Final Project Report Group 12

gcad-ee

< Name removed for privacy reasons >

< Name removed for privacy reasons >

< Name removed for privacy reasons >

Our Implementation

We used the provided IoT devices equipped with temperature/humidity sensors for two separate roles. The first device is used to monitor a chosen location. It simply sends updates to the AWS MQTTS server on the topic 'gas_detection'. The second device receives these updates and performs basic analysis on them. It determines an average of the temperature and humidity and checks the immediate values received. Two thresholds are programmed in, one that checks the average and the other that checks immediate samples. If conditions for a gas leak are met, an alert is sent to the MQTT topic 'gas_leak' which can then be used to alert further devices.

Security Challenges

A security concern was physical access to the device. If a malicious actor enters the lab space and gains access to the monitoring device, they can dump the flash information of the monitoring device to obtain keys and certificates. This also applies to the processing device, which can also edit the thresholds of a gas detection. Another challenge is the attacker listening in on data transmissions. Encrypting communications between the board and MQTT server will make this significantly harder for an attacker to listen.

Risk Assessment

We used a scale of 1 to 5 to rate both likelihood and consequence, where 1 is the least severe and 5 is the most severe. For likelihood, a 1 means that there is a very low chance of the threat happening, where a 5 mean that risk is a common occurrence and can happen quite often. For consequences if it's a 1, then it probably won’t affect the normal operations of the systems, where a 5 means that very severe damage could occur as well as permanent damage to the system or area it is in and even serious injuries to lives. The risk score will range from 1 to 25 with a higher number meaning higher risk. Then we chose common threats that could happen to our system.

The first of these security threats would be a malware infection. AWS is usually a very secure platform, so we will rate the likelihood of happening as a medium or a 3. Malware can disrupt the communication between the device and the network as well as corrupt data, meaning it has high consequences, giving it a rating of 5. Together, the risk assessment is a 15, so it is high risk assessment.

The next threat would be DoS or denial of service attacks. While AWS is robust, the component of the system is not and can still lead to a medium likelihood of it happening. If a DoS attack happens, it can prevent alerts and notifications of the alarm system from happening. So, it has a consequence level of 5 and a total risk of 15, which means that it is high risk.

The next threat to be concerned about is data breach. The likelihood of it happening is medium because while AWS is secured, data breaches are not uncommon with large databases. So, the likelihood score is a 3. There could be a risk that highly sensitive data get exploited, but it won’t cause any severe injuries, so a consequence assessment of 3 is given. This results in a risk score of 9 or medium risk.

Side channel attacks exploit hardware or implementation of a computer system rather than software. In a cloud environment, side channel attacks are not common and hard to achieve, so an assessment of 1. All side channel attacks are aimed to measure certain information about the system rather than actual data, and don’t really have much consequence if exploited. These have a consequence assessment of 1 and a risk score of 1. A cache attack can reveal more sensitive data. This type of side channel attacks has a medium consequence if exploited, so a consequence of 3 and a total risk of 3, making it low risk as well.

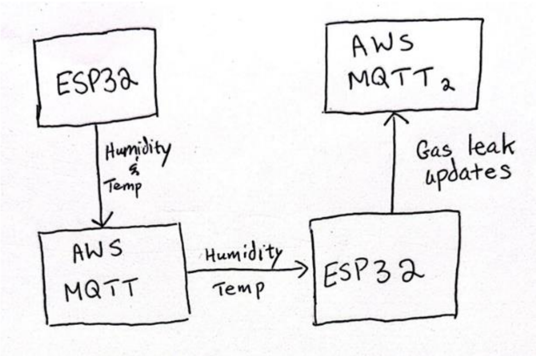
Another threat to consider is Man-In-The-Middle attacks. This kind of attack is not likely due to communications being encrypted between sender and receiver, a likelihood assessment of 2 is given. Consequences can range from a 3 if the sensitive data is exposed to a 5 if the data is tampered. This gives it a risk assessment of 5 to 10, depending on what the MitM attack can do.

Another threat to be considered would be unauthorized access to the system. This type of attack is very common, so the likelihood assessment would be a 5. It has very high consequences since the third party can get full access to the system so the consequence is a 5. For a risk assessment of 25, being of extremely high risk.

What was chosen to be addressed /why

Physical access to the device was not addressed, an attacker can obtain identification information of either device with relative ease. Wireless communications were considered, and TLS/SSL protocols were used to encrypt data communications between the devices and MQTT broker.

Proposed Solutions:



In our original plans, we wanted to send the humidity and temperature data from one board to an AWS MQTT server. The values are sent to the other board, which would calculate if a gas leak is detected, resulting in alarms being sent to a different AWS MQTT server.

Presentation Question Responses:

How were the risk likelihoods determined?

Risk likelihoods were determined by looking at the frequency of incidents in similar cases where comparable signals were sent to servers for processing. Analyzing historical data from IoT security incidents helped us determine the risk likelihoods of each security threat.

What's the threat model for data sniffing in this scenario?

While it may seem that an attacker would not gain much from data sniffing, they can use the data to cause harm to the users. If they learn the threshold values that activate the alarm, they can use MITM attacks to create false positives and evacuate the building. The opposite can happen and that would result in harm/loss of life from an undetected gas leak.

Can you give details about the consequences of SCA/MITM vs "generic" cybersecurity breaches and how SCA/MITM is a more dangerous risk?

Due to their ability to access active sessions and manipulate real time data, SCA/MITM attacks are a bigger security threat than the average cybersecurity breach. These attacks intercept and/or manipulate the data to access private information and trick users. Since these attacks are hard to notice, the attacker can covertly cause havoc to the users, resulting in long term consequences, such as financial fraud or sabotage of a whole company.