TEXAS A&M UNIVERSITY

Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Authors: Adam Hahn, Manimaran Govindarasu
Department of Electrical and Computer Engineering
Iowa State University

Presenter: Olamide Kotun

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Presentation Overview

- Introduction/Motivation
- Previous Work
- Relevant Background Information
- Smart Grid Model
- Exposure Analysis Evaluation Framework
- Exposure Analysis Algorithm
- Security Enhancement Analysis
- Conclusion/Personal Critical Assessment
- References

Introduction

- Benefits the Smart Grid
  - Supports information distribution/storage
  - Increase consumer awareness
  - More efficient energy usage
- Security concerns
  - Computers: More secure offline than online
  - Traditional electrical grid: Offline, more secure
    - Physical tampering
  - Smart grid: Exposed to new types of attacks
    - Remote attacks possible; more access points

Motivation

- The smart grid architecture would be subject to some risk, definitely
- The risk needs to be measurable
- This paper presents a method of quantifying the attack exposure of a smart grid architecture

Previous Work

- Similar problems have been addressed on other systems
  - Attack Trees
  - Attack Graphs
- Little work done smart grid exposure analysis

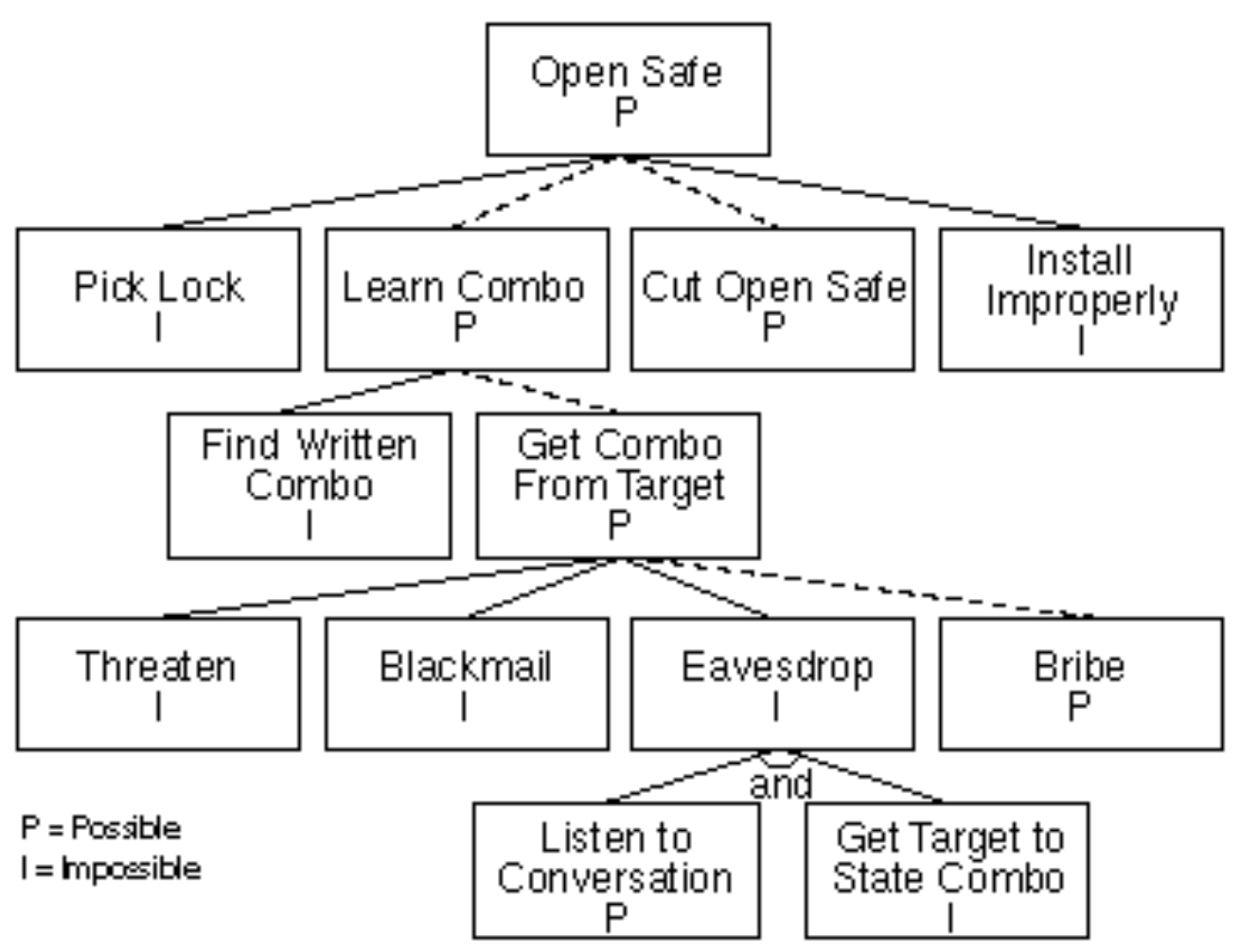
TEXAS A&M UNIVERSITY

ATTACK TREE

Attack Tree - Description

- A security analysis tool designed for computer systems
- Shows different ways that an attacker could access a critical resource
- Root node is the target
- Leaf nodes are steps in the attack

