Science of Security Meeting, Berkeley CA, 17, 18 Nov 2008

# Security and Composition

John Rushby

Computer Science Laboratory
SRI International
Menlo Park CA USA

## Problem Statement

- Given a set of components with known properties, is there a way to assure and reason about a system composed of these components?
- Is it possible to design components that behave securely regardless of how they are composed?
- Added: can we develop secure systems in a modular manner, from trusted and untrusted components?

## Reasoning About Composed Systems

- Yes, e.g., assume-guarantee
  - e.g. PCL for protocols
- But intruder/attacker model becomes complex

## Refinement of These Compositions

- May always underestimate the intruder
- Especially as we move from abstract to detailed models. . . code
- But scientifically rich field. . . lots of progress
- Software model checking, type systems, etc.

## Universally Composable Components

- Quite a lot of theory here
- Can do it sometimes (e.g., public key encryption)
- But also known impossibility results (e.g., zero knowledge)

## Modular Construction

- Tactically essential: it's the only feasible approach
- Scientifically rich
  - Independence (via separation, diversity)
  - Variants of assume-guarantee
- But plenty to do

## Why Composition Is Hard

- Trying to ensure a systemwide property. . . with components
- The system security argument may not decompose on architectural lines
  - So what is architecture?
  - A good one simplifies the assurance case