ADVISE – ADversary VIew Security Evaluation

Practical Metrics for Enterprise Security Engineering

Ken Keefe, William H. Sanders

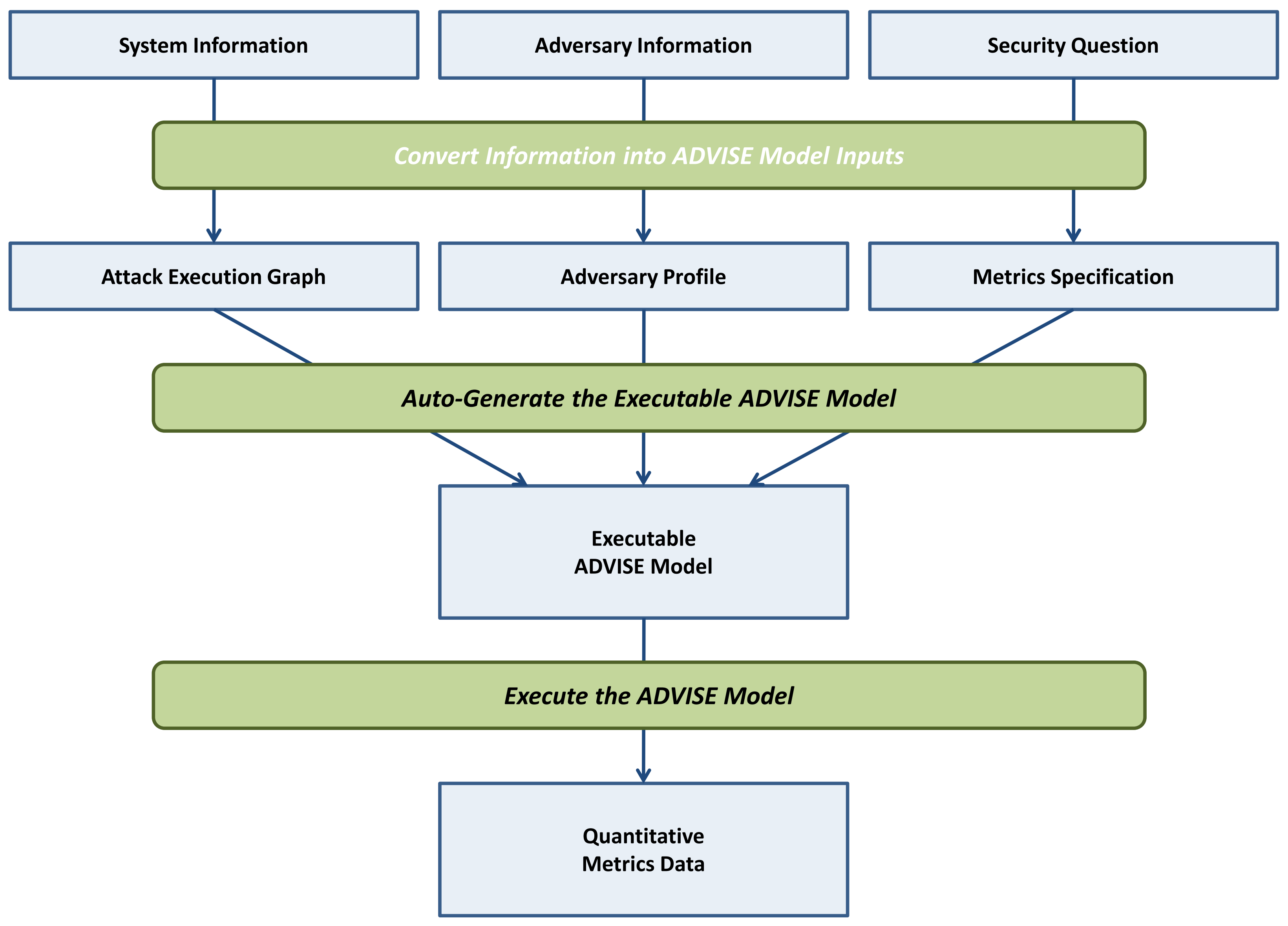
Q: How will a system be attacked? How resilient is it?
Answer 1: Deploy it and find out. (Unavoidable)
Answer 2: Expert review of the design. (Current best practice)
Answer 3: Create ADVISE model and run simulation.

What is a “system” ?