Attack Tree (Bank Safe)



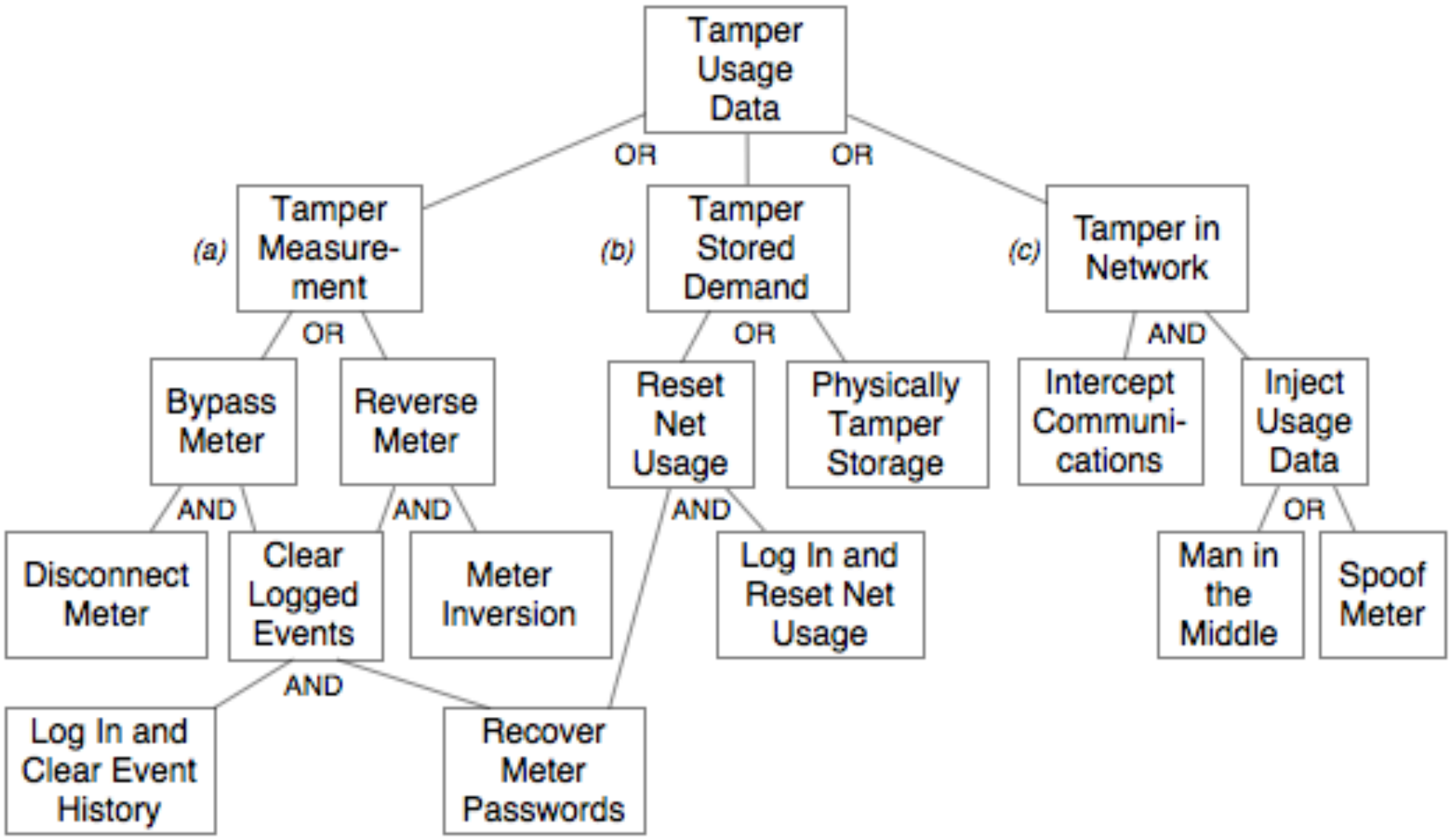
Sample Attack Tree – Bank Safe

From: "Attack trees: modeling security threats"

Attack Tree - Details

- Node types
  - AND nodes, OR nodes
    - AND: possible iff **all** children are possible
    - OR: possible if any children are possible
- Node evaluation
  - Possible or Impossible
  - Difficult vs. Easy
  - Expensive vs. Inexpensive, etc.

