# Industry 4.0 and IIoT Security Design and Architecture

By the year 2020, Gartner states there will be 26 billion Internet of Things (IoT) devices on the internet [1]. These devices provide incalculable advantages to smart factory automation, plant management, smart manufacturing processes and many other aspects of Industry 4.0, there also comes the risk of any interconnected IIoT device with access to the Internet.

These IoT devices are known to have insecure interfaces, weak authentication, lack of encryption, difficulty for security configuration, weak physical security, and in worst cases, vulnerable out of the box.

In a recent memo concerning the threat of attacks targeting IoT devices, the United States Federal Bureau of Investigation (FBI) issued an alert notifying the public of threats which may harm unprotected IoT devices, and the risks they can expose the owners of the devices to. The report details what type of devices can be targets for attack, attack vectors, as well as the indicators of compromise [2].

The threat to Industry 4.0 systems, as well as any cyber-attack in this era of cyber security, may arrive in various forms and may come from varying sources. These threat actors can range from the simple threat of an internal disgruntled employee with limited, but destructive knowledge of Industry 4.0 systems, to nation-states attempting to paralyze cyber-physical systems at the national level.

An example of one of these threats arrived in the form of the well-documented ‘Mirai’ malware. Mirai scans the Internet for unprotected IoT devices using default credentials and has the capability to take down unsecured devices. The ‘Mirai’ malware was not originally designed to be used for this use. The malware was designed by its creators to simply make money from an online game [3]. However, as the code was posted for anyone to use, it was quickly picked up by hostile actors. ‘Mirai’ was used in DDoS service attacks against popular websites such as AirBnB, GitHub, Netflix, Reddit, Twitter and many other websites [4].

Had IoT devices been placed on networks with the security of these devices in mind and the devices themselves secured, the impact of Mirai attacks could have been limited.

With this example in mind, designing or redesigning the security of the networks which house these systems must consider the full spectrum of threats. These include attacks like Mirai which sweep the internet for default credentials, to targeted attacks which may include Zero-Day vulnerabilities.

An analysis by Symantec concluded the average IoT device is scanned every two minutes. This means that a vulnerable device, such as one with a default password, could be compromised within minutes of going online [5]. This means that simply changing a default password may not be enough to protect a network in the event a vendor or system administrator forgets to change the default credentials. Security must be strong across the network which hosts Industry 4.0 systems.

Although securing these devices individually greatly protects against compromise, protecting individual devices alone is not a sustainable or practical approach to the problem. This would be a time-consuming remedy and would be futile if the attacker has scanners which can detect the IoT device within a matter of seconds, threatened by an insider with physical access to the device, or the device is already compromised from the factory.

Network security design for IoT devices must consider the changes that will occur at all levels of security. This may include changes to firewall ports to allow IoT devices to communicate over designated ports rather than default ports, which will limit the success of discovery scans seeking Industry 4.0 devices. This can also include Access Control Lists on switches to prevent unauthorized devices from connecting to untrusted devices or sensitive segments within the network. Additionally, this can include monitoring networks for unusual connections to servers outside the network, which may indicate compromise. Also, this may mean placing all IoT devices on a separate Virtual Local Area Network (VLAN) with its own special security restrictions. At the most basic level, proper physical security of these networked devices must be treated no different than any untrusted device within the network.

As with almost all cyber security trends of the 21st century such as ransomware, rootkits and social media spear-phishing campaigns, there is almost no doubt that Industry 4.0 will undergo attack from threat actors of all types. Networks which host these systems must be designed to meet these threats as they exist today or postulated for years to come.

-30-

**About the Author:** Taylor Welsh has worked as a cybersecurity specialist for the past 15 years at Ax Control Inc. -- an automation control device service and supply company based out of North Carolina. They specialize in new and obsolete drives, PLCs, HMI and related control devices. Along with being the former President of the North Carolina InfraGard Cyber Club, Taylor has worked in various capacities within cybersecurity, including government, defense, retail, manufacturing and startups. Please show your appreciation for Taylor's article by visiting their website AxControl.com.

**IIoT Security Sources:**

[1] https://www.gartner.com/newsroom/id/2636073

[2] https://www.ic3.gov/media/2018/180802.aspx
[3]https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [4] https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/

[5]https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks