2000

Security and Productivity Improvements - Sufficient for the Success of Secure Electronic Transaction?

Michael Fritscher
Vienna University of Economics and Business Administration, michael.fritscher@wu-wien.ac.at

Oliver Kump
Vienna University of Economics and Business Administration, oliver.kemp@wu-wien.ac.at

Security And Productivity Improvements – Sufficient For The Success Of Secure Electronic Transaction?

Michael Fritscher, Oliver Kump
Department of Information Systems
Vienna University of Economics and Business Administration
Augasse 2-6, A-1090 Vienna
{Michael.Fritscher, Oliver.Kump}@wu-wien.ac.at

***Abstract*- Online payments in business-to-consumer electronic commerce are mainly made with credit cards. Fraud and chargebacks are a significant issue for merchants and payment card brands, due to widespread use of unsecured or partially secured credit card transactions. The Secure Electronic Transaction (SET) protocol may not only provide a high security level. It also enables productivity improvements and therefore the reduction of transaction costs in payment processes. In the paper, the costs and benefits of SET are evaluated. The results show that security and efficiency are not sufficient to guarantee the market penetration of SET. Additional incentives for merchants and even more important for cardholders are necessary in order to gain market share.**

INTRODUCTION

There are a wide range of electronic payment systems for online purchases [1-4]. In spite of impressing growth rates in the past and audacious growth forecasts of business-to-consumer E-Commerce [5], p. 30, only a very small part of the transactions are made online. Surveys on supply [6, 7] of payments for E-Commerce transactions show that mostly traditional payment systems are used. Rumors tell us that online payments are mainly made with credit cards[1] followed far behind by other electronic payments like electronic checks and electronic bank transfers. Until now, digital or electronic cash plays only a minor part. These payment habits are also reflected by the internet fraud complaints and the used payment methods reported to the National Fraud Information Center [11].

In this paper, we first show the barriers mentioned in several surveys causing the low usage of online payments. Afterwards, we analyze online credit card payments with respect to data security and potential productivity improvements. The different parties involved in the payment process are analyzed, and the results are presented. Concluding, we show the results of the cost-benefit comparison for the introduction of Secure Electronic Transaction (SET) and introduce an incentive driven feedback control system.

What are the reasons frequently mentioned for the fact that online purchases are paid online only to a very small extent?

THE BARRIERS TO ONLINE PAYMENTS

Several surveys [12-16] show missing data security and missing privacy as the main causes for the small usage of online payments. Especially, the fear of possible fraud is a very strong barrier against the use of online payments. Other barriers with less importance are the need to see the product before paying it and too complicate procedures for consumers involved in electronic payment processes. For merchants, not widely used or available security methods, the difficult integration of new E-Commerce products with existing systems and the absence of convergence on E-Commerce standards are mentioned.

The quoted barriers for supply and use of online payments indicate that there is a lack of information and know-how. Both consumers and merchants suffer from a lack of information about fraud risk, existing payment systems and security of transaction data, and from a lack of know-how implementing and using the systems.

Moreover, the new developments in internet based payment systems bring up new chances evoked by the employment of efficient and effective payment systems to exploit the potential productivity improvements. These are not limited to the prevention of fraud, but extend to the automatic execution of the whole procedures from the online payment to the automatic settlement.

Let us now turn to the development of credit card payments in respect of data security and potential productivity improvements.

THE CURRENT STATE OF ONLINE CREDIT CARD PAYMENTS

Credit card payments have been the only online payments internationally available for business-to-consumer transactions by now. For the settlement of credit card transactions, the involved parties use the already existing world-wide infrastructure of the payment card brands. The international character of credit card payments corresponds to the nature of E-Commerce. This is an essential reason for the dominant position of credit cards within online payments. Other online payments, e.g. electronic cash, have been until now limited to the issuer and play an inferior role.

Unsecured credit card transactions use electronic mail and web forms to transmit data in plaintext from cardholder to merchant. The weaknesses of these procedures lie in the unsecured transmission through the open network and in the possibly resulting attacks.

