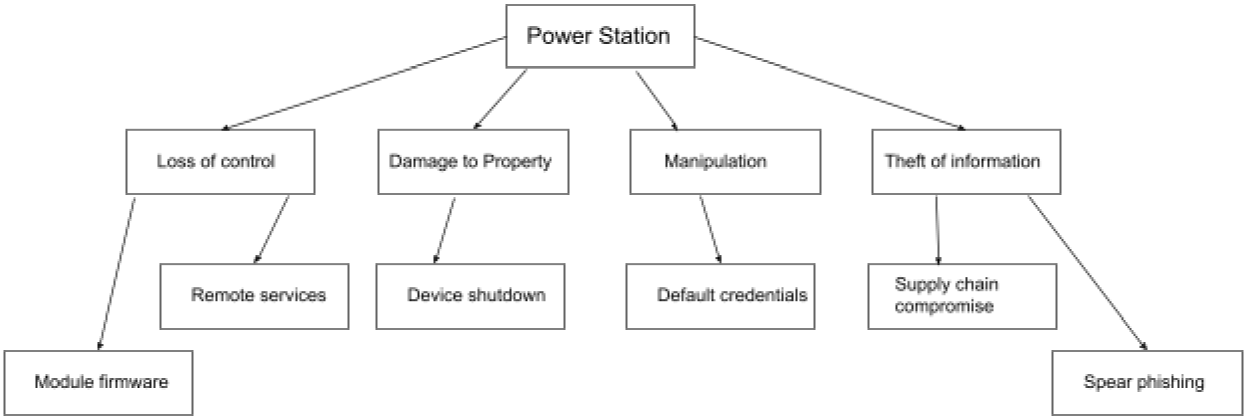
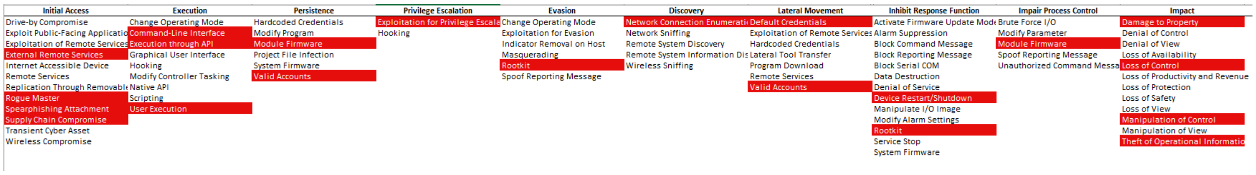
Unit 4 seminar preparation - Threat modelling exercise

A Large Nuclear Power Station in France

Attack Tree for identified threats to ICS in Critical Infrastructure (Mitre Att&ck, 2022)



Mitre Attack layer Simulation



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escala	Change Operating Mode	Network Connection Enumerati	Default Credentials	Activate Firmware Update Mod	Brute Force I/O	Damage to Property
Exploit Public-Facing Applicatio	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Dis	Lateral Tool Transfer	Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Block Serial COM	Unauthorized Command Messa	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Data Destruction		Loss of Productivity and Revenue
Replication Through Removabl	Native API					Valid Accounts	Denial of Service		Loss of Protection
Rogue Master	Scripting						Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Manipulate I/O Image		Loss of View
Supply Chain Compromise							Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset							Rootkit		Manipulation of View
Wireless Compromise							Service Stop		Theft of Operational Informatio
							System Firmware		

Mitre Attack layer Simulation representing the vector of attack to cause Loss of control, Damage to property, Manipulation and theft of information (Dragos, 2022).

<u>Mitigations</u> would be to ensure data transfer is using one directional gateways, segmented network infrastructure, DMZ, air-gapped systems, cuckoo sandboxing for emails, ensure software bill of materials is in place for supply chain, all default passwords and credentials are changed immediately, access controls and MAC identification, Endpoint detection running on all non-air gapped assets, SIEM system is in place and collecting logs for analyzing, Safe ethernet cables are tested for malware and used.

References

Dragos Inc (2022) Developing a converged threat model using mitre att&ck. Available from: https://www.dragos.com/resource/developing-a-converged-threat-model-using-mitre-attack/ [09 Accessed]

Mitre ATT&CK (2022) ICS Matrix.Available from: https://attack.mitre.org/matrices/ics/ [Accessed 10 December 2022]