

Case Studies on Cyber Attacks

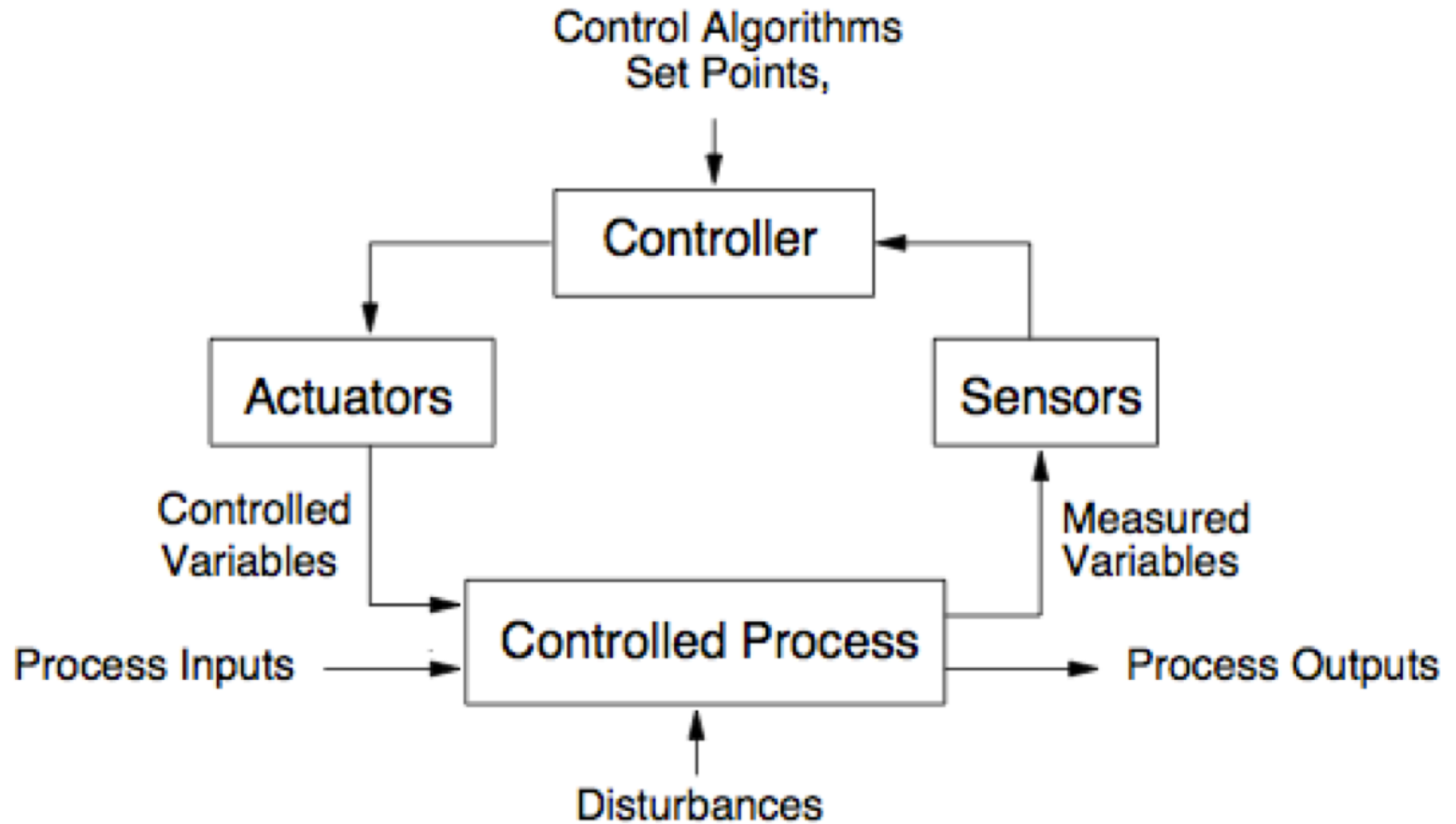
Varun Kumar
Deputy Director
NPTI

STUXNET

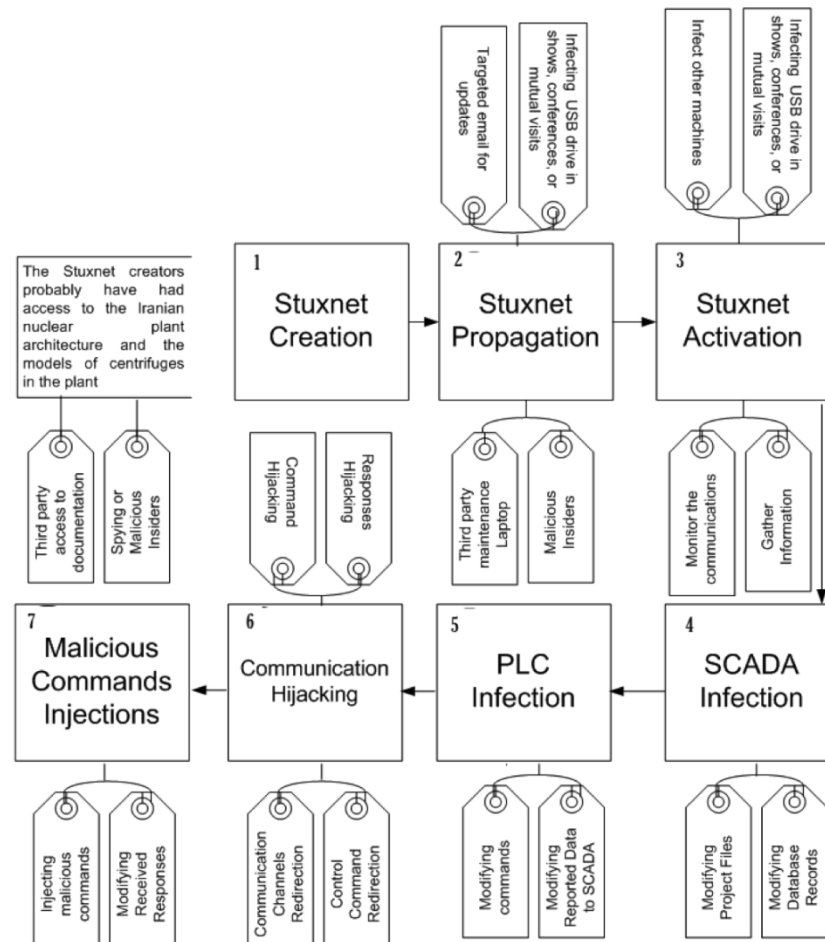
- Stuxnet reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines.
- Traveled on USB sticks and spread through Microsoft Windows computers.
- Virus searched each infected PC for signs of Siemens Step 7 software, which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment.

- After finding a PLC computer, malware updated its code over the internet and began sending damage-inducing instructions to electro-mechanical equipment, the PC controlled. At the same time, virus sent false feedback to main controller.
