11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

A Case Study Assessing the Effects of Cyber Attacks on a River Zonal Dispatcher

Ronald Joseph Wright[a], Ken Keefe[b], Brett Feddersen[b], and William H. Sanders[a]

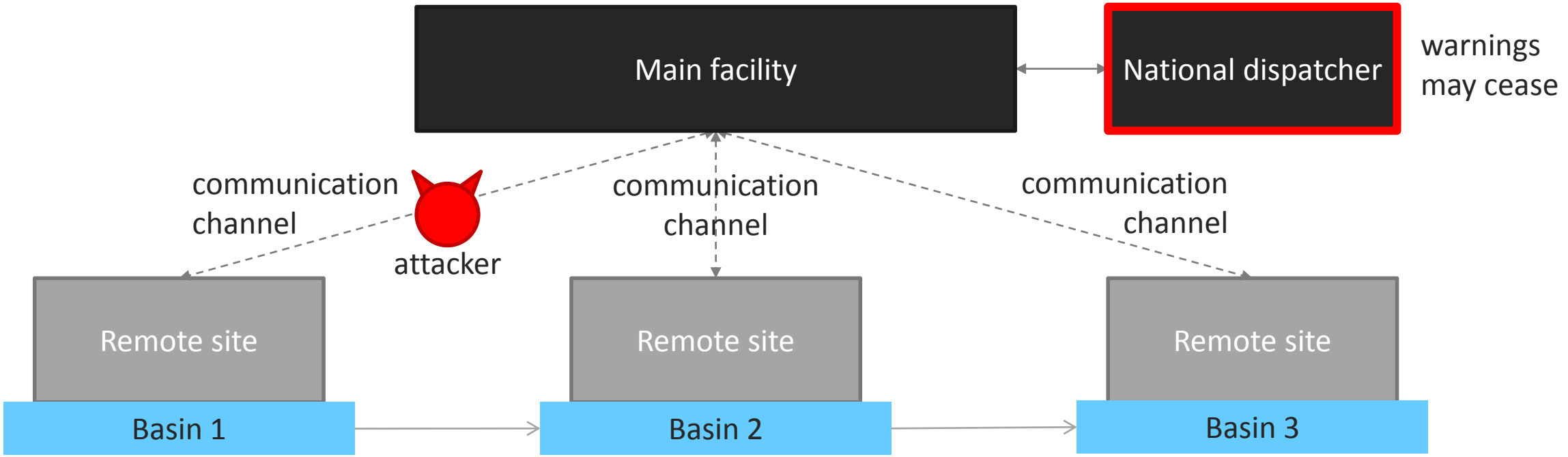
[a] *Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA*
[b] *Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA*

CSL: COORDINATED SCIENCE LAB

INFORMATIONTRUST INSTITUTE

River Zonal SCADA Dispatcher

- A system that sends collected environmental data to a national dispatcher and sends warnings in case of danger



