Lab worksheet 3

Objectives of Lab

- Explore how to compromise the sensors within the bakery scene.
- Understand the different types of attacker.
- Understand some of the attack mitigation techniques.
- Understand some attack prevention techniques.
- Understand commonly used deterrents.

Background

Following on from lab two, this lab focuses on the bakery scene and the different methods we can use to compromise the sensors from a local perspective. Doing so, will help you to understand the issues that can occur if an industrial control system has been attacked. You will also briefly explore the different potential attackers for a CPS. This lab will also cover some of the different practices used to deter attackers and to help mitigate and prevent attacks to a CPS.

System requirements and Prerequisites

- Completion of labs one and two
- Raspberry Pi 3B+ running Raspbian Operating System (32-Bit Released 11.01.2021)
- OpenPLC Runtime V3
- FactoryIO V2.4.6

Task One – Compromise the sensors

There are many ways to use the physical environment around a factory and its sensors to cause false reading on a sensor. The impact this can have varies greatly depending on what type of sensor you have compromised, and the type of CPS being attacked.

The bakery scenario we have created has limited sensors in comparison with a complete bread factory, due to it being largely scaled down in size. In the previous lab, we briefly explored what would happen if you moved one of our ingredient sensors so that it was pointing the completely wrong way. This is a largely obvious attack, that may be easily noticed by any floor workers who walk past, however most of the system control is done remotely.

Step 1 – Breaking the alignment of a retroreflective sensor

As suggested in its name, a retroreflective sensor relies on a reflection to determine if it senses an item. in this case, our sensor has an opposing reflective part that must be aligned directly opposite the sensor to enable the sensor to correctly work. Without this part, the sensor would trigger incorrectly.

In our scene, move the reflective component to one of the retroreflective sensors. FactoryIO will highlight when the part is and is not in line with the sensor itself. Once the component has been moved slightly off centre, run the scene, and analyse what happens.

Having run the scene, you can see that this triggers the sensors accompanying results instantaneously upon the batch starting. In this type of CPS, the consequences of this are not dire. Depending on the exact sensor you picked, it will either trigger a stop to come up prematurely at the mixing stations, or trigger the proofing oven incorrectly. Although this could ruin a batch of bread, and cause monetary loss for the production company, this is not as severe as an attack on a power plant would be.

Step 2 – Change the conveyor direction

Most conveyor belts have physical switches attached to them that allow a directional override, or a speed override. For this attack, we cannot create an exact replication as we do not have a switch on our conveyor belts, however we can turn one or two conveyor belts around prior to starting the scene.

To mimic the attack of changing the conveyor direction, pick a conveyor and turn it around in our bakery scene. After doing this run the scene to see what happens.

Step 3 – Explore the compromisation of other sensors

The previous two attacks only scratch the surface of what can be done when an attacker manipulates the environment around the sensors. For this task, do some further research into common sensor manipulation attacks. Use the bakery scene and the components within FactoryIO to attempt to compromise the different sensors in varying ways. Try to be creative and think like an attacker. What items are in the vicinity that could be used?

Task Two – Attackers and deterrents

Due to the broad variety of CPS's in the world, there are various types of malicious attacker, alongside accidental attackers. Accidental attackers do not mean to cause harm to the system, often they have accidentally turned a safety feature off or moved a component slightly. In comparison, you get threats from thieves, espionage, and terrorists. These attackers tend to attack larger CPS's, particularly those that are critical to national infrastructure, such as a power plant, nuclear facility, or water treatments. These attackers tend to use social engineering techniques to gain information about a CPS prior t an attack, an even use tools such as google street view to gauge security. One of the most overlooked type of attacker is that of the disgruntled employee, either current or recently let go. These attackers are privy to knowledge on how the CPS works, and may have physical access to the area.

To dissuade potential attackers, different deterrents are used. Common physical deterrents that can be seen at a glance are patrolling security guards and high security fences. Some of these fences are electric, whilst others make use of barbed or razor wire. Each of these are

effective at deterring certain types of attacker. Other deterrents such as security cameras, alarms and checkpoints are commonly used in vicinities that prioritise security. Alongside this, deterrents such as specified paths can be used. These are particularly useful if an attacker were to breach the site, as they delay and even prevent an attacker from making it very far within the complex.

Task Three – Mitigation and prevention

Back when control systems were first used, the main prevention method for attacks was to isolate the CPS from the internet. Due to developments over the years, isolating the entire system is no longer a viable option, as this opposes common practice and the efficiency developments that have been made.

To counter this, firewalls and data diodes have been implemented. Alongside this, a CPS is often separated into multiple sections, allowing different de-militarised zones to be implemented around a CPS's critical points. This helps isolate the CPS network from the general internet and any intranet that has been used on the site. 4G and 5G devices can be of high risk within a CPS, so it is vital that remote device connections are unable to be made. This reduces the chances of an external user or attacker accessing the system.

Mitigation through different access control mechanisms is advised, with it recommended to ensure employees have access to as little of the system as possible. Dual access systems may also be implemented, such as using a PIN and an RFID card per employee, rather than just RFID cards, as these can easily be duplicated.

Often cyber-physical control systems will run on a legacy system, one that tends to run for at least 25 years, meaning it cannot always have the latest security measures implemented. This can mean that new vulnerabilities are discovered in the system post installation, such as with the Heartbleed vulnerability, where many devices with the vulnerability will not be patched with a fix. A common added security measure with these systems, is to add a bump-in-the-wire. A bump-in-the-wire protects a system from untrusted parties on the network, by utilizing a secure channel to transfer unencrypted packets.

Sensor fusion is a commonly used mitigation technique to help prevent attacks such as a transduction attack. This involves using multiple sensors to ensure consistency between them. An inconsistency with this technique implemented would either suggest an attacker has got to one of the sensors, or an issue with the sensor itself. Resilient estimation can also be used to ensure the reported sensor values match up with the expectations of what they should be based upon the knowledge of the control system. For instance, in a baking oven you would expect the values to either be at zero, when it is off, or around 280 degrees Celsius. This can help a system to reject attempted attacks when the values are outside of an expected range. Actuator constraints can also be put in place to restrict how fast the operation of the system could be changed if an attacker were to gain access.

An inertial reset can also be implemented in control systems that do not need to be continuously running, such as a batch process. This consists of resetting the system code back to a secure version prior to each run of the system. This ensures that even if an attacker were to compromise the system, any issues would only impact one run of the system before being dealt with.

Takeaways

In this lab you should have come to understand the different types of attacker there are for CPS's and what deterrents are in place to prevent attackers from attempting an attack. You will also have learnt some of the different mitigation and prevention techniques, such as inertial resets and sensor fusion. Alongside this, you will have explored the different local attacks you could perform by tampering with the bakery environment to compromise the sensors in the scene.

Further reading

Cyber-Physical Systems Security Knowledge Area Issue 1.0 – available from https://www.cybok.org/knowledgebase/

Information on the Heartbleed bug - https://heartbleed.com/

The Heartbleed bug in relation to CPS - https://www.infosecurity-magazine.com/news/heartbleed-bug-hits-industrial/