IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Study & Analysis of Secured E-Commerce Transactions Information Protocols-Purchasing Order

Deepu Saini[1] and Dr. Vijay Singh Rathore[2]

[1]Research Scholar, Singhania University, Jhunjhunu, Rajasthan, India
deepu254426@yahoo.com

[2]PhD (Computer Science), Singhania University, Rajasthan, India
vijaydiamond@gmail.com

Abstract

Electronic Commerce is the very rapid growing field in today's scenario. It is used for Purchasing Order i.e. for buying and selling electronic goods and all other type of things. And there is need for development of a number of e-commerce protocols, which ensure integrity, confidentiality, atomicity and fair exchange. The protocol uses a smart card for ensuring mutual authentication, dispute resolution and fair exchange and reduces reliance on a trusted third party. Also study and analysis of the security in e-transactions may avoid some of the frauds on internet transactions for purchasing and buying orders.

Keywords: *Purchasing Order, SET Procedure, Authorization Response, SET Protocols.*

Introduction

Now a days, internet is used everywhere and everyone is aware about the computers and how it is used. The increasing use of the internet has resulted in an increased interest in e-commerce. Consequently a number of e-commerce protocols have been proposed. Most of these protocols ensure that the information that is exchanged between the parties involved in the e-commerce is protected from unauthorized disclosure and modification. Moreover, researchers have identified several other desirable properties of e-commerce protocols. Examples of these properties include money atomicity and goods atomicity, and validated receipt. Money atomicity ensures that money is neither created nor destroyed in the course of an e-commerce transaction. Goods atomicity ensures that a merchant receives payment if and only if the customer receives the product. Validated receipt ensures that the customer is able to verify the contents of the product about to be received, before making the payment. Although such properties have been identified, a major problem is verifying if a given e-commerce protocol satisfies these properties, especially in the presence of network and site failures. In this paper we address the problem of protocol verification using existing software verification techniques. In particular, we use model checking [1, 9, 13, 14] to the modernly atomicity, goods atomicity and validated receipt properties of the secure e-commerce protocol proposed in [16]. In [16] the authors have informally shown that, in the absence of failures, their protocol has the money atomicity, goods atomicity and validated receipt properties.

The reasons for using model checking are as follows. First, model checking is a completely automated technique and considerably faster than other approaches, such as, theorem proving [2, 3, 7, 15]. Second, if a Property does not hold, a counter example is produced by the model checker who helps in understanding why the property does not hold. Last, but not the least, model checking has previously been used successfully to verify security protocols [9, 10, 11, 12]. In this paper we use the Failure Divergence Refinement (FDR) model checker [8]. The protocol that is analyzed is expressed as a communicating sequential process (CSP) [18], which we call SYSTEM. Each property that we wish to check is expressed as another CSP process, which we call SPEC. If SYSTEM is a refinement of SPEC (that is, the set of behaviors generated by SYSTEM is a subset of those generated by SPEC), we can infer that the protocol satisfies the property. The impact should be the security and how to increase the

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

successfulness of the electronic transactions in purchasing orders.

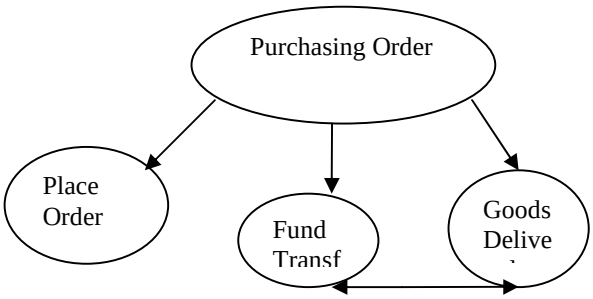

Figure 1: The Purchasing Order Structure

Advantages of E-commerce Transactions

The advantages of E-commerce transactions for business entities can be summarized thus: e-commerce can increase sales and decrease costs. A firm can use e-commerce to reach narrow market segments that are widely scattered geographically. The internet and the web are particularly useful in creating virtual communities that become ideal target markets. A virtual community is a gathering of people who share a common interest, but, instead of this gathering occurring in the physical world; it takes place on the internet.