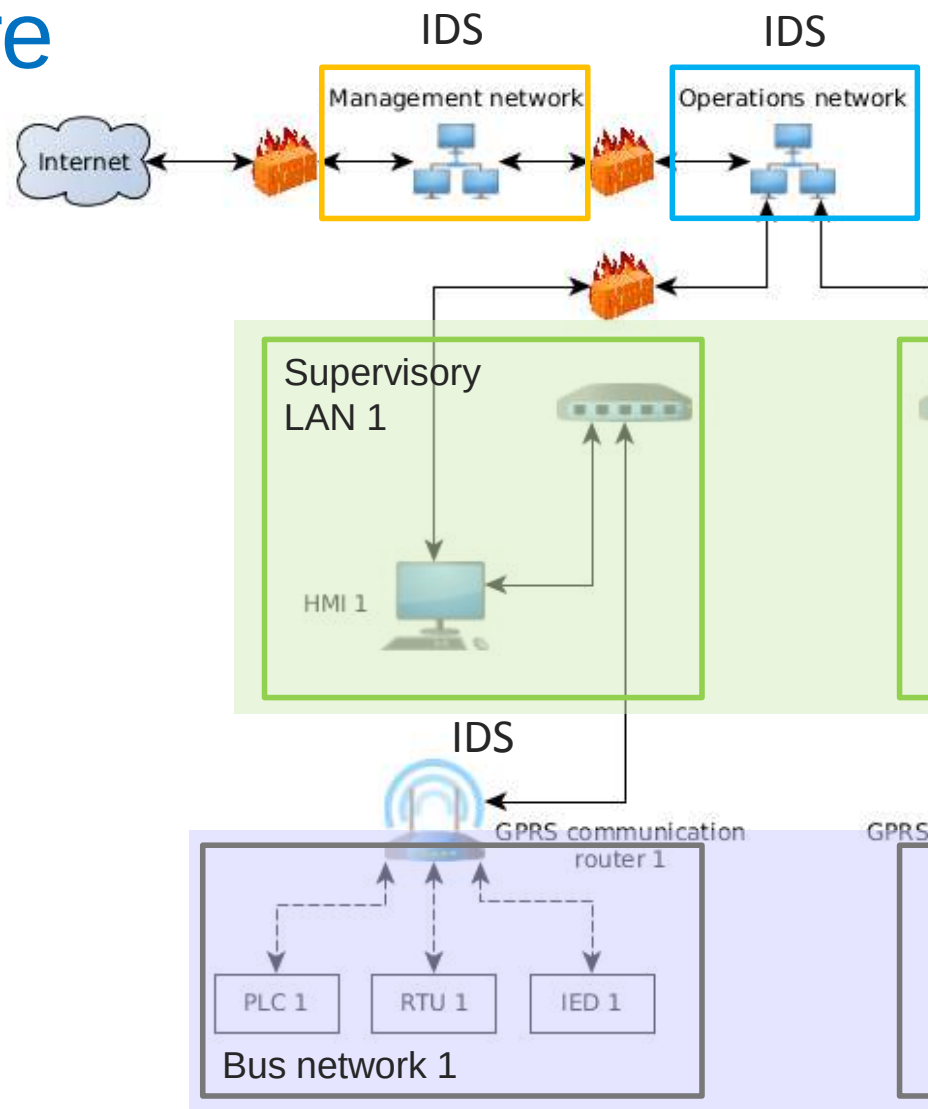
Motivation and Solution

- Motivation:
  - Multiple sectors involved
  - Security threats to integrity of water systems exist
  - Modbus lacks data protection
  - Smallest difference in protection could have life or death consequences
- Approach:
  - Case study of river zonal dispatcher
    - Multiple system configurations
    - Multiple attacker profiles
- Main contribution: analyse different trade-offs in attack scenarios through stochastic modelling and quantitative metrics

Outline

- Architecture
- Attacker model
- Response model
- Experiment
- Results and Analysis
- Conclusion

