International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 2,Issue 2 :Page No.124-128 , March - April 2013
https://www.mnkpublication.com/journal/ijlrst/index.php

E-COMERCE SECURE TRANSFER BASED ON EMBEDDED DSP

Farah Hanna Zawaideh
Irbid National University
Computer Information System Department

Abstract* - *The e-commerce is a very critical issue in information transfer because of the money is the manipulated variable. The criticality, danger, and higher priority importance of any e-commerce transfer makes it to be hot area of interest in modern computer science and informatics. The security of e-commerce transfer is an issue of computer system and informatics rather that the issue of administration. One key element that provides higher security for modern e-commerce systems is the cryptography. The cryptography is commonly known that software-based encryption has built-in security weaknesses due to storing and managing digital certificates/keys in a high-risk environment such as a local hard disk or software. The cryptography methodologies are based on complex mathematical formulation, calculus, and non-linear algebraic math. Which leads to use an embedded hardware in order to encrypt the required message and thus, makes it more reliable, and more ease to implement. In fact, the embedded encryptor represents a superior solution. Actually, the most of used embedded hardware encryption modules requires additional software to module and achieve the secure e-commerce application. Thus, it increases the cost and doubles the systems complexity. This paper, contributes new embedded encryptor based on DSP to build a rigid cryptography module. The contributed algorithm is based on RSA encryption algorithm. It is implemented and adapted to provide trusted security level on any transaction of e-commerce with respect to client, and administration. This research integrates the DSP based embedded encryption to build a module that combines both, programming flexibility and computational power. It targets the common web browsers those are commonly used in e-commerce applications. This integrated system is intended to process and store the e-commerce transactions in sensitive data inside the hardware that is used to be plugged inside the computer. This paper increases the security strength and limits the overhead by adapting the common available web browsers, thus, completing the transactions applications that required in high efficiency. The web with full functionality of e-commerce is a system that developed to measure the validity of the contributed system and algorithm. The contribution of this paper is to perform an RSA encryption that is pluggable to the computer, and it is capable to encrypt and store the critical e-commerce transitioned, it is also based on common web browsers.

***Keyword* -** Encryption, RSA, Security, E-Commerce, DSP, Web Browsing.

1. INTRODUCTION

The e-commerce security is a critical issue because of its very sensitive controlled variables. Eventhough the researches in that field is very wide, but it still do not concern the real criticality of the field. Many issues are considered to be important in the e-commerce security; access control, authentication / identificaiton, origin non-repudiation, confidentiality, intrusion detection, antivirus, integrity of the data, and such issues. The techniques that based on encryption / cryptography is widly used in problem formulation of confidentiality, non-repudiation, and integrity of the data. the cryptography of public key is providing strong cryptographic system structure. The Rivest, Shamir, and Adam (RSA) algorithm in public keying encryption is now considered to be the most used encryption mehtodology. Many engines / structures uses RSA in e-commerce. But in fact, all of the applications in that field are implemented in software, while a very few researches considers the hardware reasonability of encryption. The cryptography using software RSA is avoiding some problems like distribution of the key and inherent of the management in cryptographic of secret keys. The authority certificates requires to be sure from that the party is indeed in possession of the key that being private according to the public key that is existed in the certificate. Private key security is still considered to be big problem where the whole transfer should be secure in the whole of operation, not only during transfer. The software that needs a public key access should be able to protect the key that accessed.The reason of failure of most proposed methodologies in modern researches for such field is concerned to the fail of that techniques to ensure a real private key security and protection.

In fact, the break of the key is easier than protect of them, this come from the fact that, the researchers and developers are intended to develop new techniques in such field. While in breaking of that security, there are a kind of people helps the researchers and developers to break it, they are the happiest and students those love to learn how to attach and break the known security issues.

This paper is propses cryptography technique that base on hardware system to implement the complexity of encryption / decryption. In fact, the cryptography using hardware implementation - instead of software - could ensure advantage of high power in computations (i.e. complex domain mathmatical formulation and transformation), so, the security features is more easier to be implemented using hardware rather than software.

