Global Journal of Enterprise Information System

e-Commerce: A New Mechanism to Assign and Manage the Identity of Online Customers

Umair Ujala[1*]

[1*]Lecturer. Birla Institute of Technology, International Center,. Mauritius. umairujala@gmail.com.

Abstract

The security issues of e-Commerce are related to economic loss and privacy leak. The all kind of fraud and crime are mainly due to the anonymity in the world of Internet. These issues can efficiently be controlled by managing the true identity of e-Commerce transaction partners. The true identity of the transaction partners can be used to track and locate the unlawful activities performed by a person. The vulnerability issues in the e-Commerce linked with anonymity can also be handled by the true identity mechanism. The mechanism will not only be suitable for the e-Commerce but also can be used for the overall network security breached by the illegal perpetrator taking the advantage of anonymity on the Internet.

The anonymity is one of the strengths of e-Commerce. Therefore, revealing the identity is a loss in the generic strength of e-Commerce. In this paper, I have proposed a mechanism to manage the true identity of the transaction partners without the loss of anonymity with the help of a trusted third party. The mechanism is based upon cryptographic technique and a trusted third party identity distribution center. The mechanism has strong capability of fraud control over the Internet, taking place due to anonymity.

Keywords: Anonymity, Cryptography, Digital Signature, e-Commerce, Internet Identity, Security

1. Introduction

The Internet provided the opportunity to the common people to become a Netizen. Netizen means a world citizen in the boundary of the Internet. The world wide resources are available for accessing to the netizens through Internet. In the past decade, Internet has grown as a powerful medium of communication and seems to offer great possibilities for social, political, economical, industrial and technological changes. In fact, the Internet has removed the limitation of reach and communication barriers. The exponential growth of Internet has been observed in past years. The Internet has become the life line for business, finance, education, and all. Though, the influence of Internet in the success of each field is prominently visible but it is more than this for business. This is from success to survival. This led the development of electronic commerce (e-Commerce) and it became a revolution for business today[1,9,16,19]. The importance of Internet and development for all purposes is raising the growth rapidly becoming greater in size. This uncontrolled growth is leading the crime rise over the Internet. Nothing is new-fangled. With early stages of its development, security issues such as reliability, integrity, confidentiality, non-repudiation, and authentication[1,9,17] were in focus. All these security issues are common to the Internet and e-Commerce. I outline these issues as follows:

- Reliability: The guaranteed delivery in time. When a transaction has been made it should reach to its destination without any divergence in a reasonably available time.
- Integrity: The uncompromised delivery of message. When a message or information is sent over the Internet, it is not altered by the unauthorized user.
- Confidentiality: Protecting information from unauthorized user. The information is for whom is available to them only.
- Non-repudiation: The ability to ensure the non-denial of online actions. This is related to the action acceptance by the user when performed once on the Internet.
- Authentication: Identifying the identity. This is ensuring the claim of someone representing as is the same.

Among all these issues; non-repudiation and authentication are related to the identity of people on the Internet. The Internet is open to create accounts using false names. This feature of Internet availability has led the breach of non-repudiation and authentication. The e-Commerce merchants face problem of refutation. This is worse for the e-Commerce merchants as purchasing card (credit/debit) issuer sides with the customer due to the lack of legally valid proof [9].

There is one strange behavior of Internet related to security. Security is always opposed by ease of use and anonymity[9].

*Author for correspondence

Anonymity on the Internet is weakness and strength both, so it is supported from both ways. Authors in their research suggest the partial revealing of identity[18]. Some Internet users perform crimes taking the advantage of anonymity while the others seek security by anonymity. What is more important? Both have equal potential but nothing can be picked at the cost of security violation. A negative impact of technology brings distrust. Trust[3,4,8,10,13] is an essential factor of technology adoption and security has a positive impact on trust[7].

The fixed Internet Identity (IID) is important for commercial transactions. There is an equal importance of fixed Internet Identity in nation and society for security. For example, Terrorists are also found have been using the Internet. In brief, a successful crime controlled web service needs a unique actual digital identity of each user on the Internet.

2. Existing Mechanisms

The authentication was identified as one of the security issues in the early days of Internet. Many researchers suggested the various schemes to overcome with the problem of authentication. The most widely used mechanism which helps the authentication and ensures the non-repudiation consists of three algorithms, key generation algorithm, key fetch algorithm and verification algorithm.

