Microprocessors and Microsystems 39 (2015) 382–392

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Disposable configuration of remotely reconfigurable systems

Lilian Bossuet [a,*], Viktor Fischer [a], Lubos Gaspar [b], Lionel Torres [c], Guy Gogniat [d]

[a] *Laboratoire Hubert Curien, UMR CNRS 5516, University of Lyon, Saint-Etienne 42000, France*
[b] *TTTech Automotive GmbH, Vienna A-1040, Austria*
[c] *LIRMM, UMR CNRS 5506, University of Montpellier, Montpellier 34095, France*
[d] *Lab-STICC, UMR CNRS 6285, University of South Britanny, Lorient 56321, France*

ARTICLE INFO

Article history:
Available online 23 May 2015

Keywords:
FPGA security
Remotely reconfigurable system
Configurable computing
Configuration security

ABSTRACT

Reconfigurable architectures are being increasingly widely used thanks to their high flexibility. This flexibility is due to their inherent ability to reconfigure (whether dynamically or not) functional blocks. Many configurations can be used and changed while the application is running in the reconfigurable system, and/or the same configuration can be used by several systems at different times. The flexibility of reconfigurable systems is greatly enhanced if they can be reconfigured remotely. But in the case of remote reconfiguration, security is of paramount importance. In this article, the problem of remote configuration is addressed by the concept of disposable configuration, an efficient, secure and reliable mechanism for maintaining the flexibility and security of the system. For the implementation of the secure reconfiguration protocol, we propose to use the secure-by-design HCrypt cryptoprocessor, providing low cost, high level protection against both hardware and software attacks without configuration throughput reduction. We validated the approach on a Xilinx Virtex-6 FPGA but it can be easily mapped to any other FPGA or SoC.

1. Introduction

Reconfigurable architectures are becoming more and more popular thanks to their high flexibility. They are more and more used in applications such as software radio, high performance DSP, embedded systems, and security systems. These applications have significant computing needs and require large efficient hardware architectures, but they use different algorithms, parameters and/or configurations depending on processed data and contexts. In addition, the algorithms' parameters and configurations must often change dynamically. The flexibility of the underlying hardware is thus essential. This flexibility is due to their inherent ability to reconfigure a system whether dynamically or not. Thanks to this ability, many configurations can be used and changed within a reconfigurable system while the application is running, and/or the same configuration can be used by several systems at different times.

To enhance flexibility, nowadays remote configuration is certainly one of the most important features to embed in electronic devices. Fig. 1 describes a scenario in which several reconfigurable systems are connected to a remote configuration server. The server stores all the system configurations (i.e. FPGA configuration bitstreams) and their settings (e.g. configuration number, configuration version, encryption key and so on) that have to be safely and efficiently managed in all reconfigurable systems. The server can remotely enforce some new configurations in one of the reconfigurable systems or in all of them in a so-called multicast reconfiguration. In the case of remote reconfiguration, the security is of paramount importance. Indeed, reconfigurable systems are used more and more frequently in applications requiring remote configuration and security – e.g. in secure embedded system [1], in cloud computing [2,3], in smart-home and internet of things (*IoT*) [4–6], in supervisory control and also in data acquisition (*SCADA*) [7]. It is clear that the scenario described in Fig. 1 can be adapted to all these applications.

The objective of this paper is based on the idea that addressing the problem of remote configuration by the concept of *disposable configurations* is an efficient, secure and reliable mechanism to maintain both the flexibility and the security of the system.

In our proposed concept, disposable configurations must have four properties:

(1) The server must provide configurable systems with disposable configurations (by sending configurations individually or by multicasting them).

* Corresponding author. Tel.: +33 4 77 91 57 92.
E-mail address: lilian.bossuet@univ-st-etienne.fr (L. Bossuet).

http://dx.doi.org/10.1016/j.micpro.2015.05.007
0141-9331/© 2015 Published by Elsevier B.V.

