Soft-Products Fraud Prevention Using Trusted Delivery

SALEH ALFURAIH, RICHARD SNOW
School of Computing Science, University of Newcastle upon Tyne,
Newcastle upon Tyne, NE1 7RU
UK

Abstract: - Soft-products are intangible products such as software, music, video and phone cards whose delivery can be entirely completed over electronic means like the Internet; by entirely we mean that both the delivery and the consumption can be performed remotely and electronically over the Internet as opposed to a conventional face-to-face interaction. This particularity can be exploited by honest sellers and buyers to create a highly dynamic market; unfortunately, it can be exploited by dishonest individuals as well to commit a wide variety of frauds. In this paper, we argue that currently, most fraudsters exploit the vulnerability of the identity authentication methods that are used in most Internet shopping transactions and we propose a mechanism to address the problem. Our proposal is called trusted delivery and relies on the use of a trusted delivery party whose role is to uniquely identify and authenticate online customers, prevent unauthorized credit card transactions, and help in resolving potential disputes between the buyer and the seller.

Key-Words:- E-commerce, dispute, Trusted Delivery, soft-products, AVS, Credit Cards

1. Introduction

With the enormous demand for soft-products such as downloadable movies, music, software, and prepaid phone cards, preventing fraudulent credit card transactions is becoming more essential. E-commerce allows customers to conduct transactions by credit cards without any physical interaction and the Internet facilitates soft-products and services to be acquired via soft delivery methods: email, download, logging in... etc.

There are many reasons for the increasing number of fraudulent credit card transactions. The most apparent one is that merchants have no physical contact with the customer to verify ID or signature. This problem existed even before the Internet with both Mail Orders and Telephone Orders, which are known to the credit card community as MOTO. MOTO suffered the same problems as Internet orders do now.

Before discussing the proposed solution it is appropriate to explain some important background information about commerce using credit card.

This paper is written in part of a broad area of research investigating fraud in electronic commerce (e-commerce) with a view to developing protocols, services and a full e-commerce payment system that is fraudproof.

The layout of this paper is as follows: Section 2 covers a brief literature review of the main subjects. Section 3 lists some Fraud Prevention Systems. Sections 4 and 5 will talk about fair-exchange and non-repudiation which have a great impact on this subject. Soft products fraud is studied in section 6. In Section 7 we will illustrate our proposed system and discuss it in section 8. Section 9 will conclude this paper and some further work will also be mentioned in it.

2. Background

2.1 Electronic Commerce

Electronic Commerce (e-commerce) is the only market in the world that is doubling every year and is still not reaching a peak. Most people think it will not reach this situation in the near future. E-commerce started with the invention of the Internet. Many motives have made e-commerce one of the largest markets so far: easy access for every body, diversity in products and locations, easy navigation and search, and availability 24/7. So far one of the most significant obstacles facing e-commerce is security. People are not happy with the degree of security they have with the Internet, making them afraid of trying to buy or sell online. Even if some products are cheaper online some people prefer to buy them from a shop outside believing that their identity and payment is more protected outside the digital world. This limitation is decreasing daily because of the hard work researchers and companies are doing to make e-commerce more secure and to educate the users. Many people have been forced to buy online because of the new products which are offered exclusively on the Internet.

2.2 E-commerce Products

The huge market in e-commerce encourages some companies to offer new products that can be delivered digitally, live music is one example of such new products.

E-commerce products are mainly divided into two categories. Hard-products which cover almost all the conventional tangible products we know so far and which require shipment to the buyer, e.g. clothes, computers, toys etc. Soft-products are intangible products that can be consumed without shipping to a physical address, such as software, music and calling time [1].

Soft- products may also be services, which mean they are not pieces of digital files you will receive in your email. For example, a subscription to an online newspaper or ISP, watching a real-time movie …etc. Some conventional tangible hard-products are now converting to soft products for the ease of production and the wider availability, e.g. books and music CDs. Our proposed protocol designed specifically for soft-products but can fit hard ones also.