As a first remedy for secured transmission acts Secure Sockets Layer (SSL) [17] with web forms or the use of encryption software with electronic mail, e.g. Pretty Good Privacy (PGP) [18]. These methods offer encryption (and with it security) on a session level. PGP additionally offers digital

[1] There are various statements about credit card use in online payments ranging from 70 to 90 percent of consumer online sales, e.g. [8-10].

signatures. Once the data arrives at the merchant's server, all the information is decrypted and whether or not it is stored in a secure way preventing unauthorized access depends on the merchant.

Similar to MOTO transactions (mail order/telephone order), both unsecured and partially secured (SSL, PGP) transactions show a series of common problems:

- The cardholder looses control over her credit card information and has to trust the merchant in guarding the credit card information securely. The cardholder has no assurance that the merchant is authorized to accept credit card payment.
- The merchant has no assurance that the consumer is the authorized cardholder of the credit card used for the purchase. Moreover, he risks repudiation of the purchase by the cardholder. This also applies to credit card data transmission with PGP even if electronic signatures are legally binding.[2] The merchant is responsible himself for authorization and clearing of the transactions.

In contrast to MOTO transactions, the data already exists in electronic form with online transactions. Combined with the data processing capabilities of information technology, the damage caused by online fraud can be much higher than with conventional fraud [19]. This also applies to credit card transactions, even though the consequences of fraud are unequally distributed among the involved parties as will be shown later on.

How do fraud and chargeback with unsecured or partially secured online credit card payments affect cardholders, merchants, financial institutes and payment card brands?

FRAUD AND CHARGEBACKS

A. Fraud

Cardholders whose credit card information was fraudulently used have monetary costs of retention and card blocking but also opportunity costs for the time spent. A new credit card has to be applied for and to be issued. Depending on payment card brand or issuer, there can be solutions of goodwill so that the opportunity costs for cardholders in most of the cases are limited to the factor time.

Merchants have no costs if they are careful, i.e. the credit card is not on the revocation list and the product is shipped to the authorized address. If merchants are not careful and ship their goods or services to an unauthorized address or accept revoked credit cards, they have to bear the loss of the shipped product. In contrast to cardholders, merchants cannot anticipate goodwill from payment card brands.

Payment card brands, issuers and acquirers have to bear administrative costs. Payment card brands additionally have to cover the costs of the product shipped by a careful merchant. The lost disagio reduces their earnings.

B. Chargebacks

In case of transactions where the cardholder denies the purchase of the good or service the cardholder has to make a statutory declaration testifying that the purchase has not been executed by her. In order to be able to detect a purchase not executed, the cardholder has to regularly check her credit card balance. The costs of the cardholder are time, not money. With repeating chargebacks the cardholder will apply for a new card. It is also possible that the issuer will suggest a new card, because there obviously is some kind of fraud. The costs for the cardholder in this case corresponds to the fraud costs described above.

Merchants have to cover the acquirer's fee for the chargeback (normally divided into administrative fee and loss fee) in addition to the loss of the product. They can, of course, sue the cardholder for reimbursement of the costs.

Provided that the merchant's administrative fee covers the acquirer's and payment card brand's administrative costs, no costs remain with them. However, the lost disagio reduces the earnings of the payment card brand.

Experiences of Visa concerning fraud and chargebacks show that there are big differences depending on areas. Visa's U.S. E-Commerce sales volume remains under one percent. The share of fraud and chargebacks coming from E-Commerce transactions also remains under one percent. In contrast to the U.S., the share of fraud and chargebacks coming from E-Commerce transactions in Asia is at approximately 50 percent, although only two percent of Visa Asia-Pacific's credit card business comes from E-Commerce [20].

Experiences of merchants show that without authorization of credit card payments high fraud rates on the merchant's account can be dangerous for the merchant's existence [21]. There are procedures solving this problem, e.g. fraud detection software and off-line verification via fax or phone. More sophisticated systems perform real-time authorization requests and clearing through the internet and automatic settlement using financial networks, e.g. Open Market[3], First E-Commerce[4] or Brokat[5]. After all, the problem of non-repudiation and therefore chargebacks still remains a big issue.