Architecture

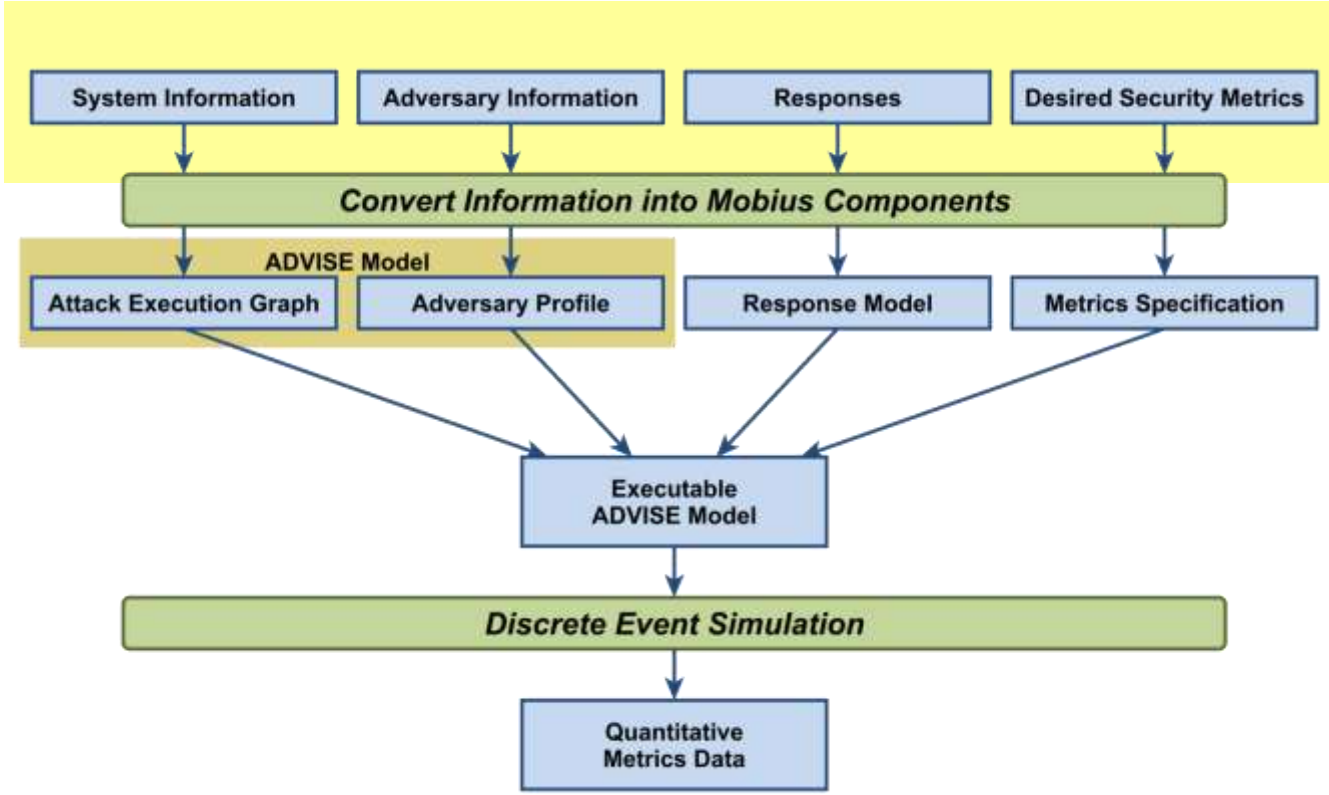


- Each LAN consists of a human-machine interface (HMI)
- Each LAN controls a corresponding subriver basin

