Principals of trust in internet security and websecure environment

Felix Musau[1], Cheruiyot Wilson[2], Joseph Cosmas Mushi[3],Juma Modie[4]
[1,2,3,4]School of Information Science and Engineering, Central South University, Changsha, Hunan Province, P. R. China, 410083
[1]School of Engineering and Technology, Kenyatta University, Nairobi, Kenya, 43844, 00100
musaunf@gmail.com[1], wilchery68@gmail.com[2], mushyjc@yahoo.co.uk[3],jumamodie@gmail.com[4]

***Abstract*-Trust and security are key enablers of the information society. Trust is an important aspect of decision making for Internet applications and particularly influences the specification of security policy. It addresses issues on who is authorised to perform actions as well as the techniques needed to manage and implement security in the applications. Trust relates to belief in honesty, truthfulness, competence, and reliability. The significance of incorporating trust in distributed systems is that trust is an enabling surety of good transaction. Its inclusion will enable Internet commerce and seamless, secure agent based applications. This paper investigates trust in relation to security in internet transactions; it specifically deals with different authentication schemes, Encryption, Trust in the websecure environment.**

Keywords-Trust; Trust management; authentication; SSL; encryption; websecure environment

I. INTRODUCTION

The migration from centralised information systems to internet-based applications meant that transactions have to span a range of domains and organisations, not all of which may be trusted to the same extent [1]. Advancements in internet information service web publishing, security, administration, and applications work together to increase performance and reliability, while lowering the cost of ownership and improving the web application environment. For the consumers and small medium enterprises (SMEs) to use e-commerce they need confidence in the security of online transactions. As the access to internet diversifies, from PCs to digital TVs, mobile phones and wireless devices, people feel increasingly concerned about the protection of their assets and privacy in the networked world[2]. As we move towards a smart digital environments based on interacting objects, devices and systems trust approach will become more important. In recent years we have witnessed a growing series of attacks on the internet applications and databases i.e. denial of service attacks, viruses, phishing, spywhere, and other malware, criminals and untrusted agents Customers will submit information via the web only if they are confident that their personal information such as credit card numbers, passwords, social security numbers, financial data, or medical history, is secure. In 2006 [3] reports that 70% of online shoppers had abandoned a purchase because of security concerns. For instance, in 2007, an estimated $3.6 billion in online revenues was lost to online fraud—up more than 16% from 2006. Total number of unique phishing reports submitted to the Anti-Phishing Working Group (APWG) in January 2008 was 29,284, an increase of nearly 9% from the previous month. In the year 2008 Australia estimated cybercrime generated over AU$126.53 billion a year, making it more profitable than the illegal drug trade. Many scholars have argued that trust is a prerequisite for successful e-commerce because consumers are hesitant to make purchases unless they trust the seller [4,5,6]. The most notable development was by CSIRO Australia 2008, which developed a prototype portable device that allowed people to do business across the internet on any computer in a trusted manner [7]. It was known as a Trust Extension Device (TED), the TED consists of software loaded onto a portable device, such as a USB memory stick or a mobile phone.

II. PRELIMINARIES

Trust is both emotional and logical act. Moorman et al. in [8] define trust as a willingness to rely on an exchange partner in whom one has confidence. Morgan et al. in [9] define trust as the perception of "confidence in the exchange of partner's reliability and integrity". The most complete definition so far is given by Hosmer in [10], who defines trust as the expectation that the other parties will behave in accordance with commitments, negotiate honestly, and not take advantage, even when opportunity arises. In [11] Trust is a particular level of subjective probability with which an agent will perform a particular action, both before we can monitor such action and in a context in which it affects our own action. If A conducts business with B and the business is successful we express it as $SucT_{AB}$, otherwise if the transaction is not successful we express it as $UnSucT_{AB}$. If many transactions take place we evaluate trust as $T_{AB}=SucT_{AB}-UnSucT_{AB}$, then after several transactions between A and B the overall transaction can be expressed as

$$T_{AB} = \begin{cases} \sum_{i=1}^{n} (SucT_{AB} - SucT_{AB}) & ,0 < i < n \\ 0 & ,otherwise \end{cases}$$

The trust can also be expressed by use of weights for the different transactions .Using Integrated direct trust degree and recommendation trust degree, we get the overall trust degree formula

$T_{AB} = \beta DT_{AB} + (1-\beta)RT_{AB}, (0 \le \beta \le 1)$ β: The weight value of direct trust degree in overall. When the system does not have a malicious node, the successful transaction percentage is 100% for the four kinds of models. The result of evaluation is described using satisfaction or dissatisfaction degree which is in the range (-1, 1).