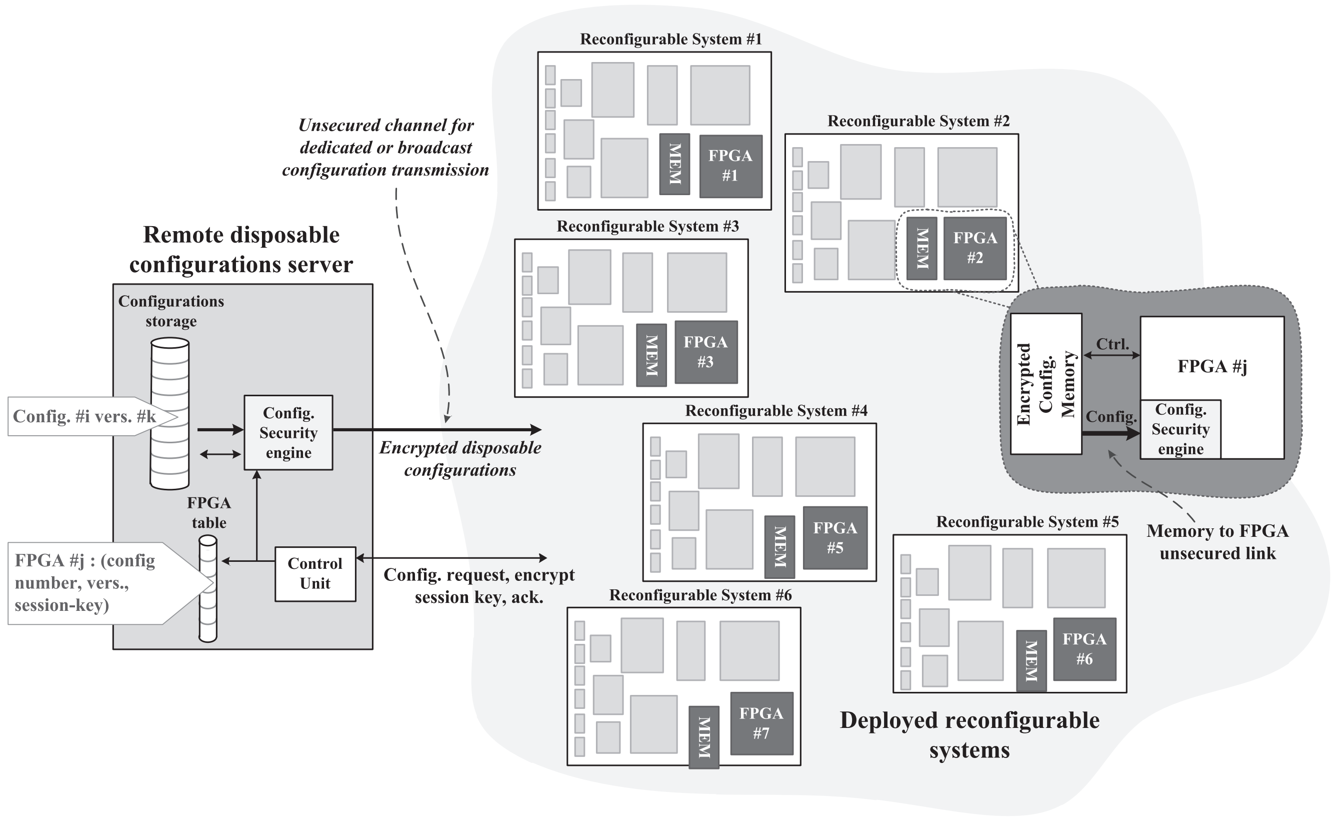

Fig. 1. A set of remotely configurable systems connected with a remote server featuring enhanced security by using disposable configurations.

(2) Each disposable configuration must be linked to a concrete version of the system or its reconfigurable part.
(3) Each disposable configuration can be used only once. If a reconfigurable system requests or accepts a new disposable configuration from the server, it can no longer use previous configurations. This is the main characteristic of disposable configurations: they are used once and only once in one concrete reconfigurable system.
(4) To guarantee security, the disposable configurations are encrypted before they are sent to the target system(s). In our case, the uniqueness of each configuration is guaranteed by using a new key for each new encrypted configuration. These newly generated disposable keys are hereafter called *session keys*.

All the above-mentioned features of disposable configurations are important to maintain security.

The rest of this paper is organized as follows. Section 2 analyzes the security of the proposed system and possible threats. Section 3 gives the background and prior work on reconfiguration security. Section 4 details the different security protocols for both unicast and multicast remote configurations. Section 5 presents the HCrypt cryptoprocessor which is the cryptographic engine used to provide security services such as confidentially, integrity and secure key management. Section 6 discusses security of the proposed remote configuration scheme and hardware features, and Section 7 concludes the paper.

2. Threat model

When describing the threat model related to the system shown in Fig. 1, we use the following assumptions:

- The server is located in a trusted area (it cannot be attacked either by hardware or software means).
- The FPGA is located in an untrusted area. The embedded hardware in charge for securing the FPGA device reconfiguration can be exposed to hardware and software attacks.
- Once configured, the FPGA is considered to be a trusted area and it cannot return the configuration data (using its data or JTAG interfaces or any other communication channel).
- The FPGA configuration cannot be modified by any external means – internal FPGA configuration memory is therefore accessible only for writing.
- The on-board configuration memory is not trusted in the model described here.
- The communication channel between the configuration server and the reconfigurable system is not trusted.

Configurable systems are particularly vulnerable to the following threats:

Cloning: without configuration security, it is easy to record configuration data during device configuration and to replay the recorded bitstream in a compatible configurable system (i.e. a cloned system using the same FPGA device). This can result in a major problem of intellectual property theft and economic risk.

Reverse engineering: if the configuration file is recorded, the design may be reverse-engineered [8]. If the attacker succeeds in reverse engineering the bitstream, he can obtain full knowledge of the system related to the configuration bitstream concerned. Although this kind of attack is more complex than recording and copying configuration bitstream, it allows the attacker to target other FPGA devices than those that were successfully attacked.

Both cloning and reverse engineering attacks on FPGAs belong to the group of passive attacks, which are difficult to detect