International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:1, No:5, 2007

# Trust and Security in Electronic Payments: What We Have and Need to Know?

Theodosios Tsiakis, George Stephanides and George Pekos

***Abstract*—** The growth of open networks created the interest to commercialise it. The establishment of an electronic business mechanism must be accompanied by a digital – electronic payment system to transfer the value of transactions. Financial organizations are requested to offer a secure e-payment synthesis with equivalent levels of trust and security served in conventional paper-based payment transactions. The paper addresses the challenge of the first trade problem in e-commerce, provides a brief literature review on electronic payment and attempts to explain the underlying concept and method of trust in relevance to electronic payment.

***Keywords*—**Electronic Payment, Security, Trust

## I. Introduction

COMMERCE partners (customers, merchants and financial organizations) are no longer interacting by direct physical experience. Instead their experience is mediated through multidimensional interactive environments. Consequently, it is an uppermost issue for the transaction process of exchange of information over open heterogeneous environments (as the Internet) to create trust. The formal procurator, the World Wide Web can be thought as an untrusted environment with no trust affiliations. In contradistinction, a desired trusted environment is the one that the entities constitute it, are unique, unquestionably identifiable and ruled by a set of priorities and conditions.

Trust has a vital influence on consumer activities and thereby on e-commerce success. To address the role of trust in e-commerce, we need to answer a number of questions such as [1]:

- What factors influence the level of trust in the Internet?
- How does trust influence participation in e-commerce?

Internet and particular the services of WWW must constitute an image of life that reflects both human knowledge and human relationships.

## II. Identification Of E-Commerce Security Skepticism

Before we give a possible approximation that can be thought as definition of security is imperative to allocate the components of a security system. We have a set of actions (A) applying on a system, a set of processes (P) functioning as a domain and a set of outputs (O) resulting the reprocess of actions. When two domains want to establish a communication channel between them, in order to exchange information, the system must designate a set of rules (security policy). Given the options and the possibilities of the information flow we can verify that a system is secure

Internet is structured as an undirected connected graph where nodes in the graph are routers and links (subnets or sub-networks). Each node and link has a unique id specified by an IP (Internet Protocol) address. In addition, each link has a cost, which can vary in time, and the distance between the two nodes is the sum of the link costs in the path between them.

Reference [2] consider the amount of time (duration) needed for a message to proceed from a network link to another, as a random variable with expected duration where the probability density function $p(t)$ for this time is known. Thus, the expected duration for the transaction is, simply:

$$\langle t \rangle = \int_0^\infty tp(t)dt \quad (1)$$

And the risk of transaction is:

$$\sigma = \sqrt{Var[t]} = \sqrt{\langle (t - \langle t \rangle)^2 \rangle} \quad (2)$$

The first step in a security project must contemplate the identification of all security requirements that can be applicable to a specific environment (the web). Next, it is critical to identify the parties that will be involved in an e-payment transaction and partition the transactions into autonomous actions that can be linked into the parties participating in an e-commerce environment. These information constitute a group of security requirements that develop security architecture (by means of procedures, mechanisms and policies [3].

By Security Architecture we mean the consideration of how a company's systems (in the widest sense) should be designed to ensure that the company meets its security objectives. It relates the security policies, and affects both systems bought and built for general use and a specific solution. A security Infrastructure is the practical realization of a security Architecture in a tangible and usable form.

Computer security refers to the process of prevention, protection and detection of the system and the data stored therein against unauthorized access, modification, destruction or use [4]. Next a question can come up, on how do we secure a faceless, non-physical, remote transaction between individuals and organisations. We must notate that the transmission of information can be materialized in two types of channels, open and secure channels. Open channels are communication channels on which communication may be intercepted by an unauthorized party, in opposition secure channels are communication channels on which data cannot

be read, written or altered. This security can be achieved either physically by securing the communication link or cryptographically by securing an open channel [5].

The critical factors for an economic organization or enterprise to both implement and operate an e-commerce mechanism are the flow of money, information flow and product flow. But security and implementation cost are the fundamental. Electronic Commerce (e-commerce) can be highly beneficial in reducing business costs and in creating opportunities for new, simple and improved customer services. Attempting to define e-commerce we can suppose that is the operation of maintaining business transactions (exchange of value) with the use of telecommunication networks

Reference [6] divide e-commerce into three classes:

1. Electronic Fund Transfer (EFT): the methods or the systems of paying electronically, transferring money or funds electronically and exchange digital information by means of electronic payments.
2. Electronic Commercial Information Transfer System: the system that exchange commercial information digitally.
3. Electronic Marketplace: the domains on the Internet where the expectant buyer can seek and purchase goods and services.

But e-commerce involves more than simple on-line transactions. We consider it as a mass of diametric unconventional activities that need to perform operation market research, identification of new opportunities, products, supplying services and exchange ways.

