

# Cyber Attack Exposure Evaluation Framework for the Smart Grid

Case 01 - Group 5

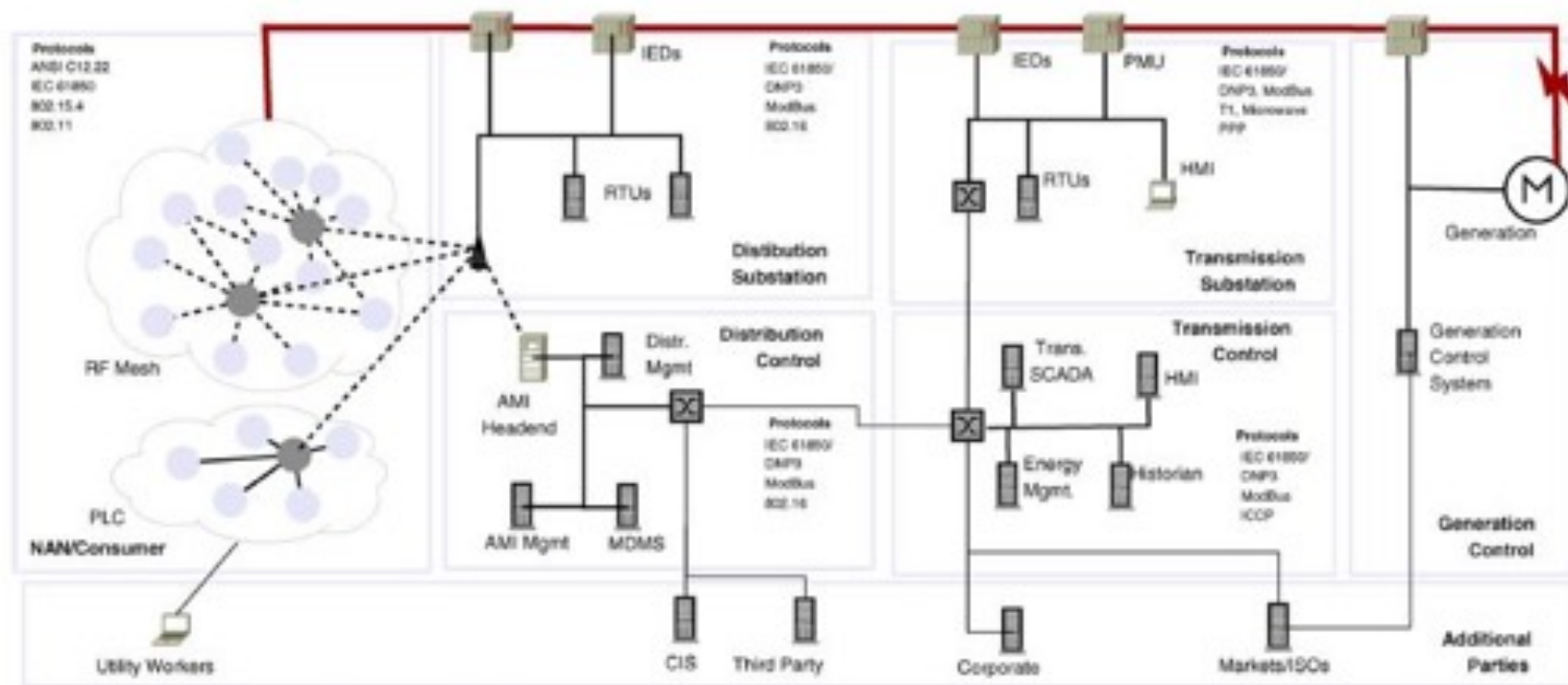
# I. Introduction

- **SMART GRID advancements** present an undetermined level of risk to electric grid reliability
- coupling of power infrastructure with complex computer networks substantially expand current cyber attack surface and will require significant advances in cyber security capabilities
- **Strong security metrics** are necessary to ensure security-based decisions accurately
- security models should focus on the **critical information** to support the grid and the resulting security
- **Research:** provides a novel network security model based on these information objects by identifying and analyzing their dependencies