2.3 E-commerce Fraud

Since the invention of the computer network hackers and crackers started misusing it. Some crackers did it for fun and some did it for money and they are still doing it. E-commerce opened a new market for crackers to have fun and also gain money, which makes any e-commerce site more vulnerable to attacks than a normal site. Fraudulent transactions are transactions where the buyer gain the product without paying for it or paying using others money. Committing fraud does not need a computer expert anymore; any Internet user can make a fraudulent purchase, especially if it is a soft-product. Those committing fraud do not fear the law since there are no laws governing the entire Internet and it is almost impossible to trace any fraudulent activity back. Several reasons make the soft-products fraud an easy job. Because of the low cost of products, diverse delivery locations and methods, and the payment methods used so far it is even harder for merchants to try to get their money or the products back since tracing may cost more than the cost of the product itself [1].

3. Fraud Prevention Systems

Because of the severe looses fraudulent activities can cause to the merchants and the payment companies, many fraud detection and prevention systems are currently in use. Most fraud prevention systems in use designed to handle a specific fraud scenario.

The most prominent systems can be summarized as follows:

3.1 Data mining and neural networks

Data mining approaches [2] and neural networks[3, 4]try to gather the information of all credit card transactions for the customer and build a history or a purchasing habit. Credit card issuers will block any transaction that looks suspicious either in terms of amount or geography

3.2 Surrogate card numbers

Microsoft, Orbiscom Inc, and Cyota [5]came up with the technology to prevent online credit card fraud by replacing users' real card numbers with a "surrogate". This replacement number is obtained from the issuer site or by installing surrogate generator software and can be used only for a given number of online transactions, after which it becomes invalid.

3.3 Verified By VISA

VISA claims that Verified by Visa enhances existing Visa Cards with a personal password. When someone shops at participating online stores, he enters his password in the same way he would enter his PIN at an ATM and Visa will verify it on real time. It assures him that he is only the one who can use his Visa Card online, giving him the same assurances he has when he uses his card in a physical store [6]. But there is one important thing has been forgotten here - creating a fake website is much easier that a fake ATM.

3.4 Secure Client

This solution offered by Master Card and Discover require customers to download some software to their machines and this software will connect with the e-commerce site every time they want to purchase. All e-commerce sites accepting Master Card and Discover will have to have the merchant’s client installed in their server too [23].

3.5 Card Verification Value (CVV2)

Card Verification Value (CVV2) [7]is a unique three or four digit number on the credit card; most credit cards have this number. This number can be verified in real time by almost all Mail Telephone and Internet Orders (MTIO) merchants [1]. This number is supposed to help merchants verify that the customer who is making this purchase actually has the card physically with him since he need to read it from the card. CVV2 can lose its purpose if it is used everywhere, since in almost all the cases where fraud can happen, the fraudulent customer can have such info[1].

3.6 Address Verification Service (AVS)

Address Verification Service (AVS) is a real-time check between the merchant and the issuer that ensures that the cardholder’s first 5 digits of the street address number and zip code are correct in order to verify that the billing address of the customer matches the information stored with the credit card issuer. This ensures that the merchants will not risk the possibility of the customer ending up disputing the transaction. It is the responsibility of the customer when the merchandise is delivered to his billing address, even if he did not sign for it. It is supposed to be the best method to fight credit card frauds but in the case of soft-products it is clear that this is not really helpful since no shipping occurs at any time [1].

4. Fair Exchange

One of the major attributes of e-commerce soft-products and services is the difficulty to be revoked or invalidated. If the buyer receives the product then the merchant has no effective means to force the buyer to return it. This is true if the merchant and the customer live in different countries with differing laws and regulations. Usually, the transaction of exchanging the money with the goods must happen at the same time to ensure that both get what they want, but this is almost impossible to do in the electronic world (at least these days) since all transactions need time to travel and will pass through many servers before they reach their final destination. The link speed and congestion are not controlled. This limitation could allow some fraudulent user to stop or interrupt the transmission before it reaches the other end, giving him an advantage over the other partner.

For this reasons a great variety of fair exchange protocols have been proposed in the past in an attempt to ensure that neither of the two exchangers will gain any advantage over the other; these protocols ensure that the transaction is either competed successfully or rolled back. Below are some of the important protocols used and a brief description about each one.

