Journal of Information Security and Applications 38 (2018) 111–121

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Bump in the wire (BITW) security solution for a marine ROV remote control application

Muzaffar Rao[a,b,c,*], Thomas Newe[a,b,*], Edin Omerdic[a], Admir Kaknjo[a], Walid Elgenaidi[a,b], Avijit Mathur[b], Gerard Dooly[a,b], Elfed Lewis[b], Daniel Toal[a]

[a] Department of Electronic and Computer Engineering, Mobile Marine Robotics Research Centre, University of Limerick, Ireland
[b] Department of Electronic and Computer Engineering, Optical Fibre Sensors Research Centre, University of Limerick, Ireland
[c] Sir Syed University of Engineering & Technology, Department of Telecommunication Engineering, Karachi, Pakistan

ARTICLE INFO

Article history:

Keywords:
BITW
AES
FPGA
ROV
Marine control
Data security

ABSTRACT

The work presented here describes a Bump-In-The-Wire (BITW) security solution for the provision of secure communications for a Marine ROV Control Application. The targeted marine application involves controlling a 'Remotely Operated Vehicle (ROV)' from a remote control station through standard Internet. A BITW solution is required as communication through the Internet is inherently insecure and open to signal modification or tampering. BITW technology is an implementation approach that places a security mechanism outside and independent of the system that is to be protected, in this case that is a ROV and its remotely located control station. Secure communications between the ROV and the remote control station is necessary to ensure that only authorised persons can issue control commands to the ROV and that no unauthorised individual can understand/sniff the communications between the ROV and control station. The proposed BITW security solution involves an efficient implementation of the AES cryptographic algorithm on a Field Programmable Gate Array (FPGA) platform. The extra delay introduced into the remote control application was well within the allowable time window of 50 ms. Other security mechanisms can also be implemented in the same way depending upon the availability of hardware resources.

1. Introduction

Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. To secure information, the following needs to be implemented: (a) The confidentiality of data must be guaranteed, (b) The integrity of data must be preserved, and (c) Data authentication should be assured. Information security issues have been important throughout history, but the significance of information security has grown with the development in digital computing and information technology. In today's high technology environment, information security is essential for every type of communication that involves the internet as the internet is an inherently insecure communication media [1].

Information security is generally achieved by using cryptography and cryptography is based on cryptographic algorithms. When these algorithms are combined into a secure solution you get security protocols. To use cryptographic solutions in practice, efficient implementations are necessary as stated by Cilardo et al. in [2] i.e;

"A mathematical construction with practical applications, such as a cryptographic algorithm, has no real interest, in an engineering sense, as long as methods for feasible implementation are not available"

The motivation for this work is to provide an efficient implementation of a security solution for a real time marine based application. While this work is capable of securing any type of communication that uses the internet, here we apply it to a specific application in a marine ROV control situation. The novelty of this work is best describes as a BITW security solution with a real time efficient implementation of AES for a marine ROV control application. To the best of the author's knowledge this is the first work that proposes a BITW security solution for use in the marine environment.

* Corresponding authors.
E-mail addresses: muzaffar.rao@ssuet.edu.pk (M. Rao), thomas.newe@ul.ie (T. Newe), edin.omerdic@ul.ie (E. Omerdic), admir.kaknjo@ul.ie (A. Kaknjo), walid.elgenaidi@ul.ie (W. Elgenaidi), avijit.mathur@ul.ie (A. Mathur), gerard.dooly@ul.ie (G. Dooly), elfed.lewis@ul.ie (E. Lewis), daniel.toal@ul.ie (D. Toal).
URL: http://www.mmrrc.ul.ie, http://www.ofsrc.ul.ie (M. Rao), http://www.mmrrc.ul.ie, http://www.ofsrc.ul.ie (T. Newe), http://www.mmrrc.ul.ie (E. Omerdic), http://www.mmrrc.ul.ie (A. Kaknjo), http://www.mmrrc.ul.ie, http://www.ofsrc.ul.ie (W. Elgenaidi), http://www.ofsrc.ul.ie (A. Mathur), http://www.mmrrc.ul.ie, http://www.ofsrc.ul.ie (G. Dooly), http://www.ofsrc.ul.ie (E. Lewis), http://www.mmrrc.ul.ie (D. Toal)

https://doi.org/10.1016/j.jisa.2018.01.001
2214-2126/

This article is presented in two parts. The first part discusses a marine application, developed by the Mobile & Marine Robotics Research Centre (MMRRC), at the University of Limerick (UL), that is used as a target application (as mentioned earlier) to implement the proposed security solution. Details of the full development of this application are not presented as they deemed out of the scope for this article. However, a brief summary of the application is discussed to give an outline of the Marine platform used for testing and verification of the proposed security solution. The second part of this article provides details about the proposed security mechanism, its design, implementation and utilization in real time with the aforementioned marine application.