Attack Tree (Smart Grid)



Sample Attack Tree – Smart Grid

From: Pennsylvania State University, SIIS Laboratory

Attack Tree – Smart Grid Issues

- Difficult to develop accurate trees
  - All possible attack vectors must be known beforehand
  - Extremely difficult in larger systems
- One root node, i.e., one target resource
  - Smart grid: different attackers, different target components

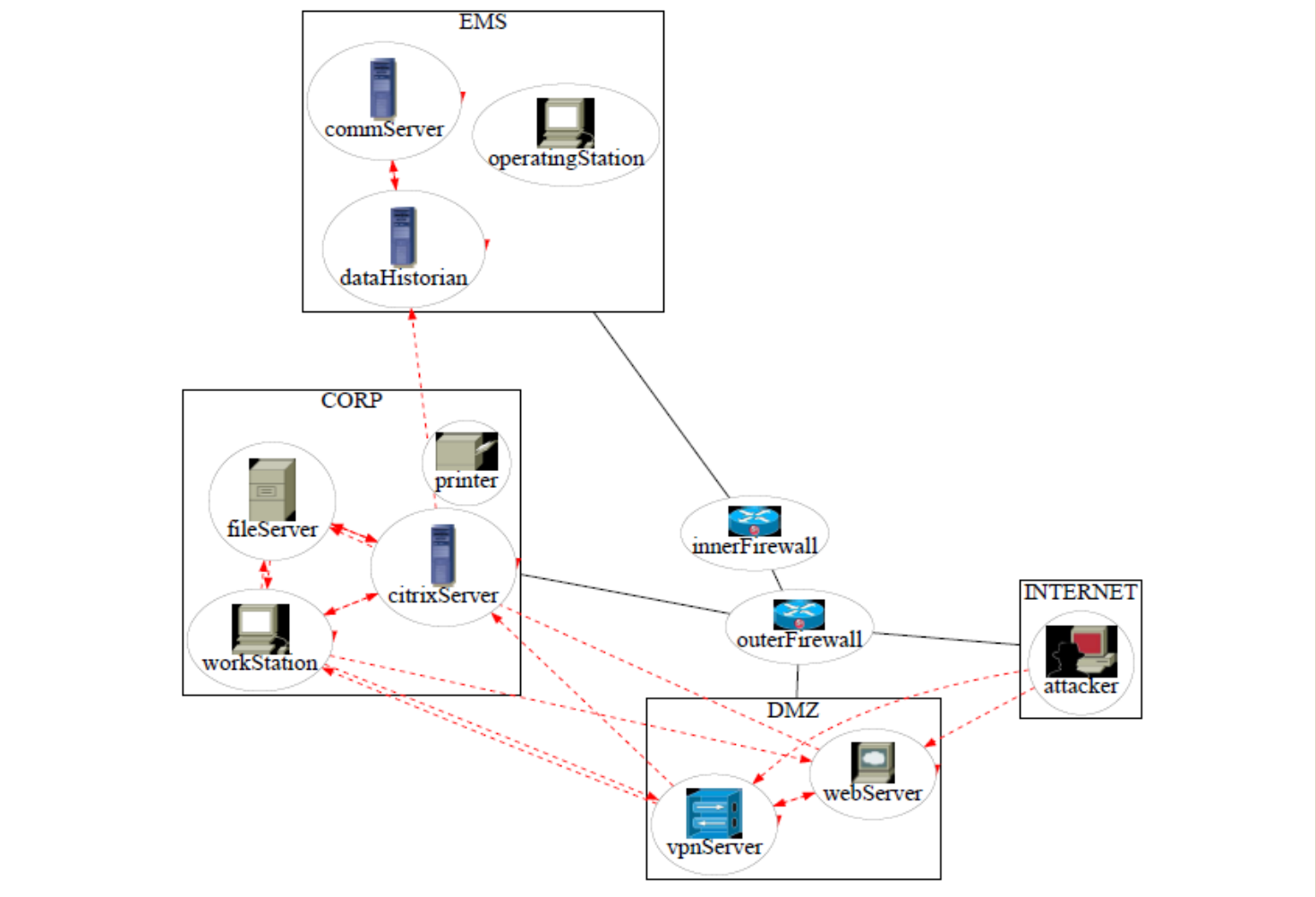
TEXAS A&M UNIVERSITY

ATTACK GRAPH

Attack Graph - Description

- Node: system vulnerability
- Path: exploitation of a vulnerability
- System security indicated by number of nodes which must be exploited

Attack Graph



Attack Graph

From: Improving Attack Graph Visualization through Data Reduction and Attack Grouping

Attack Graph - Details

- Displays only known vulnerabilities
  - Errors in vulnerability assessment are carried throughout the model
- Models are tailored to a predetermined target resource
- Different attackers, different targets
  - Inefficient for larger systems

