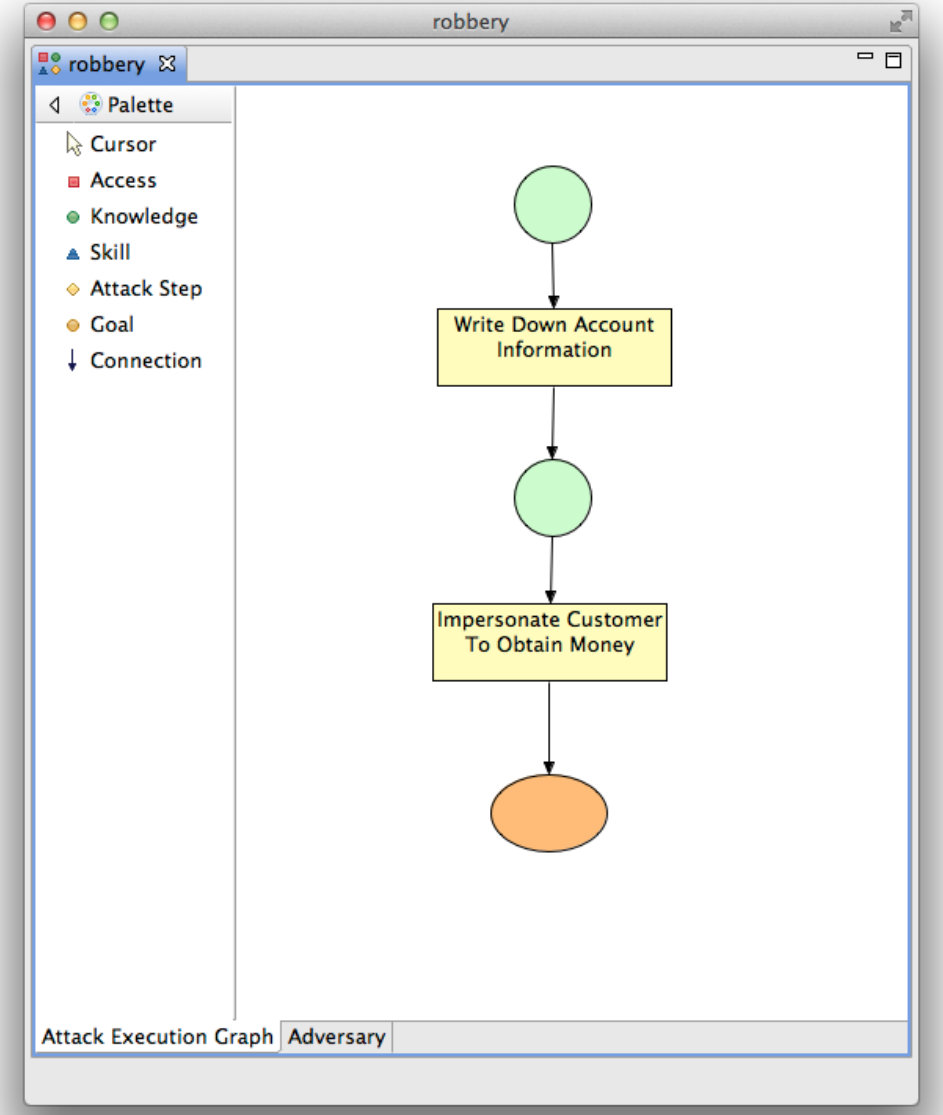
Modeling Trust in Critical Systems with Möbius

KEN KEEFE
SENIOR SOFTWARE ENGINEER
LEAD MOBIUS DEVELOPER

Session Outline

- ADVISE Hands-On Session
- Open Hands-On Session

Attack Execution Graph 1



AEG Details

- Knowledge 1 - Insider Knowledge
- Attack Step 1 - Write Down Account Information
  - Cost: return 0;
  - Time: Deterministic(5);
  - Preconditions:
    - return (!CustomerInformation->Mark() && InsiderKnowledge->Mark());
  - Outcome - Success
    - Probability: return 1;
    - Detection: return 0.1;
    - Effects: CustomerInformation->Mark() = true;
- Knowledge 2 - Customer Information
- Goal 1 - Money

AEG Details

- Attack Step 2 - Impersonate Customer To Obtain Money
  - Cost: return 0;
  - Time: Deterministic(10);
  - Preconditions:
    - return (CustomerInformation->Mark() && !Money->Mark());
  - Outcome - Failure
    - Probability: return 0.3;
    - Detection: return 0.9;
    - Effects:
  - Outcome - Success
    - Probability: return 0.7;
    - Detection: return 0;
    - Effects: Money->Mark() = true;
- Goal 1 - Money

Adversary Profile Details

- Name: Bank Employee
- Planning Horizon: 2
- Preference Weights: Cost - 0, Detection - 0.2, Payoff - 0.8
- Initial Knowledge: Insider Information
- Goals: Money (1000)

Reward Model

- Performance Variable - k_insider
  - Rate reward: `return robbery->InsiderKnowledge->Mark();`
  - Time
    - Instant of Time
    - Incremental 0-30, 5 step size
- Performance Variable - k_custinfo
  - Rate reward: `return robbery->CustomerInformation->Mark();`
  - Time
    - Instant of Time
    - Incremental 0-30, 5 step size
- Performance Variable - g_money
  - Rate reward: `return robbery->Money->Mark();`
  - Time
    - Instant of Time
    - Incremental 0-30, 5 step size

Get It Running

- Create an empty range study.
- Create a simulator and run with the defaults.
- Expand from there.