Gradual exchange protocols [8]. The basic idea behind gradual exchange is to repetitively send small low-value parts of the services and receive some of the payment every time a part is sent. Therefore, interrupting the exchange can only cause one party to gain a small advantage over the other. In that way the amount of “unfairness” which a participating party may experience is reduced. A requirement for gradual exchange protocols is that the services must be divisible into parts with “near-to-equal” value. Clearly, the smaller the parts become, the more the communication overhead increases. On the contrary, when splitting the service into larger parts the loss where the protocol is interrupted is higher. To solve the above problems or if the item is not dividable, we need a different protocol. An alternative is to involve the active participation of a trusted third party (called a “trustee” or “TTP”) in every exchange. TTP will receive both the product and the money then redistribute them after verification. Such protocols have been described by Burk and Pfitzmann [9] and by Franklin and Reiter [10]. Requiring the active participation of a trusted third party in every run has some clear drawbacks, such as the potential performance bottleneck or the need for permanent availability. To overcome these limitations, Optimistic fair exchange protocols have been suggested [11-13]. In optimistic exchange protocols both participating parties try to handle the exchange on their own and only involve the trusted third party if a dispute arise. Protocols which do not involve a trusted third party require special item properties in order to work correctly (for example the divisibility of money in Jakobsson’s ripping coins [14]) or make it necessary to resolve a dispute externally blackboard [15, 16].

5. Non-Repudiation

Non-repudiation services prevent entities from denying that they have performed an operation such as send or receive a message or read or write a file. They must ensure that when Alice sends some information to Bob over a network, neither Alice nor Bob can deny having participated in a part or the whole of this communication [17]. Therefore a non-repudiation protocol has to generate non-repudiation evidence [18].

Non-repudiation of origin (NRO) is intended to protect against the originator's false denial of having sent the message.

Non-repudiation of receipt (NRR) is intended to protect against a recipient's false denial of having received the message.

Non-repudiation of submission (NRS) is intended to protect against the originator's false denial of having submitted the message to the Delivery Agent.

Non-repudiation of delivery (NRD) is facilitated by evidence that the message was forwarded by the Delivery Agent

Many applications such as e commerce, fair exchange, certified electronic mail, etc. are related to non-repudiation.

Complete protocols providing both non-repudiation of origin and non-repudiation of receipt have been presented by Zhou and Gollmann [20]and by Zhang and Shi [19]. Their proposals use a trusted third party (TTP) that has to get involved during each protocol run. This involvement may create a communication bottleneck. To overcome this limitation Zhou and Gollmann presented a second protocol [21] which is based on the optimistic idea introduced for fair exchanges in [11]; where TTP only intervenes to recover from the situation when a problem arises[17].

6. Soft-Products Fraud

The requirement is to enable a buyer to use his credit card to purchase some soft-products online and receive them correctly and the merchant also will receive his money correctly. Neither the buyer nor the merchant should be able to deny receiving the soft-product and payment, respectively.

The example illustrated below shows a simple e-commerce transaction which we will be referring to in the rest of this paper; Figure 1 will illustrate a typical e-commerce transaction.

Alice in this example is the merchant and anything that starts with ‘A’ means it is Alice; Bob is the buyer and anything that starts with ‘B’ will mean it is Bob.

Assume that Bob needs to buy a piece of software from Alice. The current protocol used in the Internet is as follows:

1- Alice negotiates the product with Bob.

2- Bob agrees and sends to Alice the following information (B_name as it appears in the credit card, B_credit card number, B_expiration date, B_billing address where he receives his monthly statement, and B_Email) ; some other information maybe required by some merchant like (B_phone number and B_CVV2).

3- Alice uses the famous AVS system to verify the B_credit card number, expiration date, and B_billing address.

4- If Alice receives a positive response from the AVS system, she charges Bob the agreed amount and sends the software to his Email address.

5- Bob opens his Email and collects the software from it.

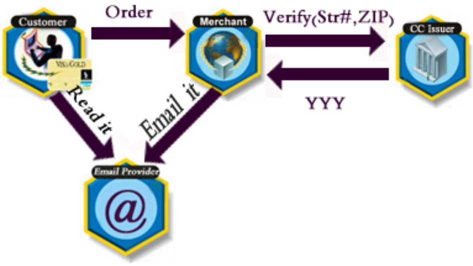

Fig 1: A typical e-commerce transaction

From the above example, we can clearly see that several problems might arise.

