IDENTIFYING THE VULNERABILITIES OF INDUSTRIAL-IOT FIELD DEVICES

By Michelle Nadboy | June 16, 2016

THE GROWTH OF INDUSTRIAL-IOT DEVICES

The Industrial Internet of Things (IIoT) industry is growing at a rapid pace. By year-end 2015, an estimated 13.4 billion IoT connected devices had flooded the global market. The number of connected devices is forecast to reach 38.5 billion by 2020.[1] But why are so many companies working to develop IIoT devices? Because most industrial processes are not fully automated, they are capital and labor intensive and need to find an effective way to identify network issues and improve performance. The main draw of IIoT devices is that they can improve safety, reliability, and energy efficiency. These devices integrate sensors that gather real-time or continuous data and connect to data analytics and control systems. Analyzing data trends is essential for delivering actionable insights in order for utilities to prioritize network upgrades or monitor supply-demand mismatch. The smartest solutions not only offer data analytics software, but also integrate with existing software and industrial control systems (ICS).

For example, sewer water levels can be monitored and programmed to send real-time alerts when the water level has reached a predetermined threshold in order to prevent combined sewer overflow (CSO) events. Sensors can also be installed inside different types of equipment to monitor if measured parameters exceed predetermined thresholds. This enables predictive maintenance – maintenance that can be scheduled before an equipment failure occurs, which prevents expensive equipment replacements or repairs. Agriculture applications can monitor soil moisture levels, humidity, and pesticide usage. Farmers can use this data to implement optimal crop growing conditions.[2]

These examples are illustrative of how IIoT devices can optimize operations for the user. But connecting devices also creates a network vulnerable to attack and compromise.

Image 1: Cyber Attacks on Utilities Can Result in Contaminated Water

As the number of connected devices increases, so do potentially devastating cyber threats. Cyber threats on critical infrastructure can have far more damaging and widespread effects than individual terror attacks. A common method of attacking consumers using ransomware, a type of malware that infects a computer and limits users from accessing the system until they pay a ransom. The Internet Crime Complaint Center reported that from April 2014 to June 2015, damages caused by ransomware alone cost companies $18 million.[3] Ransomware attacks primarily target consumers and therefore result in individual and financial damages. However, attacks on critical infrastructure could cost billions and cause far greater damage. An intentional shutdown or tampering with critical infrastructure data could result in power outages, toxic water levels, along with a communication shutdown preventing emergency response. The rising concern is a twofold attack, while emergency workers are responding to a water main break, hackers can attack a power plant and leave an entire city in the dark. Security experts continue to implement cyber defense strategies. However, with the increasing risk of cyber wars no strategy is completely secure.

THE COST OF CYBER THREATS

Three decades ago, malicious activity and cyber attacks were rarely an issue. But now threats have become a reality and cyber-security has become an absolute necessity. A recent study published by the Atlantic Council and the Zurich Insurance group estimates that cyber attacks could cost up to $90 trillion by 2030 if cyber-security fails to advance at a rapid pace.[4] Therefore, every IIoT company should be aware that their device can serve as a backdoor to an industrial control system.

ICS or Supervisory Control And Data Acquisition (SCADA) systems are extremely vulnerable, as they are the brain of critical infrastructure. Surprisingly, companies still create devices with insufficient security technology, lacking even basic features such as authentication and authorization.

> ***Without proper security, attackers can use these devices as an entry point into the SCADA system. Once the SCADA system is compromised, the attackers can leak critical information and even reconfigure the programmable logic controllers (PLCs) to cause significant damage.***

For example, in a water utility this could be executed by setting the water network to a very high pressure, resulting in network-wide pipe leaks and main breaks. False low sewer water level data could be transmitted, resulting in CSO events which would flood the streets and result in public health and safety risks and heavy regulatory fines.

Even with cyber defense on the rise, there have been many more documented and undocumented attacks. There were over 160,000 reported attacks on SCADA systems worldwide during 2013 and over 675,000 attacks in 2014. Many of the attacks were carried out by exploiting simple buffer overflows (e.g. feeding more data than the system's temporary memory storage could hold), which can result in corrupted data, a program crash, or cause the execution of malicious code. The number of unreported attacks is potentially significantly greater, as most companies are only required to report data breaches that compromise payment or personal information.[5]

The threats to critical infrastructure are increasing, especially on infrastructure controlled by ICS. As our world becomes more connected, the potential scale of damage to critical infrastructure begins to boggle the mind. In 2003, the infamous Northeast Blackout left 50 million people in eight states without power. It cost around $6 billion and resulted in 11 fatalities.[6] The power outage was caused by a software bug. Imagine the severity and scale of damage that could have transpired had the blackout been caused intentionally by a hacker.

SECURING AN IIOT DEVICE

As an IIoT company, Ayyeka developed a device that incorporates current best practices in cyber-security. This paper will cover the key steps to securing an IIoT devices and understanding device vulnerabilities. These include: embedding cyber-security into the IT architecture, securing communication protocols, and implementing additional security measures for delivering data to SCADA systems.