- Anyone monitoring the equipment would have had no indication of a problem until equipment began to self-destruct.

Simple Control Loop

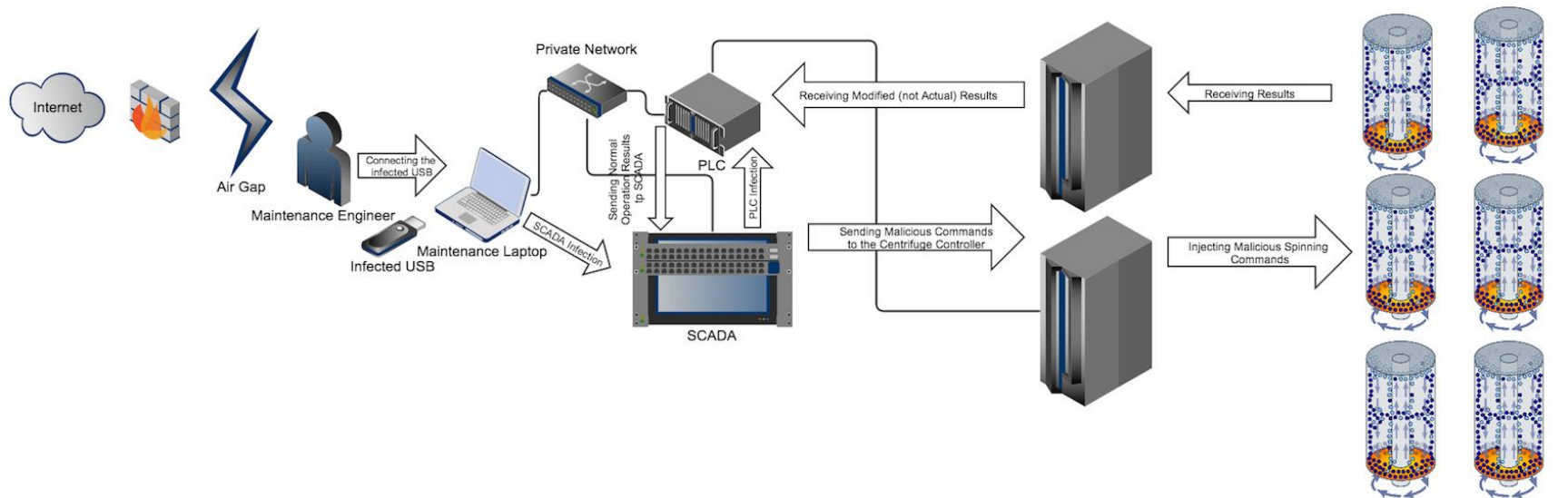


Stuxnet Attack Process



- Inside a uranium enrichment infrastructure, PLCs are responsible for controlling centrifuges. As each PLC is configured uniquely, configuration documentations are needed for any type of targeted attacks.
- In the case of Stuxnet, possible ways of accessing these documents were either by manufacturers, an insider, third party contractors or even snooping malwares that are designed specifically to gather information about an ICS.