The AVS is not performing the expected verification since it was mainly built to handle hard-products where there is a physical shipping address that can be verified; with e-commerce soft-products this verification is not helpful at all.

The Main problem here is that any one who steals Bob's credit card and knows his address can use Bobs card for purchasing any soft-products he wants. On the other hand Alice has no means to prove that she delivered the goods as she has no signed receipt from Bob to use in any future dispute.

Several Approaches to address this problem have been suggested and deployed; unfortunately they do not appear to be satisfying solutions. It is clear that the data mining approach will not help since the Internet is diverse in locations and also most soft-product transactions have low cost which means that it will not be triggered by the system. Microsoft surrogate card numbers are very complicated to use if the allowed number of transactions are small and are likely to suffer from the same problem encountered so far if the number is set to a higher limit. A big hole in both the Microsoft Surrogate Card and the Verified By VISA systems is that both, at the checking out stage, automatically pop up a window asking B to provide his user name and password. This popup window can be easily emulated by a fraudulent website and get hold of B's credit card information and his username and password. CVV2 is like any other piece of information you provide on the web, after some time it will become public in the same way as credit card number and if someone steals B's credit card then the CVV2 is exposed because it is written on the card

It is clear that this is a complicated problem from which many soft-products companies suffer. This is why most of them pay higher processing fees and insurance to protect them selves from frauds arising from these vulnerabilities.

7. The proposed system

With the discussion presented in section [6] in mind, we now propose a solution which is based on the use of Trusted Delivery Server (TDS) and Full Address Verification System (FAVS). The main Ideas are as follows:

We link every Internet user with a delivery address to simulate his physical address in the Internet and use an enhanced version of the AVS system where we also verify this online in real-time. We called this enhanced AVS "the Full AVS" since it will verify all the information needed; Figure 2 will illustrate an e-commerce transaction with the FAVS.

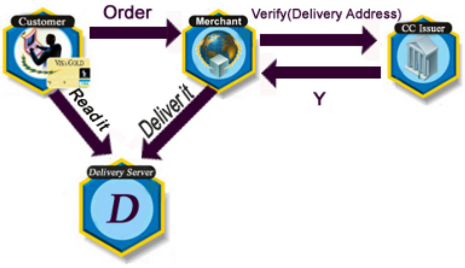

Fig 2 E-commerce transaction with FAVS

We use a special delivery server that is a TTP, so it provides non-repudiation services to the customer and the merchant. This is called TDS.

Our approach can be summarized by the flowchart diagram shown in Figure 3.

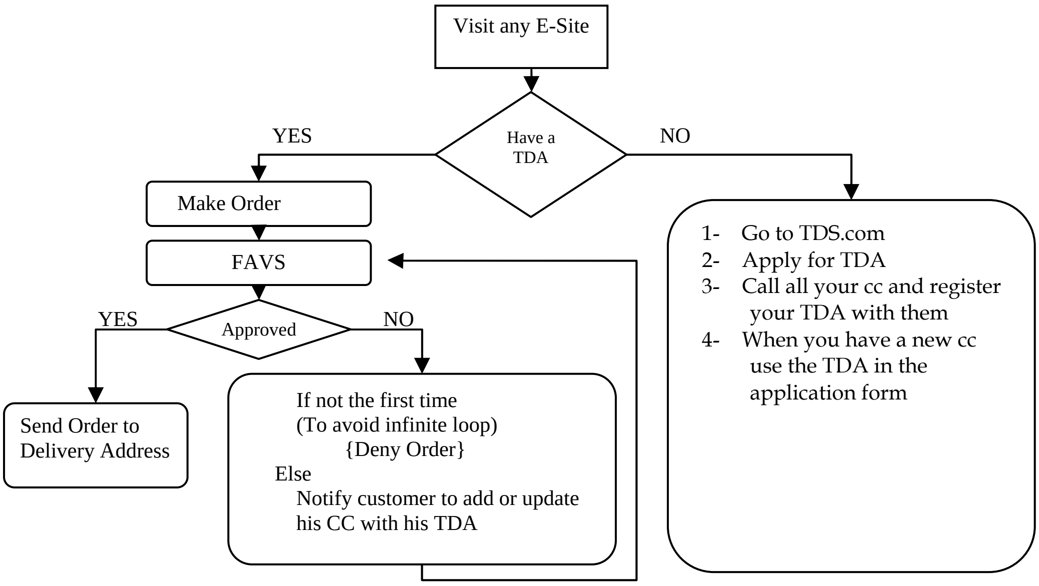
Visit any E-Site
Have a TDA
YES
NO
Make Order
FAVS
YES
Approved
NO
Send Order to Delivery Address
If not the first time
(To avoid infinite loop)
{Deny Order}
Else
Notify customer to add or update his CC with his TDA
1- Go to TDS.com
2- Apply for TDA
3- Call all your cc and register your TDA with them
4- When you have a new cc use the TDA in the application form