TEXAS A&M UNIVERSITY

ACCESS GRAPHS

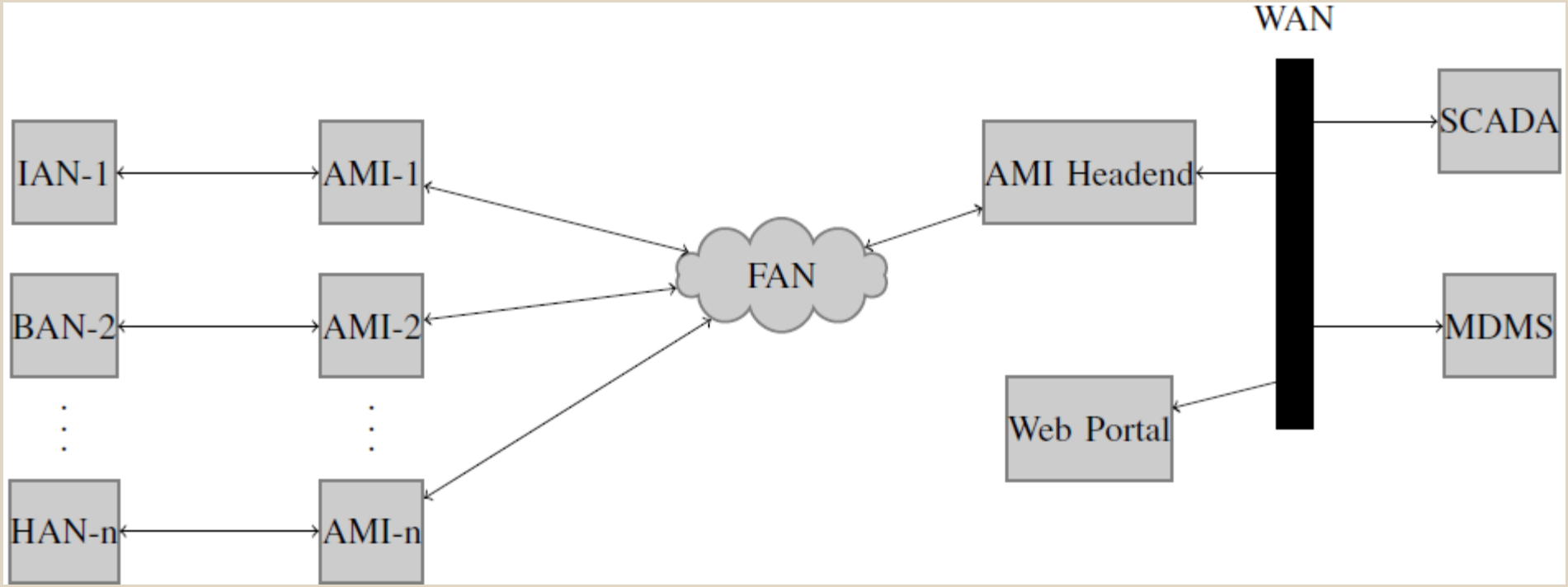
TEXAS A&M UNIVERSITY

SMART GRID ARCHITECTURE

Smart Grid Architecture

- Consists of:
  - Home Area Networks
  - Business Area Networks
  - Industrial Area Networks
  - AMI meters connected to MDMS through AMI headend device
  - SCADA
  - Web Portal (for users)