How can SET solve problems caused by unsecured or partially secured online payments?

SECURITY AND PRODUCTIVITY IMPROVEMENTS THROUGH SET

The SET specification describes a public-key infrastructure and protocol definitions at the application layer, which can be used to make secure electronic payments with credit cards over open, insecure networks like the internet. The fundamental steps of SET transactions are described in [22] pp. 55-72. Given that all parties of a transaction are certified, the SET protocol aims to provide the confidentiality of the transmitted data, the authentication of the involved parties, the ability of the cardholder to pay and the non-repudiation of the transaction. This leads to the following improvements:

[2] As one anonymous reviewer pointed out, electronic signatures may be legally binding in a number of countries based on a contractual relationship but the emerging laws on electronic signatures do not pertain to the credit card applications.

[3] http://www.openmarket.com/
[4] http://www.firstecom.com/
[5] http://www.brokat.de/

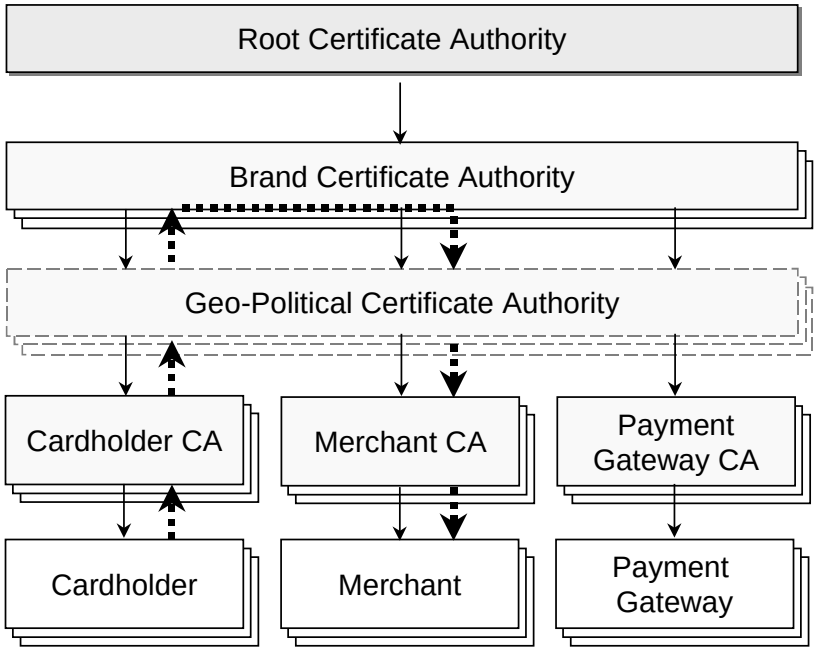

Fig. 1. Chain of trust from cardholder to merchant through SET Public Key Infrastructure [23], p. 115

- The use of digital certificates ensures for both merchants and cardholders that their counterparts are authorized cardholders or merchants. This is only true under the assumption that cardholders and merchants keep their private key safe.
- The concept of dual signatures separates Order Instruction (OI) and Payment Instruction (PI). The data is transmitted by the cardholder in two parts within one packet, the OI visible only for the merchant, the PI visible only for the payment gateway.
- The automated authorization of payments guarantees that the merchant gets the money for the sold goods.
- The clearing of payments is also automated over the internet. No additional infrastructure is necessary.
- No external collection of data is necessary during the whole process. The data of cardholder and credit card comes from the Consumer Wallet, the data of the product comes from the Merchant Server. Authorization and clearing are processed through the internet. Settlement is processed through financial networks. This way, printouts, mailings, telephone calls and recollection of data become superfluous, at least to a certain extent.