The targeted Marine application consists of a control station and ROV. In this application the ROV is controlled and monitored through the Internet using a remote control station. To secure the communication between the control station and the ROV a BITW architecture is introduced. A BITW architecture is an implementation approach that places an information security device/mechanism outside of the system that is to be protected, thereby facilitating secure communications without existing system major hardware modifications. The BITW security solution proposed here is suitable to use in applications where existing network interface devices do not support security checks or services. These applications/interfaces are susceptible to various security attacks [3,4] like, denial of service (DOS) attack, attacks on information in transit where signals are altered or deleted etc. To provide security for many of these applications it generally requires considerable hardware changes, in particular to network interface devices that attach to the Internet, so, the simplest and most cost effective solution to secure these applications is the BITW solution proposed here.

As mentioned earlier security services like data confidentiality, integrity and authentication are required to fully secure communications for any application. This article concentrates on the data confidentiality security service because the available hardware resources in the targeted marine control application cannot facilitate all three services due to a restricted FPGA size. Although it should be noted that the same procedure/process can be used to introduce integrity and authentication services in the case of a larger FPGA becoming available.

The confidentiality security service is implemented using a symmetric-key cryptographic algorithm like the Advanced Encryption Standard, AES. AES is a secure and well researched algorithm that is used to provide encryption security services. AES is the most popular encryption technique trusted by various organizations including the National Security Agency (NSA), (the cryptologic intelligence and security agency of the US government). The NSA allows AES to be used for classified data up to top secret level [5]. This work presents an efficient implementation of AES on an FPGA platform.

Cryptographic algorithms are computationally expensive [6–9] and their software based implementations are often too slow for real time applications, which yields a need for hardware implementation. For hardware implementation of cryptographic algorithms FPGAs are one of the best development platforms, because they provide both speed and re-configurability. The use of FPGAs for cryptography has been intensively studied by researchers and proved to be the best research hardware platform for cryptographic algorithm implementations.

The metrics used in this work for the evaluation of the FPGA implementation are: maximum operating frequency (maximum allowable clock frequency on which the designed circuit can operate); latency (Total number of clock cycles require to process one block of the input message); throughput (TP) calculated using Eq. (1); TPA (ratio of throughput and area) calculated using Eq. (2);

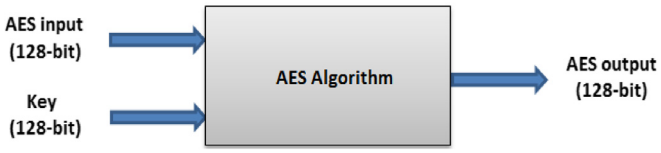

Fig. 1. AES with key size of 128-bit.

and area (number of slices utilized in the FPGA device).

$$TP = \text{Block Size}/(T_{min} * N_{clk}) \quad \ldots. \tag{1}$$

$$TPA = TP/\text{Area} \ldots. \tag{2}$$

Where,

Tmin = Minimum allowable time period of the operating clock.
Nclk = Number of clock cycles required to process one block of input message.
Block Size = 128-bit (For AES).
Area = Number of Slices utilized.

The structure of this article is as follows: Section 2 summarizes the AES algorithm; Section 3 discusses related work; Section 4 provides detail of the proposed AES implementation; Section 5 presents a comparison and discussion of related work with the proposed AES implementation; Section 6 presents an overview of the developed marine application; Section 7 outlines the experimental setup and its implementation details; Section 8 discusses performance results and Section 9 presents testing and verification details while Section 10 concludes the paper.

2. Advanced encryption standard (AES)

AES [10] is a symmetric-key based encryption algorithm, which has a fixed block size of 128-bit (or 16-bytes). This algorithm supports the key sizes of 128, 192 and 256 bits with iterative rounds of 10, 12 and 14 respectively. The selection of the number of rounds depends on the chosen key size. Each round of the AES algorithm uses a different key, derived from a separate key-expansion unit. Here, a key size of 128-bits is used for the proposed AES implementation, as shown in Fig. 1.

AES [10] comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). It can therefore be said that AES is based on a 'substitution–permutation (SP)' network.

The input, output and key bit-series of AES are processed as arrays of bytes, called 'states'. The state array consists of a 4×4 matrix in which every row consists of 4- bytes (So, total bytes $= 4 \times 4 = 16$). This state array is updated after the execution of each step of the AES operation. Each round of AES consists of 04 steps, as shown in Fig. 2: **(1)** Byte Substitution (BS), **(2)** Shift Row (SR), **(3)** Mix Column (MC) and **(4)** Add Round Key (ARK). Details of these steps is given in [10].

The AES algorithm has both excellent confusion and diffusion characteristics. The confusion is provided by the 'BS' operation, in which the use of the S-box is non-linear and good at destroying patterns. The diffusion is achieved by using the above mentioned 'SR' and 'MC' operations. The diffusion stage spreads the influence of each plaintext bit over many cipher text bits. Both confusion and diffusion are repeated several times for each input to increase the amount of scrambling. The secret key is mixed in at every stage, so that an attacker cannot pre-calculate/anticipate what the cipher stages will output. The only way to crack the AES is with luck or a brute force attack, but even with a supercomputer, it