On the Evolution of Adversary Models in Security Protocols

Virgil D. Gligor
Electrical and Computer Engineering Department
University of Maryland
College Park, Maryalnd 20742

Abstract

Invariably, new technologies introduce new vulnerabilities which, in principle, enable new attacks by increasingly potent adversaries. Yet new systems are more adept at handling well-known attacks by old adversaries than anticipating new ones. Our adversary models seem to be perpetually out of date: often they do not capture adversary attacks enabled by new vulnerabilities and sometimes they address attacks rendered impractical by new technologies.

In this talk, I provide a brief overview of adversary models beginning with those required by program and data sharing technologies, continuing with those required by computer communication and networking technologies, and ending with those required by mobile ad-hoc and sensor network technologies. I argue that mobile ad-hoc and sensor networks require new models, different from those of Dolev-Yao and Byzantine adversaries. I illustrate this with adversaries that attack perfectly sensible and otherwise correct protocols of mobile ad-hoc and sensor networks. These attacks cannot be countered with traditional security protocols as they require emergent security properties.