

Security Challenges of Future Internet-based Applications and Services

Summary:

The tremendous impetus of internet-based applications and services has resulted in the conception of a state of affairs that is completely different than what was envisioned when internet's architecture was designed in the 1970s. It is therefore become indispensable to develop the future internet that can cope with the emerging demands of information society of tomorrow. Future internet-based infrastructures present promising landscape to cope with the ever increasing requirements of modern scientific and business applications. However, the progress of security technologies is somehow lagging behind the evolution of modern distributed systems. Core of the current security technologies were developed several years ago even before the inception of world wide web (HTTP protocol) – Kerberos (1987), X.509 digital certificates (1988), IPSec (1992), SSL (1994), etc. The growth of the world wide web and consequently the need of securing web-based services have only seen the adaptation of these core security technologies at the application layer. The cosmetic adaptation of core security technologies is eventually taking its toll on the performance and quality of security services. Major reason is the inability of these technologies to cope with the security challenges of dynamic and highly scalable environments.

This tutorial will provide an overview of the existing security solutions and their scope in the emerging computing paradigms. Results of some of the related European and Belgian national projects will be presented to provide an insight into the various ongoing R&D activities that aim to fix the shortcomings of existing security solutions ranging from the performance and quality of security services to addressing the return on security investments and compliance with the legal directives and the industrial standards. Finally some open issues in the area of ICT security will be presented to stimulate ideas on new research directions for addressing them.

Speaker's biography:

Syed Naqvi is a R&D Project Manager at CETIC. He is the project manager of European Future Internet Security Research Experiment BonFIRE-ExSec. He is coordinating the Security Compliance activity of the European e-Health project PONTE. He is leading the platform evaluation activity of European Cloud Computing project Comod-IT. He has previously worked as a security architect in a number of European projects notably GridTrust and RESERVOIR. Syed is a senior member of IEEE; co-chair of NESSI-TSD (Networked European Software and Services Initiative – Trust, Security and Dependability Working Group); and a member of Security and Trust Collaborative Working Group (CWG) of European Community for Software and Services (ECSS). Syed spent several years in industry before starting his research career in information and communication technologies. He has a PhD in Distributed Systems Security from ParisTech. He has held a visiting scientist position at the University of Washington at Seattle; and was a research fellow at the Science and Technology Facilities Council of UK.