- Each network consists of on-site devices

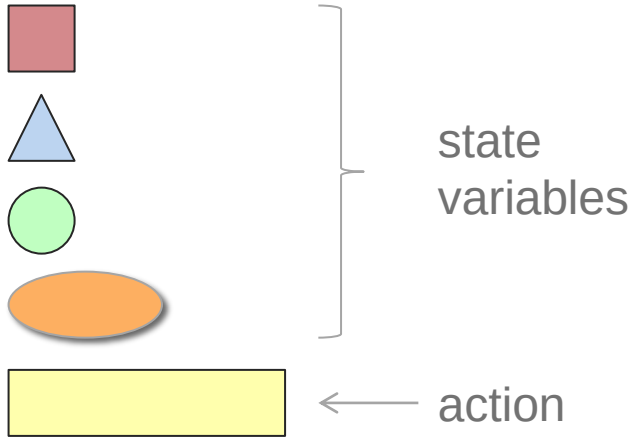
ADVISE Model Development Process

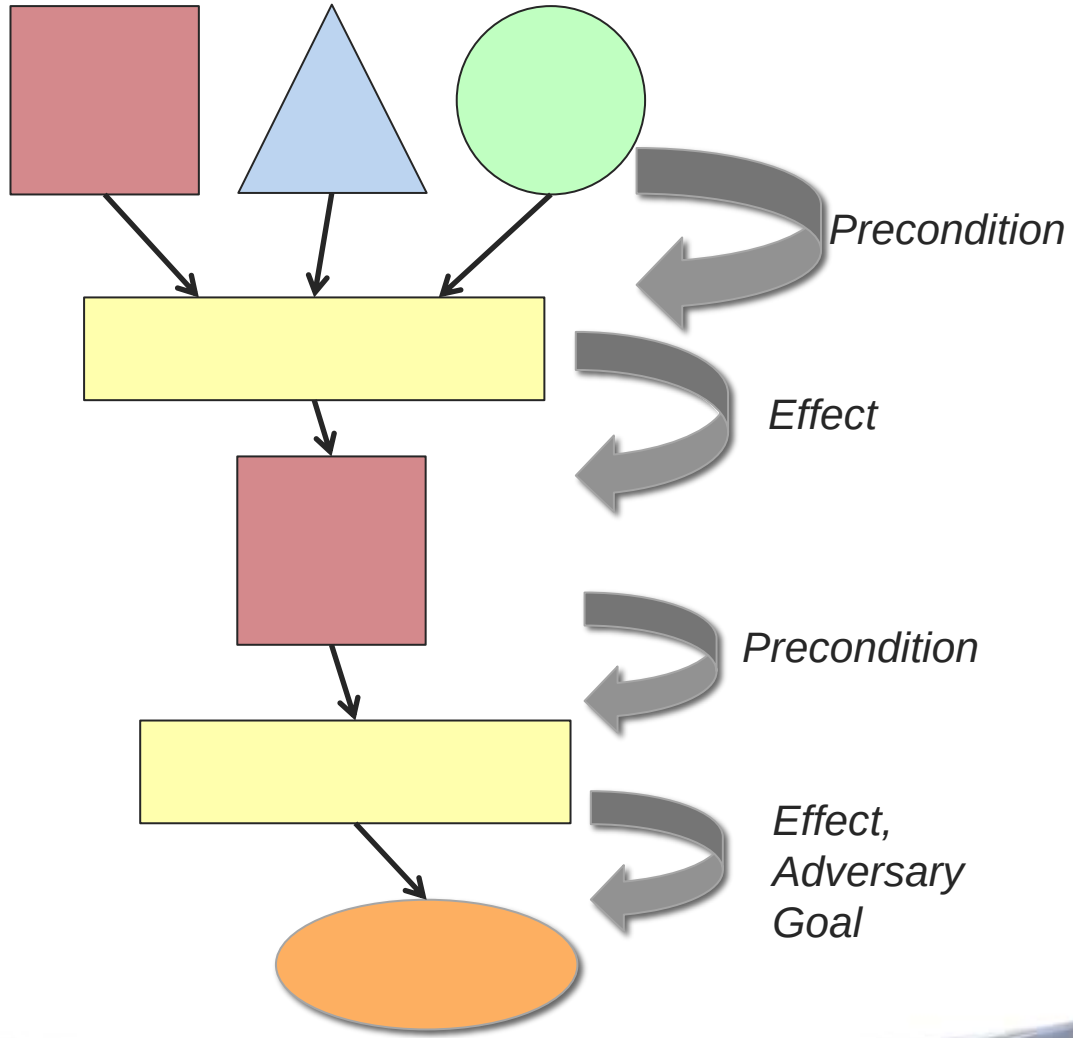
- ADversary VIew Security Evaluation
- Assumes perspective of adversary
- Selects optimal attack based on level of attractiveness