Despite the separation of OI and PI using dual signatures, merchants authorized by the acquirer may receive the card number. This depends on the boolean *MerAuthFlag* of the *MerchantData* private extension whose default value is TRUE [23], pp. 234f.. As this seems to be true with most merchants [24], the cardholder looses control over his credit card number in the same way as with insecure or partially secure methods. Unlike with these methods, there is the certification of the merchants within SET. As can be seen in Fig. 1, a chain of trust from cardholder to merchant can be established with the adequate certification policy.

For cardholders, this is only a second best solution and inferior to the invisibility of the credit card number for merchants.

What are the costs and benefits for cardholders, merchants and payment card brands for implementation and use of secure systems?

The Costs And Benefits Of Migrating To SET

Since cardholders have no or low monetary costs, as stated earlier, the main benefits of using SET accrue from a higher security level. This may result in additional time due to avoidance of fraudulent use of credit card data.[6] On the other hand the costs of using SET depend on cardholders' information technology know-how and the price of the certificate and the wallet, if there is any. One can also imagine, that installation and update of the wallet and the certificate management are time consuming activities for the cardholder. Therefore, the magnitude of the benefits of SET, measured mainly in time, are highly dependent on the future inconvenience through fraud to each cardholder. The risks of the cardholder are small due to established procedures for resolving fraud and the right to dispute charges. The data published by the Internet Fraud Watch shows that credit cards only make up 8% of all fraudulent transactions reported [25]. Unless people are risk avers or already had a lot of trouble without secure systems, they might not be willing to switch to SET because in general costs will exceed benefits.

For merchants, the costs of system implementation, i.e. merchant server, merchant certificate, the integration with existing systems and the training of the staff, have to be inferior to the reduction of losses invoked by fraud and chargebacks, and the benefits from rationalization by the automation of

[6] If one assumes that SET will be successfully attacked once in widespread use, things change. Cardholders will not be able to dispute charges as easily as without SET and the benefits diminish.

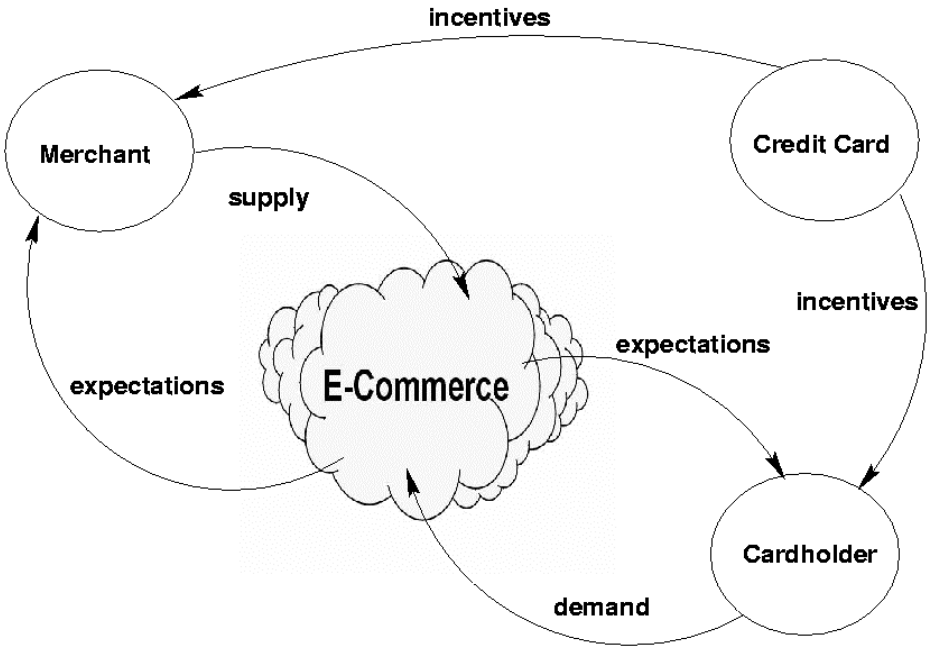

Fig. 2. Incentive driven feedback control system

authorization and payment settlement. This mainly depends on the actual or expected number of transactions and on the expected fraudulent transactions and chargebacks.

