

# A Systems Theoretical Approach to prevent Stuxnet-like Attack

Tejas Jamdade  
jamdade.2@iitj.ac.in

Microsoft Cybersecurity Expert,  
Cybersecurity Engage 2022 Mentee  
Microsoft, India

## 1 Methodology & Assumptions

In this work, we focus on a nuclear power plant just to recall the critical infrastructure entity where it all started. This approach can be used later to identify the opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs.

## 2 Cyber Deterrence Challenges

To answer the question of whether cyber deterrence is possible, one must understand the theories or concepts behind successful deterrent strategies and how they apply to cyber. In his book *Cyber Deterrent and Cyber War*, Martin Libicki describes these options as (1) "deterrence by denial (the ability to frustrate the attacks)" or passive deterrence and (2) "deterrence by punishment (the threat of retaliation)" or active deterrence.

Following are the challenges for Cyber Deterrence:

- Attribution
- Understanding Adversary Motives and level of Risk Tolerance

### 2.1 Attribution

One of the biggest barriers of effective cyber deterrence is the concept of attribution. The complex structure of the Internet, immature political and legal policies, and global nature of the cyber domain make operating anonymously possible. Adversaries can exploit any number of system or protocol vulnerabilities to hide or spoof their location and operate from nearly any physical location. The more sophisticated the attacker, the more difficult attribution becomes. These attackers will take actions to hide their true location and make it appear that another attacker or nation-state may have conducted the attack. Technical attribution is the ability to associate an attack with a responsible party through technical means based on information made available by the cyber operation itself.

## 2.2 Understanding Adversary Motives and level of Risk Tolerance

Our ability to deter each group of cyber adversaries will vary. Cyber-criminal activity is the largest group of cyber threats and one of the most difficult to effectively deter. This group of hackers ranges in sophistication from low ability to elite-level hackers motivated by financial gain. Our ability to punish and deter this group is sometimes limited and largely dependent on law enforcement and effective cooperation from foreign nations.

## 3 Legal & Treaty Assumptions

Additionally legal and political hurdles may make attribution difficult and time-consuming, especially when international cooperation among multiple organizations, agencies, and government is required to determine the source of an attack. The current approach is unable to move as quickly and flexibly as the cyber threat and is unevenly applied geographically. Too many countries with nuclear materials or high consequence nuclear facilities lack appropriate legal and regulatory frameworks in this area. Finally, cyber-security strategies tend to rely on technological measures like air-gaps, firewalls, and antivirus tools that have been proven fallible to the execution to the exclusion of other, perhaps more effective measures.

## 4 Stuxnet

The Stuxnet worm is a sophisticated malware designed to sabotage industrial control systems (ICSs). It exploits vulnerabilities in removable drives, local area communication networks, and programmable logic controllers (PLCs) to penetrate the process control network (PCN) and the control system network (CSN). Being a sophisticated malware agent it was part of a multi-stage attack, which is outlined in Figure 1. The initial stage called for the development of computer code called a beacon created a network blueprint, or map of the Natanz plant, to detail how the computer systems controlled the centrifuges. Duqu, a data-stealing piece of malware, is believed to be the reconnaissance agent used to map the Natanz computer network in 2007. Once the mapping task was completed, the beacon covertly reported home on its work, through the Internet, using the networked computers to which it had spread. This covert data transmission, sent back to the Stuxnet command and control servers in Malaysia and Denmark, was facilitated through two bogus websites set up cleverly to disguise the web traffic as legitimate soccer fan activity through "*mypremierfutbol.com*" and "*todayfutbol.com*". In the later stages, the Stuxnet worm modified the code running the facility's PLCs to change their programmed operations. These PLCs controlled the precise speed needed to spin the centrifuges used for uranium enrichment properly. Stuxnet caused the centrifuges to spin off speed and out of control, while at the same time, reporting false data to the operators that operations were progressing normally.

## 5 Solution Architecture

After Stuxnet it's clear that what threat an advanced cyber attack can have to critical infrastructure systems including utility organizations. With the risks to utility services and the possibility of a cyber incident seemingly lurking both inside and outside the networks of utility plants across the nations, what to do for securing specific infrastructures? Proper

governance including policies and procedures are extremely important, but without the wise application of mitigating preventative and detective technical control; mission critical systems will remain insecure. The methods given below are not unique ideas to the utility control system environment, these are just the variation of existing methods that are required to mitigate the possibility of a Stuxnet-like attack:

- Restrict the use of USB media other portable storage devices and enforce encryption of sensitive data.
- Air gap control system networks where possible and restrict connection points to other networks using specialized firewalls and/or one-way data transmission devices.
- Utilize a rigid and methodical procedure for moving code to and from production networks and control systems.
- Make use of a dedicated source code management system for control system/PLC code allowing for version control (like Git) and rollback to a known good version when unexpected behavior occurs after a modification is made.


While restricting the use of USB storage devices prevents one entry vector for a threat such as Stuxnet, for isolated networks such as the air gapped control systems used in nuclear power generation facilities the use of portable storage media is one of the only ways to move data between physically separate networks. One possible method for risk reduction for portable storage media is to use WORM (write-once-read-many) storage for backups. Another possible procedure for minimizing the risks introduced by the USB storage media would be to perform a low level format of all USB devices on a stand-alone computer running a boot-able operating system such as Knoppix Linux.

Below are the methods or approaches that address the security issues in a CPS:

- Identifying hazards-a situation with the potential for creating damage
  - Hazards related to actions: undesirable system actions are taken or desirable system actions are not taken
  - Hazards related to timing: A desirable system actions is performed too soon or too late
  - Hazards related to sequence: A desired action in a sequence of actions is skipped or the actions in a sequence are performed out of order
  - Hazards related to amounts: A desired action is performed too much or too little.
- Quantifying risks-the likelihood of a specific effect within a specified period
- Determining components safety measures

## 6 Prototype

### 6.1 AES-128

As handling of sensitive data is an important step in reducing the risk from a Stuxnet-like attack, I have implemented a research paper of AES-128 which is written purely in python (not included any external libraries). Check it out here: [AES-128](#) 

---

## 6.2 Packet Analyzer

I have also tried implementing a packet analyzer which as of now is able to count the number of packets in a given 'pcap' and find the number of interesting packets (considering all IPv4/TCP packets as interesting) Check it out here: [Packet-Analyzer](#) 