Threat Modeling in ICS Environments

SSgt Jake Marullo
SSgt Brandon Grimes

Marine Corps Cyberspace Warfare Group(MCCYWG)
Individual Mobilization Augmentees (IMA) Detachment

4 November 2020

MOSAICS
2020
INDUSTRY
DAY

Marine Corps Forces Cyberspace Command Presenters

SSgt Marullo – MCCYWG IMA Detachment, OT/FRCS Cybersecurity Team Lead. SSgt Marullo has over 18 years of cybersecurity experience. In his civilian capacity, SSgt Marullo is the OT Cybersecurity Leader for Rivian Automotive.

SSgt Grimes – MCCYWG IMA Detachment. SSgt Grimes is the Deputy Chief the ICS Section within CISA's Threat Hunting Subdivision. This team provides ICS Hunt and Incident Response services, SME support, and research collaboration to both public and private partners. SSgt Grimes began his career in ICS at Ft. Drum, NY supporting the garrison's building management and water/energy telemetry systems.

MOSAICS
2020
INDUSTRY
DAY

2019 Worldwide Threat Assessment

Office of the Director of National Intelligence

Russia. Russia poses a cybersecurity threat to the United States and our allies. It is a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve political and military objectives.

China. China presents a persistent cyber threat to our military and CI. It remains the most active strategic competitor responsible for cyber espionage against the U.S. Government, corporations, and allies.

Iran. Iran continues to present a cyber threat, using increasingly sophisticated techniques to conduct cyber espionage and deploy capabilities that would enable cyber attacks against CI in the United States.

North Korea. North Korea poses a cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks.

Non-State Actors. Foreign cyber criminals, terrorists, and others will continue to conduct malicious cyber attacks to further their goals, aided by the growing availability and use of publicly available cyber tools.

MOSAICS 2020 INDUSTRY

MITRE ICS ATT&CK Framework

MITRE ICS ATT&CK Framework is a comprehensive register of adversarial tactics and techniques from initial access to adverse impact

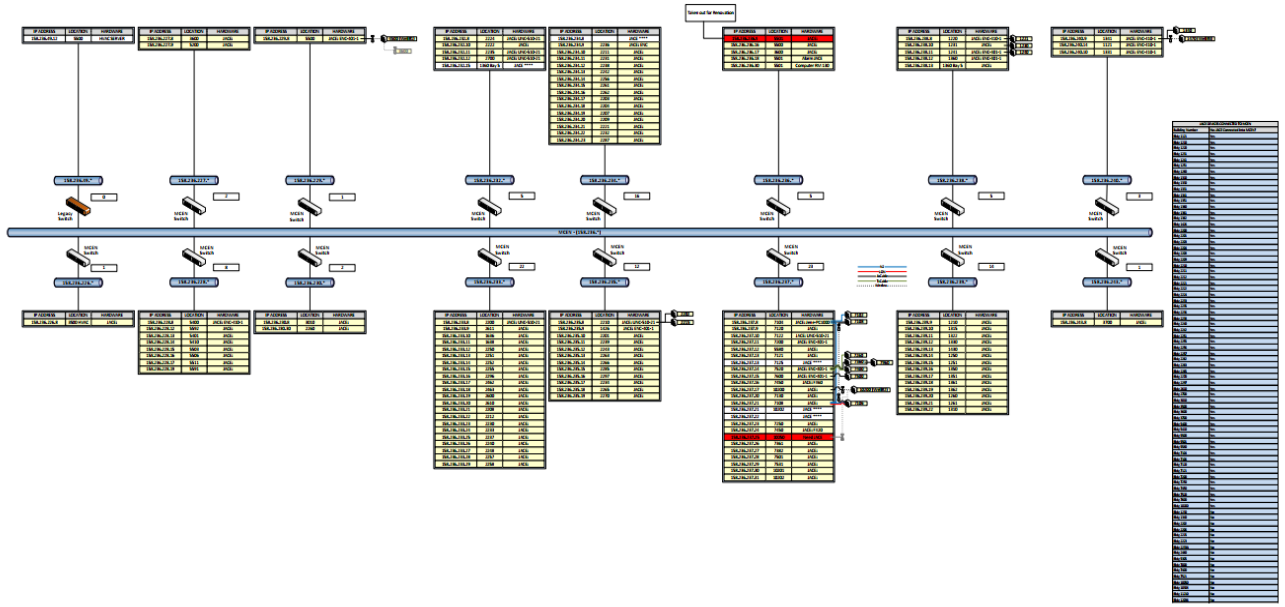
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

MOSAICS 2020 INDUSTRY DAY

Marine Corps Logistics Base (MCLB) Model Site Survey

Purpose: To gain a detailed understanding of our network architecture to better understand our attack surface and inform our defensive requirements.

