Creating a Cybersafety Analysis Discipline (CAD) for Resilient Energy Delivery Infrastructure

1st Step: Learn from Prior Events

Stuart Madnick, James Kirtley, and Mohammad Jalali

INTRODUCTION AND GOAL

- Our proposed cybersafety analysis discipline (CAD) approach is based on an adaptation of the System-Theoretic Accident Model and Processes (STAMP) method, originally developed for accident or incident analysis, such the Challenger Space Shuttle disaster.
- With STAMP, the overall system is viewed as a hierarchy of control loop structures, which incorporate human and organizational controls, where constraints at a higher level control behavior at lower levels.
- The goal is to eliminate hazard conditions that can lead to a loss, and implement effective countermeasures during design and/or operation to prevent losses.
- As an initial step, we have been looking at prior major cyberattacks on Energy Delivery Systems and other Industrial Control Systems (ICS).
- NOTE: A key challenge has been that details of cyberattacks on ICS are usually not provided. Some of the cases mentioned below have conflicting reports, and even their existence is disputed. We base our analysis on available reports.

1) CASE ONE

People's Liberation Army Unit 61398

WHEN, WHERE, WHAT

- December 2011–June 2012; U.S. natural gas utilities.
- UglyGorilla, a Chinese hacking operative, along with Unit 61398 of the Chinese Army, attempted to hack into 23 U.S. natural gas utilities.
- 10 were definitely breached, and 12 more may have been.

WHAT HAVE THE HACKERS DISRUPTED?

- Nothing… yet!
- Chinese operatives have been systematically mapping U.S. utility assets and computing networks.
- Hackers have shown specific interest in accessing networks that regulate the flow of natural gas.

WHAT INFORMATION HAS BEEN TAKEN?

- Passwords, engineering PDFs, and data that would let them back into the systems through a remote access for employees.
- Field site locations that include block valve stations and compressors that can be actuated remotely.
- SCADA log-ons and user manuals for servers.
- Mail accounts of executives and managers at utilities in PA, NJ, and GA, according to the documents.

HOW DO WE KNOW ABOUT THE ATTACK?

- UglyGorilla was using U.S. servers as staging points.
- The FBI issued subpoenas and, using specialized software, were able to watch in real-time as UglyGorilla infiltrated the system.
- The FBI was able to track UglyGorilla's hacking pathway as well as capture their passwords. UglyGorilla paid special attention to SCADA information.

LESSONS LEARNED FROM CASE ONE

- It's possible that there has been a breach even if there are no signs of attack and nothing seems to have been altered.
- Information that may not seem critical, such as an instruction manual, might be a vulnerable and valuable target.

Sources: bloomberg.com | mandiant.com | csmonitor.com

2) CASE TWO

2008 Turkey Pipeline Blast

WHEN, WHERE, WHAT

- August 7, 2008; the Baku-Tbilisi-Ceyhan pipeline in Turkey, majority-owned by BP, running from the Caspian Sea to the Mediterranean.
- An explosion on the pipeline sent flames 150 feet into the air, caused over 30,000 barrels of oil to spill, and cost millions of dollars per day in transit tariffs during the two and a half weeks the pipeline was down.
- The Turkish government reported it as a mechanical failure. However, in 2014, Bloomberg reported that hackers had super-pressurized the crude oil in the line.

HOW IT HAPPENED

- Hackers entered the operational controls of the pipeline through poor security in the video surveillance system.
- They shut down alarms and cut off communications.
- They super-pressurized the crude oil in the line, which may have resulted in the explosion; no physical bomb was ever found.
- The control room didn't learn about the blast until 40 minutes after it happened, from a security worker who saw the flames.

WHY IS THIS WORRISOME TO THE U.S.?

- 182,000 miles of pipelines carry oil and other hazardous liquids.
- 325,000 miles of pipelines transmit natural gas between states.
- 2.2 million miles of pipelines distribute natural gas to homes and businesses.

LESSONS LEARNED FROM CASE TWO

- Any digital property can be exploited to gain unauthorized access.
- Often, little attention is paid to auxiliary systems, e.g., IP-based cameras.
- The camera system supposedly watching the site was not only useless (after the hacker erased the video feeds), but indeed provided entry for the attackers!
- While we can't be sure what happened in this case, it's raised the possibility that companies may try to pass off attacks as mere accidents, and not alert others to the danger.

Sources: bloomberg.com | sourcesecurity.com | slate.com | sans.org

3) CASE THREE

2000, Australia, Maroochy Shire

WHEN, WHERE, WHAT

- Early February–late April, 2000; Maroochy Shire, a rural area in Queensland, Australia.
- 142 sewage pumping stations; each station controlled by two computers, from a central computer, using radio frequency.
- A contractor working for an Australian firm installed radio-controlled SCADA sewage equipment.
- Contractor resigned after Maroochy Shire Council refused to hire him as a full-time employee.
- He stole wireless radio, SCADA controller, and control software.
- He used the stolen equipment to issue radio commands to sewage equipment he had most likely contributed to installing.
- Pumping stations' data were altered, resulting in the following faults:
  - Pumps not running according to schedule.
  - Alarms not being reported to SCADA.
  - A loss of communication between the central computer and various pumping stations.
- As a result of the cyber attack, 800,000 liters (211,337 U.S. gallons) of raw sewage spilled out and polluted local parks, rivers, and the grounds of a Hyatt Regency hotel.
- Attack, initially assumed to be malfunctions, continued for 3 months.
- Contractor was caught at a traffic stop, with stolen equipment.

LESSONS LEARNED FROM CASE THREE

- Weak oversight and policy/procedures of contract personnel.
- Weak oversight of ICS equipment with reference to procedure/policy for issuing/tracking equipment.
- Attack was mistaken for a malfunction of pumps for weeks. For ICS, it may be difficult to attribute a malfunction to a cyber attack.
- Employees were not trained in preventing, recognizing, or responding to cyber-related incidents. Training might have helped reduce the impact of cyber attack.
- Missing or weak software security.

Sources: nist.gov | acsac.org | theregister.co.uk

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY