Modern Cryptography Algorithms in the Embedded Environment

Antti Hakkala
University of Turku
Turku, Finland
antti.hakkala@utu.fi

Seppo Virtanen
University of Turku, TUCS
Turku, Finland
seppo.virtanen@utu.fi

Abstract

Cryptography is an important part of modern security solutions. As embedded systems are used to process more and more sensitive data, the need for secure communication channels and secure data processing for embedded systems has been already recognized to be an important issue. Some future directions of embedded systems research have already hinted at a networked architecture for embedded systems, and as such devices exchange information internally, this must also be protected. Some methods for this kind of security currently exist, such as the Trusted Platform Module.

Securing information flow in embedded systems has been shown to be a difficult problem, which is not restricted to a single level of design. As embedded devices are vulnerable to many different attacks – some of which are not feasible on traditional computing platforms such as Differential Power Analysis and other side-channel attacks – the implementation of crypto algorithms must be secure considering the hostile environment.

The calculation of cryptographic operations can be very demanding in terms of processing power and memory use – both something that embedded devices do not have a lot to spread around. Different kinds of auxiliary processors and crypto chips have been developed to address this problem and to make such calculations more efficient and thus viable in the embedded environment. This is made possible by specialized circuits designed to handle certain resource-intensive algebraic operations on the hardware level. The flexibility of such circuits is poor, however, as they are built for a specific purpose.

This presentation will examine modern implementations of cryptography algorithms, especially in embedded environments, and focus on similarities in the algorithms that make it possible to use generalized implementations to support a broad field of different algorithms in different applications. The focus will be on symmetric ciphers such as AES, but the use of asymmetric ciphers and cryptographic hash algorithms will also be examined.

INDEX TERMS: CRYPTOGRAPHY, EMBEDDED COMPUTING, ALGORITHMS.