Title: Trustworthy Communication Infrastructure: Principles and Framework

Abstract:

Internet-based information and communication technologies (ICTs) have become an inevitable tool in daily life around the world. The proliferation of the Internet has exposed vulnerabilities to various attacks and there has been numerous attempts to cure these security vulnerabilities. However, the situation has not improved and indeed has gotten even worse, that is, protections on ever-sophisticating attacks become endless battles of “spear and shield”. To make an ultimate solution for this situation, we need to go back to fundamentals of communication frameworks.

This talk proposes a new paradigm for trustworthy communication framework where security concerns never exist. First, it suggests a trust model based on confidence, in contrast to the security model that is based on doubts and suspicions. Second, This talk lists up principles for defining the trustworthy communication framework. The principles are based on separation of concerns: entities and environment. Entities are denoted by self-certifying ID for identification as well as privacy. The environment is viewed as hierarchically structured network spaces, each of which is abstracted as a domain. For trust domains where all members trust each other, intra-domain communications are allowed without any constraint and inter-domain communications is done under well-defined trust evaluating procedures. Third, the trustworthy communication framework shows how to build trust domains, how to manage members of domains, how to expand domains while keeping them trustworthy, and how to manage trust relations among entities and domains. Lastly, this talk concludes with some typical applications and further studies.