- Key Generation Algorithm: This algorithm is capable to select a uniformly random private key from a set of possible keys. Then it produces a corresponding public key.
- Key Fetch Algorithm: This algorithm produces an electronic stamp/signature with the message and the given private key.
- Verification Algorithm: Whatever is produced from key fetch is verified using the public key to check the authenticity.

In this mechanism a private key is crucial. The private key works as an IID. The possession of private key is possession of trusted IID. The mechanism is generally known as digital signature scheme. The above mechanism was used in RSA algorithm[17], Lamport signatures[11], Merkle signatures[15], Rabin signatures[14]. The other digital signature algorithms are DSA, ECDSA, EIGamal Signature Scheme, Schnorr Signature, Pointcheval-Stern Signature Algorithm, and Undeniable Signatures. The digital signatures in its present form are used to authenticate the source of message, to ensure the integrity of the message and to overcome with the non-repudiation. In fact, it restricts the source of message for later denial even when it is blamed to be sent by a fraudster because having mere a public key the signature cannot be copied.

With all these availability and practice do not provide certification of IID to each of the Internet user. The Internet IID has been remaining the focus of not only the technological domain but also of the governments. Many developed country has started the practice of IID on local level. American government has set NSTIC (National Strategy for Trusted Identity in Cyberspace)[12], which promotes the use of IID among the Internet user. The European Union proposed EID (Electronic Identity) and e-Signature in their action plans[6]. The Japanese government implemented e-Japan Strategy and Korean government has implemented the real name system on the Internet[2].

The above mentioned mechanisms and strategies for implementing IID are not in the global perspective. In some of the implementations the anonymity is lost which is a loss in the strength of Internet and specially e-Commerce. Therefore, the field is under an intense research among the public and private sector both to achieve a globally agreeable result.

In this paper, I propose a model to create IID maintaining anonymity over the Internet in global perspective. The proposed IID scheme is equally capable to control the privacy of user and reveal the identity in case of fraud.

2.1 Proposed Mechanism

The mechanism has two phases: Registration and Processing. Registration is a onetime activity for the lifetime Internet use. Processing is after registration activities not limited upon number.

2.1.1 Registration

In this phase there are three participants: The User, a Central Authority (CA) and a National Authority (NA).

Here we need an actual identity of user to use the facilities of Internet so a National Authority is needed. The National Authority may be a government organization having the data record of citizens or nationals. The role of Central Authority is to maintain anonymity and ubiquity. The process flow is depicted by the diagram given in Figure 1;

In this process the user provides personal detail and requests an IID from a CA, the CA requests an NA for the detail of the person. The NA provides the detail to the CA. The CA performs

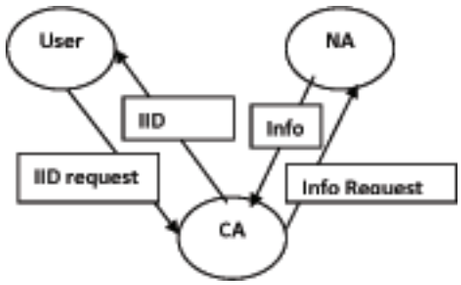

Figure 1. Central Authority (CA) and a National Authority (NA) Linkages.

GJEIS | Print ISSN: 0975-153X | Online ISSN: 0975-1432

the validation check and issues an IID to the user on the basis of right validation.

2.1.2 Verification

After acquiring the IID user is allowed to access the Internet and perform communications and transactions using the Internet. This involves three parties the sender (S), the Central Authority (CA) and the receiver (R). The process flow is shown in the diagram given in Figure 2;

In this process the user (S) sends request (SR) for a service to the e-service provider (R). Getting the IID from the user R sends a verification request (VRe) to the Central Authority (CA). The CA sends a verification report (VR). The S sends a Service Granted (SG) or Service Rejected (SRej) on the basis of VR.

3. Derivations and Interpretation

3.1 Preliminaries

Here, I give a brief introduction of the mathematical theory and results which I will be using in this paper.

3.1.1 RSA Cryptology

RSA is a public key cryptography algorithm that is based on the assumption of hardness of factoring the large numbers. RSA works on five parameters (*p, q, n, d, e*)**.** *p* and *q* are two large prime numbers, *n* is the product of *p* and *q*. And $d \equiv e \ mod\ \phi(n)$ that is *d* is multiplicative inverse *e* mod $\phi(n)$, where $\phi(n)$ is Euler *φ-function* and is equal to *(p-1). (q-1)*. Here, *(p, q, d)* are private while *(n, e)* are public. The RSA cryptography on a message *m* can be applied as $C = m^e \bmod n$ for encryption and $m = C^d \bmod n$ for decryption.