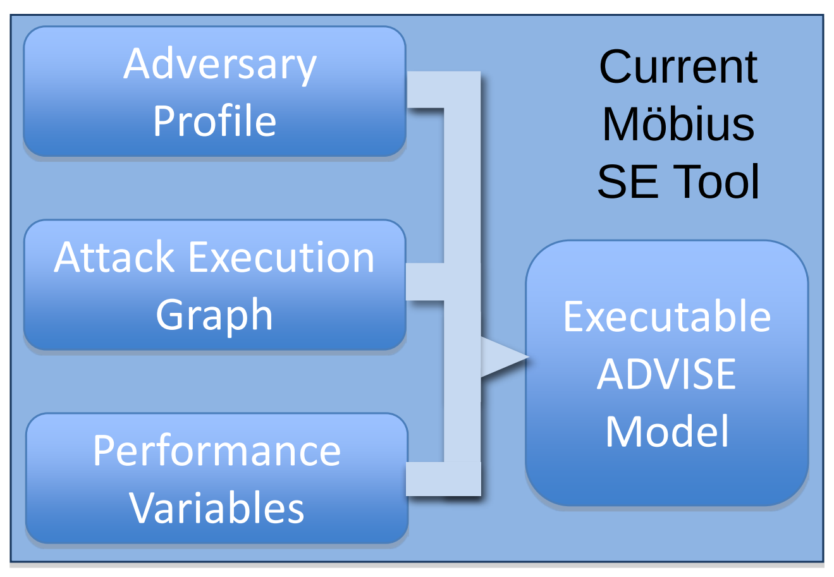
- Architecture to support stock trading
- SCADA architecture supporting an electric utility
- Control systems in a water treatment plant
- Operations and administration systems for a telecommunications provider
- 911 computer systems architecture
- Reactor safety architecture for a nuclear power plant
- Systems in a hospital that process patient information
- Air traffic or train control systems
- Computer infrastructure for a research and development facility
- Computer infrastructure for an ISP

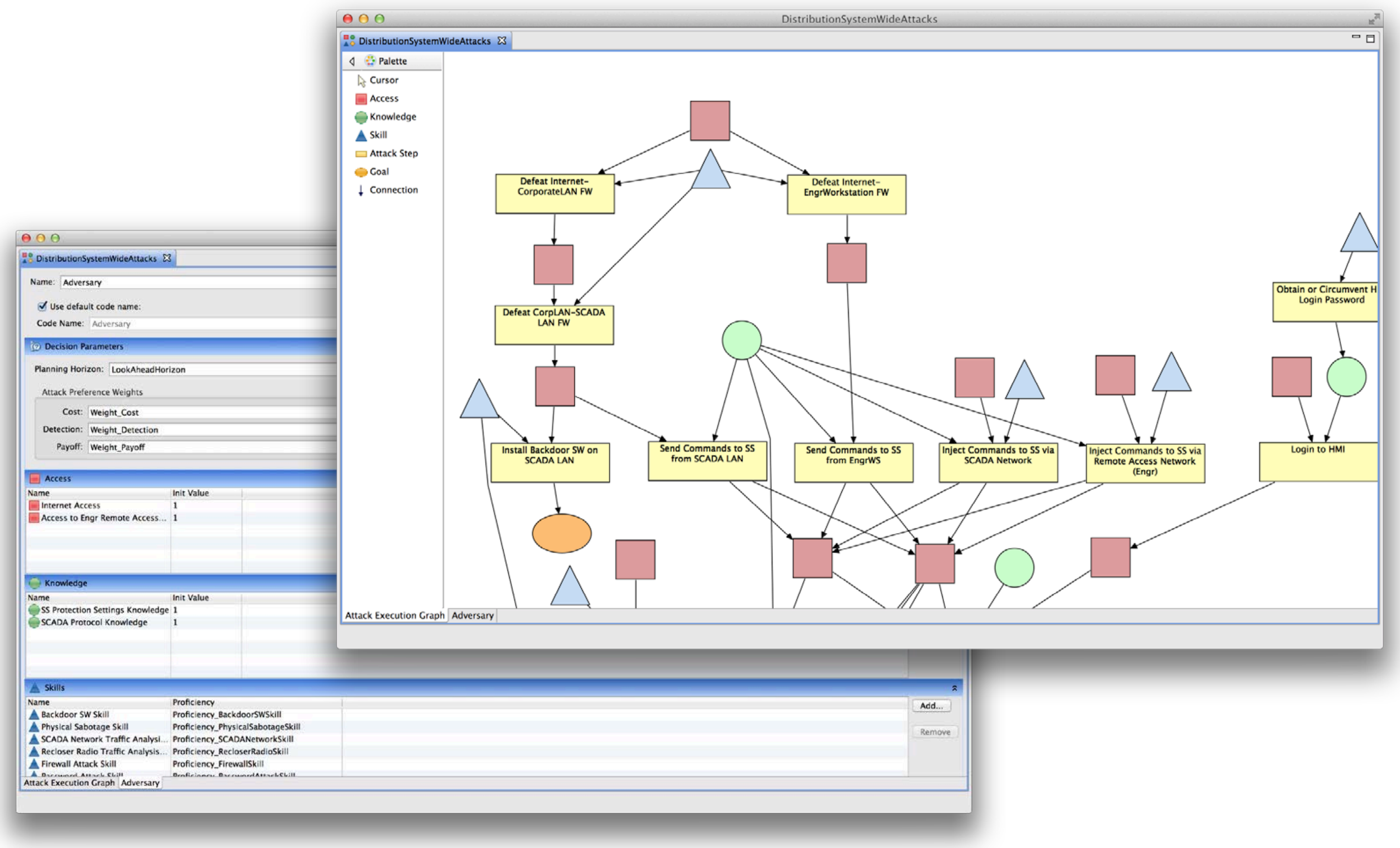
Tool users need minimal security or modeling expertise and can benefit from the collective efforts of other users of the planned tool. An executable ADVISE model will be generated from a high-level component model description and use the Möbius modeling tool to accurately estimate custom security metrics.