Smart Grid Architecture



Smart Grid Architecture

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

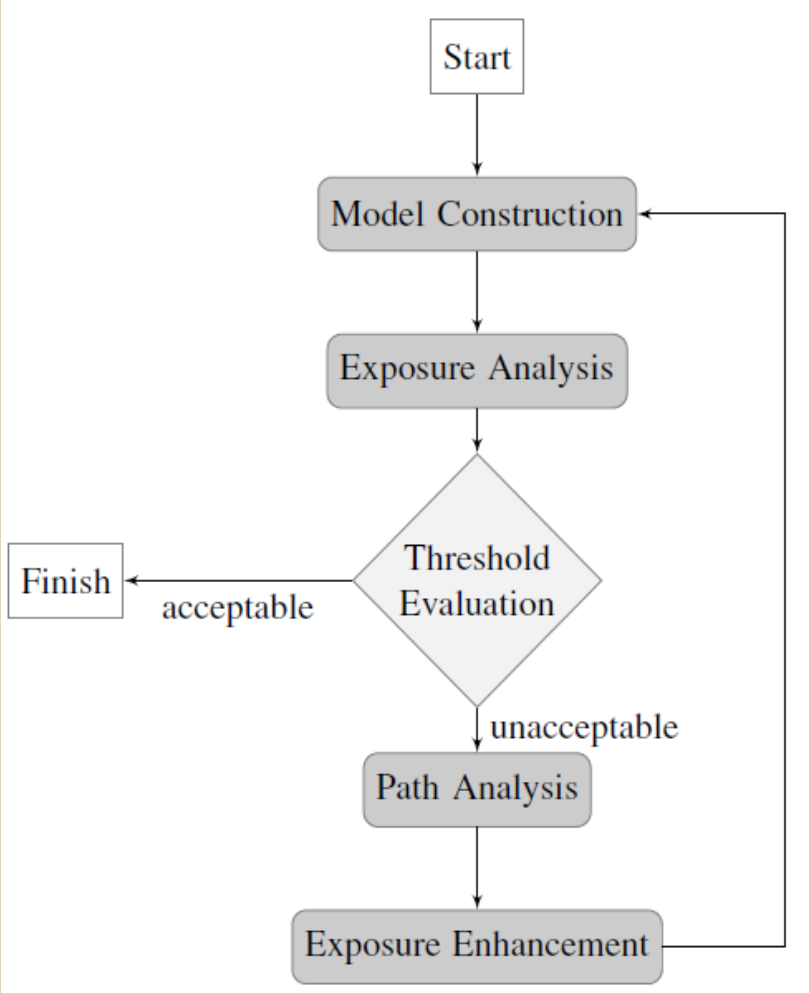
TEXAS A&M UNIVERSITY

EXPOSURE ANALYSIS

Exposure Analysis and Evaluation Framework

- Models potential risk and introduces metrics to quantify the risk
- Determine attack exposure of critical resources and compare with predetermined exposure threshold
- Analysis of security improvements

Exposure Analysis and Evaluation Framework



Exposure Analysis and Evaluation Framework

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

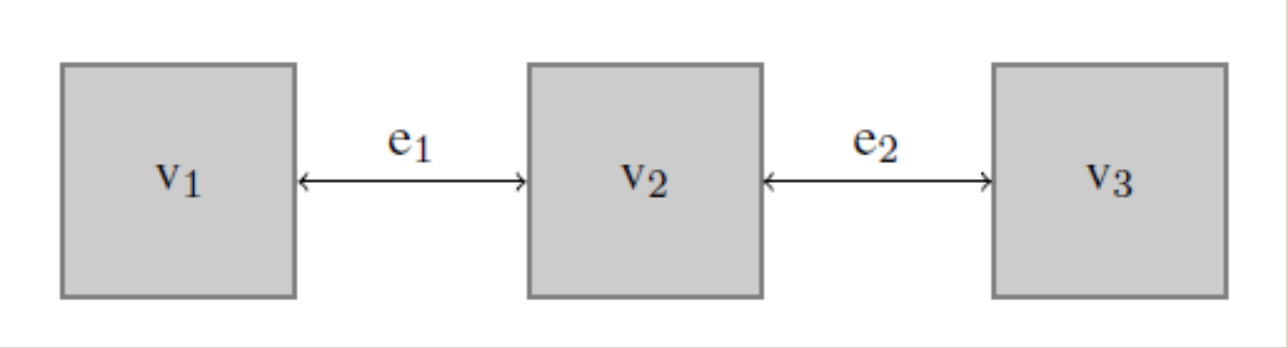
Exposure Analysis and Evaluation Framework

TEXAS A&M UNIVERSITY

- System model
  - Physical Layer
  - Component Layer
  - Security Layer
- Exposure Analysis
  - Exposure Determination
  - Threshold Evaluation
  - Security Enhancement Analysis

Exposure Analysis – System Model

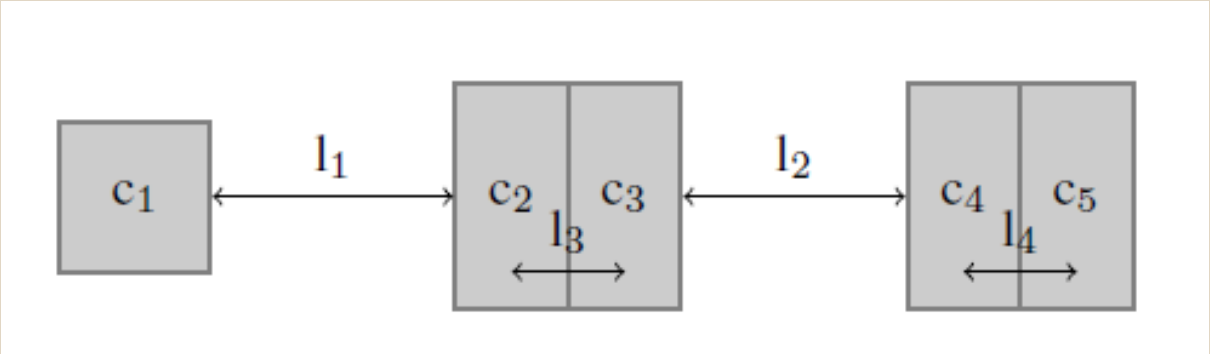
- Physical Layer
  - Physical model of network
  - V: Hosts
  - E: Communication links



From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Exposure Analysis – System Model

