Protocol eXchange Meeting

University of Maryland Baltimore County
Information Technology and Engineering Building
Room 325B
October 26, 2007

09:00 – 09:10  Welcome

09:10 – 10:05  Flaws in Group Delegated Authentication Protocols
               Ed Ziegler (NSA)

10:05 – 11:00  Protocol Independence via Disjoint Encryption: A New
               proof using the completeness of the authentication tests
               Joshua Guttman (MITRE)

11:00 – 11:10  Break

11:10 – 12:05  A Formal Analysis of Onion Routing
               Aaron Johnson (Yale University)

12:05 – 13:30  Lunch

13:30 – 14:25  Maude Semantics for Toolip
               Carolyn Talcott (SRI)

14:25 – 15:20  Maude-NPA: Status and Demonstration
               Cathy Meadows (NRL)

15:20 – 15:30  Break

15:30 – 16:25  Mechanized Security Proofs of Kerberos
               Joe-Kai Tsay (University of Pennsylvania)

16:25 – 16:30  Wrap-up