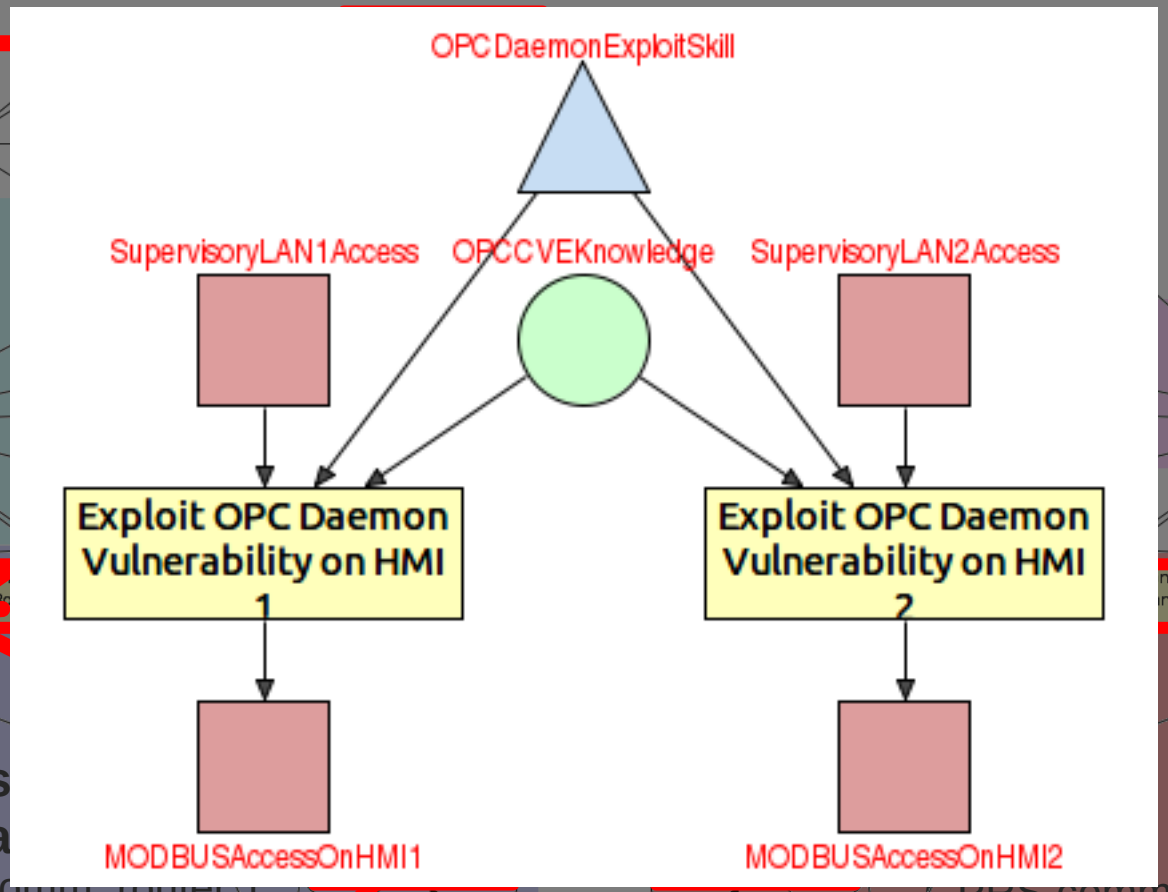
ADVISE Formalism

- Expressed using an attack execution graph (AEG)
- Elements of AEGs include:
  - *Access*
  - *Skill*
  - *Knowledge*
  - *Goal*
  - *Attack step*