MODELING ATTACKERS



- Achieved tool applicable at system design phase
- Simulates system under attack
- Calculates custom metrics
- User builds attack execution graph (AEG)
- Active user base of early adopters
- Publicly available at https://www.mobius.illinois.edu/




DistributionSystemWideAttacks
Palette
Cursor
Access
Knowledge
Skill
Attack Step
Goal
Connection
Defeat Internet-CorporateLAN FW
Defeat Internet-EngrWorkstation FW
Defeat CorpLAN-SCADA LAN FW
Obtain or Circumvent H Login Password
Install Backdoor SW on SCADA LAN
Send Commands to SS from SCADA LAN
Send Commands to SS from EngrWS
Inject Commands to SS via SCADA Network
Inject Commands to SS via Remote Access Network (Engr)
Login to HMI
Attack Execution Graph
Adversary
Add...
Remove

Name: Adversary
☑ Use default code name:
Code Name: Adversary

Decision Parameters
Planning Horizon: LookAheadHorizon
Attack Preference Weights
Cost: Weight_Cost
Detection: Weight_Detection
Payoff: Weight_Payoff

Access

Name	Init Value
Internet Access	1
Access to Engr Remote Access...	1

Knowledge

Name	Init Value
SS Protection Settings Knowledge	1
SCADA Protocol Knowledge	1

Skills

Name	Proficiency
Backdoor SW Skill	Proficiency_BackdoorSWSkill
Physical Sabotage Skill	Proficiency_PhysicalSabotageSkill
SCADA Network Traffic Analysi...	Proficiency_SCADANetworkSkill
Recloser Radio Traffic Analysis...	Proficiency_RecloserRadioSkill
Firewall Attack Skill	Proficiency_FirewallSkill
Password Attack Skill	Proficiency_PasswordAttackSkill

ANALYZE SYSTEM SECURITY DESIGN

Configuration 1
Adversary:
Foreign government well resourced at war
System:
Power distrib system without recloser radio network
Metric:
Avg time goal met (Compromise availability of Service: Electric Power; QoS: System-wide disruption)

Configuration 2
Adversary:
Foreign government well resourced at war
System:
Power distrib system with recloser radio network
Metric:
Avg time goal met (Compromise availability of Service: Electric Power; QoS: System-wide disruption)