The most basic security level is to install a firewall along with an intrusion detection system (IDS). Humans cannot be programmed to detect when a suspicious person is looming on their property, but firewalls can. A firewall is run by security rules that control the incoming and outgoing network traffic as protection from unauthorized attackers.

The next step is to encrypt sensitive data. For utilities, it is a given that hackers will try to intercept the communication from field devices. Therefore, it is crucial to think like a hacker and identify the weakest link in the network and implement additional security measures. For example, encrypt all communications between field devices and the SCADA system.

INVESTING IN CYBER-SECURITY

Devices that communicate from the field to a SCADA system create an entry point into the SCADA system. The most notorious example of a digital weapon attacking a SCADA system was a malicious virus known as Stuxnet. The virus silently took over Iranian uranium enrichment plant for over a year without being detected. Stuxnet manipulated the SCADA system and damaged the centrifuges as well as the enrichment process. Many believe the attack was carried out via infected USB drives, clearly demonstrating the vulnerability of SCADA systems.[7] After the attack made headlines, world leaders began to worry about their own critical infrastructure and started to implement cyber-security task forces to regulate security requirements.

Although these issues are under the radar for some private companies, the U.S. Federal Administration is investing in and enforcing stringent cyber security regulations which will quickly spillover into the private sector. In the U.S. alone, the 2016 proposed national cyber-security budget has reached $19 billion.[8] The budget includes a proposal for a National Center for Cybersecurity Resilience where companies and organizations can test security measures by initiating a cyber attack on a replica power grid, investing in enhanced cyber-security, and securing the

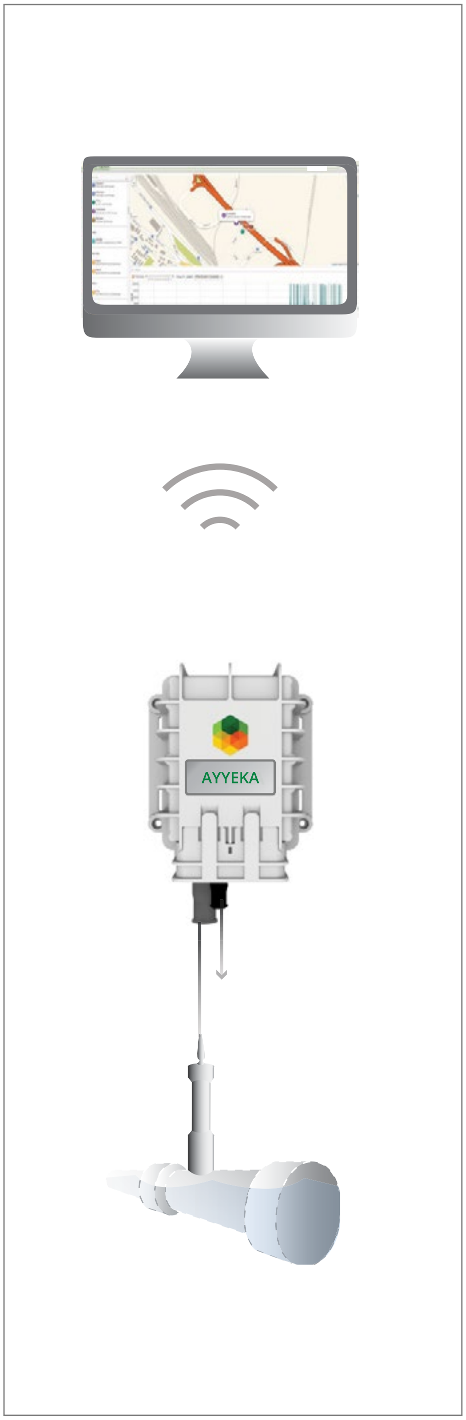

Image 2: Ayyeka's Schematic Diagram

personal data of its many citizens. While government is taking a more proactive approach, cyber attackers continue to become increasingly sophisticated. Cyber attacks come in many forms.

After an IIoT company secures all the endpoints, the next step is securing the data. For example, in a water treatment plant, attackers could inject false chlorine readings and then feed the false data to the SCADA system. It is very difficult to detect tampered data, which is why critical infrastructure operators need to implement preventative security measures. A useful tool for preventing false data injection is an automated system to detect suspicious activity. For example, when monitoring drinking water, if the pH level spikes, the chlorine levels are likely to drop. Machine learning algorithms can automatically learn such relationships between various parameters and warn if one parameter deviates from its expected behavior.

Image 3: IIoT Best Practices: Sensor Fingerprinting

CLOUD STORAGE AND REVERSE ENTRY POINTS

While cloud storage is the most common data storage method in the consumer market, many industrial end users prefer to bypass third-party cloud storage and ensure the data is securely stored and delivered from field devices to their closed networks or SCADA systems. This can only be achieved by investing in cyber-security and ensuring seamless SCADA integration for end-users. Some government offices worry about the security of cloud storage when considering the damage that could result if the data was accessed by someone intending to do harm. For this reason, companies should offer secure data transmission with on-premises servers in addition to cloud storage. Non-critical data can be viewed on the cloud and used as an auxiliary system, entirely outside a SCADA system.