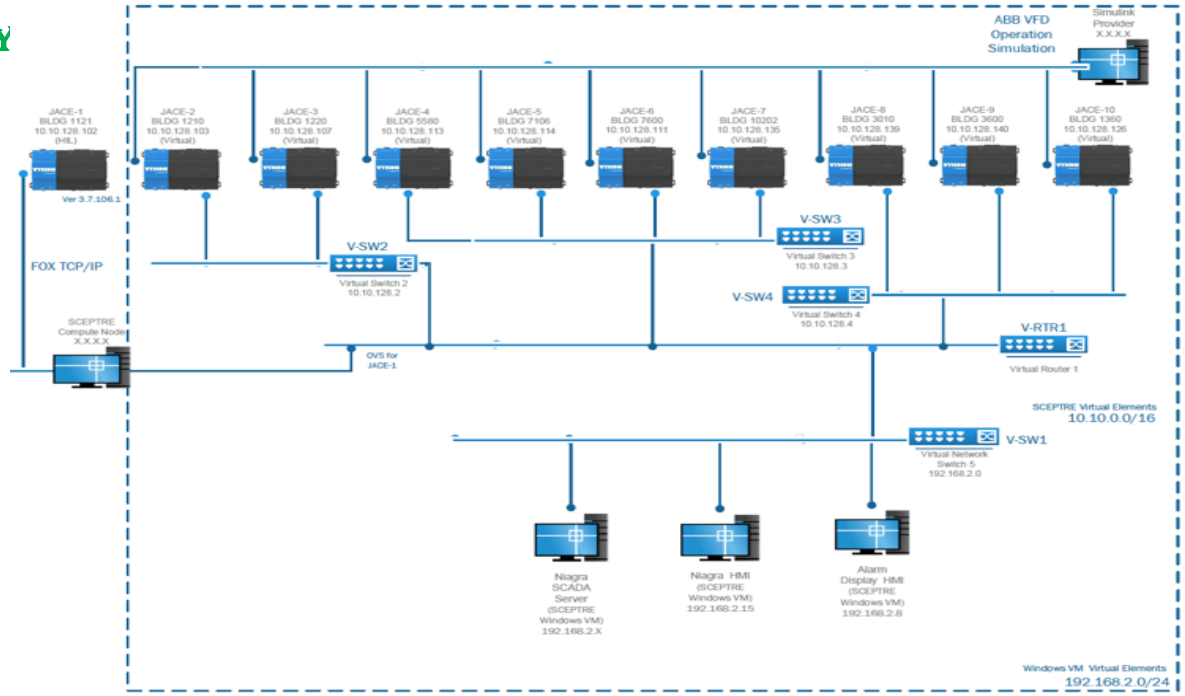
MCLB Albany DDC Network Components and Connections



- Heating and cooling system for each building (x9)
- ABB VFD's (variable frequency drive)
- Java Application Control Engine (JACE) Controllers (PLC)
- Niagara Software
- Simulation environment endpoints - Simulink

MOSAICS 2020 INDUSTRY DAY

Process Modeling with SCEPTRE



USMC Albany SCEPTRE Model: What is it?

- SCEPTRE - Virtualization government owned software which provides a comprehensive ICS/SCADA modeling and simulation capability that captures the physical impacts of targeted cyber events on critical infrastructure and control systems.
- SCEPTRE uses Minimega as its virtualization backend.

What will it deliver?

- A flexible, close fidelity IT/OT network model with hardware in the loop
- Training environment for CPTs to better understand OT protocols, vulnerabilities and physical effects of cyber attacks
- Can be expanded to more complex simulated IT/OT networks

MOSAICS
2020
INDUSTRY
DAY

Next Steps

- Leverage MITRE ICS ATT&CK to conduct realistic attack scenarios
- Attack systems within model in order to disrupt the physical process, learning impact consequences
  - Compare effectiveness of security controls and solutions
- Define core competencies for network defenders
- Present findings and data to USMC Network Governance Board
  - Cost-effective approaches to risk mitigation
  - Define requirements based on tangible risk and criticality