Publication History

Manuscript Received	:	*29 March 2013*
Manuscript Accepted	:	*25 April 2013*
Revision Received	:	*28 April 2013*
Manuscript Published	:	*30 April 2013*

This paper implements a hardware for cryptography that implements an RSA encryption / decryption technique. This implementation is concerns on using microprocessor sub-system which is required to implement a rigid RSA cryptographic system. The design is based on DSP processor in addition to re-programmable memory inside the processor, which is benefit in increasing up the speed of processing.

The hardware of cryptographic system that is implemented using DSP microprocessor ensures the most power full mathematical formulation in RSA encryption / decryption process. A description of one powerful attack, called fault-based cryptanalysis, was released by Bell core. But in fact, this paper does not aims to formulate this problem.

The implemented hardware is embedded system for cryptographic formulation. It is dedicated microprocessor based hardware that can provide very high computational power, it involves high lacks flexibility and investment cost. Embedded hardware, such as smart cards, and especially DSP is a unique solution for this problem. A digital signal processor can provide high computational power and much higher than the computational power of normal microprocessors. In addition, the DSP ensures flexibility in implementation and coding, more than any other hardware or software based cores. It also has a low cost with respect to other hardware sub-system. Another significant advantage is that nearly every PC has a USB interface and communication ports that is capable to support DSP boards. Implementation of the RSA cryptosystem on a DSP chip is non-trivial. The RSA cryptosystem is based on the theory of large prime number factorization and thus requires very intensive modulo computation as well as storage-intensive big number processing, which is very difficult to accommodate on a single DSP chip with limited computing capacity and storage space. In the literature very few reports of RSA implementations on DSP hardware have been found.

The research of [2] presents design and implementation of RSA cryptosystem using multiple DSP chips is presented. The system allows for additional DSP chips to be inserted in allocated slots to improve performance. In that system, the DSP application could be controlled by a PC application using RS232 serial communication port.

The research [3] is demonstrating a fast RSA encryption module that is developed through exploiting the computational characteristics of Motorola brand DSP. Nowadays most hardware RSA cryptosystems have been developed either as an isolated encryption module that is not easily integrated into existing e-commerce systems to provide secure transactions, or as a complicated and expensive system that requires additional dedicated software packages to perform e-commerce functions. On the other hand web browsers have played a dominant role in business to customer e-commerce services.

Obviously, the integration of existing e-commerce resources, such as web browsers, with the embedded hardware encryption module is of significant interest. Comparing with conventional e-commerce systems deploying standalone and dedicated software, the proposed integrated systems would have the benefits of a higher security level by using embedded RSA encryption hardware as well as limited overhead cost and reduced complexity by using existing web browser software.

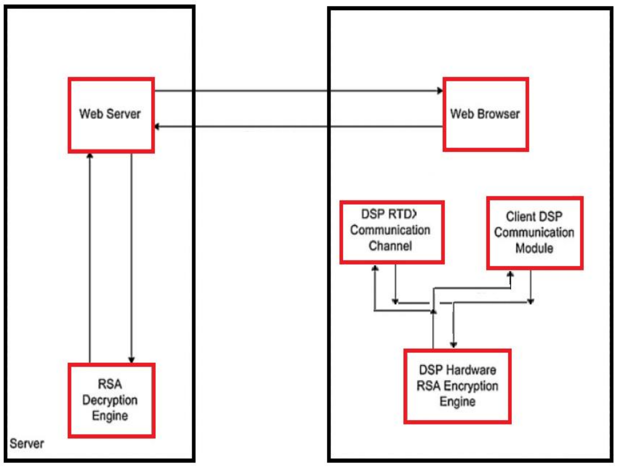

Figure-1: Proposed Encryption / Decryption Scheme

2. DSP BASED TRANSFER

For secure e-commerce transactions an implementation of the RSA public key encryption algorithm embedded in DSP hardware is proposed as shown in Figure 1.

The system is based on the client/server model and consists of two major parts: the server and the client. The server consists of a web server, a database server, and an embedded RSA software decryption engine. The client includes a web browser, a client DSP communication module, and a DSP hardware RSA encryption engine. The server and the client communicate with each other using TCP/IP protocols in the Internet/Intranet environments. On the server side, the RSA decryption engine is only activated when there are decryption requests from the web server. The client DSP communication module can be downloaded and installed rom server to client. It can also run embedded inside the client web browser.