IIOT DEVICES: A STEP BY STEP SECURITY STRATEGY

It is critical to develop multi-layered cyber-security solutions that reduce the risk to the ICS. IIoT devices that deliver data to ICS need to have a communication pathway that is secure and difficult to intercept. Ideally, devices should not be connected via a fixed IP address and wait for incoming connections – such devices are sitting ducks begging to be infiltrated. Instead, devices should use dynamic IP addresses and initiate the data sessions to the SCADA system only when needed. The logic is simple – it is easier to protect the SCADA side from malicious incoming connections than it is to protect the device side.

Authentication is just as important; it guarantees that unidentified devices cannot intercept the communication. An additional level of security is restricting the device's communication to short intervals and as soon as the data transmission is complete, the device shuts off the communication chanel. Hackers looking to attack a field device would have a narrow window to do so. They would need to call into the private network at the right time, successfully proceed past authentication, and decipher the encryption, which is difficult to acheive.

ENDPOINT SECURITY FOR CELLULAR IIOT DEVICES

Endpoint security is just as important for IIoT devices. The device must meet certain criteria before transmitting data to an internal server or cloud storage. Since many IIoT devices communicate over cellular networks, they use SIM cards. Many end users rely on cellular operators to provide them with a 'secured' Access Point Name (APN). They assume the information is secure and therefore do not encrypt their data. But how can one secure something one does not control? APNs lack full security monitoring capabilities, thus securing the endpoints and encrypting the data is vital. If an unauthorized user gains access to the SIM card, they could easily access all the devices under the same APN.

IIoT is built upon a device to device communication, or Machine to Machine

(M2M) communication. Sensors enable us to measure and monitor almost anything. Integrating sensors with IIoT devices enables equipment (like a water tank) to become a smart device and transmit data to an internal server or cloud based software.

When considering reverse entry points to ICS, many overlook the vulnerability of sensors because they have yet to be reported in malicious attacks. A cyber attacker can easily uninstall a sensor from an IIoT device and reinstall a malicious sensor to feed false data to the control system. Worse yet, an attacker could use the sensor as an entry point into the SCADA system and carry out an attack and damage critical infrastructure. The best way to protect the sensor is through sensor fingerprinting, which provides an additional layer of authentication. Moreover, sensors with built-in alarms can be programmed to send an alert anytime a sensor is tampered with. These two security features are designed to prevent unauthorized users from accessing or tampering with the sensor.

BEST PRACTICES IN CYBER-SECURITY

Cyber-security is not a one-time investment. Each and every utility and critical infrastructure operator needs to take into account every device that has communication capabilities. Cyber protections require a holistic approach; a customized solution should be designed for each utility and operator. It begins with assessing every component in the internal network and identifying the devices with communication capabilities supplied by external vendors.

Ayyeka researches and invests in implementing best practices in the IIoT industry: this includes encrypting data, using a private network or subnet for field deployed devices, authentication, minimizing the usage of the device's communication channel, restricting the communication between the device and the ICS, and securing the sensor. Security features should be designed to protect the SCADA system and to secure every connection point where data is being collected and delivered. Today, more advanced sensors are being developed and integrated with autonomous IIoT devices. Cyber-security must evolve and anticipate more sophisticated and creative attacks.

There are currently over 13 billion connected devices operating in the field; each device likely has at least one loophole or backdoor that could serve as an entry into critical infrastructure data. Therefore, we have a pressing need to secure all these devices before we continue to flood the market with additional IIoT devices.

> ***Advanced cyber-security practices need to be implemented now; before we reach a point of no return, with the predicted 38.5 billion insecure IoT devices deployed in the field.***

References

1. "'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020." Juniper Research, 28 July 2015. Web. Retrieved 8 Mar. 2016 <http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020>

2. "Internet of Things: Example Applications." Internet of Things. Postscapes, n.d. Web. 30 May 2016. <http://postscapes.com/internet-of-things-examples/>.

3. FBI, IC3. "Internet Crime Complaint Center (IC3) Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes." Internet Crime Complaint Center. 23 June 2015. Web. Retrieved 10 March 2016. <http://www.ic3.gov/media/2015/150623.aspx>.

4. Morgan, Steven C. "Cyber Security Market Report." Cyber-Security Ventures. People's Communications Inc., 3 Aug. 2015. Web. 21 Mar. 2016. <http://cybersecurityventures.com/cybersecurity-market-report-q3-2015/>.

5. "SCADA Vulnerability on the Rise | EE Times." EETimes. Rich Quinnell, 24 Sept. 2015. Web. 26 Apr. 2016. <http://www.eetimes.com/document.asp?doc_id=1327785>.

6. Minkel, J. R. "The 2003 Northeast Blackout -Five Years Later." Scientific American, 13 Aug. 2008. Retrieved 8 Mar. 2016. <http://www.scientificamerican.com/article/2003-blackout-five-years-later/>.

7. Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. N.p., 23 Feb. 2016. Web. 1 June 2016. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

8. "FACT SHEET: Cybersecurity National Action Plan." The White House. Office of the Press Secretary, 09 Feb. 2016. Web. 01 June 2016. <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.