## II. Related Work

- **NERC (North American Electric Reliability Corporation):** developed a CIP - Critical Infrastructure Corporation - which introduce cyber security compliance requirements for power systems
- **Manadatha & Wing:** Research on attack surface evaluation
- **Attack tree:** model which enumerates all potential vectors an attacker could use to gain access to some target resource, each branch in the tree represents a set of intermediate steps the attacker must take prior to gaining access to the target
- **Privilege/Attack Graphs:** evaluate various privilege states in a computer system to determine whether known security states are violated

### III. Smart Grid Introduction



# III. Smart Grid Introduction

Technologies:

- **PMU** (phasor measurement units)
- improved fault management
- **AMI** (advanced metering infrastructure): deployment of smart meters at consumer location attempts to reduce cost and increase electricity reliability
- enables demand side management (DSM) which exercises direct/indirect control over consumer power consumption
- Maintaining a secure AMI infrastructure is very difficult (different locations)
- **CIM** (Common information model)

## IV. Exposure Evaluation Framework

- To develop an Exposure Evaluation Framework all patch an attacker must take to access critical resources need to be examined
- The following framework was developed based on NIST:

### A. Identifying Cyber Risks

- A set of privileges ( $P$ ) identify the set of available states in the system
- Each privilege represents the access to some set of information objects ( $IO$ )
- Each privilege is enforced with a set of security mechanisms ( $SM$ )