2.1 Management of Trust

Trust in ecommerce transactions goes with risk. If ***r*** is the Risk, ***c*** the cost after occurrence of a risk, and ***p*** probability

978-1-4244-9283-1/11/$26.00 ©2011 IEEE

that a risk will occur where $r \in Z$, and $0 \le p \le 1$, r , $c \ge 0$ then, $r = c \times p$. The design goal is to minimize ***r*** so that ***r***→0. This is possible when ***p***→0 or ***c***→0. Since ***c*** may not be determined unless risk has occurred, then $r \to 0$ if ***p***→0. A security formula for an internet business environment can be expressed as follows $SE = (P2 + T) * C$, Where *SE* means Secure Environment (Trust), *P2* means Policy and Procedures, *T* means Tools, and *C* means Commitment. Tools help implement the security of requirements and commitment is required to make it work. Prior to any business transaction customers must trust that sellers will provide the services they advertise, and will not disclose private customer information. Sellers must also trust that the buyer is able to pay for goods or services. Trust is usually specified in terms of a relationship between a *trustor*, the subject that trusts a target entity, which is known as the *trustee*. Keen et al. in [12] argues that the most significant long-term barrier for realising the potential of Internet marketing to consumers was the lack of consumer trust, both in the merchant's honesty and in the merchant's competence to fill Internet orders. Erkki Liikanen – member of the European Commission, responsible for issues of Information Society, in one of his speeches about perspectives of the ecommerce development [13] said: "No trust, no transactions".

III. SECURITY APPROACH PRINCIPLES IN MANAGING TRUST

A. basic authentication

The basic authentication is a method designed to allow a web browser or other client program to provide credentials in the form of a user name and password. It works on the comparison of the password and the ID you entered and the one on the database. Before transmission, the user name is appended with a colon and concatenated with the password from the trusted registered user. The resulting string is encoded with the Base64 algorithm i.e. given the user name Aladdin and password open sesame, the string Aladdin: open sesame is Base64 encoded, resulting in QWxhZGRpbjpvcGVuIHNlc2FtZQ==. The Base64-encoded string is transmitted and decoded by the receiver, resulting in the colon-separated username and password string. While encoding the username and password with the Base64 algorithm typically makes them unreadable by the naked eye[14].An example from Internet Explorer can be found in Figure.1.

Figure 1: Internet Explorer authentication

Since username/password combinations are often easy to discover or guess, more robust methods of authentication such as client certificates, biometrics and two factor authentication such as secureID are more trusted hence can be used.

B. Digital Authentication and access control trust

Once a user has been authenticated, the software must answer the question "What information is available to the user". Cryptography or encryption protects the privacy of the data, especially when on transit across a network. The figure 2 shows how information goes through a secure or trusted channel and decrypted by a key.

