Application of Cyber Physical System in Automating Air Conditioning Systems

Okstynn Rodrigues #1, Shahesta Ahmed #2
Department of Information Technology, Padre Conceicao College of Engineering, India
Department of Information Technology, Padre Conceicao College of Engineering, India

1 mecta2k7@gmail.com
2 shahistar1996@gmail.com

Abstract: Cyber-Physical Systems have revolutionized the way people interact with engineered systems. They represent an intricate interplay between the physical and cyber domains. In this paper we first look at safety and security associated with a CPS. Security issues in Cyber Physical Systems based applications are of paramount importance due to the often safety-critical nature associated with them. A first step in understanding how to protect such systems requires an understanding of emergent weaknesses that are often overlooked during the implementation phase and design phase. This paper documents the potential threats that could cause disruption in the functioning of an Air Conditioner and programming fixes to resolve them.

Keywords: Cyber- Physical Systems, Safety, Security Attack, Threats, Vulnerability issues

I. Introduction
The IT industry in recent years has played an active role in trying to automate our everyday lives. The major participants involved in many of these applications are a smart-phone and a decent connectivity to the internet. Any such application that we create or is existing has quite a few many “loopholes” or technically called programming conditions that are taken for granted or sometimes prioritized very poorly. Such conditions would to lead to vulnerability issues in the system. Vulnerability in a system thus exists when there is a weakness in the system, and the opponent has the capability or means to exploit this weakness.

Today's technology aims at controlling the effects on the physical world through the use of smart technologies created by computers. CPS requires a tight coupling between the physical and cyber controlling components. Thus it is crucial to ensure that the system is not only safe but also secure for all cyber and physical processes. In this paper, we first attempt to examine, the types of vulnerabilities that an Air Conditioner may likely discover, and how they affect its working. Finally we propose quick programming fixes to try and resolve the vulnerabilities identified. Section II of this paper gives a brief overview of the security risks that may arise when wirelessly controlling an Air Conditioner. Section III proposes an implementation methodology that could be employed. Section IV concludes this paper and recommends future scope.

II. Safety And Security In A Cyber-Physical System
A. What is a Cyber-Physical System?
There exists no clear definition as such, but briefly speaking a CPS is a system in which the cyber and physical components are tightly coupled at all levels and scales. In other words a Cyber-Physical System integrates computation and physical processes, enables computation, communication and control of the physical processes using embedded computers and networks and last but not the least it receives feedback on how physical processes affect computations and vice versa.

B. Characteristics of Cyber-Physical Systems
1) Security and Privacy: Cyber attacks are a common place occurrence in information technology based systems. CPS’s are especially vulnerable, because they are either located in open environments or can be easily communicated with wirelessly. System designers in charge of designing a CPS should make note of the security and privacy risks involved, and have handy techniques to protect them; this is very crucial.

2) Interoperability: A large-scale CPS, would be composed of numerous components, manufactured by different vendors, and each such component operated by separate entities within the system. To realize the full potential of a CPS, interoperability among these heterogeneous components would be very important. Interoperability can be realized by tirelessly studying the common architectures, standardized interfaces and data standards.

3) Reliability and Dependability: Cyber-Physical systems are a part of our everyday lives, and their utility demands that they be highly reliable and dependable. CPS devices having limited computational power,
memory and energy would more often than not lead to new problems. In order to avoid these, reliability (and safety) should be incorporated as part of system design during the early stages, and not thought of as something to be fixed during testing. So also any uncertainties, that could arise, would require the CPS to be robust. These uncertainties are often difficult to quantify in the design phase. Thus to address these uncertainties, they must be tracked and addressed during the implementation stages.

4) **Power and Energy Management**: Some CPS components have a compact size, and operate autonomously, making energy management a critical engineering design priority.

5) **Safety**: The proliferation of CPS technology into daily lives, has made it exceedingly important to ensure that actions taken on humans and the environment are safe, and that the risks involved with these actions can be easily assessed and managed.

6) **Stability and Performance**: The stability and performance of a CPS may heavily depend on factors such as limitations of sensors and actuators, the modeling of noise and uncertainty affecting the system and other factors.

7) **Human Factors and Usability**: Understanding and accounting for the behavioral responses of humans, humans in the loop control, and human design factors are all important for most CPS applications.

C. **What is Safety and Security in Cyber Physical Systems?**

Safety and Security are two fundamental properties of a CPS and have a shared and aligned goal—protecting CPS from failures. Safety aims to protect a system from accidental failures to prevent disastrous hazards that could physically damage a system. In contrast, security aims at protecting a system from intentional attacks that risk a systems functioning. For a healthy functioning of a CPS safety and security should be adequately aligned in terms of their activities and processes. Poor alignment may cause a major fall out of the physical system, where recovery may not be possible.

D. **Vulnerability Issues**

1) **Poor input validation**: The most common type of attack on any system is when the input is ill-formed. We need to effectively validate if the device (AC) is receiving the correct source of signal. For implementation purposes we make use of an IR (Infra-red) receiver to read the signal from the AC’s remote control.