At the start of the operation, the client web browser requests a web page that contains the client DSP communication module as an embedded script. The server sends the requested page to the client. The client DSP communication module is then installed and activated. The server can also send its public key to the client in the requested web page if the client does not obtain it from another source such as a Certificate Authority. How to effectively deliver and install the product is not the concern of this paper. The user can purchase the product directly from the software retailer and install it accordingly.

When the user enters data (plain text) into a data entry form in a web page and submits the information, the client DSP communication module captures the plain text, it then establishes an input communication channel to the DSP hardware encryption engine, and sends the public key and the plain text to the encryption engine.

Upon receiving the public key (or obtaining it by other methods and storing it in the DSP chip) and the plain text, the DSP hardware RSA encryption engine encrypts the plain text, and then sends the cipher text back to the client DSP communication module through an output communication channel.

The client DSP communication module embedded in the web browser is responsible for all communications between the client (the web browser) and the DSP hardware RSA encryption engine. Since the communication module is an embedded component of the browser, it exchanges the information with the browser via the browser's object programming interface. Communications with the hardware encryption engine proceed using DSP Real-Time Data Exchange (RTDX) channels, which come as a software library together with the DSP application development tools. The RTDX communication channels can support real-time and full duplex data exchanges.

RTDX communication channels can be operated in non-continuous and continuous modes. In non-continuous mode, the transferred data are recorded into a log file that has been specified in RTDX configuration. Non-continuous mode is used when the programmers want to capture a finite amount of data and save it into a log file. In continuous mode, data are logged into a circular memory buffer in the RTDX Host Library. This mode is used when users want to continuously obtain and display the data from a target application, with no requirement for storage of the data in a log file. For the purpose of this project, we use RTDX in continuous mode to process the data in real-time, while avoiding the storage of plain text data on the hard disk.

3. METHODOLOGY

This paper presents a novel DSP based RSA encryption / decryption hardware module that is developed using a general floating-point TMS DSP microprocessor evaluation board and software development tools. The hardware RSA encryption module is integrated into the client side of a functional e-commerce system to enhance its security performance. The use of multi-DSP hardware encryption/decryption modules on the server side of the web system is also an option. This topic is not discussed here and left for future work. Experimental results have shown that the DSP hardware RSA encryption module could be used efficiently to improve security for e-commerce transactions.

The system implementation is capable for RSA commercial plugging availability. RSA plug-in encryption device which can store and encrypt sensitive information originated from the e-commerce process using standard web browsers.

Implementation details addressing challenging issues such as big integer, large message, and communication components have been provided which have never been reported in the public literature. This can be very useful for real-life industry security applications. The choice of DSP hardware to be TMS is simply for the convenience of illustrating the concepts due to our existing relevant expertise, majority technical issues such as system architecture, big integer implementation, message block size calculation, etc. where those are common or similar in other DSP hardware.

A functional prototype system has been built for the proof of concepts. The DSP hardware RSA encryption engine consists of two parts; the implementation of RSA encryption algorithm to encrypt the messages and the RTDX communication library to communicate with the web browser through the client DSP communication module.

On most modern 32-bit computer architectures, integers are defined as a maximum of 32 bits, and optionally the size can be reduced to 16 bits. The maximum values representable by a 16-bit and 32-bit unsigned integers are 216 −1=65 535 and 232 −1=4 294 967 295, respectively. However, the RSA algorithm requires keys on the order of 10100 or larger, which are clearly larger than the standard integer types. The solution is to use an array of fixed integers to represent the big integers or multiple precision integers. This allows the accommodation of any integer values, and is limited only by the size of the physical memory.

Numbers are stored in a redundant representation and additions/subtractions are performed without carry propagation. The algorithm was found efficient, especially in applications where modular multiplications are carried out iteratively. However, the described algorithm is suitable for DSP with a general architecture. The base for multiple precision integer representation is selected as 65 536 or 216. The major advantage of representing the integer in base 65 536 over base 10 is that it requires far less memory. This is very important, especially in the embedded systems that typically have limited memory. Furthermore, with base 65 536 (216), fast shift operations can be used to replace high-cost multiplication and division operations. This, in turn gives better computational performance. A larger base than 65 536 will make implementation of the normal arithmetic operations more complicated because on most currently used computing systems, the largest integer supported is 32-bit length. With 32-bit integers the built-in machine level arithmetic functions cannot be used directly as the results would overflow the 32-bit registers.

