Implementing Security Measures for Smart Sensors Detecting Toxic Fumes

CYSE 494

Carl L. Rumberg

5/30/2023

Carl Rumberg
CYSE 494
5/30/2023

Proposal

The problem to be addressed with our innovation is that of cybersecurity issues faced by smart sensors used by RePlast. Replast is a company that utilizes steam and compression to convert "all types of plastic waste into an advanced, zero-waste building material called ByBlock" (Byfusion, 2023). The smart sensors in question are used to monitor for toxic fumes in the production environment, and alert staff if and when toxic fumes past a certain threshold are detected. These smart sensors are crucial to not only the safety of any staff in production environments, but also are necessary to reach compliance with environmental and workers regulations. However, the lack of proper access control, authentication, and encryption schemes pose various risks to the sensor itself and the network the sensor is implemented within. The lack of these measures could lead to tampering of the sensor itself, unauthorized access, threshold/data manipulation, and overall brings the reliability and integrity of these sensors into question.

Context

This is a clear problem as human safety and environmental protection standards rely heavily upon the reliability of these sensors, as well as the integrity of the data sent and received from these sensors to production networks. Considering the large uptick in cyberattacks in general, especially within critical infrastructure, it is of the utmost importance that sensors as critical as these be as resilient as possible to attacks. It isn't hard to imagine a scenario by which malicious actors gain unauthorized access to these sensors and, for example, raise the alarm threshold by which the sensors send an alert in order to protect the workers within the environment. Another example could be that a lack of encryption could give an attacker the opportunity to create bogus packets and send them through the network "from" a smart sensor and continually halt production for investigation. Seeing as human lives are on the line each time a sensor alerts, sending bogus alerts constantly through the network could potentially shut down production for extended periods of time.

Solution

The proposed solution would be to implement access control, authentication, and encryption measures within these smart sensors in order to mitigate the risks that come along with the severe reliance on their proper functionality.

1. **Access Control:** Using role-based access control(RBAC) within these smart sensors would ensure that only those authorized by system administrators would have access to the interface to sensors. As with all RBAC systems, all staff within facilities would be given roles based on their responsibilities within the workplace, and privileges to access sensors, among other technologies within the workplace, will be granted as appropriate to

their job description. This would ensure that only those that **need** access to smart sensors would be given it. This will be done via access control lists(ACL's) that can be fine-tuned as necessary, for example maybe some employees will be given access to read sensor settings but not manipulate them, while others will have full access.

2. **Authentication:** Strong authentication protocols for not only the sensors themselves, but also the production network will ensure that only those authorized to access the network and sensors will be granted access. These measures could include two-factor authentication, biometric authentication, and/or digital certificates. Two-factor and biometric authentication would be used to prevent unauthorized users from masquerading as authenticated users with high-level access, either to log in to sensors to manipulate settings or to gain access to the surrounding network. Individual sensors could be assigned different digital certificates, creating a public-key infrastructure for the network and the systems monitoring the sensors themselves. This would ensure that mutual authentication could be performed when sensors communicate with devices throughout the network, greatly increasing the protection from aforementioned "bogus packets."
3. **Encryption:** Encryption in this case would tie hand-in-hand with the usage of PKI. As digital certificates mutually authenticate both parties in an exchange, the key pairs of each party are also used to encrypt communications between said two parties. This would ensure that any communications performed between sensors and monitoring systems would be confidential and secure from tampering.

While outside the scope of this proposal, it should also be noted that past these methods, various other security measures should be implemented for the network that these sensors are a part of. Intrusion detection/ prevention systems(IDS/IPS), robust firewalls, and secure physical facilities should be a bare minimum for any production environment.

Barriers

There are a multitude of expected barriers that come with the implementation of this technology.

1. **Resistance to Change:** Most people, and workplaces, have some form of resistance to change. After doing things one way for a long time, some can have issues with the necessity to learn new technologies or processes. This is often expected and can be mitigated via simply talking employees through the risks involved with not implementing these changes, and in this case explaining to them that their own safety is significantly increased by implementing these measures.
2. **Budget:** Budget is often an issue with most companies, especially when it comes to technology. The hardware and software included within this proposal aren't cheap, as with the actual labor included in implementation and maintenance. It is likely that another IT employee familiar with the systems would need to be onboarded in order to keep up with maintenance, and to help with expansion given growth of facilities.

3. **Integration:** Integration of these security features may pose issues given that some environments may run legacy software that doesn't "play nice" with the new measures, or simply isn't compatible. This can tie into budget as sometimes existing infrastructure/hardware may need to be upgraded in order to make the implementation successful.

Assessment

The success of the implementation can be measured via many metrics. I will list a few below with explanations.

1. **Reduced Cybersecurity Attacks/Incidents:** The number of successful cybersecurity attacks should be either zero, or significantly lower than the previous baseline prior to implementation. This can be monitored via logging of unauthorized access attempts(failed and successful vs. baseline) or the tampering of settings for smart sensors**.**
2. **Compliance with Standards:** If the production environment, after implementation of these measures, is compliant with industry standards taken from credible parties such as NIST or the ISO, it is a certain sign of success.
3. **User Feedback:** Simply put, if the users within production and system administrators are happy with the usability and effectiveness of the measures, it is a good sign that everything is working as intended without difficulty.

References

Reshape the future of plastic waste. ByFusion Global Inc. (2023, April 12). https://www.byfusion.com/