American Journal of Applied Sciences, 2012, 9 (11), 1868-1871
ISSN 1546-9239

doi:10.3844/ajassp.2012.1868.1871 Published Online 9 (11) 2012 (http://www.thescipub.com/ajas.toc)

E-Commerce: Security and Applications

[1]Ashraf Abdel-Karim Abu-Ein, [2]Hazem (Moh'd Said) Hatamleh, [1]Ahmed A.M. Sharadqeh, [2]As'ad Mahmoud Alnaser and [1]Omar AlHeyasat

[1]Department of Computer Engineering,
Faculty of Engineering Technology, Al-Balqa Applied University, P.O. Box: 15008 Amman 11134, Jordan
[2]Department of Computer Science,
Faculty of Ajlun, Al-Balqa Applied University, P.O. Box: 15008 Amman 11134, Jordan

Received 2012-04-21, Revised 2012-08-19; Accepted 2012-09-05

ABSTRACT

This study presents an investigation and comparing of all methods used in E-commerce security. Also it presents suggested methods to make e-commerce more secure. Applications of the E-commerce are demonstrated here. The efficiency of the security methods are measured and such efficiency increases as we combined more security methods with each other. A new method of security is suggested which is a combination between hash algorithm and Public Key Infrastructures (PKI). Index term-public Key Infrastructures (PKI), hash algorithm, E-commerce, security.

Keywords: Public Key Infrastructures (PKI), Efficiency Increases, Security is Suggested, E-Commerce Emonstrated Security Methods, Combined More, Commerce Security

1. INTRODUCTION

Electronic commerce or E-commerce can be defined as the use of all utilities offered by the networks and intenet in the processes of commerce like selling goods, petrol contracts and any other trading operations. The main advantages of this new trading methods is its rapidity and the two teams of the trading process can make the contract easily and in short given period of time. There are many estimations for the size of e-commerce, one of this estimations done by International Data Corp (IDC) which estimates the value of global e-commerce in 2000 at US$350.38 billion. In 2004 the size were increase to US$3.14 trillion. IDC founds that also in Asia's countries the size of e-commerce percentage share in worldwide e-commerce revenue from 5% in 2000 to 10% while some use e-commerce and e-business interchangeably,. In e-commerce, Information and Communications Technology (ICT) is used in inter-business or inter-organizational transactions (transactions between and among firms/organizations) and in business-to-consumer transactions (transactions between firms/organizations and individuals). Three primary processes are enhanced in e-business.

1.1. Production Processes

1.1.2. Customer-Focused Processes

1.1.3. Internal Management Processes (Ackerman *et al*., 2002; Krawczyk *et al*., 1997)

1.1.4. E-Commerce Applications

Various applications of e-commerce are continually affecting trends and prospects for business over the Internet, including:

- e-banking,
- e-tailing
- online publishing/online retailing. **Figure 1** (Ackerman *et al*., 1999; Keen, 2000)

2. MATERIALS AND METHODS

The short comings of e-commerce is the security, hackers and non-trusted persons may make such type of commerce insecure and nontrusted so a good and an efficient security method are required. One of the effective tools for ensuring the safety of e-commerce transactions, Public Key Infrastructures (PKI) combines a digital signature and Certificate Authority (CA), which can be public or private-a business acting as its own CA is private while a public one offers its services to businesses and provides secure key management.

Corresponding Author: Ashraf Abdel-Karim Abu-Ein, Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqa' Applied University, P.O. Box, 15008 Amman 11134, Jordan

Many researches treated the safety of the e-commerce, Marchany and Tront (2002) discussed a pertinent network and computer security issues and presented some of the threats to e-commerce and customer privacy. These threats originate from both hackers as well as the ecommerce site itself. A straightforward comparison could be made of the security weaknesses in the postal system vs. security weaknesses on the Net. The vulnerable spots in both cases are at the endpoints-the customer's computer/network and the business' servers/network.

Information flowing in the conduit (trucks/planes and wires) is relatively immune to everyday break-ins. Li *et al*. (2009), stated that most of studies about E-Commerce Security focus on the data confidentiality issue. Although security mechanisms, such as Secure Socket Layer (SSL) or Secure Electronic Transaction (SET), have been adopted in websites, catastrophic events that confidential data in Ecommerce are revealed happened more than once. The essential reason for this is that there exist potential security vulnerabilities in the E-Commerce applications themselves. The origins of these vulnerabilities are mainly from the lack of reliable input validation that can prevent E-commerce application from attacks. SQL Injection, Cross-Site Scripting (XSS) and Price Changing Attack are mainly known security threats to E-Commerce applications. These attacks and the protecting ways by using XML validation technology have been discussed and a framework that prevents E-Commerce applications from attacks. This study measures the efficency of the different safety methods used in e-commerce.

