Modeling and Analysis of Access Control Failure
Prasad Naldurg, Roy H. Campbell,

Problem Statement
- Access control security: Devise mechanisms that deny access to unauthorized users based on policy, preserve safety
  - Systems have vulnerabilities that attackers exploit compromising safety and invalidating integrity, confidentiality and availability guarantees. E.g., password guessing, buffer overflows
  - Furthermore, access mechanisms can also become a method of attack (DoS)
- Once attack occurs, safety property models are of no further use to designers and cannot reason about attack containment and recovery

Key Concepts
- Methodology: Extend state transition models of access control to simulate attacks.
  - Include explicit states and transitions representing insecure or imprecise behavior. Focus on information exposure and DoS attacks
  - Study impact of attacks on preserving integrity, confidentiality and availability.
  - Model attack recovery mechanisms explicitly
- Define survivability properties in this context as the ability to restore system to a safe state in a bounded number of transitions

Methodology
- Model access control systems as a PNS (Probabilistic Non-Deterministic System) augmented with atomic propositions to define attack semantics
  - Support for stochastic and real-time behavior
- Interactive framework for modeling adversaries, controllers, and different recovery strategies
  - Automated validation of survivability properties using standard and probabilistic model checking techniques
  - Extensions to automated synthesis of flexible response strategies with respect to preserving properties

Applications
- Dynamic access control
- Buffer overflow containment
  - Simulated post-mortem analysis of explicit information flows
  - Theory of safe design of privilege separation
- DoS and DDoS analysis
  - Analytical model of DDoS Survivability
  - Automated analysis of DDoS prevention strategies measured on the ability of a victim to do useful work even under attack