Reference [7] differentiates e-commerce in 1) Business-to-business transactions, 2) Consumer-to-business transactions and identifies that the transaction of e-commerce process can be visualized as a cycle of four phases:

1. Request (request of providence)
2. Negotiation (conditions of satisfaction)
3. Performance (fulfilment and notification of realization process)
4. Settlement (acceptation and payment)

Although the progress that has been made for the amplification of methods for achieving secure business transaction electronically, the use of e-commerce has not reach satisfactory limits and it is not considered being a concerted system for transactions, especially financial.

This can be identified as high transactional risk [8]. Transactional risk results when markets fail to provide standard level of security in payments and services.

Inadequacy of trust to electronic commercial and security is a result of the geographical separation of buyers and sellers, often coupled with a lack of real time physical presence [9].

The electronic systems that support the infrastructure of electronic commerce are vulnerable to three aspects of risk: abuse, misuse, and failure. Examining these risks from a business perspective we can identify the primary loss of asset (both in monetary and informational value) and lack of trust to conduct business electronically. What can outspread the universal acceptation, adoption and use of electronic commerce are trusted, secure, reliable, speeder, available, renovate-able and user-friendly infrastructure.

For Internet to be accepted as a medium of conducting monetary transactions, there will need to be a higher degree of confidence in the technology's reliability and security. As with any communications medium, it has both advantages (flow of information and digital assets) and disadvantages (the risk of loss transforming progressively to damage the asset). Reference [10] in a micro and macro analysis have concluded that for Internet to be further accepted as a medium to conduct monetary transactions there will need to be a higher degree of confidence in the technology's reliability and security.

The risks of enabling commercial transactions on network operation can be vitiated by the enforcement of security management and policy.

There are therefore three goals in securing electronic communications:

1. prevention from the maximum of the threats
2. detection of violations as soon as possible after they occur
3. reaction to security violations within the minimum of time

## III. E-Payment Phase

Consumers and providers of products and services are not expected to use widely electronic commerce applications unless they are confident that electronic communications and transactions will be confidential, the origin of messages can be verified and the personal privacy can be protected [11].

Payments are considered to be the integral component of any commerce activity. The needfulness to accelerate the flow of e-commerce transaction leads to establish a scrutable, friendly and secure payment system. Acceptance of e-commerce depends on the confidence of discernible security. Only one security issue is solitary to electronic commerce, which is the electronic payment.

It is preferable to make a distinction between electronic transaction protocols and electronic payment protocols. Electronic payment deals with the actual money transfer, electronic transaction protocols deals with the transactions as a whole. Electronic transaction protocols group together operations and implement failure atomicity, permanence and serializability and electronic payment protocols transfer trust, either as cryptographically signed promises, or as digital cash [12].

Reference [13] defines "Electronic payment" or "e-payment" as the transfer of electronic means of payment from the payer to the payee through the use of an electronic payment instrument. An "electronic mean of payment" would be defined as a mean of payment that is represented and transferable in electronic form. In a similar vein, an "electronic payment instrument" can be understood to be a payment instrument where the forms are represented electronically and the processes that change the ownership of the means of payment are electronic.

Electronic payment mechanisms as mentioned before provide the infrastructure (financial) that is indispensable to open and then establish an aggregate electronic marketplace. Within similar types of electronic payment systems, the encoding and decoding mechanisms of individualized payment systems follow different procedures [14].

The first distinctive feature of e-payment systems is the money model.

- Token – when the medium of exchange represents a value
- Notational – when a value is stored and exchanged by authorisation

A payer and a payee are the conceptual parts that exchange money for goods or services, and a financial institution is the one which links "bits" to "money." Payments can be performed either on-line (real time authorisation) or off-line (without contacting any third party during payment) [15]. On-line payment means that the payment systems requires from the payee to contact a third party in order to verify the process of payment and Off-line that there is no need of contacting and verifying the transaction of payment). We can add semi-online category as the involvement of a trusted third party but not in every payment transaction. The element of order is the validation of payment

Next, the time when the monetary value is actually taken from the payer attributes e-payments into

- Pre-paid systems – customer's account debited before payment
- Pay-now systems – customer's account debited at the time of payment
- Post-pay systems – merchant's account credited before customer's account is debited

Last distinctive feature, but not final, can be considered the payment amount.

- Micro payments, when amount is less than 1€
- Small payments, amounts between 1€ and 15€
- Macro payments, when the amount is bigger than 15€

In the current evaluation process our concerns are the on-line, macro payment systems that offer the ability of interactivity and access to services and large amounts of value.

The stimulants to turn to electronic equivalent fermentations are the need to achieve inferior processing cost, payment anonymity and confidentiality and payer untraceability.

