2015 Draft Revised Scope of ACM TISSEC

ACM Transactions on Privacy and Security

ACM TOPS publishes high-quality research results in the fields of information and system security and privacy. Studies addressing all aspects of these fields are welcomed, ranging from technologies, to systems and applications, to the crafting of policies. Topics of interest include:

*Security Technologies***:** authentication; authorization models and mechanisms; auditing and intrusion detection; cryptographic algorithms, protocols, services, and infrastructure; recovery and survivable operation; risk analysis; assurance including cryptanalysis and formal methods; penetration technologies including viruses, Trojan horses, spoofing, sniffing, cracking, and covert channels.

Fundamentals: theory of security and privacy; models of trust; methods for quantifying the risk of the disclosure of private information or the risk a system will be compromised; mechanisms and algorithms that have wide application, including privacy models (e.g. *k*-anonymity based models and knowledge hiding models), and methods of secure communication with various properties (e.g. non-repudiation or forward secrecy).

*Secure Systems***:** secure operating systems, database systems and networks; secure distributed systems including security middleware; secure web browsers, servers, and mobile code; specialized secure systems for specific application areas; interoperability, and composition.

Privacy Methods: methods to offer location privacy; anonymization techniques for users and their data; statistical disclosure control techniques; private information retrieval; protocols for secure multiparty communications, protecting confidential consumer data, and the like.

*Security and Privacy Applications***:** threats, system tradeoffs, and unique needs of applications; representative application areas include information systems, workflows, cloud computing, cyber-physical systems, electronic commerce, electronic cash, electronic voting, copyright and intellectual property protection, telecommunications systems, wireless systems, and health care. Design of security and privacy (user experience and usability).

*Privacy and Security Policies***:** confidentiality, integrity, availability, privacy, usage, and survivability policies; tradeoffs, conflicts and synergy among security and privacy objectives.