DomainCert: A Simple, Scalable, Trustworthy Key Management System
Tamal Das, Indian Institute of Technology, Delhi, India
ADVISOR: Himanshu Khurana

Background
- Need for a globally available and trusted public key distribution and management system
- Shortcomings of PKI that need to be addressed
  - Trust establishment in anchors
  - Revocation
- Focus applications
  - Power Grids
  - Email

Goals
- Lightweight alternative to X.509 PKI
  - Trust
  - Distribution
  - Revocation
- Implement and deploy the key management system in a test environment.
- Analysis of the prototype.

Research Plan
- Approach
  - Use DNSSEC for key management
- Time plan
  - Read on PKI, DNSSEC, DomainKeys, etc.
  - Deploy a prototype of the model
  - Integrate the model with SSL
  - Integrate the model with L2TP/IPsec
  - Integration with Power grids
  - Integration with email
  - Integration with user identities
  - Testing & enhancement

Research Results
- Contributions
  - Key management System for Power Grid, using DNSSEC
  - Integration with SSL and L2TP/IPsec (ongoing) as example applications

Related Work/Interaction with Other Projects
- TCIP: Trustworthy Cyber Infrastructure for the Power Grid
  - Integration with Next-Generation Secure IEDs (SIED)
  - Integration with Legacy Devices via SMOCK

Fundamental Questions/Challenges
- How would the certificates be distributed?
- What are the trusted entities and are they trustable?
- Is the key management system scalable?
- How will revocation be handled?
- Why should users adopt this key management system, instead of their own?
- Is the scheme simple and user-friendly?
- What are the costs associated with its deployment?