Chapter 20

Embedded System Security Risk in a Green–House Environment

Trailokya Oraon
Jorhat Engineering College, India

ABSTRACT

Embedded systems are extensively used in the field of pervasive computing. These systems are used to such an extent that embedded systems are now controlled and monitored from remote locations by using Web services. Internet authorities are able to assign every device a unique Internet protocol address with the introduction of IPv6 on the Web. Peer-to-peer communication between Internet-enabled devices helped Web services to make performance improvement. On the worse side, it created new attacks on the components used in the embedded systems. The chapter discusses the details of security issues on a Web-enabled embedded system used in greenhouse environment. The devices used in greenhouse environment are monitored and controlled by different software components used in the entire system. Various vulnerabilities are introduced during entire development process of the greenhouse environment. The problem is to search the real threats, then define security policies and implement them during development process. The chapter discusses most of the vulnerabilities of a generalized greenhouse project and tries to find out possible security techniques to deal with the vulnerabilities. Instead of showing the design to build a greenhouse embedded system, it shows to introduce security policies at various levels of life-cycle, be it before development, during development, or after development.

1. INTRODUCTION

Our lives and our businesses depend unavoidably on computing systems and, increasingly, on embedded systems in particular. Applications of embedded systems to monitor and control the greenhouse environment has become a notion of pervasive computing and now these computing devices can be applied and are available anywhere and anytime. Embedded systems are generally hidden from the user (Marwedel, P., 2003). For example, proper use of greenhouse environment helps the crop-growers to maximize the productivity and better the quality of crops and seeds.
Embedded products and tools that growers have at their disposal to control the environment, are manipulated with respect to the important environmental influences on plant growth and development, for the actual optimization of the greenhouse environment. These embedded systems, which are ubiquitously used to sense, capture, store, process and transmit vital data used for control of the environment to maximize the photosynthetic process in the crop. Security observation is a basic requirement when an embedded system performs any of these tasks. As more and more embedded systems came to be accessed from remote locations, security became a major concern. Security of embedded systems employed in greenhouse environment provided new business opportunities and also prevents dangers of economical loss. For example, it prevents undue change of environmental changes and should help preserve grower’s expectations. Examples of new business opportunities are secure embedded devices that are applied for use in timely production of crops. With the adoption of Internet Protocol version 6 (IPv6), network solutions for embedded devices, peer-to-peer communication is now possible and thereby giving easy access and control of such devices from remote locations. This has resulted an increasing number of security breaches, which have been detected in embedded systems in recent years, which also reveals the importance of fundamental security solutions. Security solutions, which are basically applied to embedded systems that also incorporate the concept of network model, are specific cryptographic algorithms, adding security functionality to the network security protocols or adding one more security layer to the embedded device (Summers, R., C., 1997). In general, most developers apply security ‘patches’ only at the beginning of implementation phase or only if a security faults is detected. The embedded system data processing itself is vulnerable to its own system as we shall see this in section 7. The chapter discusses the various embedded system security issues with reference to systems employed in greenhouse environment. A very specific concept of life-cycle of embedded products and the vulnerabilities is discussed in section 2 and 3 respectively. The section 4 and 5 discusses secure design policies and why secure design is needed. The reason and concept of greenhouse security is discussed in section 6. To design a highly secure system, different design strategies are proposed. This strategy consists of prevention, tolerance, removal and forecasting. Prevention and tolerance are basic security strategies while removal and forecasting are strategies for security assurance.

It is often argued for giving too much importance to security of embedded systems (Paar, C., & Weimerskirch, A., Jan. 2007). Security policies should be implemented to tackle real threats. Vulnerabilities arises when a system is connected to network and also when working as a single system. Mere encryption and decryption of incoming and outgoing data does not provide a complete integrated solution of security. Security should not be on short term benefits, but long-term benefits should be taken keeping the cost factors into account.

The security philosophy of almost all greenhouse embedded systems is quite same. The example project given in the chapter does not show how the system is designed, but it shows the real security threats, the security policies built on these threats and which security policies are can be applied for the greenhouse system. Since most embedded systems can be controlled and monitored through wired and wireless network.

2. LIFE-CYCLE OF EMBEDDED SYSTEM FOR GREENHOUSE ENVIRONMENT

In general, there are three phases of any embedded system: development, use and disposal.

• Development of the system for the environment