ECOLE
POLYTECHNIQUE
DE BRUXELLES

ULB

UNIVERSITÉ LIBRE DE BRUXELLES

Implementation of High-Level Cryptographic Protocols using a SoC Plateform

Mémoire présenté en vue de l'obtention du diplôme
d'Ingénieur Civil en informatique à finalité spécialisée

Quentin Delhaye

Directeur
Professeur Frédéric Robert

Superviseur
Sébastien Rabou (Barco Silex)

Service
BEAMS

Année académique
2014 - 2015

Abstract

by Quentin Delhaye, Arnaud Dumont, Camille Giaux, Pierre Lasbleis and Gauthier Roig; Université Libre de Bruxelles, 2011–2012.

Résumé

par Quentin Delhaye, Arnaud Dumont, Camille Giaux, Pierre Lasbleis et Gauthier Roig ; Université Libre de Bruxelles, 2011–2012.

Aknowledgements

Thanks a bunch of people here : - Frédéric Robert for his support - Sébastien Rabou for his insight - Batien Heneffe for his extensive help

Contents

Chapter 1

Introduction

1.1 Challenge

1.2 Network security

Chapter 2

Presentation

Here we talk about the protocols, the platform. Show The OS stack (kernel/user)

2.1 Experimental setup

The experimental environment is build around a standard x86 host and an ARM Cortex-A9 alongside an Altera Cyclone V FPGA as the target.

2.1.1 x86 host

OS Ubuntu 12.04 LTS, kernel 3.16

CPU Intel Core-i3 ... (two logical core out of four)

RAM 1.5GB DDR3

2.1.2 Altera Socrates SoCFPGA

OS Yocto project, kernel 3.14

CPU Dual core ARM Cortex-A9, 800MHz

RAM ...GB DDR3

FPGA Altera Cyclone V

Chapter 3

Implementation

Appendix A

Cross-compilation

A.1 OpenSSL

A.2 OpenVPN

A.3 nginx

A.4 Strongswan