The Big Integer package has been implemented with all the big integer arithmetic functions to support RSA encryption/decryption algorithm. The implementation of arithmetic functions is based on efficient arithmetic implementations in Ref. [1]. Other functions such as input and output are also implemented to convert string messages to Big Integer and vice versa.

In the RSA algorithm, the equation C= memod(n) is used to encrypt message m using the public key (n, e). In order to make RSA encryption work properly, the message m must be represented as an integer and value of (m) must be less than value of (n) [10]. Therefore, for large message, the first step is to decide on a message block size based on the size of public key n. Next, the message is divided into blocks and converted to the appropriate big integers.

The final step is to use the RSA algorithm to encrypt the blocks and compose a cipher text output. The size of the block could be a fixed or changeable value depending on the system's design. Theoretically, the block size could be any value provided that value which must be less than value of (n). However, the block size should not be too small as a block cipher with a small block size may be vulnerable to the attacks based on statistical analysis. One such attack involves simple frequency analysis of cipher text blocks. Therefore, to maximize security, the block size must be as large as possible and roughly the same size as public key n.

In addition, a large block size increases the complexity of the implementation. In this paper, the selected message block size in characters is equal to the bit-size of public key divided by 2.5 (taking rounded off integer value)..

The TMS RTDX library has been included in the DSP hardware RSA encryption engine to support real-time communication between the DSP and the client DSP communication module. The built-in RTDX library provides functions to initialize the RTDX communications, open communication channels, read/write data to the channels and close the channels. In order to make the RTDX communication channels work properly, they need to be configured with the correct mode and a suitable data buffer size.

As discussed above, because the client DSP communication module plays the role of a communication bridge, it must be able to communicate with both the web browser and the DSP hardware RSA encryption engine. The module exchanges information with the DSP application using RTDX channels while it communicates with the browser via object linking and embedded interface.

The implementation of the communication module consists of two groups of functions: the browser interface functions and the DSP interface functions. The browser interface functions are used to exchange data with the web browser and are callable from the browser using scripting languages such as JavaScript. The DSP interface functions are implemented based on RTDX exported library functions that provide communication channels to and from the DSP application.

So, in order to maximize the performance of the RTDX communication channels, the number of read/write operations to the channels in a session should be minimized. In our implementation, we use the read/write operations in batch mode to improve the performance of the RTDX channels. In order to use the client communication module, it is embedded in a web page using an HTML <OBJECT> tag. The module is designed so that it can be downloaded and installed automatically on the client machine.

The decryption engine was developed using Microsoft Visual C++ and linked as a Dynamic Link Library (DLL) to run on the server. It supplies all of the necessary functions of an RSA decryption library. The decryption engine was installed on the server and integrated into the web server. The engine is only active when there is a request for message decryption from the web server.

4. RESULTS

Several experiments were conducted on the client/server systems using hardware and software described above with the various RSA key lengths and message sizes. Encryption performance was tested with RSA key pairs ranging from 128 bits to 2048 bits and message sizes of 512 bytes, 1024 bytes, and 2048 bytes. The performance statistics of the model are shown in Tables I. Table I shows the overall encryption speed, including communication overheads between the client and the DSP, and the encryption speed within the DSP.

Performance of the system is fast enough for small to medium size messages, especially with RSA key lengths up to 1024 bits. In this papers experiments the encryption time of credit card information is less than 0.5 and less than 1.3 s with the key lengths of 256 and 512 bits respectively, which is very satisfactory from point of user's experience. It should be noted that speed performance is not the primary consideration of this project. Therefore, an external plug-in DSP board is chosen to maximize the convenience of the client and the system security as the keys stored on this board are much more securely protected than keys stored in software on the PC or on the PC hard disk.

