The Fine Print of Security

(Invited Lecture)

Martín Abadi
Microsoft Research, Silicon Valley and
University of California, Santa Cruz

***Abstract*—Simple views of systems are often convenient in their design and analysis. However, attackers may attempt to exploit any oversimplification. For security, it is therefore useful to understand the value and the limitations of simplistic models. Computational-soundness theorems, which are the main subject of this lecture, can sometimes shed light on this question.**

We discuss them first in the context of security protocols. There, two distinct, rigorous views of cryptography have developed over the years. One of the views relies on a simple but powerful symbolic approach; the other, on a detailed computational model that considers issues of probability and complexity. In the last decade, however, we have made substantial progress in bridging the gap between these views. This progress, of which a paper with Phil Rogaway was one of the early steps, is due to many researchers. By now, this line of work provides computational justifications for formal treatments of cryptographic operations and security protocols, and also explores hybrid approaches.

Similar ideas can apply in the domain of software protection, although they are less mature in this domain. Specifically, we can relate high-level security guarantees, of the kind offered by programming-language semantics, with lower-level properties of implementations. Layout randomization, one popular and effective implementation technique, again brings up issues of probability and complexity. The lecture introduces some recent work with Gordon Plotkin on this topic.