Analytics for Enterprise Cybersecurity

Application Example Summary

Nazli Choucri
Professor of Political Science
nchoucri@mit.edu

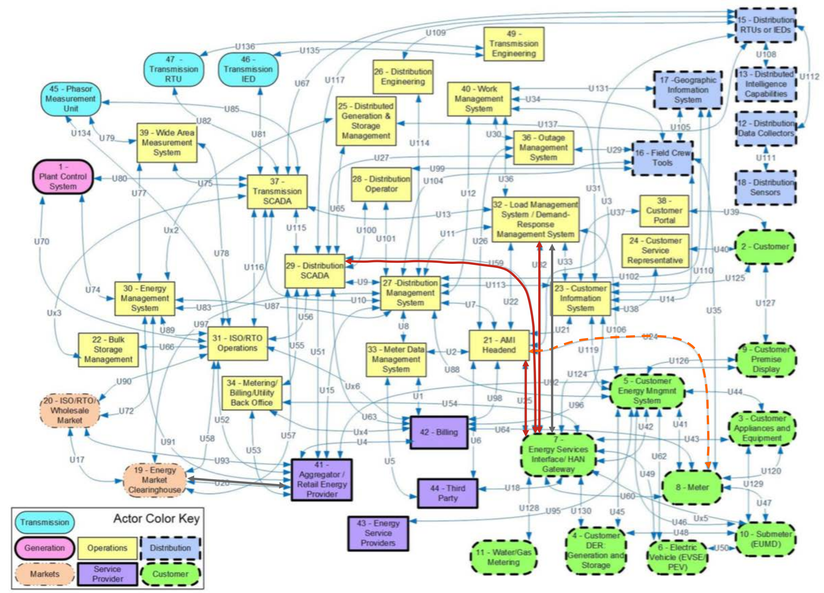
Gaurav Agarwal
Research Affiliate, MIT Political Science
gauravag@mit.edu

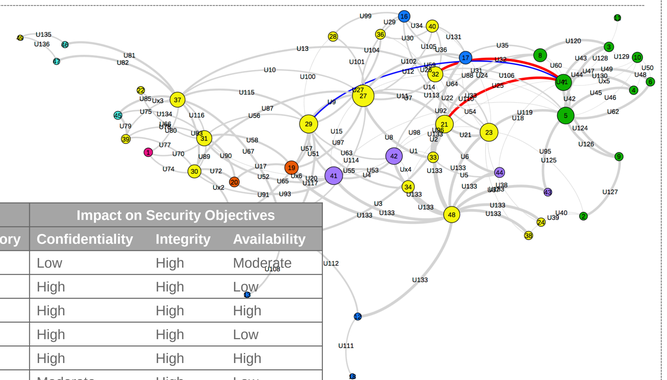
Case Study I: Aviation

Conditions

Airport acts as an Energy Services Interface as it combines the loads of multiple end-use customers in facilitating the sale and purchase of electric energy, transmission, and other services on behalf of these customers and coordinates with the SCADA systems and Load Management Systems to ensure Power Supply.

Airport coordinates with information exchanges between third party systems or systems not considered headend, such as the Meter Data Management System (MDMS) and the AMI network, among other functions





Logical Interface*			Impact on Security Objectives		
Name	Actors	Category	Confidentiality	Integrity	Availability
U59	7 and 29	10	Low	High	Moderate
U32	7 and 32	13	High	High	Low
		14	High	High	High
U25	7 and 21	13	High	High	Low
		14	High	High	High
		18	Moderate	High	Low

Case Study II: Electric Transportation

Intrusion Scenario 1

Intrusion A targets the Energy and Management layer (SCADA) of EVs by interfering with data submitted between Energy Management System peripherals connecting the aggregator with the system operator. At time *t*, a cyber-intruder changes the cost function hourly parameter that the aggregator sends to the operator from a predetermined value 1 (no intrusion) to 0 $/MWh.

This results in the operator buying the full amount of available electricity from the EVs. While, at time *t+1*, the same intruder changes the same parameter from: predetermined value 2 (no intrusion) to 1000 $/MWh. So in this case, in order to make a profit, the operator will sell the electricity to the aggregator at the "fake" high price set by the intruder.

Intrusion Scenario 2

Intrusion B targets the Energy and Management layer (SCADA) of EVs by interfering with data submitted between Energy Management System peripherals connecting the aggregator with the EVs. The intrusion targets the EVs directly by varying their charging orders from the aggregator.

At time t, the operator dispatches the power produced by EVs from 50 MW to 125 MW (discharging). The aggregator receives these levels from the operator and needs to communicate this with the EVs at each bus. The cyber-intruder changes the level of charging levels that the EV's should follow and that was to be communicated from the aggregator to the EVs. The intruder sets all these levels to the maximum possible discharging.

Spatial distances between nodes based on relative distance to other nodes.
Node represents an actor.
Node color based on domain.
Node size based on eigenvector centrality of node in the network.
Edge represents a logical interface (or connection) between two actors.
Interface strength – illustrated by thickness of connection.
Impact scale and scope, defined in system-wide terms – represented by edge color.

Impact level	U20	U32
Confidentiality (C)	High 13 (H);14 (H)	High 9 (H)
Integrity (I)	High 13 (H);14 (H)	High 9 (H)
Availability (A)	High 13 (L);14 (H)	Moderate 9 (M)

Mapping vulnerability classes and the recommended security requirements.

Case Study III: SCADA Operations

Conditions : Meter Sends Information

A meter sends automated energy usage information to the Utility (e.g., meter read (usage data)). The automated send of energy usage information is initiated by the meter and is sent to the Advanced metering Infrastructure (AMI) Head End System (HES).

The Head End system message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC archives the automated energy usage information and forwards the information onto the meter Data Management Systems (MDMS).

Source: NIST. "*Guidelines for Smart Grid Cybersecurity-Volume 1*," NISTIR 7628 Revision I, September, 2014; **doi:** NIST.IR.7628r1, Volume 3, Chapter 10; Overall Use Case # 1.

Logical Interface			Impact on Security Objectives		
Name	Category	Actors	Confidentiality	Integrity	Availability
U24	13, 14 & 18	8 & 21	High	High	High

Vulnerability Description: Password Management Vulnerability (CWE-255)§

The Management Software application has a hardcoded password for an administrative account, which allows local users to gain privileges via unspecified vectors.

Likelihood of Vulnerability					
Vulnerability Class	Attack Vector	Attack Complexity	Scope	Privilege Required	User Interaction
CWE-255§	Adjacent Network	Low	Changed	None	None

§ Illustration Purpose only; see NIST, "National Vulnerability Database", Online resource, https://nvd.nist.gov/cwe.cfm for details.

	CVSS Score (Rescaled)	Business Context
Business Impact	6.06 (10)	Existence threatening (5)
Probability of Occurrence	3.89 (10)	Very Likely (5)

Risk Priority Group Ordering:

6 ≺ 5 ≺ 4 ≺ 3 ≺ 2 ≺ 1