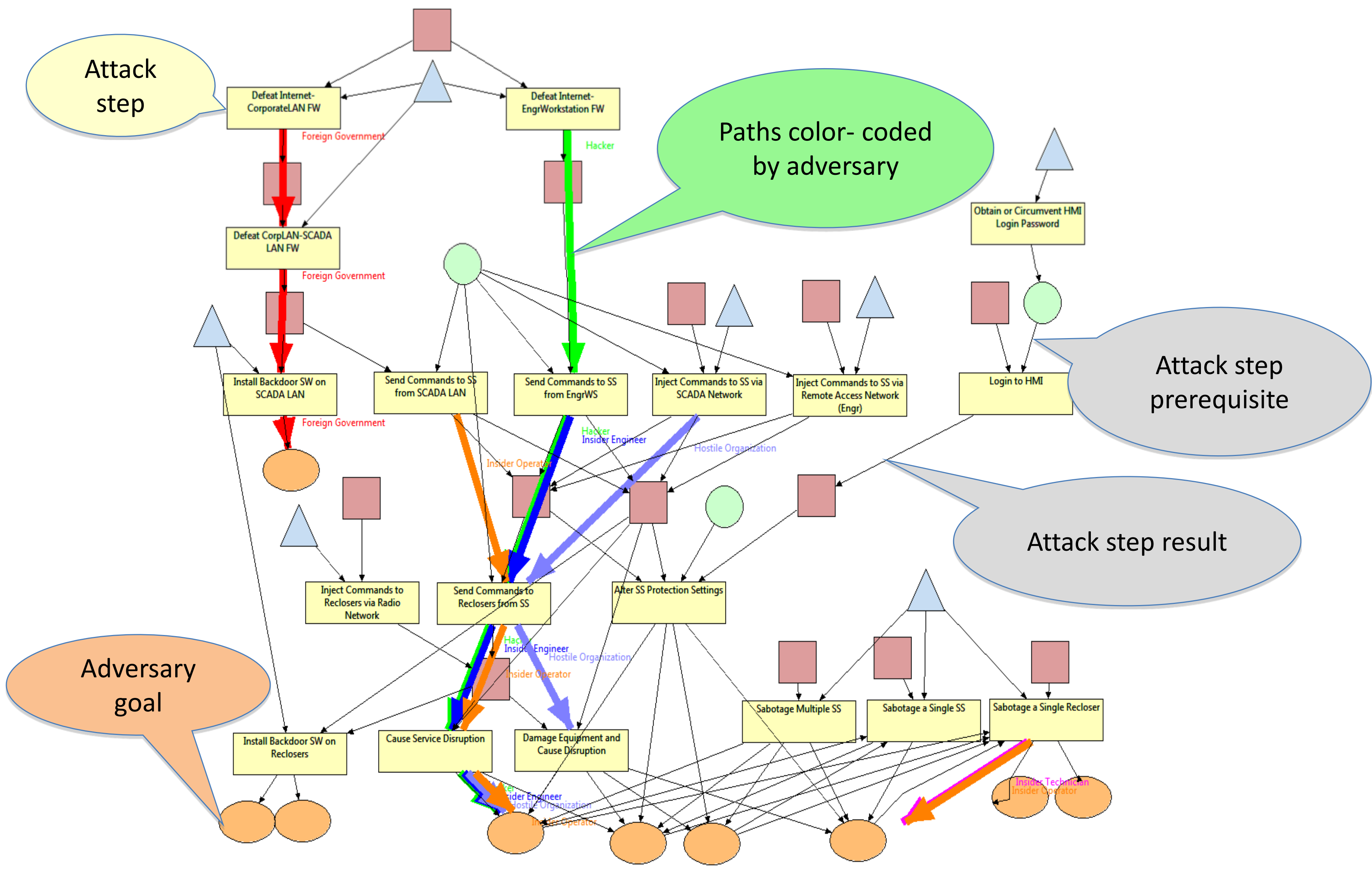
Avg time goal met: hours
(Compromise availability of Service: Electric power; QoS: System-wide disruption)

	Foreign Gov Well Resourced At War	Economic Competitor	Insider Technical Expert
Power distrib system without recloser radio network	6.0	14.9	2.0
Power distrib system with recloser radio network	4.3	16.0	.9