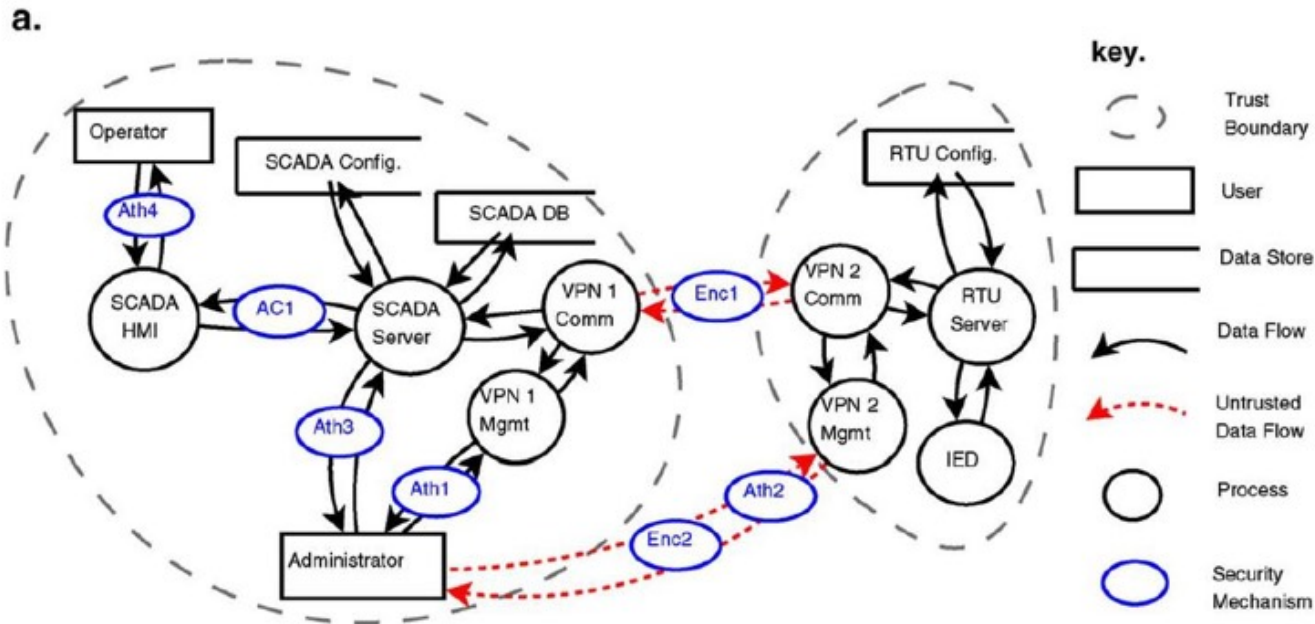
# IV. Exposure Evaluation Framework

## A. (continued)

- Utilizing the threat modeling process by Microsoft, all users, processes, data flows, entry and exit points and data stores are identified
- Then each data flow is reviewed for possible vulnerabilities (spoofing, tampering, repudiation, information disclosure, denial of service, escalation of privileges)
- With this a data flow diagram (DFD) is developed to identify trusted boundaries and potential untrusted input

# IV. Exposure Evaluation Framework

A. (continued)

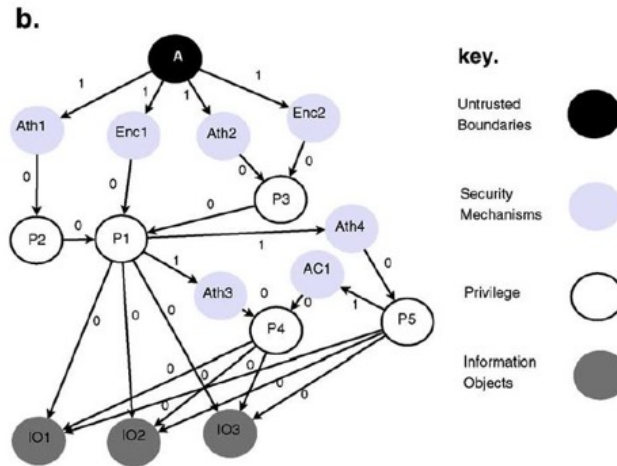




# IV. Exposure Evaluation Framework

## B. Exposure Graph Development

- From the previous DFD, an exposure graph is developed starting from a potential attacker access (A)



# IV. Exposure Evaluation Framework

## C. Exposure Evaluation

- All paths to information objects from the previously developed exposure graph are calculated
- The length of each path determines the attack surface (exposure metric)
  - 4 possible paths
  - Starting from each information object and traced back to the attacker (A), the length is 4
  - Each path has a length of 1 to access the information object

# V. Exposure Metric Applications

## A. Vulnerability Analysis

- Due to the continuous development of new vulnerabilities, the exposure analysis should be recomputed during a continual monitoring process
- All paths from the exposure graph should be recalculated
- If the resulting architecture leaves the system in an unacceptably exposed state (paths get shorter), additional security mechanisms are necessary

# V. Exposure Metric Applications

## B. Cyber Security Investment Optimization

- Starting from the exposure graph, comparing the current graph with a desired one can be used to evaluate on investment options in terms of comparing the value of the additional security provided by the additional enhancements

## C. Cyber Contingency Analysis

- Direct correlations can be made between failures of cyber security mechanism and physical system occurrences
- This could instigate the development of cyber contingency analysis policies