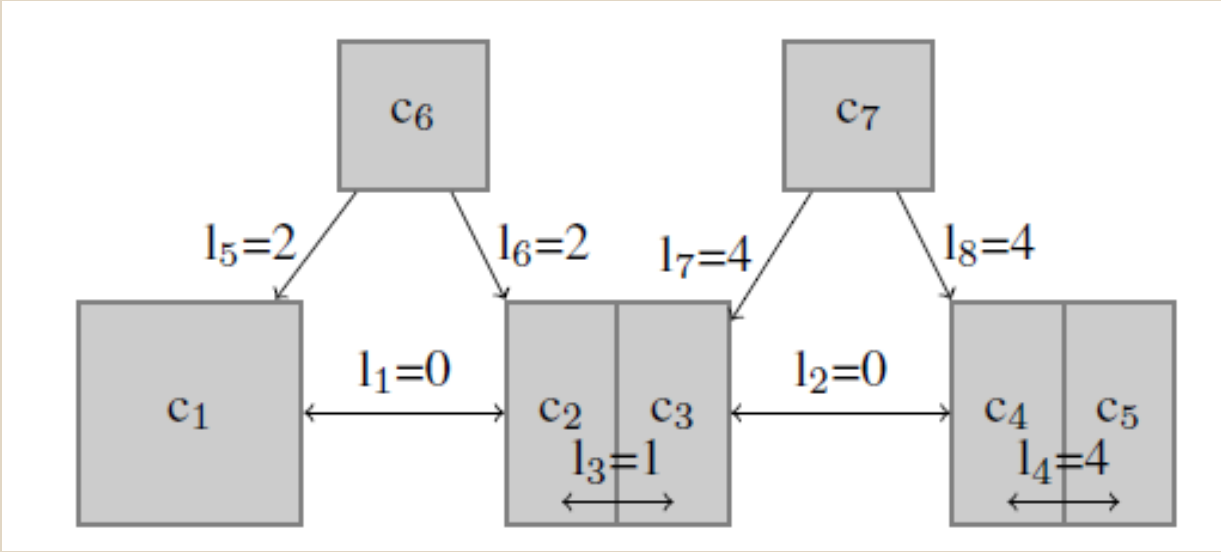
- Component Layer
  - Separate assets into components
  - Shows data flow
  - C: Components
  - L: Logical connections



From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Exposure Analysis – System Model

- Security Layer
  - Introduces edge weights
  - Edge weight: Difficulty of crossing that edge
  - C6, C7: effort required to access to physical link



From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Exposure Analysis – System Model

- Link weight assignment

S_l= <medium, encryption, keystrength>

weight(wired, NA, NA) = 4
weight(wireless, WPA, 128-bit) = 2
weight(wireless, WEP, 128-bit) = 1

Exposure Analysis – System Model

- Component security assignment

S_c= <priviledge,sharedcomponents,enforcement>

weight(service,none,virtual machine) = 4
weight(service,none,OS privileges) = 3
weight(admin,c_i,OS privileges) = 2
weight(admin,c_i,web application) = 1

Exposure Analysis – Exposure Determination

- Performs a shortest path analysis-
  - Returns an exposure level $E(t_i)$ for each target-source pair (t_i,s_j)
  - $E(t_i)$: easiest path to t_i

```
input : S - set of all source nodes
input : T - set of all critical resource nodes
begin;
current_weight ⇐ ∞;
foreach t ∈ T do
    foreach s ∈ S do
        new_weight ⇐ BellmanFord(s, t) ;
        if j < i then
            current_weight ← new_weight; ;
        end
    end
end
```

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Exposure Analysis – Exposure Determination

- Exposure of critical assets, SCADA

  $E(t_i) = \min(E(t_i,s_j))$, $j = 1,\ldots,l$

- Lower $E(t_i)$ means easier access to target
  - Minimum $E(t_i)$ established
- There is an exposure threshold R
- Exposure - difficulty of penetration
- All hosts in the system must maintain an exposure level of at least R