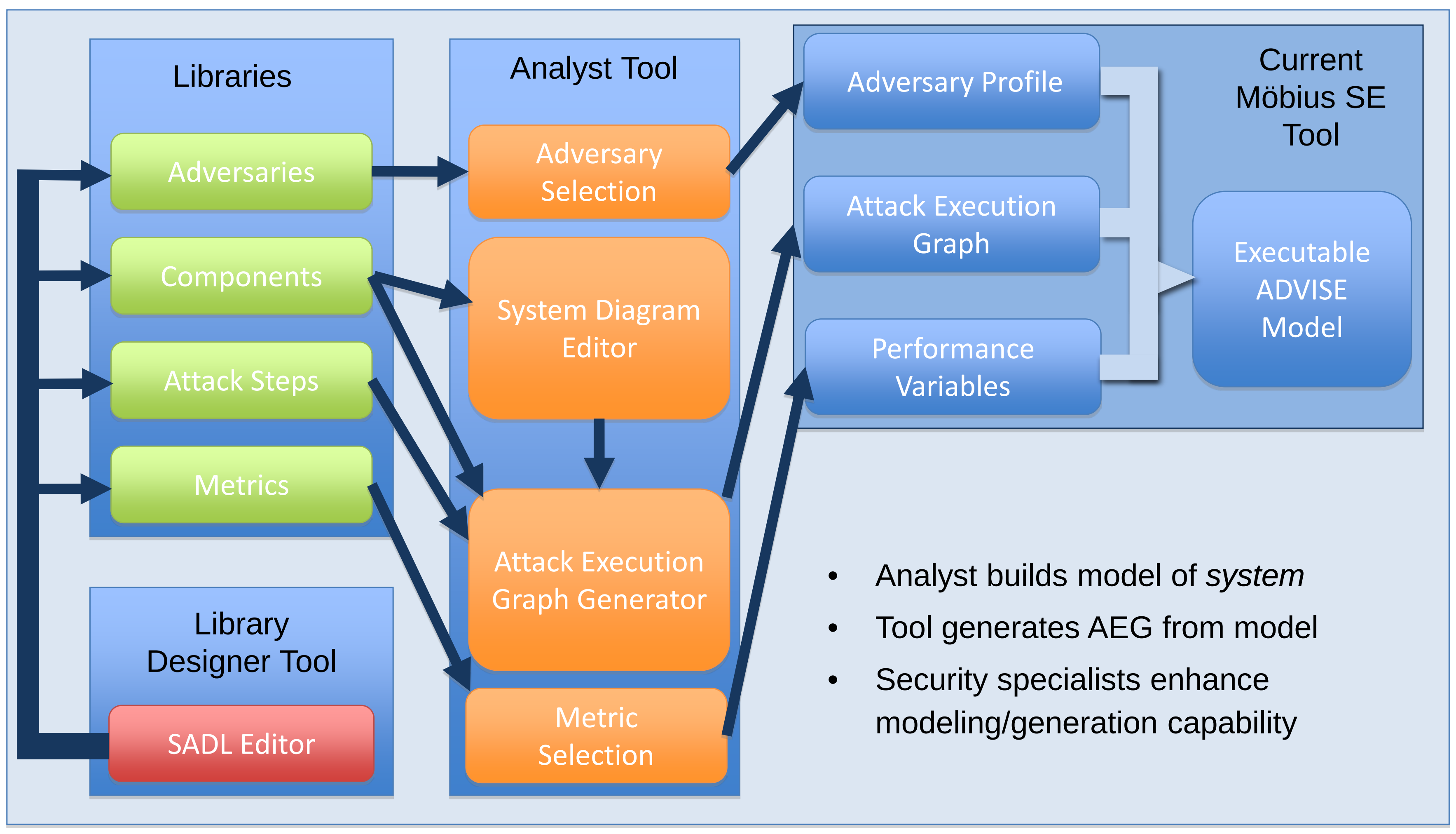
Configuration 1

Configuration 2

RESULTS VISUALIZATION


Attack step
Paths color- coded by adversary
Attack step prerequisite
Attack step result
Adversary goal
Defeat Internet-CorporateLAN FW
Defeat Internet-EngrWorkstation FW
Defeat CorpLAN-SCADA LAN FW
Obtain or Circumvent HMI Login Password
Install Backdoor SW on SCADA LAN
Send Commands to SS from SCADA LAN
Send Commands to SS from EngrWS
Inject Commands to SS via SCADA Network
Inject Commands to SS via Remote Access Network (Engr)
Login to HMI
Inject Commands to Reclosers via Radio Network
Send Commands to Reclosers from SS
After SS Protection Settings
Install Backdoor SW on Reclosers
Cause Service Disruption
Damage Equipment and Cause Disruption
Sabotage Multiple SS
Sabotage a Single SS
Sabotage a Single Recloser
Foreign Government
Hacker
Insider Engineer
Hostile Organization
Insider Operator
Insider Technician

TOOL ARCHITECTURE



- Analyst builds model of *system*
- Tool generates AEG from model
- Security specialists enhance modeling/generation capability

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST
INSTITUTE