Payment Models classify the digital payment systems according to the necessary flow of information between the participants of an electronic transaction [16]. Considering payments that take action over the Internet the keys issues are to prevent double spending (digital cash is represented by bytes that can easily be copied and re-spent), counterfeiting (digital money can only represent real value) and privacy control (confidentiality, anonymity and untraceability).

## IV. Enabling The Trust Factor

Reference [17] identifies that the majority of trust theories and mechanisms put the emphasis on trust based on the history of transaction experiences the partners had. More specifically, the challenge of the first trade problem in electronic commerce is to develop on line services that will lead companies to build trust among them without any previous experience. To design for trust, it is necessary to determine if, and under what conditions trust mechanisms are brittle [18].

Trust is a function of context, identity, reputation, capability and stake. Trust is also conditioned by social and cultural factors; in certain cultures tradition may provide a strong influence [19]. The need of trust in electronic commerce is usually explained by time asymmetry, lack of power, or inability to conclude perfect contracts. The time asymmetry argument draws on the fact that usually transactions are performed over a period of time [20]. Reference [21] have reported that trust is a catalyst for human cooperation and that people will trust and embrace e-commerce if they perceive sufficient security. They mention that is often ignored the trade-off between functionality and security. In addition, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects [22].

There is a strain to simulate off line an on line trust. The cases might be similar (commerce transaction) and the element to be the exchange might be common however, the nature of the environment, the type of process and many more make the issue of trust variable. Reference [23] sustains this aspect and suggests that in the on-line world, there are two approaches defining relationships between trustors and objects of trust; computer-mediated communication for individual-to-individual trust relationships mediated through technology and in contrast, technology as the object of trust.

Trust and trustworthiness are the foundations of security. The basis for these trust relationships and how they are formed can dramatically affect the underlying security of any system—be it home protection or online privacy [24]. A trust relationship is a relationship involving multiple entities to trust each other having or not certain properties (the so-called trust assumptions). If the trusted entities satisfy these properties, then they are trustworthy.

Given a network of (n) participating members we can consider individuals member trust as Direct or Indirect (Recommended). The direct trust relationship exists, as the word implies, from direct experiences two members develop. In a payment framework let us suppose customer *c* and merchant *m*. The preference of member *c* to pay a curtain amount (a) is represented by $\rho_c(a) \in \{0, 1\}$, where 0 indicates that member *c* does not have sufficient trust to proceed in a payment transaction and 1 indicates the acceptance to proceed. Next the member *m* in the network operates as *c ? m* and so the function that indicates how *c* trusts direct or not *m*:

$$\rho_{cm}(a) = \begin{cases} 1 \ if \ \rho_c(a) = \rho_m(a) \\ 0 \ otherwise \end{cases} \quad (3)$$

Reference l [25] define a recommendation of trust as:

$$C \text{ trusts. rec}_x^{seq} M when. path \, S_p when. t \arg et \, S_t \text{ Value V}$$

A recommendation trust relationship exists if C is willing to accept reports from M about experiences with third parties with respect to trust class x. Seq is the sequence of entities that mediated the experience excluding C and M. Let p be the number of positive experiences with Q which P knows about with regard to the trust class x. Then the value $v_z$ of these experiences is computed as follows:

$$V_z(p)=1-a^p \quad (4)$$

This trust is restricted to experiences with entities in $S_t$ (the target constraint set) mediated by entities in $S_p$ (the path constraint set). If p and n represent positive and negative experiences respectively with the recommended entities, the

recommendation trust value $v_r$ is computed according to the following formula.

$$V_r(p,n) = \begin{cases} 1-a^{p-n} & if\ p>n \\ 0 & else \end{cases} \quad (5)$$

According to the Figure 1, $V_2$ represents direct trust and $V_3$, $V_1$ represent recommendation trust.

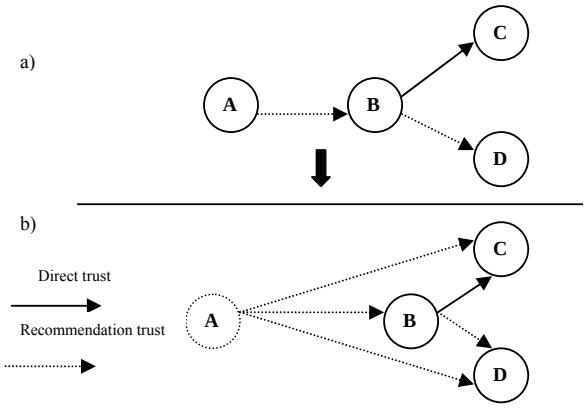


Fig. 1 Trust relationships

Due to an existing relationship, a new trust relationship can brought out between A and C as well as A and D can be derived. These processes are represented by the following equations:

Derived direct trust between A and C

$$V_1 \circ V_2 = 1-(1-V_2)^{V_1}$$
$$= 1-(1-(1-a^{p}))^{V_1} \quad p = number\ of\ \ positive\ \text{experiences B had about C}$$
$$= 1-a^{v_1 p}$$

Derived recommendation trust between A and D

$V_1V_3$ = simply multiplication between $V_1$ and $V_3$

This multiplication shows that the value of derived recommendation trust decreases as the recommendation path grows.