Just as e-commerce increases sales opportunities for the seller, it increases purchasing opportunities for the buyer. Businesses can use e-commerce in their purchasing processes to identify new suppliers and business partners. Negotiating price and delivery terms is easier in e-commerce, because the web can provide competitive bid information very efficiently.

E-Commerce increases the speed and accuracy with which businesses can exchange information, which reduces costs on both sides of transactions.

E-Commerce provides buyers with a wider range of choices than traditional commerce, because they can consider many different products and services from a wider variety of sellers. The benefits of e-commerce also extend to the general welfare of society. Electronic payments of tax refunds, public retirement, and welfare support cost less to issue and arrive securely and quickly when transmitted via the Internet. Furthermore, electronic payments can be easier to audit and monitor than payments made by check, which can help protect against fraud and theft losses. E-Commerce can make products and services available in remote areas. For example, distance education is making it possible for people to learn skills and earn degrees no matter where they live or what hours of the day they have available for study.

Disadvantages of E-commerce Transactions

E-Commerce transactions also have its disadvantages. It is difficult to conduct a few businesses electronically. For example, perishable foods and high-cost items such as jewellery or antiques may be impossible to adequately inspect from a remote location, regardless of the technologies that are devised in the future. However, most of the disadvantages of e-commerce today are due to the newness and rapidly developing pace of the underlying technologies.

Return on investment numbers is difficult to compute for investments in e-commerce, because the costs and benefits are hard to quantify. Costs, which are a function of technology, can change dramatically during even short-lived e-commerce implementation projects, because the underlying technologies change rapidly.

In addition to technology issues, many businesses face cultural and legal impediments to e-commerce. Some consumers are still somewhat fearful of sending their credit card numbers over the Internet. The legal environment in which e-commerce is conducted is full of unclear and conflicting laws. In many cases, government regulators have not kept up with technologies.

As more businesses and individuals find the benefits of e-commerce compelling, many of these technology- and culture-related disadvantages will disappear.

Another important issue is security. Transactions between buyers and sellers in e-commerce include requests for information, quotation of prices, placement of orders and payment, and after sales services. The high

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet. The interception of transactions, and in particular credit card details, during transmission over the Internet is often a major obstacle to public confidence in e-commerce.

Secure Electronic Transaction Purchase Protocols

The purchase phase is complicated, involving interaction among three parties and several alternative protocol paths. For instance, Purchase Requests may be signed or unsigned, depending upon whether the Cardholder has run the Registration phase. Payment Authorization may be invoked during Purchase Request, or authorizations may be batched for processing later. Other complications include split shipments, payment by installments, frequent-flyer bonuses, car rental ratings and other frills.

Here, we simplify and combine Payment Authorization with Purchase Request, yielding in effect a six-step protocol. The version below is slightly simpler even than that modeled in Isabelle: certificates are omitted and the PKCS digital envelopes are replaced by simple public-key encryption.

Reducing the SET purchase phase to six messages has not been trivial. A number of tricky issues in the modeling are discussed elsewhere.

Initial Shopping Agreement: The Cardholder and Merchant agree upon the order description (OrderDesc) and the purchase amount (PurchAmt).

This agreement step, called the SET Initiation Process in the Programmer's Guide [11, page 45], is not part of SET and occurs just before it.

Purchase Initialization Request: The Cardholder sends the Merchant a freshness challenge (Chall C) and a local transaction identi_er (LID M).

1: C → M: LID M; Chall C

Purchase Initialization Response. The Merchant replies with a signed message that includes a freshness challenge (Chall M) and generates a nonce that serves as a globally unique transaction identi_er1 XID. Also returned is the public-key certi_cate of a Payment Gateway, which is determined by the Merchant's bank and the card brand.