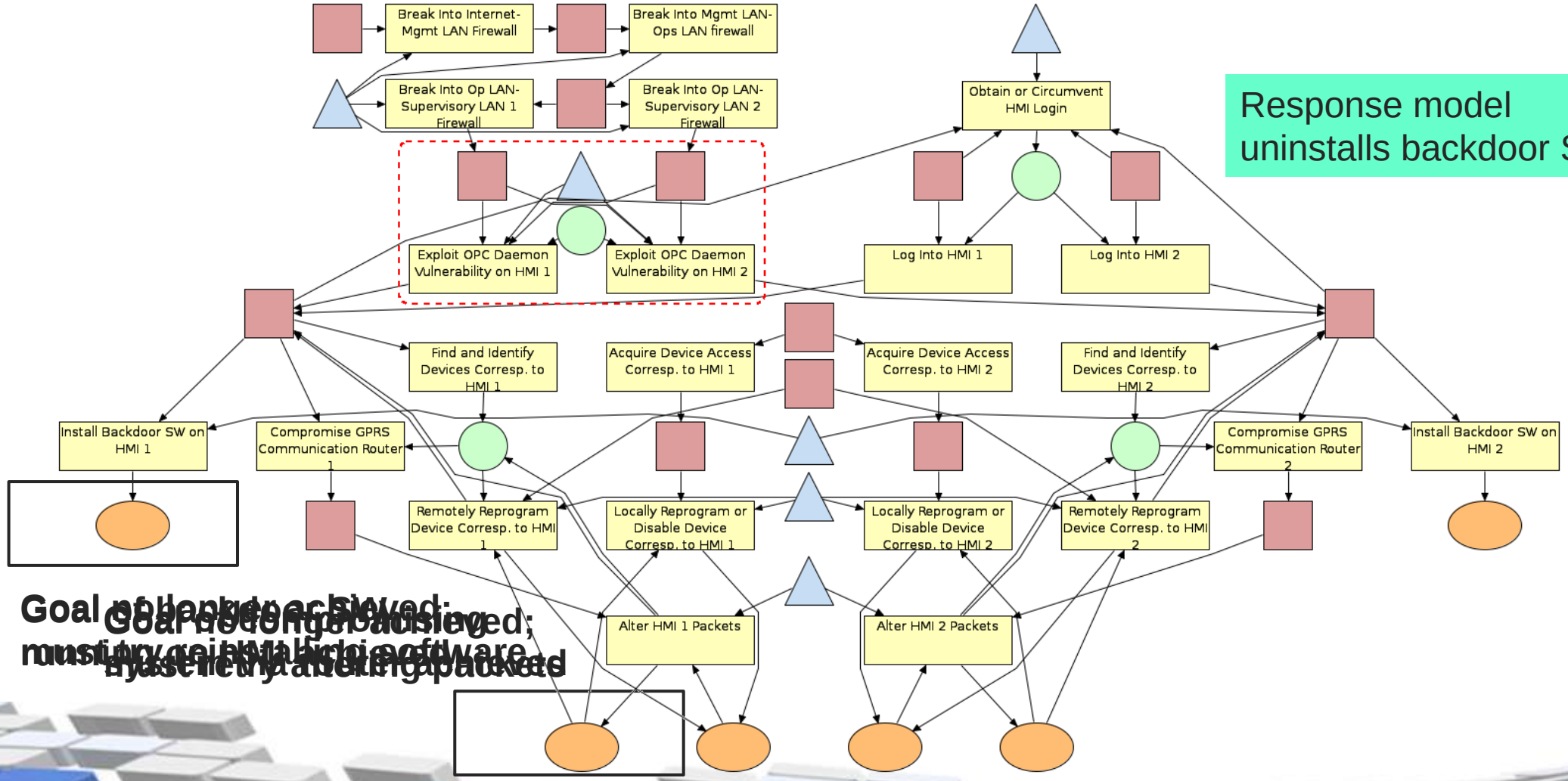
ADVISE Model



Response Model

- Complements ADVISE model
- Restores state of system after attack is carried out
- Modelled with Stochastic Activity Network (SAN) formalism

Response Model Process



Response model uninstalls backdoor SW

Experiment

- System configurations:
  - Presence or absence of IDSes
  - Isolation or non-isolation of supervisory LANs
- Adversaries:

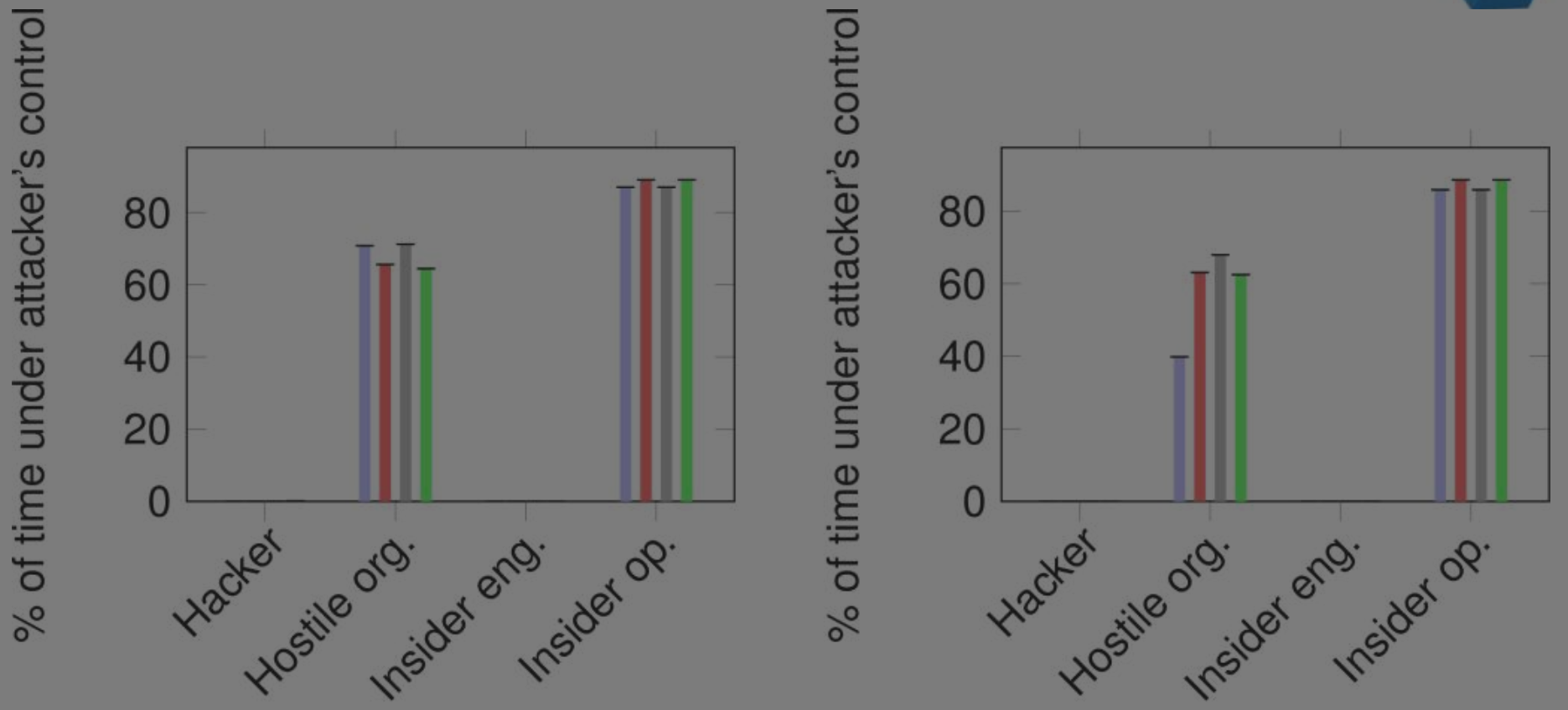
Adversary Type	*Access*	*Skill*	*Knowledge*
Hacker	**Low**	**High**	**Low**
Hostile Organization	**Low**	**High**	**Low**
Insider Engineer	**Medium**	**Low**	**Low**
Insider Operator	**High**	**Medium**	**High**