2) **Lack of authentication**: Authentication is ensuring that no third party can access your device or your application. In other words we have to ensure that any external application cannot access your Air Conditioner, and any access to it is monitored by the customized application designed by us. We design an Android application to control our Air Conditioner.

3) **Naive assumptions about security**: Often many times, designers find themselves thinking questions such as “Who would think that this security risks exists?”; “Who would figure this out?” System designers often underestimate the fact that there exist programmers and skilled professionals that are capable of destroying the security features in place, and manipulating a system to benefit them. This is very naive of them. Similarly when designing an Air Conditioner, we may think, why does it matter if anyone can control it? But in some domains securing an Air Conditioner may be critical in nature.

4) **Implementation Errors**: Implementation errors may risk the security of the Air Conditioner. Say, for instance there is no limit in place for the temperature control of an AC. That is if we require that the AC temperature be at ‘22’ at all times, then being able to change it to ‘25’ or even ‘18’ would be classified as an implementation error. Cases wherein the AC detects that the temperature was modified too late or temperature modification is not detected at all. Such errors reduce the efficiency of an Air Conditioner.

5) **Lack of robustness**: Many applications fail to understand the conditions under which they would operate. For instance, an Air Conditioner is programmed to take one command at a time. A case wherein, it receives more than one signal may cause untimely shutdown of an Air Conditioner.

III. Implementation Methodology

*National Conference On Recent Innovations In Engineering Science, Technology & Management*

*Agnel Institute Of Technology And Design Assagao, Bardez, Goa – 403 507*
A. Attack Diagram

![Attack Diagram](image)

**Fig. 1** Attack process on AC

<table>
<thead>
<tr>
<th>TABLE I: SYSTEM THREATS IDENTIFIED FOR AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>THREAT (T)</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>T1</td>
</tr>
<tr>
<td>T2</td>
</tr>
<tr>
<td>T3</td>
</tr>
<tr>
<td>T4</td>
</tr>
<tr>
<td>T5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE II: SYSTEM SECURITY REQUIREMENTS AND CONSTRAINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>THREAT (T)</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>T1</td>
</tr>
<tr>
<td>T2</td>
</tr>
<tr>
<td>T3</td>
</tr>
<tr>
<td>T4</td>
</tr>
<tr>
<td>T5</td>
</tr>
<tr>
<td>T6</td>
</tr>
</tbody>
</table>

B. Software and Hardware Requirements

The implementation of this project requires the following:

**Hardware requirements:**
- Arduino Mega 2560 microcontroller
- Blue Star AC
- Blue Star AC remote
- Jumper cables
- IR sensor

**Software requirements:**
- IRremote library
- Arduino 1.8.7 editor
- C/C++ language
- Pin descriptions of the Arduino Mega 2560 Microcontroller
C. Current Work Done

Step 1: Setting Up Everything: Connect the IR sensor to the Arduino board with the following pin configuration.

- Pin 1 from sensor goes to Pin 19 of Arduino
- Pin 2 from sensor goes to Ground Pin of Arduino
- Pin 3 from sensor goes to 5V Pin.

![Fig. 2 Pin Configuration for Arduino Mega 2560](image)

Step 2: Select the board and the port: To select the board go to Arduino sketch. Under Tools go to Board and select the Board Arduino/Genuino Mega or Mega 2560.

![Fig. 3 Arduino Board Selection](image)

To select the Port connect your Arduino board to your laptop using the CH340G USB cable. It will detect the port. Select COM6.

![Fig. 4 Arduino Port Selection](image)

Step 3: Decode IR codes: Now Go to Sketch from the file menu. Select Include Library → Manage Libraries. In the search bar type IRremote, select the version and install into your sketch.
Fig. 5 Arduino Manage Libraries

Fig. 6 IRremote Library search

To decode the IR codes of the remote Go to File → Examples → IRremote → IRecvDemo. Change the RECV_PIN from default 11 to 19

Fig. 7 IRecvDemo of IRremote
Application of Cyber Physical System in Automating Air Conditioning Systems

Fig. 8 Modifying IRecvDemo

Step 4: Verify and Upload the code

Step 5: Read the decoded values on Serial monitor: Now open the Serial Monitor from tools and point your AC remote to the IR sensor. Press each button on the remote to decode its code. You will get a similar output depending on the AC remote.

Fig. 9 Verify and Upload code

Fig. 10 Read results on Serial Monitor

IV. Conclusion

We have successfully identified the numerous security threats that can arise in an Air Conditioner and we attempt to resolve them. A partial implementation of the application is already implemented. The resulting application would be a simple Android application wirelessly controlling the Air Conditioner. We also include solutions to resolve the security threats so that our application is safer. Future work includes trying to integrate security solutions to the project.

Acknowledgement

We would like to acknowledge the contributions of Mrs. Cassandra Fernandes, Assistant professor at Padre Conceicao College Of Engineering in the making and reviewing of this project. We also appreciate the help offered by lab staff, for assisting with hardware requirements.
References