2: M → C: SignpriSKM(LID M; XID; Chall C; Chall M)

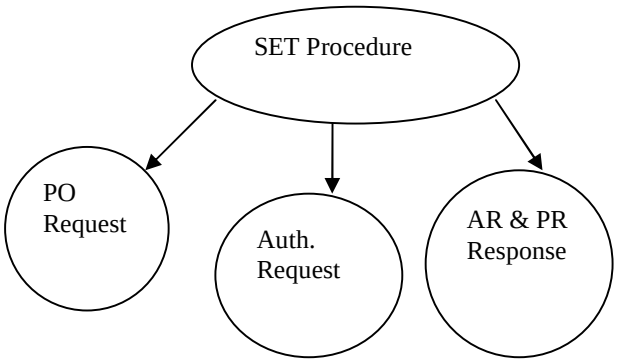

Figure 2: SET Structure

Purchasing Order Request

This is the most interesting message in SET. The Merchant and Payment Gateway must agree on the Cardholder's purchase, although each of them gets only partial information: the Merchant does not know the card details, and the Payment Gateway does not know what is being bought. To meet this objective, SET uses a dual signature. The Cardholder signs the concatenation of the hashes of the Payment Instructions and the Order Information. He combines this with the card details, including the PAN and other secret numbers, CardSecret and PANSecret, which help to authenticate him. Then he encrypts everything using the Payment Gateway's public key, pubEK P. He sends this to the Merchant, along with the Order Information and the hash of the Payment Instructions. Much information is duplicated so that the various parties can con_rm the hashes.

3: C → M: PIDualSigned; OIDualSigned

Here, C has computed

HOD = Hash (OrderDesc; PurchAmt)

PIHead = LID M; XID;HOD; PurchAmt;M; Hash(XID; CardSecret)

OIData = XID; Chall C;HOD; Chall M

PANData = PAN; PANSecret

PIData = PIHead; PANData

PIDualSigned = SignpriSKC(Hash(PIData); Hash(OIData));

CryptpubEK P (PIHead; Hash(OIData); PANData)

OIDualSigned = OIData; Hash(PIData)

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

An unsigned Purchase Request obviously lacks these interesting features and does not authenticate the Cardholder. Merchants may reject such requests.

Authorization Request

The Merchant seeks authorization from the Payment Gateway after receiving the Purchase Request. First, he verifies the dual signature, using the supplied hash of the Payment Instructions. He also verifies the Order Information. He takes the Payment Instructions (which he cannot read) and combines them with transaction identifiers and the hash of the Order Information. This he signs and encrypts using the Payment
Gateway's public key.
4: M → P: CryptpubEK P (SignpriSKM(LID M; XID;
Hash (OIData); HOD; PIDualSigned))

Authorization Response

The Payment Gateway verifies the dual signature using the supplied hash of the Order Information. He also compares certain hash values to check that the Cardholder and Merchant agree on the Order Description and Purchase Amount. The Payment Gateway can also verify the validity of the Cardholder's secret account information, using the Cardholder's certificate. If satisfied, he confirms authorization to the Merchant by signing a brief message containing the transaction identifier and
Purchase amount.
5: P → M: CryptpubEKM(SignpriSK P (LID M; XID; PurchAmt; authCode))

Purchase Response

The Merchant now sends a similar signed message to the Cardholder. It contains the hash of the Purchase Amount, which the Cardholder can verify. Disputes are resolved \out of band."
6: M → C: SignpriSKM(LID M; XID; Chall C; Hash(PurchAmt))

Future Work and Conclusions

Until now, the most complex protocols analyzed using the inductive method were Kerberos IV [4], TLS (the successor to SSL) [15], and the Cardholder Registration Phase of SET [2]. The verification of the Purchase Phase has still been an open problem.
People have used other methods. Meadows and Syverson [12] have proposed a language for describing SET specifications but have not actually verified the protocol. They have used the temporal language NPATRL (the NRL Protocol Analyzer Temporal Requirements Language) for specifying a number of SET's requirements. Some requirements are more technical, such as \honest principals will faithfully execute the protocol", others concern more closely the protocol goals. The paper is not about verifying those requirements, which is left as future work. Instead, it concentrates on the difficulties in specifying them formally, an issue that concerns us too.
Kessler and Neuman [5] have extended existing belief logic with predicates and rules to reason about accountability. (Although accountability is not among the stated goals of SET, it is clearly desirable.) They concentrate upon the Merchant's ability to prove to a third party that the Order Information originated with the Cardholder. Using the calculus of the logic, they conclude by pen and paper that the goal is met, so the Cardholder cannot repudiate his having initiated the transaction. Equivalently, we have proved that the dual signature being in the traffic implies that the Cardholder sent it. Stoller has proposed a theoretical framework for the bounded analysis of e-commerce protocols but has only considered an overly simplified description of the payment phase of SET. Lin and Lowe have also independently proposed a general theory to take complex protocols and map them into simpler model checkable protocol. However, they limited their actual analysis to the Cybercash protocol.
We succeeded in analyzing an abstract, but still highly complex, version of the SET purchase protocols. Novel techniques were not required; the difficulty consisted in digesting the specification and scaling up. SET's dual signatures were found to work. The necessary repetition of fields generated huge expressions and rendered the proofs harder. We found no major protocol flaws, but a lack of explicitness makes the proofs more difficult than they should