Values backdoor SW installation and router compromise

Values device and router compromise

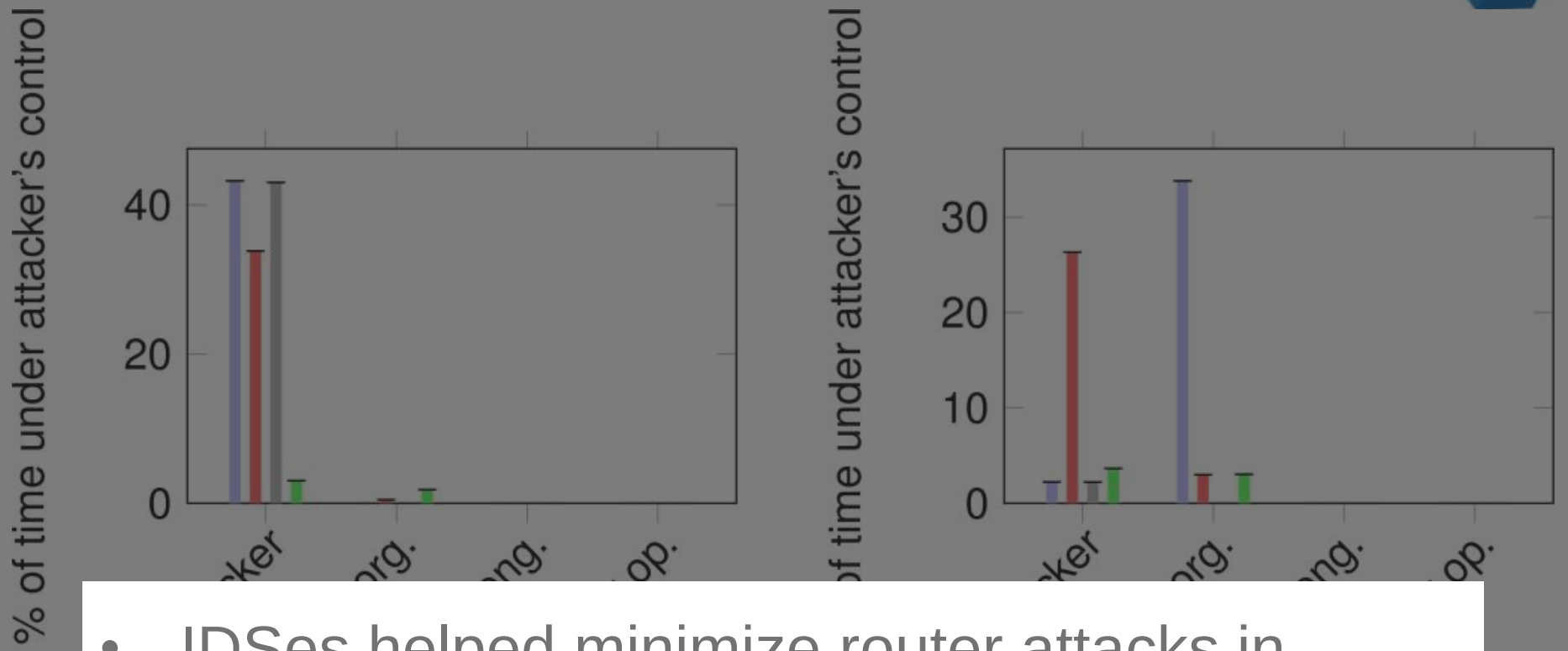
- Total of 16 cases for each simulation
- Simulation models adversary behaviour over one year