Fig 3 E-commerce transaction with TDS

8. Discussion

The Trusted Delivery Server and in turn the FAVS of our proposal provides the collection of enough non-repudiable evidence to prevent fraudulent transactions. By using standard Internet applications and services like web services that all the Internet users know, together with new Internet verification protocols, the soft-products market will reach every where and merchants will not fear the loss through fraud. Our aim in this Paper is to solve the fraud in soft-products by a technical solution rather than laws and regulation, since if laws and regulations are not enforced by the system then it has no means in the Internet because of it is globalness.

Two main requirements are needed to solve this kind of fraud for credit card users.

- Linking the identity of the credit card owner to delivery address where the soft-products will be shipped (Delivered)
- Having a Trusted delivery server which will provide the non-repudiation evidences required using the new protocols.

This system may not solve the problem of the merchant denying receiving the payment since it will focus on credit card transactions which represent around 70% of the online transaction [22] and with credit cards the merchant can not repudiate receiving the money since once he has received the money it is logged in the credit card company system and he can not repudiate having received it.

Some will argue that the person committing the fraud can obtain the delivery address, or can ‘sniff’ unsecure delivery channels contents, which results in the customer paying the price for the fraud, instead of the merchants or the credit card issuers. This argument can be true with every solution: Assume the thief got access to your physical mailbox, home key, or he obtained your Verified by Visa password: There are no silver bullet solutions. We believe that our proposed solution is superior to current systems that use billing addresses or other codes for verification. With some modification like confirmation of purchase, such frauds can be 100% prevented. This solution is easier to implement than credit card secret codes or having a surrogate credit card number. The solution has none of the common drawbacks of other proposed solutions[23], such as altering current e-commerce sites checkout procedures (as in verified by Visa), requiring customers to download (as in MasterCard or Discover), or changing the systems of existing credit card numbers (as in surrogate numbers).

The best solution to prevent credit card fraud transactions is the one that can be implemented with minimum cost, requires minimum changes for all parties (customers, merchants, and credit card companies/banks), and has incentive for all parties to participate.

9. Conclusion and further research

In this paper we reviewed the fraud types that occur in e-commerce transactions using credit card as payment method. We classified the merchant products into soft and hard in terms of their delivery method. Our proposed Trusted Delivery system solution is a novel solution that uses familiar concepts to satisfy the fraud prevention requirement and minimizes disturbance in the current credit card and e-commerce systems. A successful implantation of the system is illustrated.

We are model checking the current protocol in use to prove using SPIN validator that it fails to some important correctness requirements for example the merchant will always deliver the goods to the right customer and also the merchant will always have a proof of delivery. Then we are going to model checking our protocol using SPIN to show that our new protocol solves most of the current system problems. We are going to publish both validations in a complete paper as soon as we done with it.

References:

1. Saleh I. Alfuraih, Nien T. Sui, Dennis McLeod, *Using trusted Email to Prevent Credit Card Frauds in Multimedia Products. World Wide Web 5(2): 245-262 (2002).*

2. P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, *Distributed data mining in credit card fraud detection.* IEEE Intelligent Systems, November–December 1999. **14(6)**: p. 67-74.

3. R. Brause, T. Langsdorf, and M. Hepp. *Neural data mining for credit card fraud detection*. in Proceedings of *11th IEEE International Conference on Tools with Artificial Intelligence*,. 1999. P. 103-106.

4. S. Ghosh, and D. L. Reilly. *Credit card fraud detection with a neural-network*. in Proceedings of *the Twenty-Seventh Hawaii International Conference on nformation Systems:*. 1994. P. 621–630.