Stuxnet Attack Diagram



- As the targeted uranium enrichment infrastructure was air-gapped (i.e. no cyber connections to outside world), propagation of Stuxnet was probably done whether through a USB drive or other infected external devices. Once the infected USB was connected to the maintenance laptop, Stuxnet was activated and infected all the network devices particularly printers, computers, database servers, and application servers.
- Stuxnet also infected major systems components ranging from SCADA to sensor readers .
- Original data flow from controllers to centrifuges was modified by the Stuxnet and these modification were not detected by safety measures in place.

- Stuxnet targeted Siemens S7/WinCC products that were commonly used in Iranian uranium enrichment infrastructure.
- PLCs in the S7 product were the target element exploited to launch the attack.
- To achieve this goal, Stuxnet utilized 3 zero-day vulnerabilities on Microsoft Windows operating systems to gain root access required for manipulation of PLCs.

- 1) secretly recording normal operations for a full operation cycle,
- 2) playing the recording back to the controllers to maintain the appearance of a legitimate entity,
- 3) infecting other computers, and
- 4) maintaining the list of infected computers, monitor spread, and determine success in infecting attacked computers.

- Utilizing the WinCC database connections was another technique for spreading the malware. In this technique, the connection is used to infect the database. Once a database is infected, further connections to the database by other machines infected them.

- Targets : SCADA, web-servers(used to report some statistics to remote clients on the same network), sensors/Network adapters firmwares, CAS (central archive server), and database servers.
- Utilizing the information gathered during the probe-phase, Stuxnet replaced the legitimate modules of both functional and software components with illegitimate ones. Such modules were executing the commands designed by Stuxnet designers while reporting something else to the operators and informing them that their commands were successfully executed.

Colonial Pipeline Attack

- Attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication in place.
- Some \$2.3 million in crypto currency ransom paid by Colonial Pipeline.
- Goal was not to disrupt the economy by taking a pipeline offline but to hold corporate data for ransom.
- Most visible effects — long lines of nervous motorists at gas stations.

Cyber Attack on Nuclear Power Plant

- Malware infection on KKNPP administrative network used for day to day administrative activities.
- Affected system contains data related to administrative function.
- Plant control and instrumentation system is not connected to any external network such as Intranet, Internet and administrative system.
- Malware infection was not able to get access to the controls of the Nuclear Power Plant.

- Investigations have been carried out by Computer & Information Security Advisory Group (CISAG) – DAE along with the national agency, Indian Computer Emergency Response Team (CERT-In).
- The investigation concluded that the malware infection was limited to the administrative network of KKNPP.

Black Energy 3

- On 23 December 2015, hackers remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers.
- 30 substations were switched off, and about 230000 people were without electricity for a period from 1 to 6 hours.
- Prior compromise of corporate networks using spear-phishing emails with Black Energy malware.

- Seizing SCADA under control, remotely switching substations off.
- Disabling/destroying IT infrastructure components (uninterruptible commutators).
- Destruction of files stored on servers and workstations with the Kill Disk malware.
- Denial-of-service attack on call-center to deny consumers up-to-date information on the blackout.

Solar Winds Attack

- Deployment of malicious code into its *Orion IT monitoring and management software* used by thousands of enterprises and government agencies worldwide.
- Supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly.

- September 2019 : Threat actors gain unauthorized access to SolarWinds network
- October 2019 : Threat actors test initial code injection into Orion
- Feb. 20, 2020 : Malicious code known as Sunburst injected into Orion
- March 26, 2020 : SolarWinds unknowingly starts sending out Orion software updates with hacked code.

- Even government departments such as Homeland Security, State, Commerce and Treasury were affected, as there was evidence that emails were missing from their systems.
- Private companies such as FireEye, Microsoft, Intel, Cisco and Deloitte also suffered from this attack.

ISGEC Heavy Engineering Ransom ware Attack

- On 7th June 2022 at around 6.55 am, IT Team noticed that servers are encrypted.
- This type of malware is a fraudulent money-making scheme that can be installed by deceptive links in an email, instant message, or website. It can lock a computer screen or encrypt crucial, predefined files with a password.

- 1) Periodic backup of data to be taken. If data is critical, it must be backed up daily. Alternately, weekly full backup with daily incremental backup; In case of any ransomware attack, the previous day's clean backup must be restored.
- (2) Secure network architecture by putting the database in a secure zone behind DMZ.
- (3) Implementation of IPS/IDS/hardening of firewall with all logs on.
- (4) Having the latest licensed Anti-Malware with scanning of each and every mail and data item.

- 5) Blocking all USB ports except desired ones
- (6) Blocking all not required services/ports
- (7) Regular patching
- (8) Creating awareness amongst users to (a) identify phishing/spam/ malicious mail; (b) not to use pen drives/other-media to copy data/programs; (c) not to visit undesirable websites; (d) incident reporting; (e) cyber hygiene.

- (9) Defining risk mitigation for malware/ransomware in business continuity plan (BCP) and regular drill.
- (10) In a critical data center, monitor all data traffic using Security Operations Center (SOC).

References

- www.reuters.com
- www.kaspersky.co.in
- attack.mitre.org
- www.mcafee.com
- pib.gov.in
- IEEE Transactions on Dependable and Secure Computing