CALL FOR PAPERS
IEEE Security and Privacy

Issue on **Securing the Domain Name System**

September/October 2009 Issue
Submissions due January 15, 2009

The Domain Name System (DNS) is a critical part of the Internet infrastructure and virtually every Internet application depends on some form of DNS data. Security was not a major goal of the original DNS design and basic security issues are well known. Today, both the attacks and defenses are becoming increasingly sophisticated. Motivated by both the importance of the DNS and recent enhancements, this upcoming issue of IEEE Security & Privacy looks at the challenges in securing the DNS.

We seek feature articles with an in-depth coverage of topics relating to all aspects of DNS security. Among potential topics are:

- analysis of DNS vulnerabilities,
- techniques of mitigating the impact of denial of service attacks on the DNS,
- deployment experience with DNS Security,
- techniques for managing DNSSEC public keys and signatures,
- providing DNSSEC benefits to end system resolvers,
- proposals for learning DNSSEC public keys, and
- legal and privacy issues in DNS data Submissions will be subject to peer-review resulting in refereed scientific papers.

Articles should be understandable to a broad audience of people interested in security and privacy and be less than 6,000 words. 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 professionally copyedited according to the IEEE Computer Society style guide.

Submission instructions:

Guidelines for authors and manuscript submission at:
http://www.computer.org/portal/pages/security/author.xml

Guest editors:

Daniel Massey (Colorado State University) and Dorothy Denning (Naval Postgraduate School)