For payment card brands, the costs of implementation, i.e. the payment gateway, the integration with existing systems and the implementation and maintenance of the certification infrastructure, have to be inferior to the reduction of fraud losses, the benefits from rationalization by the automation of authorization and payment settlement, and the additional disagio from the expected rise of turnover induced by stronger trust of cardholders in the secure system.

Feedback Control System

Payment card brands benefit from the implementation of a secure system like SET which aims to provide confidentiality, authentication of the involved parties, ability to pay by the cardholder and non-repudiation of transactions.

The benefit for merchants mainly depends on the kind of goods and services sold, on the way they authorize card payments and the volume of transactions which essentially influences the potential of rationalization.

Cardholders on the other hand hardly have any monetary costs from fraud or chargebacks, as shown earlier in Fraud And Chargebacks. If cardholders are risk avers and data security is an issue, they will use SET provided that they have or are willing to learn the adequate know-how and trust the system. The combination of these assumptions will hardly be found among cardholders, especially because of simple widespread alternatives.

From this follows that payment card brands and financial institutes have to set further steps and measures. Security alone may not be sufficient for cardholders and merchants, neither perceived productivity improvements through SET for merchants. After all, expectations play an important role. If merchants expect E-Commerce and, through this, their own growth rates to rise, they will be more willing to adapt secure systems due to possibly rising fraud and chargebacks.

From the above one can also state that the supply of SET payments increases or decreases according to the expectations of merchants concerning the future development of E-Commerce and their own derived growth. The variations of the supply affect the number and the volume of E-Commerce transactions executed by cardholders. The demand on SET transactions in turn influences the expectations in the growth of E-Commerce. This leads to a feedback control system (see Fig. 2) which influences E-Commerce growth positively or negatively according to the starting position. Payment card brands act on this feedback control system – on the cardholders' as well as on the merchants' side – by giving positive or negative incentives for using SET or other sorts of internet-based credit card payments. The design of efficient and effective incentives still remains to be done.

Conclusions

The role of SET in future E-Commerce remains uncertain, although the biggest payment card brands back this open standard. Furthermore, there are already several software companies providing solutions which implement the SET protocol, e.g. IBM, Microsoft, Brokat CyberCash, VeriFone and others [26]. The Secure Electronic Transaction (SET) protocol does not only provide a high security level but also enables productivity improvements and therefore the reduction of transaction costs in payment processes. However, this is not sufficient. The analysis of costs and benefits showed that additional incentives for merchants and, above all, for cardholders are necessary to promote the diffusion and use of

SET. Expectations are essential in this process, whereby positive externalities for E-Commerce could arise.

ACKNOWLEDGEMENTS

We thank two anonymous reviewers for their valuable comments. Special thanks go to Willi Langenberger.

REFERENCES

[1] N. Asokan, P. A. Janson, M. Steiner, and M. Waidner , "The State of the Art in Electronic Payment Systems," *IEEE Computer*, vol. 30, pp. 28-35, 1997.

[2] G. Pernul and A. W. Röhm, "Neuer Markt - neues Geld?," *Wirtschaftsinformatik*, vol. 39, pp. 345-355, 1997.

[3] R. Schuster, J. Färber, and M. Eberl, *Digital Cash: Zahlungssysteme im Internet*. Berlin Heidelberg: Springer, 1997.

[4] P. Wayner, *Digital Cash: Commerce on the Net*, 2. ed. Boston, Mass.: AP Professional, 1997.

[5] A. Wyckoff and A. Colecchia, *The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda*. Paris: OECD Publications, 1999.

[6] N. N., "inTouch-Umfrage bei Online-Shops: Nutzung von Zahlungssystemen," inTouch, 1998, http://www.intouch.de/get_in_contact_newsletter_onlinepayment.htm, 1999-11-12.

[7] K. Kurbel and F. Teuteberg, "The Current State of Business Internet Use: Results from an Empirical Study of German Companies," presented at 6th European Conference on Information Systems, Aix-en-Provence, France, 1998.

