Title of Presentation: RSA Digital Signature Standards

Speaker: Burt Kaliski, RSA Laboratories

Summary of Topics: Standards, theory and practice have resulted in a variety of digital signature schemes based on the RSA public-key cryptosystem, including PKCS #1, ANSI X9.31, and the Bellare-Rogaway Probabilistic Signature Scheme (PSS). This presentation describes these schemes and gives a strategy for improving long-term security as well as interoperability of digital signature standards based on the RSA algorithm.

Short Bio: Burt Kaliski received B.S., M.S. and Ph.D. degrees from MIT in 1984, 1987 and 1988 respectively. In 1989 he joined RSA Security and since 1991 has been chief scientist of RSA Laboratories (http://www.rsasecurity.com/rsalabs). Dr. Kaliski has served as general chair of CRYPTO ‘91, program chair of CRYPTO ‘97, and chair of the IEEE P1363 working group.