Threshold Evaluation

- Overall exposure

$$\lambda = \sum_{i=1}^{k} (R - E(t_i))$$

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

λ = Exposure of the entire architecture

R = Exposure threshold, minimum $E(t_i)$

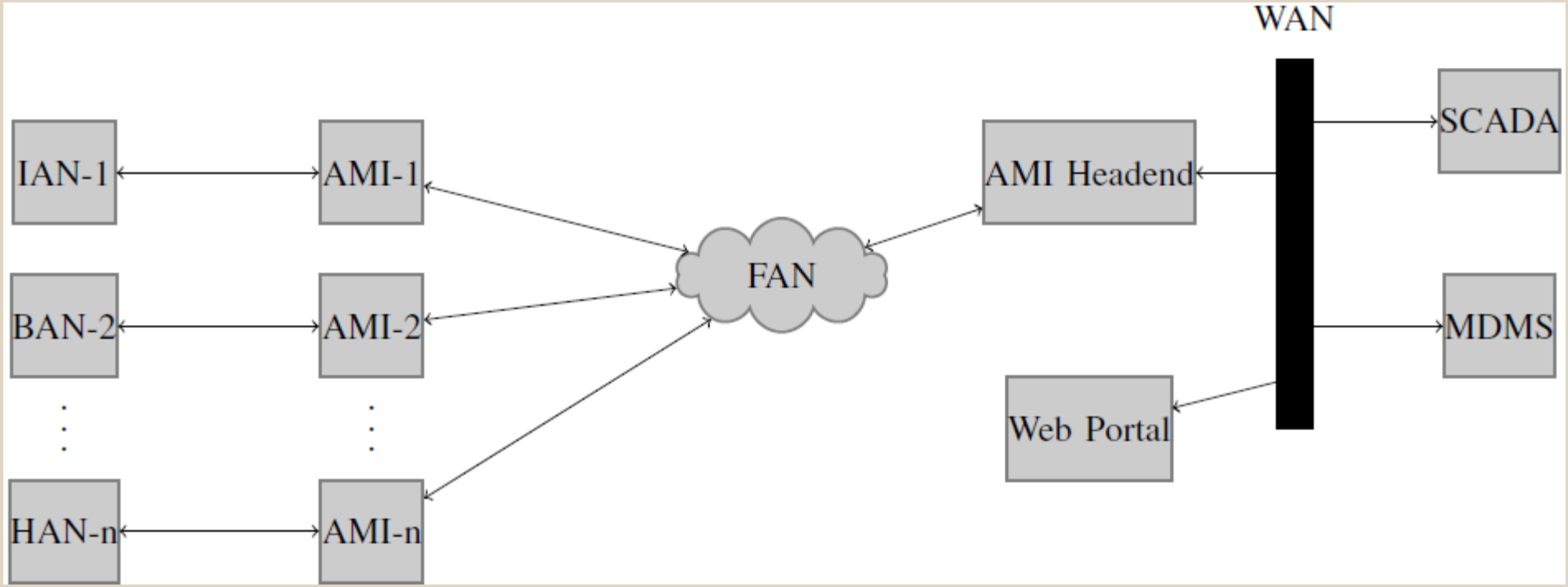
$E(t_i)$ = Exposure of target

Threshold Evaluation

- $\lambda < 0$ implies each component exceeds requirements
- $\lambda = 0$ implies each component meets requirements
- $\lambda > 0$ implies some or all components do not meet requirements