Control of Device



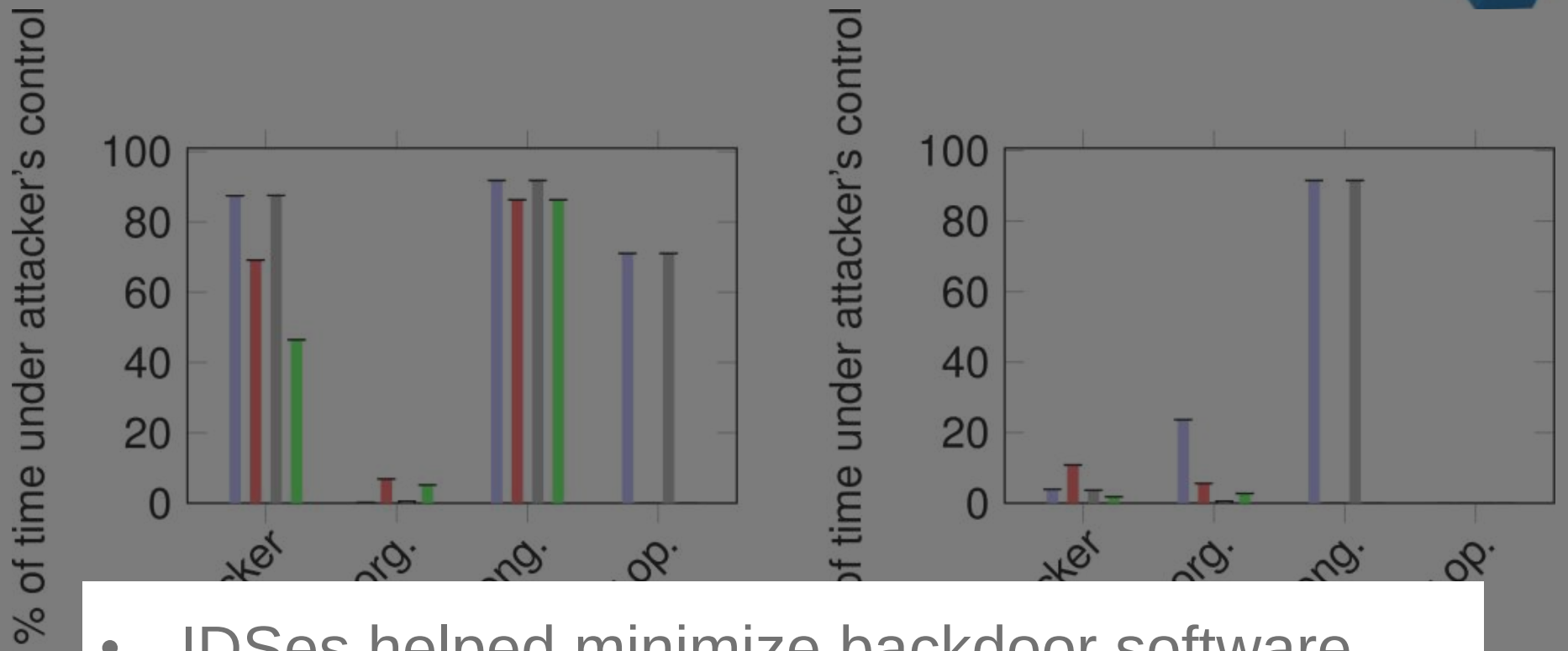
Neither IDSes nor isolation were very effective in stopping device reprogramming attacks

Control of Router



- IDSes helped minimize router attacks in supervisory LAN 1, but did not perform as well in supervisory LAN 2
- Isolation provided an extra layer of security

Control by Backdoor Software Installation



- IDSes helped minimize backdoor software installations in both LANs
- Isolation was not as effective but still played some role

Conclusion

- ADVISE modelling is useful for comparing the security of different configurations under different attack scenarios
- Network isolation and IDS presence play major role in security of system
- Results indicated that attackers with certain abilities and focused goals are the most dangerous ones
- Results suggest that security practitioners must account for as many types of adversaries as possible