Abstract:

Public Key Infrastructure (PKI) provides an essential foundation to applications of public key cryptography, and crucial for security in open networks and systems. Since its introduction in 1988, the PKI landscape was dominated by the X.509 standard, widely deployed by many protocols and systems, most notably TLS/SSL, used to secure connections between web server and browser.

Unfortunately, the web-PKI deployment has inherent weaknesses, and over the years, we have seen many failures of this trusted-Certificate Authority (CA) approach. PKI failures allow attackers to issue fake certificates, launch website spoofing and man-in-the-middle attacks, possibly leading to identity theft, surveillance, compromises of personal and confidential information, and other serious security breaches.

These failures motivated efforts to develop and adopt next-generation, improved-security PKI schemes, i.e., PKI schemes that ensure security against corrupt CAs. During the recent years, there have been extensive efforts toward this goal by researchers, developers and the IETF. These efforts focus on additional security goals such as transparency, non-equivocation, privacy and more.

This talk will provide a concise review of this important area, and give the highlights of our research toward well-defined security goals for PKI schemes, and toward practical, efficient and yet provably-secure PKI schemes.