SECURITY ENHANCEMENT ANALYSIS

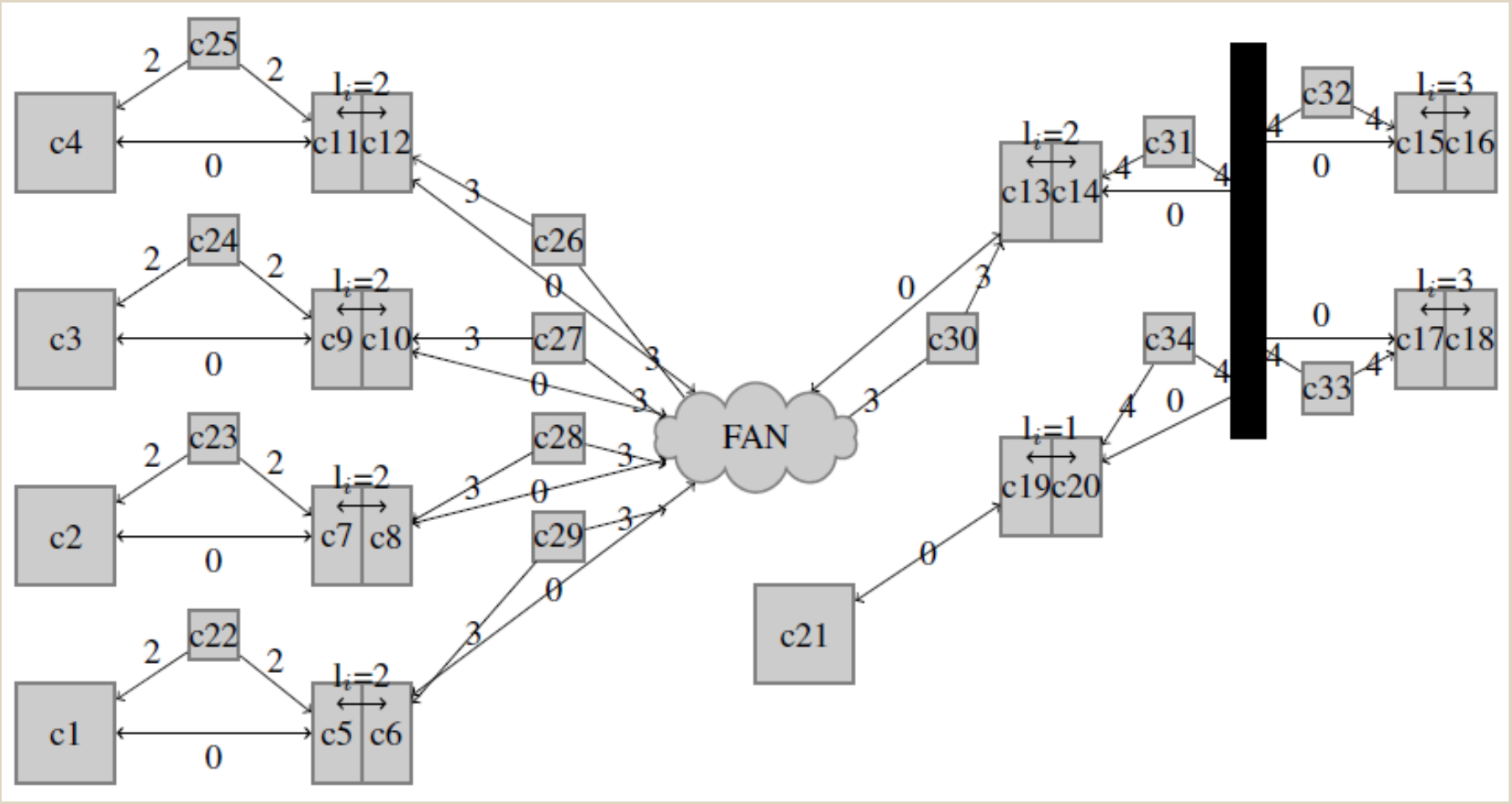
Smart Grid Architecture – for reference



Smart Grid Architecture

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Security Enhancement Analysis – Sample Scenario



Sample Security Layer Graph for Smart Grid Architecture
From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Security Enhancement Analysis

- Shortest path analysis carried out for the tabulated components

T(sink)	S(source)
$t_1 = c_{16}$	$s_{\{1,\ldots,4\}} = c_{\{1,\ldots,4\}}$
$t_2 = c_{17}$	$s_{\{4,\ldots,8\}} = c_{\{22,\ldots,26\}}$
$t_3 = c_{20}$	$s_{\{9,\ldots,12\}} = c_{\{26-29\}}$
	$s_{13} = c_{21}$

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

  - t : SCADA, MSMS, Web Portal
  - s : Customer area networks

Security Enhancement Analysis

- Exposures are determined by traversing the sample security layer graph

Path Exposures		
Target	Source	Exposure
t_1	$s_{\{1,\ldots,4\}}$	7
	$s_{\{4,\ldots,8\}}$	9
	$s_{\{9,\ldots,12\}}$	8
	s_{13}	4
t_2	$s_{\{1,\ldots,4\}}$	4
	$s_{\{4,\ldots,8\}}$	6
	$s_{\{9,\ldots,12\}}$	5
	s_{13}	1
t_3	$s_{\{1,\ldots,4\}}$	4
	$s_{\{4,\ldots,8\}}$	6
	$s_{\{9,\ldots,12\}}$	5
	s_{13}	1

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

Security Enhancement Analysis

- Computing Security Enhancement
  - Network security is tightened by some means
  - Framework used to quantify the effect of the security improvement measures employed.

$$\beta = \sum E'(t_i, s_j) - E(t_i, s_j)$$

From: Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework

  - β : Benefit of the enhancement
  - $E'(t_i,s_j)$: New exposure level
  - $E(t_i,s_j)$: Previous exposure level

Personal Critical Analysis

- The authors do a good job of modeling the exposure if the system.
- The authors have identified a practical application of their work
- After system security has been improved, this algorithm could be used to visualize, numerically, the amount if improvement seen by doing a before-and-after comparison.
- The authors noted that attack trees inherently do not work well in large systems. Consequently, readers would be interested in seeing how this method addresses that issue. This could have been satisfied by more rigorous simulations (A system of more than 100 nodes).

Conclusion

- An important question has been attempted, and successfully answered, at least on a small scale
- Future work could be done on actual security enhancement measures

References

[1] Hahn, A.; Govindarasu, M.; , "Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework," *Power and Energy Society General Meeting, 2010 IEEE* , vol., no., pp.1-6, 25-29 July 2010

[2] Xiaochun Xiao, Tiange Zhang, Gendu Zhang, "Access Graph to Analyze Network Vulnerabilities," PACIIA, vol. 2, pp.781-786, 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008

[3] Lippman, R.P.; Ingols, K.W. *"An Annotated Review of Past Papers on Attack Graphs*," Project Report, Lincoln Laboratory, 2005.

[4] B. Schneier, "Attack trees: modeling security threats," Dr. Dobb's Journal, December 1999.