

Job talk for CAISS/ Computer Science

"Cryptographically Sound Analysis of Basic and Public-key Kerberos"

Abstract: In my talk I will discuss some results of the ongoing analysis of the widely deployed authentication and key exchange protocol Kerberos 5. During the analysis we discovered a serious protocol-level attack against the then-current specification of a Kerberos public-key extension (PKINIT). Furthermore, the purely symbolic analysis of Kerberos was extended by providing the first computationally sound security proofs of the core aspects of such a complex industrial protocol. Most recently, in addition to the by-hand proofs for Kerberos 5, we used the mechanized tool CryptoVerif on the full Kerberos protocol. We obtained security proofs that are conducted directly in the computational model and that represent the first computationally sound mechanized proofs for a full industrial protocol. We also generalized the notion of key usability and used CryptoVerif to prove that this definition is satisfied by keys in Kerberos.

Tuesday, March 4, 2008

4 p.m.

NAC 8/207

Joe-Kai Tsay

Bio: Joe-Kai will receive his Doctorate of Philosophy in Mathematics from the University of Pennsylvania in August 2008. He previously studied mathematics at the University of Essen, Germany, where he worked with linear codes of algebraic function fields. In conjunction with Andre Scedrov, University of Pennsylvania, Joe-Kai is currently analyzing the Kerberos protocol suite. His research interests include the foundations of computer security and cryptography.