

TELCOM 2011: Telecommunications Seminar

On the Fragility of Adversary Definitions for Security Protocols

Prof. Virgil Gligor

ECE Department and CyLab, Carnegie Mellon University

Abstract: New computing technologies and applications introduce new security vulnerabilities that often require a re-definition of the adversary. Hence that question of whether an adversary model is robust enough to be reused for multiple applications and technologies arises naturally. In this talk I will also show that adversary definitions can be fragile; i.e., restrictions placed on the adversary behavior in theory can be circumvented in practice. Fragility is caused by mismatches between the adversary models, and the practical realities of large-scale networks, such as the Internet. I illustrate these mismatches with two examples of new adversaries: a "concurrent" and a "network" adversary. In the first example, bounds placed on the number of attack queries launched by an adversary against password-based authenticated key exchange (PAKE) protocols, whose security is correctly proven in either the standard or the random oracle models, can be circumvented by multi-threaded, client-server models of computation in the Internet. In the second example, I argue that a PPT adversary with access to a large, but bounded, number of different oracles can break encryption-scheme properties with non-negligible probability. I conclude that security proofs must come with "warning labels" regarding the adversary definitions and models assumed and the security vulnerabilities that might arise in practice.

Bio: Virgil D. Gligor received his B.Sc., M.Sc., and Ph.D. degrees from the University of California at Berkeley. Prior to joining Carnegie Mellon, Gligor was at the University of Maryland from 1976, and was a Professor of Electrical and Computer Engineering. Over the past 29 years, his research interests have ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography. Dr. Gligor was a consultant to the Burroughs (1977-1981) and IBM (1984-1999) Corporations, and is currently serving on Microsoft's Trusted Computing Academic Advisory Board. He served the profession as the chair or co-chair of several conferences and symposia, including the IEEE Security and Privacy Symposium, the Internet Society's Network and Distributed Systems Security Symposium, the IEEE Dependable Computing for Critical Applications, and the IEEE-ACM Symposium on Reliability in Distributed Software and Databases. He received the outstanding paper award at the 1988 IEEE Symposium on Security and Privacy. He was a member of several U.S. Government INFOSEC Study Groups that set research agendas in information security, and served on a National Research Council panel on information security.