Chapter 21
Security and Cryptographic Engineering in Embedded Systems

Apostolos P. Fournaris
University of Patras, Greece & Technological Educational Institute of Patras, Greece

Paris Kitsos
Technological Educational Institute of Patras, Greece & Hellenic Open University, Greece

Nicolas Sklavos
Technological Educational Institute of Patras, Greece

ABSTRACT

Strong security is a necessity in the modern IT world and is broadly provided though Hardware Security Modules (HSM) capable of realizing a wide variety of security algorithms and protocols. Such modules are no longer only found in expensive computer systems like servers, corporate PC, or laptops but also in every device where security is required, including embedded systems like smart cards or smart grid, smart environment, automobile, game station, and aviation processors. The chapter provides to the reader the necessary information on how strong security is structured in a hardware embedded system environment from cryptographic engineering point of view. The focus is efficient design on symmetric, asymmetric cryptography and hash function systems, and design approaches that can be used in order to provide strong security to the embedded system user.

INTRODUCTION

The immense growth of portable and mobile systems (smart phones, tablets, netbooks) and the increasing integration of computational logic into any devices through initiatives like future Internet and Internet of things have led to a flourish in embedded system technology stemming the creativity of the IT market to new levels. Wireless, mobile and portable devices are gradually replacing many traditional computer systems due to the increasing user need for mobility in high-end technology

DOI: 10.4018/978-1-4666-3922-5.ch021

applications while a new generation of intelligent machines that include embedded processor systems have hit the market, capable of providing very sophisticated functionality to users. So, from cars to mobile devices, video equipment to mp3 players and dishwashers to home thermostats, embedded computer systems have invaded our lives and are capable of collecting-processing a wide variety of information. Some of that information are sensitive to the user, like passwords, keys, credentials, even confidential data and life habits. This creates the need for protecting those data and calls for strong security features realized in the embedded system's structure.

In the IT world, strong security demands are satisfied by cryptographic solutions providing personal certificate for each communicating entity, encrypting the transmitted message or the communication channel in general and by generating/managing appropriate keys or certificates for encrypted transactions, authentication and privacy. For message encryption-decryption, a fast cryptographic algorithm, usually a symmetric key cryptographic algorithm is required. For the rest of the security operations, public key digital signatures schemes are employed along with corresponding key agreement and hash function mechanisms.

There are several approaches on how to provide strong security characteristics to a computer system. Most of them involve hardware structures that are physically connected to the computer system like usb tokens, smart cards or specialized security chips (Anderson et al., 2006; Potlapally, 2011). We can discriminate such devices by the level of protection they can provide to a user. Basic protection devices offer user authentication and identification by providing unique identification numbers or PINs stored or generated inside a USB token or smart card system. More advanced protection devices offer data integrity, data confidentiality and user digital signature/sign-on services. High end security protection devices can enforce security and trust in a target computer system and provide trust guarantees as well as malicious user evidence, detection, protection and resistance. However, in an embedded system, security functionality cannot be provided by independent structures. The security structure must be embedded inside the system along with any other functionality that the system needs to service. This means that security for embedded systems involves additional issues that are beyond the problems currently being addressed for enterprise and desktop computing. Those issues are related to the fundamentally different design and implementation approach of embedded systems, to their highly constrained resource technological environment (processing power, battery lifetime, chip covered area, etc.) and to their high vulnerability to attacks.

Cryptographic engineering offers solutions to the above concerns since it views cryptography and therefore security from a practical perspective, always in relation to the system at hand. One of the main goals of a cryptographic engineer is to design a cryptographic function in a secure yet efficient way so as to match the functional and non-functional requirements of the system (Koc, 2008). Using this approach, a cryptographic primitive (which is the structural element of a security system) is designed taking into account its hardware, software performance, its resistance against attacks on it (not only the crypto-algorithm but also its implementation) and how the resulted structure can be fitted into the overall system. Thus, cryptographic engineering principles can be very useful when adding security features and associated hardware structures in an embedded computing system where the constrains are very strict and the environment the system works is very hostile.

In this chapter, an account of the current approaches toward designing secure embedded systems is provided, the problems of realizing strong security functionality on embedded systems are highlighted and cryptographic engineering methodologies on providing attack resistant tam-