The challenge of creating secure systems from many components, each of varying security assurance level, has vexed system builders for several decades. There are few examples of engineering and integration of large-scale security systems that can be used to guide security practitioners today. In some cases, systems were classified, and in others, the systems were proprietary. Concerns regarding the assurance of systems have resulted in requirements that often result in the development of systems that, although they might be secure, have been bypassed by technology trends and products, thus rendering them irrelevant. At the other end of the spectrum, some have proposed the construction of secure systems from insecure components.

How can the forces propelling the inclusion of the newest technologies and software in systems be balanced against the need to assess their security properties? Is there a scientific basis for secure system engineering and integration? Can previous development efforts be used either as object lessons or as the basis for integration rules? How is security part of the overall system design and development process? Should security be balanced against other system requirements and, if it can, is it possible to predict the consequences of these concessions?

Current systems are rarely isolated or simple. For technical security policies to be enforced in complex, distributed systems, security engineers must understand how security elements can be integrated into the overall system design. Analysis is required to determine whether the collection of mechanisms is sufficient to achieve the security objectives of the overall system. In addition, based upon assumptions regarding the environment, they must select mechanisms that offer a combination of functional strength in the operational sense as well as developmental credibility in terms of the trustworthiness of the elements. Further considerations associated with these choices include the usability, maintenance, extensibility, and flexibility of such systems. A balance between security objectives and other operational objectives must be achieved, and must be articulated by the system integrators so that customers understand the risks they will accept when operating these systems.

Possible topics include:

- case studies of security engineering and integration successes, failures, lessons learned;
- techniques, tools and metrics for security integration as applicable to various stages of system development: security architecture description, security design analysis, security implementation assessment, the role of testing;
- methodologies and guiding principles for security engineering and integration;
- policy issues in security integration including policy articulation and impact of policy objectives;
- risk analysis and security integration;
- system extensibility as a security objective;
- roles of standards and regulations in security integrations including applicable standards, laws and constraints, international concerns in security integration;
- differences between security integration and other integration activities; and
- managing customer expectations (they can ask for the impossible)

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 interested in security and privacy. The writing should be down to earth, practical, and original. Do not assume an audience with specialized experience in a particular subfield.

All accepted articles will be edited according to the IEEE Computer Society style guide.

Submit your papers to Manuscript Central at https://mc.manuscriptcentral.com/cs-ieee.

Guest Editors:
- Cynthia Irvine, Naval Postgraduate School
- JR Rao, IBM Research