The problem is how to enable the traditional ways of paying for goods and services to work similarly and suitably over the Internet. Similar is the theme of what measures are needed to insure an open network as Internet, to transfer the digital image of information with compliance to security services.

## REFERENCES

[1] B. Corbitt, T. Thanasankit, H.Yi, Trust and e-commerce: a study of consumer perceptions, Electronic Commerce Research and Applications, 2, 2003, pp. 203–215

[2] R. Lukose, B. Huberman, A methodology for managing risk in electronic transactions over the Internet, Netnomics, 2000, pp. 25–36

[3] S. Gaines, Z. Norman, Some Security Principles and Their Application to Computer Security, the National Science Foundation under Grant No.MCS76-00720

[4] G. Whitson, Computer security: theory, process and management' Consortium for Computing Sciences in Colleges, JCSC 18, 2003

[5] D. Pipkin, Information Security. Prentice Hall PTR, 2000

[6] L. Fera, M. Hu, G. Cheung, M. Soper, Digital cash payment systems, Report, 1996

[7] S. Katsikas, The Role of Public Key Infrastructure in Electronic Commerce' The electronic journal for e-Commerce Tools & Applications, eJETA.org, Vol.1, No.1, 2002

[8] C. Westland, Transaction Risk in Electronic Commerce, Decision Support Systems 33, Elsevier, 2002, pp. 82-103

[9] P. Skevington, T. Hart, Trusted third parties in electronic commerce, BT Technology Journal, Vol. 15, No 2, 1997

[10] S. Lancaster, S. Yen, S. Huang, Public key infrastructure: a micro and macro analysis, Computer Standards & Interfaces 25, Elsevier Science, 2003, pp. 437–446

[11] I. Mavridis, G. Pangalos, T. Koukouvinos, S. Muftic, A Secure Payment System for Electronic Commerce, 10th International Workshop on Database & Expert Systems Applications, Florence, Italy, 1999

[12] P. Havinga, G. Smit, A. Helme, Survey of electronic payment methods and systems, University of Twente, department of Computer Science

[13] electronic Payment Systems Observatory (ePSO), Building Security and Consumer Trust in Internet Payments, Background Paper No. 7, 2002

[14] Yu Hsiao-Cheng, His Kuo-Hua, Kuo Pei-Jen, Electronic payment systems: an analysis and comparison of types, Technology in Society 24, 2002, pp. 331–347

[15] D. Abrazhevich, Classification and Characteristics of Electronic Payment Systems, Lecture Notes in Computer Science, Vol. 2115, 2001, pp. 81-90

[16] J.L. Abad-Peiro, N. Asokan, M. Steiner, M. Waidner, Designing a generic payment service, Technical Report 212ZR055, IBM Zurich Research Laboratory, 1996, Availiable: http://www.semper.org/info/212ZR055.ps.gz,

[17] Y. Tan, A Trust Matrix Model for Electronic Commerce, Trust Management, LNCS Springer-Verlag, 2692, 2003, pp. 33–45

[18] J. Camp, Designing for Trust, LNAI 2631, Springer-Verlag, 2003, pp. 15–29

[19] J. Daniel, Patterns of Trust and Policy, New Security Paradigms Workshop Langdale, 1998, Cumbria UK

[20] S. Brainov, T. Sandholm, Contracting with Uncertain Level of Trust, 1999, ACM 158113-176

[21] M. Patton, A. Josang, Technologies for Trust in Electronic Commerce, Electronic Commerce Research, Vol. 4, 2004, pp. 9–21

[22] ITU-T Recommendation X.509 (2000) Information Technology, Open systems interconnection - The Directory: Public-key and attribute certificate frameworks

[23] C. Corritorea, B. Krachera, S. Wiedenbeck, On-line trust: concepts, evolving themes, a model, Int. J. Human-Computer Studies 58, 2003, pp. 737–758

[24] J. Viega, T. Kohno, B. Potter, Trust (and mistrust) in secure applications, Communications of the ACM, Vol. 44, No. 2, 2001

[25] T. Beth, M. Borcherding, B. Klien, Valuation of Trust in Open Networks, Proceedings of the European Symposium on Research in Computer Security, Brighton, 1994

[26] M. Chesher, R. Kaura, Electronic commerce and business communications, Springer-Verlag, 1998