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

have been, while weakening the eventual guarantees.

References

[1] M. Abadi and R. M. Needham. Prudent engineering practice for cryptographic protocols. IEEE Trans. on Software Engineering, 22(1):6{15, January 1996.

[2] G. Bella, F. Massacci, L. C. Paulson, and P. Tramontano. Formal veri_cation of cardholder registration in SET. In F. Cuppens, Y. Deswarte, D. Gollman, and M. Waidner, editors, Computer Security | ESORICS 2000, LNCS 1895, pages 159{174. Springer, 2000.

[3] G. Bella, F. Massacci, L. C. Paulson, and P. Tramontano. Issues in modelling the SET protocol, 2001. in preparation.

[4] G. Bella and L. C. Paulson. Kerberos version IV: Inductive analysis of the secrecy goals. In Quisquater et al. [16], pages 361{375}.

[5] V. Kessler and H. Neumann. A sound logic for analysing electronic commerce protocols. In Quisquater et al.

[6] G. Lowe. Breaking and _xing the Needham-Schroeder public-key protocol using CSP and FDR. In T. Margaria and B. Ste_en, editors, Tools and Algorithms for the Construction and Analysis of Systems: second international workshop, TACAS '96, LNCS 1055, pages 147{166. Springer, 1996.

[7] G. Lowe and M. Lin Hui. Fault-preserving simplifying transformations for security protocols. J. of Comp. Sec., 9(3-46), 2001

[8] Mastercard & VISA. SET Secure Electronic Transaction: External Interface Guide May 1997. Available electronically at http://www.setco.org/set specifications.html

[9] Mastercard & VISA. SET Secure Electronic Transaction Specification: Business Description, May 1997. Available electronically at http://www.setco.org/set specifications html.

[10] Mastercard & VISA. SET Secure Electronic Transaction Specification: Formal Protocol Definition, May 1997 Available electronically at http://www.setco.org/set specifications.html.

[11] Mastercard & VISA. SET Secure Electronic Transaction Specification: Programmer's Guide, May 1997 Available electronically at http://www.setco.org/set specifications html.

[12] C. Meadows and P. Syverson A formal speci_cation of requirements for payment transactions in the SET protocol. In R. Hirschfeld, editor, Proceedings of Financial Cryptography 98, volume 1465 of Lecture
Notes in Comp. Sci. Springer-Verlag, 1998

[13] A. Paller. Alert: Large criminal hacker attack on Windows NTE-banking and E-commerce sites. On the Internet at http://www.sans.org/newlook/alerts/NTE-bank.htm, Mar. 2001 SANS Institute

[14] L. C. Paulson. The inductive approach to verifying cryptographic protocols J. of Comp. Sec., 6:85{128, 1998

[15] L. C. Paulson. Inductive analysis of the internet protocol TLS. ACM Trans on Inform and Sys. Sec., 2(3):332{351, 1999.

[16] J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, editors Computer Security | ESORICS 98, LNCS 1485 Springer, 1998

[17] RSA Laboratories. PKCS-7: Cryptographic Message Syntax Standard, 1993. Available electronically at http://www.rsasecurity.com/rsalabs/pkcs

[18] S. D. Stoller. A bound on attacks on payment protocols In Proc. 16th Annual IEEE Symposium on Logic in Computer Science (LICS), June 2001