

Enabling Security in Embedded System: A New Dimension

Mansoor, CMM.* , Roshan G. Ragel & Swarnalatha Radhakrishnan

Abstract

Recent advances in digital electronics and wireless communications have enabled a widespread proliferation of embedded systems which are becoming more ubiquitous within our daily lives. Technological advances that have spurred the development of electronic systems have also ushered in seemingly parallel trends in the sophistication of attacks they face. Security in embedded systems is a topic that has received an increasing amount of attention from industry and academia in recent years. Indeed, the success and adoption of several next-generation applications and services are predicted on the ability of embedded systems' designers and manufacturers to ensure adequate security, and gain the trust and confidence of consumers, suppliers and involved government institutions. The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. The challenges unique to embedded systems require new approaches to security covering all aspects of embedded system design from architecture to implementation. Security processing, which refers to the computations that must be performed in a system for the purpose of security, can easily overwhelm the computational capabilities of processors in both low- and high-end embedded systems. In reality, it is a new dimension that designers should consider throughout the design process, along with other metrics such as cost, performance, and power. In this paper, we provide an overview on embedded system security and intended to introduce embedded system designers and design tool developers to the challenges involved in designing secure embedded systems. We discuss how the characteristics of embedded systems lead to a set of potential vulnerabilities. We also provide a brief survey of attacks on embedded systems and corresponding countermeasures.

Keywords: Embedded System, Security, Cryptography, Vulnerabilities

To whom correspondence should be addressed:

*Lecturer, Computer Unit, South Eastern University of Sri Lanka.