3.1.2 Conjugate Elements

If *a, b* be two elements of a group *G*, then *b* is said to be conjugate to *a* if there exists an element $x \in G$ such that $b = x^{-1}ax$, *b* is also called the transform of *a* by x[5]**.**

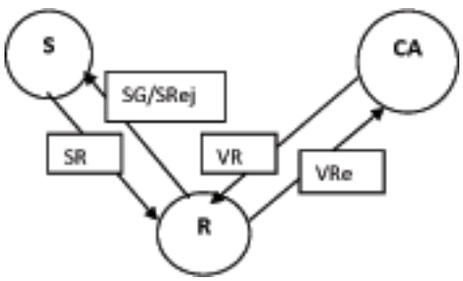

Figure 2. Conjugate Elements.

3.2 The Role of CA

3.2.1 Registration

Step1: Takes the identity of user from National Authority and assigns '*a*' the identity, '*a*' is initial UIID given by CA.

Step2: Selects two sufficiently large primes *p* & *q*.

Step 3: Calculates *x* and *y* such that *x* is multiplicative inverse *y* mod $\phi(n)$.

Step4: Selects *z* upon H_z, where H_z is a transformation function having *x, y* and *a* as parameters, where z is private UIID of user.

Step5: Provides (z, k) and H_u to the user. H_u is a function to encrypt *z* using private key *k*. The output of H_u is public and denote it by $H_u(z, k)$, which is public UIID of user.

Step6: Stores (*z, a*) and the data from NA corresponding to (*z, a*).

3.2.2 Verification

Takes the UIID and implements H_u^{-1} & H_z^{-1}. The output of H_u^{-1} & H_z^{-1} verifies the validity of UIID.

3.2.3 Description of H_z

$H_z(p, q, n, a)$: Calculate $n = pq$ and $\phi(n) = (p\text{-}1)\ (q\text{-}1)$,

Select *e* as per the RSA specifications and find a suitable $d \ni de \equiv 1 \bmod \phi(n)$.

Calculate $z = ead \bmod \phi(n)$

Lemma 1: $H_z(p, q, n, a)$: returns a unique value.

Proof 1:

Suppose z_1 & z_2 be two productions for two distinct values a_1 & a_2 such that $z_1 = ea_1d \bmod \phi(n)$ and $z_2 = ea_2d \bmod \phi(n)$

If $z_1 = z_2 \Rightarrow ea_1d \bmod \phi(n) = ea_2d \bmod \phi(n)$

Which is possible only when $a_1 = a_2$.

Therefore, each production of $H_z(p, q, n, a)$ is unique.

Lemma 2: For every $H_z(p, q, n, a)$ there exists one $H_z^{-1}(p, q, n, a)$.

Proof 2:

As, $a, d, e \in U_n$, the product under modulo $\phi(n)$is also an element of U_n. Therefore, $z \in U_n$.

$(dz = ad) \bmod n$

$(dze = a) \bmod n$

$(dze) \bmod n = a$

$a = (dze) \bmod n$

Therefore, $H_z^{-1}(p, q, n, a)$ exists.

3.2.4 The Role of User

Step1: User provides all the details for the registration including National Identity.

Step2: Takes (z, k) and keeps z as IID and k as processing key. Stores H_u.

Step3: provides output of H_u before availing Internet services.

4. Analysis

4.1 Anonymity

The entire process is considered to be anonymous if the actual identity of the user remains unrevealed after using the Internet for all purpose including online shopping. The anonymity is maintained throughout the transaction process in all kind of Internet usage. The Anonymity is strongly supported due to the double layer of physical identity protection in the proposed mechanism. To check the degree of anonymity in my IID scheme consider, $z = H_z^{-1}(p, q, n, a)$, and $u = H_u(z, k)$ where, all the symbols are as defined above. The whole identity creation and exchange mechanism can be interpreted as follows.

1. u is exchanged during all purpose Internet use. u is created by the encryption of z upon the encryption function H_u using the private key k.
2. One a is chosen, if $a \in U_n$ then a UIID, $z = H_z(p, q, n, a)$ is created.
3. z is the UIID derived from IID a against the actual identity kept with the trusted third party.

Therefore, to know the actual identity by any unauthorized party first z then a should be known. To find z the required parameters are (H_u, k). The hardness of finding z can be increased by implementing most secure available hash function having minimum possibility to be scanned through cryptanalysis.