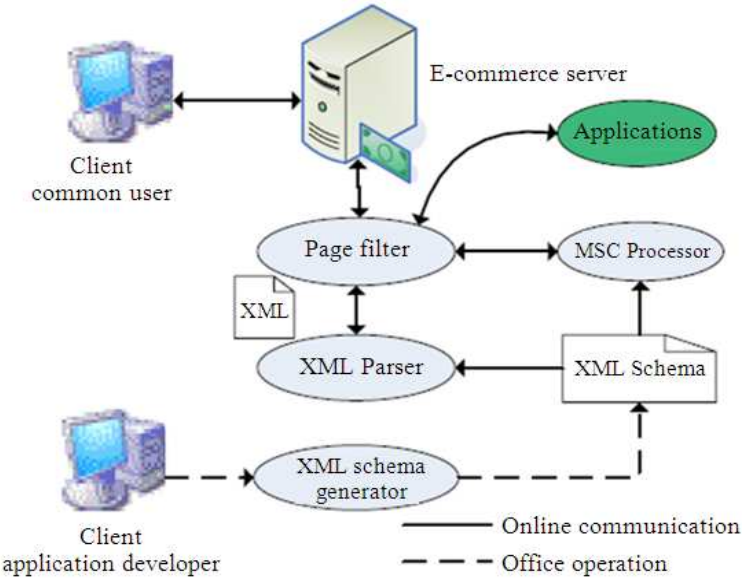

Fig. 1. E-commerce applications

Fig. 2. Hash algorithm

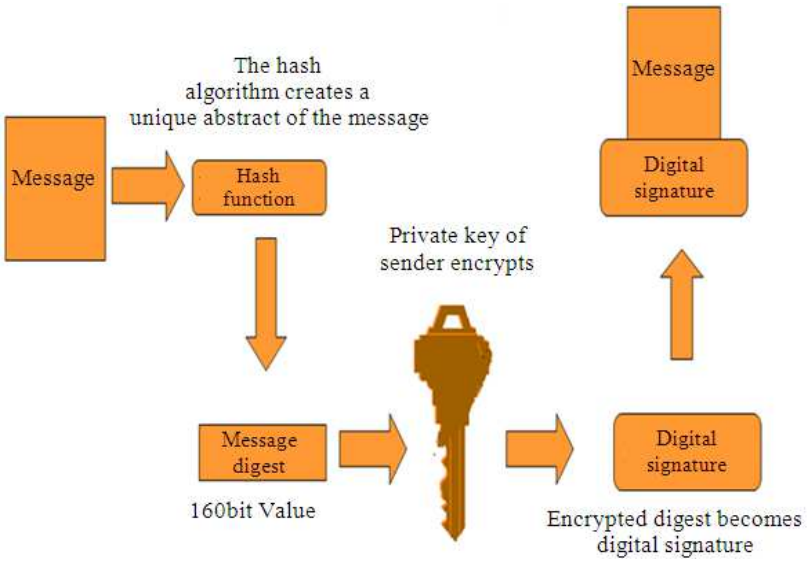

Fig. 3. suggested method block diagram

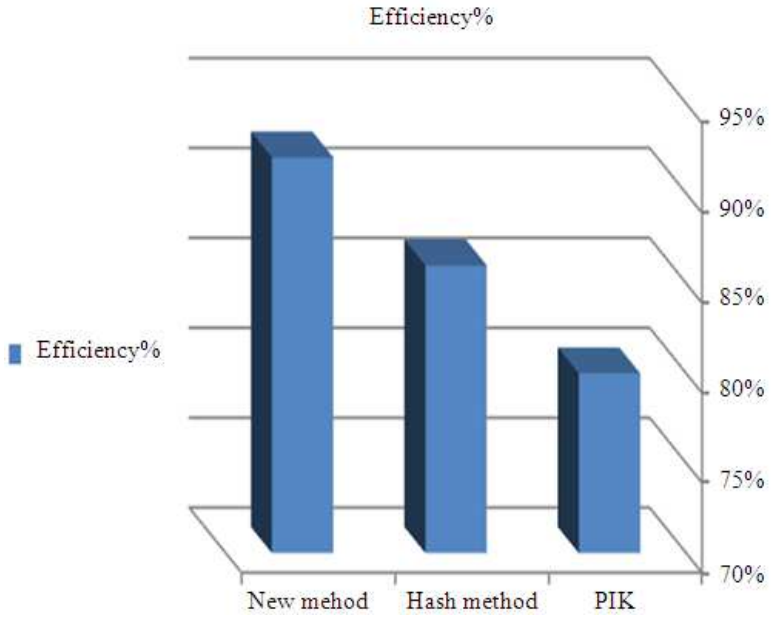

Fig. 4. Efficiency of E-commerce security methods

3. RESULTS

3.1. Suggested Method

The suggested method in E-commerce security combined between Public Key Infrastructures (PKI) which combines a digital signature and Certificate Authority (CA) and hash algorithm, **Fig. 2 and 3**.

4. DISCUSSION

The efficiency of the Public Key Infrastructures (PKI) is about 80%, while for hash algorithm it is about 86%, the new method reaches about 92%. As in **Fig. 4** below. The efficiency of the security of the method increases about 12% by average.

5. CONCLUSION

It can noticed that as more guards added for any information system more secure system is resulted this is clear from percent of efficiency of security methods shown above. So combining more security methods with each other may increase efficiency but may increase costs.

6. REFERENCES

Ackerman, M.S., L.F. Cranor and J. Reagle, 1999. Privacy in E-Commerce: Examining user scenarios and privacy preferences. Proceedings of the 1st ACM Conference on Electronic Commerce, (EC' 99), ACM New York, USA., pp: 1-8. DOI: 10.1145/336992.336995

Ackerman, S., S. Mark, D. Trevor and J. Daniel, 2002. Privacy in context. Hum. Comput. Interact., 16: 167-176. DOI: 10.1207/S15327051HCI16234_03

Keen, P.G.W., 2000. Ensuring E-trust. Computerworld Inc.

Krawczyk, H., M. Bellare and R. Canett, 1997. HMAC: Keyed-hashing for message authentication.

Li, Z., W. Guo and X. Zhao, 2009. Study on the application layer security in E-Commerce websites. Proceedings of the International Symposium on Web Information Systems and Applications, May 22-24, Nanchang, P. R. China, pp: 120-123.

Marchany, R.C. and J.G. Tront, 2002. E-Commerce security issues. Proceedings of the 35th Hawaii International Conference on System Sciences, (SS' 02), IEEE, pp: 1-9.