Chapter 20
Securing Embedded Computing Systems through Elliptic Curve Cryptography

Elisavet Konstantinou
University of the Aegean, Greece

Yannis C. Stamatiou
University of Patras, Greece

Panayotis E. Nastou
University of the Aegean, Greece

Christos Zaroliagis
University of Patras, Greece

ABSTRACT

Embedded computing devices dominate our everyday activities, from cell phones to wireless sensors that collect and process data for various applications. Although desktop and high-end server security seems to be under control by the use of current security technology, securing the low-end embedded computing systems is a difficult long-term problem. This is mainly due to the fact that the embedded systems are constrained by their operational environment and the limited resources they are equipped with. Recent research activities focus on the deployment of lightweight cryptographic algorithms and security protocols that are well suited to the limited resources of low-end embedded systems. Elliptic Curve Cryptography (ECC) offers an interesting alternative to the classical public key cryptography for embedded systems (e.g., RSA and ElGamal), since it uses smaller key sizes for achieving the same security level, thus making ECC an attractive and efficient alternative for deployment in embedded systems. In this chapter, the processing requirements and architectures for secure network access, communication functions, storage, and high availability of embedded devices are discussed. In addition, ECC-based state-of-the-art lightweight cryptographic primitives for the deployment of security protocols in embedded systems that fulfill the requirements are presented.

DOI: 10.4018/978-1-4666-3922-5.ch020

INTRODUCTION

Today we are witnessing a proliferation of all kinds of inexpensive, portable computing and communication devices with complex versatile wireless connection capabilities. This has as a consequence that Internet is accessible from everywhere by anyone who carries such devices. Internet services proliferate, accordingly, offering services of increasing sophistication and coverage of user needs. However, this ubiquitous existence of devices and services, which exchange volumes of, possibly, sensitive user data and information has given rise to an unprecedented demand for security measures capable of protecting users and service providers alike.

Despite the enhancements in memory and speed capabilities of devices, which came through the technological advances in chip manufacturing processes, most of the portable wireless devices in the market today (Smart phones, VoIP phones, portable computers etc.) do not have sufficient resources for the execution of computationally expensive, multi-step cryptographic protocols essential for the security of the users. In view of the resource limitations of wireless devices modern mobile network protocols involve the heavy use of lightweight private key data encryption algorithms as well as *Elliptic Curve based* public key protocols.

The main objective of this chapter is to discuss the basic principles of the cryptographic primitives and protocols employed for the security of *resource limited devices*, which may be generally seen as belonging to the general class of *embedded systems*. A central theme of our discussion is the mathematical construct of Elliptic Curves and its applications to cryptography. Elliptic Curve Cryptography, or ECC for short, offers an attractive alternative to the classical public key cryptography protocols such as RSA (Rivest, Shamir & Adleman, 1978) and ElGamal (ElGamal, 1985). One of the main advantages of ECC is that ECC-based protocols use smaller key sizes than traditional cryptosystems for achieving the same security levels. For instance, an ECC system with a key size of 160 bits is roughly equivalent, in terms of security, to an RSA system with a key size of 1024 bits. As the key size is much smaller, the requirements in space and memory are also small, rendering ECC an excellent candidate for implementation in embedded devices.

The chapter is organized in three parts. The first part presents some of the most frequently employed cryptographic primitives and protocols, which include block and stream ciphers, private and public key ciphers, digital signatures and key exchange. The second part is focused on Elliptic Curves and ECC and presents the basic definitions and primitives. The third part builds on the first and second parts and presents real world security protocols for embedded devices that employ the primitives discussed in these parts.

Given the space constraints, our aim is not to provide an in depth coverage on all issues pertaining to embedded systems security, but to raise awareness in a (possibly) non-expert audience to security solutions and provide pointers for more extensive information.

A BRIEF INTRODUCTION TO CRYPTOGRAPHIC PRIMITIVES

We briefly review in this part the basic cryptographic primitives and protocols. For more in-depth information on the concepts discussed in this chapter, the reader may consult the excellent book (Stallings, 1999).

A message to be subjected to encryption is called the *plaintext* or *cleartext*. *Encryption* is the process that transforms the message into a form so that it cannot be understood by parties who do not possess a special *key*. The transformed message is called *ciphertext*. *Decryption* is the process of transforming back the ciphertext into its original (plaintext) form. The science of keeping messages secure from being understood by unauthorised