Let us suppose, z is known to the unauthorized party. To get the actual identity; a should be known. To find a, the required parameters are (e, d, n) and n is the product of (p, q). Therefore, the hardness of the problem is dependent upon the size of (p, q)[17].

4.2 Authenticity

A person dealing with whom on the Internet, if is identifiable the authenticity is ensured. In this mechanism every transaction over the Internet is guarded by (H_u, k) where k is a private key and does not have any inverse public key. Therefore, it is hard to get k. Impersonation is possible in the case of fortuitous theft of k.

As the entire mechanism is controlled by a trusted third party, so the transaction cannot be denied under any (H_u, k). In any required situation the actual identity can be obtained by using (H_u^{-1}, k^{-1}) and then $H_z^{-1}(p, q, n, a)$.

5. Conclusion

In this paper, a mechanism is proposed to maintain the identity of online customer without revealing it. The basic idea is to ensure the authenticity of the customers with a strong support to the anonymity. This twofold property of the mechanism protects the merchants and the customer both. It prevents the opportunistic traders from exploiting the customers after the market; on the other hand it provides the assurance of authenticity of the customer. The mechanism can be generalized for all purpose Internet handling

6. References

1. Bajaj KK, Nag D. e-Commerce, the cutting edge of business. 2nd Ed. New Delhi: Tata McGraw-Hill; 2009. p. 14–58 and p. 250–74.
2. Chen B, Zou X, Zhou G. The development trend of the network identity management. Netinfo Security. 2014 Apr; 9(4):5–8.
3. Gefen D. E-commerce: the role of familiarity and trust. Omega: The International Journal of Management Science. 2000; 28(6):725–37.
4. Gefen D, Straub D. Managing user trust in B2C e-Services. e-Services Quart. 2000; 1(1). Available from: http://www.lebow.drexel.edu/gefen/eServiceJournal2001.pdf [accessed 2003 Jan 4].
5. Herstien IN. Topics in algebra. 2nd ed. New Delhi: Wiley Eastern Ltd; 1993. p. 35–80.
6. i2010: Information Society and the media working towards growth and jobs. Available from: http://europa.eu/legislation_summaries/information_society/strategies/c11328_en.htm [accessed 2012 Mar 28].
7. Lai IKW, Tong VWL, Lai DCF. Trust factors influencing the adoption of internet-based interorganizational systems. Electron Commerce Res Appl. 2011; 10(1):85–93.
8. Jarvenpaa S, Tractinsky N, Saarinen L, Vitale M. Consumer trust in an internet store: a cross cultural validation. JCMC. 1999; 5(2).
9. Laudon KC, Traver CG. e-Commerce, business, technology and society. 6th ed. Delhi: Pearson Education; 2009. p. 265–315.
10. Koufaris M, Hampton-Sosa W. Customer trust online: examining the role of the experience with the Web-site. CIS Working Paper Series. New York, NY: Zicklin School of Business, Baruch College; 2002. Available from: http://cisnet.baruch.cuny.edu/papers/cis200205.pdf [accessed 2011 Dec 23].
11. Lamport L. Constructing digital signatures from a one-way function. Technical Report. SRI International; 1979 Oct. CSL-98.
12. Making Online Transactions Safer, Faster, and More Private. Available from: http://www.nist.gov/nstic/ [accessed 2012 Mar 28].

13. Papadopoulou P, Anreou A, Kanellis P, Martakos D. Trust and relationship building in electronic commerce. Inter Res: Elect Network Appl Pol. 2001; 11(4)322–32.
14. Rabin MO. Digitalized signatures and public-key functions as intractable as Factorization. 1979. MIT/LCS/TR-212
15. Merkle R. A Certified digital signature. In: Brassard G, editor. Advances in cryptography-CRYPTO, '89. Spring Verlag; 1990. p. 218–38 (Lecture Notes in Computer Science; vol. 435).
16. Kalakota R, Whinston AB. Frontiers of electronic commerce. 3rd ed. Pearson Education; 2009. p. 5–21.
17. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Comm ACM. 1978; 21(2)120–6.
18. Shim S, Lee B. An economic model of optimal fraud control and aftermarket for security services in online market places. Electron Commerce Res Appl. 2010; 9(5):435–45.
19. Whitely D. e-Commerce: strategy, technologies and applications. New Delhi: Tata McGraw-Hill; 2001. p. 7–21.