Security and Safety of IIoT

Overview

Vulnerabilities are present everywhere throughout variety of systems, regardless of a system’s scale of operation, data capacity and network traffic volume. A small blunder or mishap in certain parts of a system could set the domino effect into motion that’ll greatly implicates other parts of an intricate system. This unfortunate turn of event would gradually drag the system’s performance and expose the bulk of the system to outside breaches that such the chain reaction of system malfunctions might also be orchestrated and caused by third-party interference. In short, even a slight mistake or distortion could cripple an impenetrable, impregnable and security-critical system causing influxes of trust issue among the clients and employees of such a “horridly-desingned” system so as not mention the huge repair bills amounting on the desk of the executives. Similar things could be uttered for IIoT, since it’s fundamental idea is to heavily relied on high-degree of interconnection between the sets of sensors, actuators and etc. The very concept of the IIoT could be used to go against it, as smart devices dependent on constant feedbacks from other devices to cooperate and operate, the attackers could exploit it to the fullest by either by severing the connection between the interconnected devices or sending false data feedbacks to the devices or eavesdropping on the communication between the devices to attain vital data so that it can be used for further attacks.

Cyber threats are mainly targeted at the Industrial Control Systems (ICS), such as the Sitributed Control Systems (DCS); Supervisory Control and Data Acquisiotion (SCADA) systems; Programmable Logic Computers (PLC) and Human Machine Interfaces (HMI). Furthermore, following the introduction of IP-based connectivity to be used as the communicational link between multiple industrial devices has drastically elevate the concerns regarding security risks. This ever increasing and creeping possibilities of threats had caused numerous distrust amongst the oil giants to integrate and enhance their operations using IIoT concept since the unknown was not made clear and encountered effectively. If the situation remains, this could haphazardly jeopardize the chances of technological improvements and benefits that could be bring forth by the wave of IIoT integration so as to hinder the IIoT future breakthroughs altogether. So to speak, on public level, this situation appeared to be not needing any desperate urge or massive widespread of awareness as it wouldn't directly effect the mass public, but still on the hindsight or according to human developmental view, this situation is perilous on it's own unique way. This part of the report would descriptively discuss on countermeasures or techiques that were suggested by the IT professionals or know-hows so that the knowledge could be applied and implemented to combat malicious and endearing cyberattacks on IIoT infrastructure and it's incorporated devices.

Recent Attacks on Oil and Gas Industry Major Players

-Attacks on Rosneft and other oil giants

A known and well-positioned Russian O&G Moghuls, Rosneft and Evraz were recently became victims of a massive cyber attack conducted by anonymous group of hackers who sought for unknown intents or motives. The attack caused Rosneft's company servers to go abuzz, luckily the attack doesn't inflicted any physical damage or distrupted it's oil production capability. The malicious code named NotPetya was the culprit as it infiltrated the servers, demanded ransom to be paid in order to regain acces to the system. The Petya variant, NotPetya commonly targets Microsoft Windows-based systems, the ransoware infected the master boot record to execute a payload that encrypts a hard drive's file system table and prevents the Windows from booting or shuting down. This ransomware troublesome appearance scouts a never-ending and impeding problem for companies across the world and uncover the baffling question to fully ensure the safety of corporate data of accumulated by companies.

IIoT security measure applied by GazProm Neft

IIoT security measure applied by Exxon

IIoT security measure applied by Chevron

Threats, Countermeasures and Preemptive Preventation Approaches



Threats :

a) Man-in-The-Middle :

Happens when an attacker manages to breach, interrupt and spoof communicational links between two systems. In the reality of an IIoT scenario, an attacker might be able to assume control of a smart actuator and knock an industrial robot out of it's designated lane and speed limit - which will arises the potential of damaging an assembly line or injuring operators who're supposed to maintain the machine's integrity.

b) Device Hijacking :

Actively happens when the attacker hijacks and assumes the control of a device effectively so as holistically. This type of attack is highly difficult to be detected prematurely due to the action the attacker to not change the basic functionality of the device. Furthermore, the potential to might as well reinfect other unaffected devices as very likely, for example, smart meters that are connected to the grid. Generally, according to an IIoT scenario; a hijacker could gain enough control of a smart meter and utilize the compromised device to launch staunch ransomware attacks against Energy Management Systems (EMSs) or illegally siphon unmetered power lines.

c) Distributed Denial of Service (DDoS) :

A denial-of-service varaint of attack (DoS attack) in hope to render a machine or network resource to be unavailable or unrecheable to its intended users by temporarily or indefinitely distrupting services of a host connected to the Internet. In the case of a ditributed denial-of-service attack (DDoS), influx of traffic flooding a target originates from multiple unclarified sources, elevating the difficulty to abruptly halt the cyber offensive by simply blocking a single source. DoS and DDoS attacks can negatively affect a wide range IIoT applications, causing critical distruptions for utility services and manufacturing facilities.

d) Permanent Denial of Service (PDoS) :

Permanent Denial-of -Service attacks (PDoS), briefly acknowledged as phlashing, is the type of an attack that ruthlessly inflicts damage of a device that it the only plausible solution is to substitute or reinstall the hardware. There is one particular example of a hazardous malware that is capable of disabling critical equipment on a factory floor, that is available in wastewater treatment plant, or in an electrical substation, BricekrBot, was coded to to exploit hard-coded passwords available in IoT appliances and cause long-lasting if not permanent denial of service.

Countermeasures and preventations

All of the infrastructure in relation to IIoT have to be shielded using a cyclopedic security solution (device-to-cloud) that doesn't wreak out any distruption to the operations, amenity, dependability or economic accountability. Rather than opting for a 'super solution' that horribly unsuccessful in gaining any noteworthy traction, a more profound, simplistic, yet secure solution that is able to be incorporated vastly and with ease by IIoT operators and their respective amenities is extensively more acceptable. The capabilities that should be present in a solution follows :

i) Firmware robustness and assured boot

To make sure that an aplliance does only run code synthesized by the appliance OEM or another trustworthy party, the secure boot has to apply cryptographic code signing techniques. The practicality of of implementing the utilization of assured boot technology inadvertently stops hackers from substituting firmware with malevolent instruction sets, abruptly eliminating any attempt of attacks. Sadly, there are some of IIoT chipsets aren't equipped with secure boot capabilities. Generally, it is crucial to assure that IIoT appliances can only establish communicational link with authorized amenities to prevent any endangering possibility of substituting firmware with spitful instruction sets.

ii) Reciprocal authentication

Before receiving or trasmitting data, a smart actuator will tries to establish a connection to the network, so every time the smart actuator attempts to do that, it should be authenticated. This practical countermeasure safely assure the data is coming from a legitimate appliance and not an illicit source.

iii) Assured Communicational link (end-to-end encryption)

iv) Safeguarding surveilance and inspection

v) Security lifecycle management

[Insert a diagram here]

Reference

<https://www.computerweekly.com/news/252443327/CDO-interview-Andrei-Belevtsev-Gazprom-Neft>

<https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/>

<https://www.rambus.com/iot/industrial-iot/>