Recent Advances and Existing Research Questions in Platform Security

Ernie Brickell

Chief Security Architect for Intel Corporation, USA

Abstract. In this talk I will provide a description of recent uses Intel has made of cryptography in our platforms, including providing a hardware random number generator, using anonymous signatures, and improving performance of cryptographic algorithms. I will discuss how processor capabilities could be used more effectively by cryptographic algorithms. I will then discuss research questions in cryptographic protocols and platform security that are motivated by our goals.