5. Bruno, M., Microsoft gives boost to surrogate card numbers, Bank Technology News, 2002 http://www.breakbanktechnews.com/btn/articles/btnoct01-1.shtml

6. VISA, Verified by Visa, OCT 20 2003, https://usa.visa.com/personal/secure_with_visa/verified_by_visa.html

7. Ondra, Dan, What is CVV2?, 15-Sep. 2003, http://www.danondra.com/scs/index.htm?ext_firt.htm&1

8. T.W. Sandholm, and V.R. Lesser. *Equilibrium analysis of the possibilities of unenforced exchange in multiagent systems*. in Proceedings of *the Fourteenth International Joint Conference on Artificial Intelligence*,. Aug.20-25 1995. San Mateo. P. 694-703.

9. H. Burk , A. Pfitzmann, *Value exchange systems enabling security and unobservability. Computers & Security, 9(8):715–721, 1990.*

10. M. K. Franklin , M. K. Reiter., *Fair exchange with a semi-trusted third party. In T. Matsumoto, editor, 4th ACM Conference on Computer and Communications Security, pages 1–5,7, Zurich, Switzerland, Apr. 1997. ACM Press.*

11. N. Asokan, M.Schunter, and M. Waidner, *Optimistic protocols for fair exchange. In T. Matsumoto, editor, 4th ACM Conference on Computer and Communications Security, pages 8–17, Zurich, Switzerland, Apr. 1997. ACM Press.*

12. N. Asokan, V. Shoup, and M. Waidner., *Optimistic fair exchange of*

digital signatures. In K. Nyberg, editor,EUROCRYPT '98, Lecture Notes in Computer Science, pages 591–606. Springer-Verlag, 1998. A longer version is available as Technical Report RZ 2973 (#93019), IBM Research, November 1997 at[*http://www.zurich.ibm.com/Technology/Security/publications/1997/ASW97b.ps.gz*](http://www.zurich.ibm.com/Technology/Security/publications/1997/ASW97b.ps.gz)*.*

13. N. Asokan, V. Shoup, and M. Waidner. *Asynchronous protocols for optimistic fair exchange*. in Proceedings of *the IEEE Symposium on Research in Security and Privacy,*. May 1998. P. 86–99.

14. M. Jakobsson, *Ripping coins for fair exchange. In L. C. Guillou and J.-J. Quisquater, editors, Advances in Cryptology—EUROCRYPT '95, volume 921 of Lecture Notes in Computer Science, pages 220–230. Springer-Verlag, 21–25 May 1995.*

15. H. Pagnia, R. Jansen., *Towards multiple-payment schemes for digital money. In R. Hirschfeld, editor,Financial Cryptography: First International Conference, FC '97, volume 1318 of Lecture Notes in Computer Science, pages 203–215, Anguilla, British West Indies, 24–28 Feb. 1997. pringer-Verlag.*

16. H. Vogt, H. Pagnia, and F. C. Gartner. *Modular fair exchange protocols for electronic commerce*. in Proceedings of *the 15th Annual Computer Security Applications Conference*. Dec. 1999. Phoenix, Arizona: IEEE Computer Society Press. P. 3-11.

17. Olivier Markowitch, Steve Kremer, *An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party. ISC 2001: 363-378.*

18. *ISO/IEC WD 138883. 6th working draft on Non-repudiation, Part 3: Mechanisms using asymmetric techniques. ISO/IEC JTC1/SC27 N993, 1995-04-07.*

19. N. Zhang, Q. Shi., *Achieving non-repudiation of receipt. The Computer Journal, 39(10):844-853, 1996.*

20. Jianying Zhou, Dieter Gollmann., *A fair non-repudiation protocol. In Proceedings of the IEEE Symposium on Research in Security and Privacy [IEE96], p 55-61.*

21. J. Zhou, D. Gollmann., *An effcient non-repudiation protocol. In PCSFW: Proceedings of The 10th Computer Security Foundations Workshop. IEEE Computer Society Press, 1997.*

22. cardweb, What is the current percentage of card transactions on-line, 2003, http://www.cardweb.com/cardlearn/faqs/2002/jul/6.amp

23. Heun, Christopher T., Fear of Fraud InformationWeek.com March 4, 2002., http://www.informationweek.com/story/IWK20020301S0002