MỘT GIAO THỨC AN TOÀN ĐỂ TRAO ĐỔI KHÓA BẢO MẬT CHO VIỆC CẬP NHẬT HỆ THỐNG NHÚNG CẤU HÌNH LẠI ĐƯỢC TỪNG PHẦN

A SECURE PROTOCOL TO EXCHANGE SECURITY KEY FOR UPDATING PARTIALLY RECONFIGURABLE EMBEDDED SYSTEM

Tác giả: *Trần Thanh; Trần Hoàng Vũ; Nguyễn Văn Cường; Phạm Ngọc Nam*

Tóm tắt bằng tiếng Việt:

Để đảm bảo tính bảo mật và tính sẵn sàng của dữ liệu, khóa đối xứng, còn được gọi là khóa bí mật, phải được trao đổi một cách an toàn giữa các bên để mã hóa dữ liệu trước khi bắt đầu một phiên giao dịch thông qua mạng công cộng không an toàn. Bài viết này trình bày một giao thức nhằm nâng cao tính bảo mật của sự trao đổi khóa đối xứng và tính linh hoạt của việc cập nhật các hệ thống nhúng cấu hình lại được từng phần qua Internet. Giao thức đề xuất sử dụng một thuật toán mã hóa bất đối xứng để bảo vệ các khóa mã hóa đối xứng để ngăn ngừa trộm cắp và giả mạo trên đường truyền tải. Ngoài ra, bài báo này trình bày một giao thức để bảo vệ các lõi IP từ việc cập nhật từ xa. Kết quả thử nghiệm từ một hệ thống nguyên mẫu dựa trên FPGA cũng được đưa ra và phân tích rõ ràng.

Từ khóa: Khóa bảo mật; khóa đối xứng; khóa công khai; thuật toán bảo mật; FPGA.

Tóm tắt bằng tiếng Anh:

To ensure the data confidentiality and availability, a symmetric key, called secret key, must be exchanged securely between parties for encrypting data before beginning a transaction session pass through an insecure public network. This paper presents a protocol to enhance the secrecy of exchanging symmetric key and the flexibility of updating the partially reconfigurable embedded system over the Internet. The proposed protocol uses an asymmetric encryption algorithm to protect symmetric encryption keys from thefts and tampers over a transmission line. In addition, this paper presents a protocol to protect the IP cores of remote updating. Experimental results from a prototype system based on FPGA are also revealed.

Key words: Security key; symmetric key; public key; security algorithm; FPGA.