explore computational techniques for releasing useful information in such a way that data privacy cannot be violated.

Rapid growth of information technologies nowadays has brought tremendous opportunities for data sharing and integration, and also demands for privacy protection. It is critical to discuss issues of privacy and security in various information systems such as data mining system, synergize different views of techniques and policies, and brainstorm future research directions. Although techniques, such as k-anonymity, random perturbation, cryptographic-based methods, and database inference control have been

developed, many of the key problems still remain open. Especially, new privacy and security issues have been identified, and the scope of this problem has been expanded. In addition to these existing technologies, people attempt to explore new approaches to tackle the problem.

We believe that it would be valuable to examine the progress achieved in this area. We strongly encourage researchers with interest in the areas of privacy and security as well as information systems to attend the special session.

Topics of interest

- Security requirements engineering processes
- Security requirements elicitation
- Security requirements prioritization
- Security requirements analysis
- Security requirements specification
- Security risk analysis
- Threat modeling
- Misuse/abuse cases
- Security requirements cost/benefit analysis
- Privacy and security protection during the phase of data collection, including privacy and security policies, data ownership, identity theft protection.
- Access control techniques and secure data models.
- Secure learning algorithms for randomized/perturbed data.
- Privacy-Preserving multi-party computation.
- Trust management.
- Learning from imbalanced data, streaming data, and bioinformatics data while preserving data privacy.
- Inference/disclosure.
- Privacy protection in E-Commerce.
- Privacy laws for fraud detection and for protecting personal data, medical data, and the public release of data.
- Secure link analysis and social network analysis.
- Data mining applications for terrorist detection.
- Privacy enhancement technologies in web environments.
- Privacy guarantees and usability of perturbation and randomization techniques.

- Analysis of confidentiality control methods.

Special Session Organizer

Prof. Nancy Mead
Carnegie Mellon University
4720 Forbes Ave,
Pittsburgh, PA, USA
nrm@sei.cmu.edu

Prof. Justin Zhan
Carnegie Mellon University
4720 Forbes Ave,
Pittsburgh, PA, USA
justinz@andrew.cmu.edu

Important Dates

Submission of Papers : **January 15, 2007**

Notification of acceptance : **January 29, 2008**

Submission of the camera ready: **February 5, 2008**