Designing Secure Systems

- Don’t know how powerful attacker is
- When designing a security protocol need to

1. Specify Attacker Model: Capabilities of attacker

(Attacker model should be tied to reality)

2. Design security mechanisms to satisfy policy under the attacker model
3. Prove that mechanisms satisfy policy under attacker model
4. Measure effect on overall performance (e.g., throughput) in the common case, i.e., no attacks