[8] N. N., "Who we are," e-Visa, 1999, http://206.132.10.134/who.html, 1999-11-12.

[9] T. Arndt, "Electronic Commerce 1998 – der ECIN-Jahresrückblick," Electronic Commerce InfoNet, 1999, http://www.electronic-commerce.org/spotlight/1998/jahresrueck98.html, 1999-11-12.

[10] J. Kutler, "Internet Envisioning Growth, Stressing Security," American Banker, 1999, http://www.software.ibm.com/commerce/payment/J4370.pdf, 1999-11-12.

[11] N. N., "Top Ten Internet Fraud Reports Charts: Internet Fraud Watch Payment Methods," National Consumers League, 1999, http://www.nclnet.org/Internetscamfactsheet.html, 1999-11-12.

[12] N. N., "The Second Annual Ernst & Young Internet Shopping Study: The Digital Channel Continues To Gather Steam," Ernst & Young LLP, 1999, http://www.ey.com/publicate/consumer/pdf/internetshopping.pdf, 1999-11-12.

[13] N. N., "Electronic Commerce Barriers Survey Results," ITAA and Ernst & Young LLP, 1999, http://www.itaa.org/software/research/indpulse/barriers.htm, 1999-11-12.

[14] N. N., "Internet Shoppers Ask: 'Who's looking over my shoulder?' – But Keep On Buying Anyway," NetZero, 1999, http://www.netzero.net/company/19990407shoppersask.html, 1999-11-12.

[15] N. N., "64 Percent of Online Consumers Are Unlikely to Trust a Web Site," Jupiter Communications, 1999, http://www.jup.com/jupiter/press/releases/1999/0817.html, 1999-11-12.

[16] N. N., "Umfrage: Was spricht aus Ihrer Sicht gegen das Einkaufen über Internet?," Der Auer, 1999, ftp://ftp.auer.wvnet.at/1999_02feb_pdf/4c_wm_10_ifabo_angst.pdf, 1999-11-12.

[17] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL Protocol Version 3.0," 1996, http://www.netscape.com/eng/ssl3/draft302.txt, 1999-11-12.

[18] S. Garfinkel, *PGP: Pretty Good Privacy: Encryption for everyone*. Sebastopol, Calif.: O'Reilly, 1995.

[19] B. Schneier, "Electronic Commerce: The Future of Fraud," Crypto-Gram Newsletter, 1998, http://www.counterpane.com/crypto-gram-9811.html#commerce, 1999-11-12.

[20] D. Legard and M. Jones, "E-commerce a Headache for Visa in Asia," The Industry Standard, 1999, http://www.thestandard.com/articles/display/0,1449,4027,00.html, 1999-11-12.

[21] C. Morgan, "Web merchants stung by credit-card fraud," Computerworld, 1999, http://www.cnn.com/TECH/computing/9903/11/webfraud.idg/index.html, 1999-11-12.

[22] N. N., "SET Secure Electronic Transaction Specification: Book 1: Business Description. Version 1.0," SETCo, 1997, http://www.setco.org/set_specifications.html, 1999-11-12.

[23] N. N., "SET Secure Electronic Transaction Specification: Book 2: Programmer's Guide. Version 1.0," SETCo, 1997, http://www.setco.org/set_specifications.html, 1999-11-12.

[24] T. Lewis, "RE: PLEASE HELP: questions on non-repudiation, smartcards, ...," Monthly Archives for set-discuss, 1999, http://www.elistx.com/archives/set-discuss/199903/msg00000.html, 1999-11-12.

[25] P. C. McKee, "Internet Fraud Statistics for the first half of 1998," National Fraud Information Center (NFIC), 1998, http://www.fraud.org/internet/9810stat.htm, 1999-11-12.

[26] N. N., "SETCo Vendor Status Matrix," SETCo, 1999, http://www.setco.org/cgi-bin/vsm.cgi, 1999-11-12.