Message Size	Speed (K bit / Sec)						
(Byte)	128	256	512	1024	2048	4096	8192
512	3.05	1.723	0.410	0.098	0.042	0.019	0.005
1024	3.285	1.840	0.415	0.105	0.051	0.021	0.006
2048	3.306	2.090	0.428	0.112	0.055	0.022	0.009

Table I: DSP Encryption Speed

Plugging a DSP card into the PCs USB port could reduce overheads in transmission and improve the overall speed of the system. It is also inconvenient since it requires opening the PC case and represents a potential security risk since the keys are now stored in a software-accessible location within the PC. Experiments have shown that the TMS optimizing compiler used in our project generates code that is poorly parallelized, which leaves scope for significant performance improvement. Experience indicates that assembly coding of critical sections could also provide significant improvement of the overall system speed performance.

5. CONCLUSION

A successful efficient implementation of RSA DSP hardware encryption module using TMS DSP board is presented. The paper also provides details of efficient communication between a web browser and this RSA hardware module. A fully functional e-commerce system including the web and database server was built to test the concept proposed in this paper. The test bed built in this project is used for the purpose of a proof of concept; hence the speed performance is not the primary consideration. Further speed improvement can be obtained either by assembly coding of critical sections or by the use of an improved optimizing compiler. It should be noted that the external plug-in RSA encryptor can be protected by using password or PIN. For stronger protection, the emerging biometric security mechanism can be adopted.

REFERENCES

[1] Hu J. Mobile fingerprint template protection: progress and open issues. IEEE ICIEA Conference, Singapore, 3 - 5 June, 2008.

[2] Hoang XD, Hu J, Bertok P. A program based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference. Journal of Network and Computer Applications 2009; 32: 1219--1228.

[3] Hu J, Bertok P, Tari Z. Taxonomy and framework for integrating dependability and security. Chapter 6 Part II: Modelling the Interaction between Dependability and Security. In Information Assurance: Dependability and Security in Networked Systems, Qian Y, Joshi J, Tipper D, Kirshanamurthy P (eds). Elsevier, The Netherlands, 2008; 149--170. ISBN: 978-0-12-373566-9.

[4] Hu J, Qiu D, Chen HH, Yu X. A simple and efficient data processing scheme for HMM based anomaly intrusion detection. Special Issue of Advances on Network Intrusion Detection. IEEE Network 2009; 23(1): 42--47.

[5] Wang Y, Hu J, Philip D. A fingerprint orientation model based on 2D Fourier Expansion (FOMFE) and its application to singular-point detection and fingerprint Indexing. Special Issue on Biometrics: Progress and Directions, IEEE Transactions on Pattern Analysis and Machine Intelligence, April 2007.

[6] Izumi M, Sakiyama K, Ohta K. A new approach for implementing the MPL method toward higher SPA resistance. International Conference on Availability, Reliability and Security (ARES ’09),March 16--19, 2009, pp. 181--186.

[7] Han F, Hu J, Yu X, Feng Y, Zhou J. A novel hybrid crypto-biometric authentication scheme for ATM based banking applications. IAPR International Conference on Biometrics (ICB2006), 5--7 January, 2006, Hong Kong China. Published at Lecture Notes in Computer Science, Springer, 2005, 3832, pp. 675--681.

[8] 14. Kim CH, Oh S, Lim L. A new hardware architecture for operations in GF (2n). Transactions IEEE Computers 2002, 51(1): 90--92.

[9] 19. Hu J, Xi Z, Jennings A, Lee HYJ, Wahyudi D. DSP application in e-commerce security. Processing of IEEE International Conference on Acoustics, Speech, and Signal, 2, 2001, pp. 1005--1008.

[10] Han F, Hu J, Yu X. A biometric encryption approach incorporating fingerprint indexing in key generation. International Conference on Intelligence Computing (ICIC06), Kunming, China, 2006. Published at Computational Intelligence and Bioinformatics, Lecture Notes in Computer Science, Springer, 0302--9743, 4115, 2006, pp. 342--251.

[11] 21. Hoang XD. E-Commerce Security Enhancement and Anomaly Intrusion Detection using Machine Learning Techniques. PhD thesis, 2006, RMIT.