# VI. Metrics Evaluation

-> evaluate the metric's applicability within a smart grid environment

## A. Simulated Environment

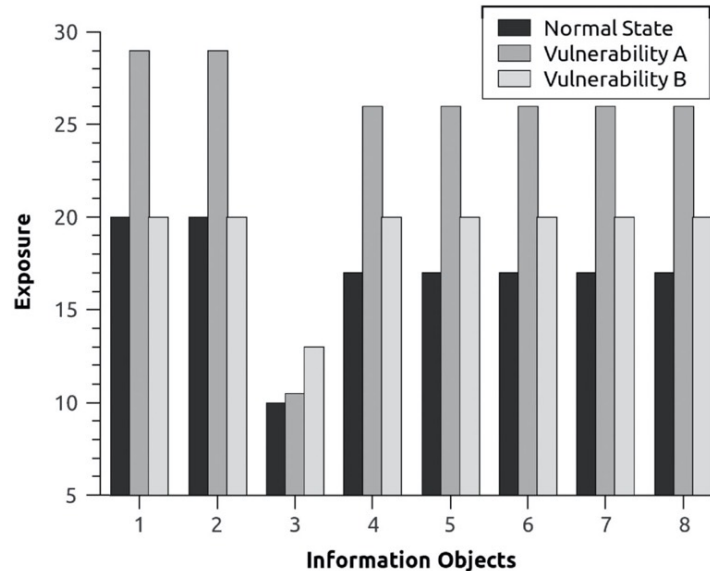
Domain	Device/Protocol	Security Requirement	Implementation Type	Protected Privileges
<b>HAN</b>	HAN GW	Authentication	x.509 Cert (Meter)	Individual HAN gateway
	Zigbee	Encryption	Link/Network Key Exchange Link/Network Algorithm	All HAN gateways & meters All HAN gateways & meters
		Authentication	Network Key	Individual HAN gateway & meter
<b>NAN</b>	Meter	Physical		Individual meter
		Authentication	Meter-NAN private key	Individual meter
	Zigbee	Key Establishment		All meters
		Access Control	DAC (customer/mgmt function)	All meters
		Encryption	Link/Network Key Exchange Link/Network Algorithm	All NAN meters All NAN meters
<b>FAN</b>	Headend	Authentication	Network Key	All NAN meters
		Access Control	x509 Cert (Meter) Key Signer DAC (inter-customer)	Individual meter All meter All meter
	WiMax [1]	Authentication Key Establishment Encryption	x509 (meter), EAP KEK, TEK DES/AES (Payload)	All FAN Stations All FAN Stations All FAN Stations
<b>Enterprise LAN</b>	MDMS	Authentication Access Control	x509 Cert (Headend) DAC (inter-customer)	

# VI. Metrics Evaluation

## B. Simulation Results

-> perform the resulting exposure computation and then provide demonstrations of the impact on the systems security

### 1. Vulnerability Assessment

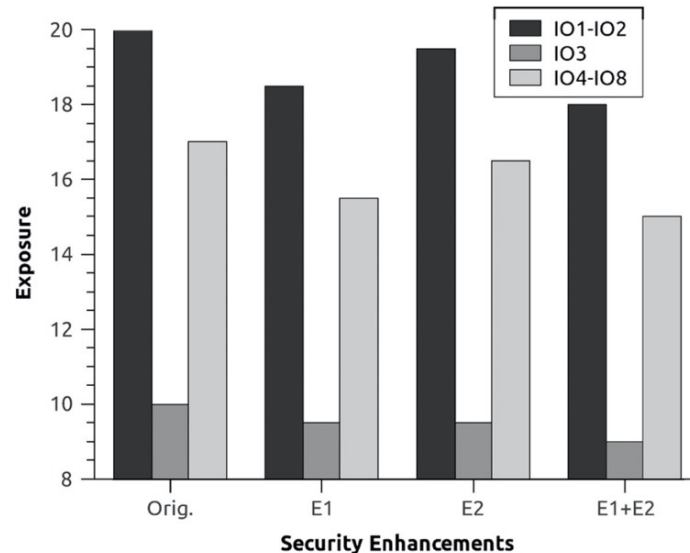


# VI. Metrics Evaluation

## B. Simulation Results

-> perform the resulting exposure computation and then provide demonstrations of the impact on the systems security

## 2. Security Investment



# VI. Conclusion

- addressed quantitative security metrics for large scale networked environment such as a smart grid
- proposed model utilizes a pragmatic development process which integrates within a modern risk management process and is based on information that is well known to security engineers and operators
- An exposure metric has been proposed to identify the set of security mechanisms required to protect the various information objects utilized within a network
- test the metrics with a model likely AMI developments
- metrics has shown how vulnerability impacts can be evaluated by simulating vulnerabilities and demonstrating their impact on information object's exposure
- Future research within this domain will address scalability to larger system deployments and system-level metrics to facilitate more comprehensive architecture analysis