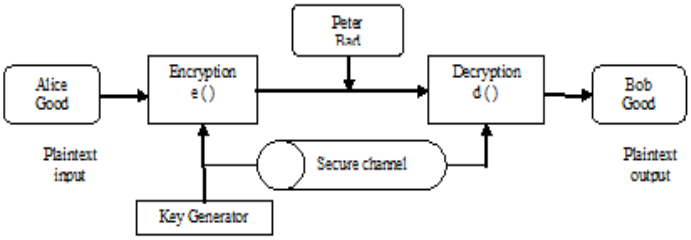

Figure 2: Secure communications over an insecure channel

Cryptography software and the hardware portions are responsible for enforcing its security. The use of a digital signature can be likened to the use of hand-written signatures that both authenticates and guarantees that the message is original. The use of mathematical functions and cryptographic techniques allow confidentially, integrity, and non-repudiation. A digital certificate contains credentials about the new individual: a digital signature and some of the individual's attributes, it also contains the digital signature of the introducer [15]. The internet use a Net PKI, this is for all transactions which take place on the internet. The medium could be private communication lines or over insecure public networks. The Net PKI provides for X.509 based digital certificates that can identify trusted individuals, organisations, Internet web addresses, and even software developers. Also when necessary, provide a means to revoke digital certificates. X.509 certificate encoding format is a binding between a public key and an identity. In Net PKI the introducer is the Certificate Authority (CA) (or also known as an Issuing Authority) which is delivered by the web browsers. The paper notes that since root certificates are distributed with the browsers they cannot easily be upgraded. The Root key management must follow the pace of browser releases and distribution. Certificate authority is a combination of hardware and software. It can issue certificates to individuals, organizations, network devices, servers or other CAs. The certificate authority in Net PKI can be inform of hierarchies.

C. Key management

The easiest way to break encrypted text is to have the key. Security of keys is the most important factor with any form of digital signature[16]. There are two kinds of cryptosystems; symmetric and asymmetric. Symmetric cryptosystems use the same key to encrypt and decrypt a message, and asymmetric cryptosystems use one key to encrypt a message and a different to decrypt it, or vice versa. Data Encryption standard (DES) is used as a privacy protection using a symmetric algorithm .It is relatively easy in small networks, requiring the exchange of secret

encryption keys among each party. DES has drawback as it requires sharing of a secret key.

Definition 1

Two large random primes, *p* and *q*, of approximately equal size are generated such that their product,

n=pq is of the required bit length i.e. 1024 bits
Compute n=pq and (f) phi= (p-1)(q-1)
Choose an integer e,1<e<phi, such that gcd(e,phi)=1.
Compute the secret exponent d,1<d<phi, such that ed=1(mod phi)
The public key is (n,d).Keep all the values d,p,q and phi secret
n is known as the modulus
e is known as the public exponent or encryption exponent, or just the exponent
d is known as the secret exponent or decryption exponent

After the key is generated it's very important to determine the key length for security information. Key length refer to modulus n in bits. The minimum recommended key length for a secure RSA transmission is 1024 bits. The other keys of shorter length are no longer secure .

Key length =ceiling (log_2 (n+1))
Ceiling (log_{256} (n+1))

If the most significant byte 0X04 in binary is 00001010B, then the most significant bit is at position 508, and its key length is 508 bits. In some cases the value needs 64 bytes to store it, so the key length could also be referred to by some as 64*8=512bits.

Definition 2

Let *G* be a group of prime order *p* and *q* be a random generator of *G*. Following [17], identity is represented as a bit-strength of length n , our initial trusted scheme constructs as follows:

Setup: pick $\alpha, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_n$ in Z_p as random. Set $g1 = g^{\alpha}$ .Then chooses g_2 randomly in *G*. The public key is *PK*=(g,g1,g2). The Trusted master key is $MSK = (g2^{\alpha}, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$

Extract : Let $ID = (v_1, v_n)$ be a n-bit string representing an identity, where $v_i \in \{0,1\}$,*PKG* first generated the auxiliary information parameters as follows: Let $h_0 = g$,then for $i = 1, \ldots, n$, complete $h_i = (h_{i-1})^{\alpha_i^{v_i} \beta_i^{1-v_i}}$, The private key is computed as $d_{ID} = (d_0, d_1) = (g2^{\alpha}(h_n)^r, g^r)$

Encryption: Let M be a encrypted message for identity *ID* and $H = (h_0, \ldots, h_n)$ be the auxiliary information parameters. The ciphertexts is constructed as $C = (C_0, C_1, C_2) = (e(g_1, g_2)^s M, g^s, h^s)$, Where s is selected randomly in Z^*p

Decryption: Let $C = (C_0, C_1, C_2)$ be valid ciphertexts .Then the message M can be recovered by private key $d_{ID}=(d_0.d_1)$ as follows: $M = C_0 \frac{e(d_2, c_2)}{e(d_0, C_1)}$ On the above it can be shown that

$$\frac{e(d_2, c_2)}{e(d_0, C_1)} = \frac{e(g^r, h_n^s)}{e(g2^{\alpha}(h_n)^r, g^s)} = \frac{1}{e(g2^{\alpha}, g^s)} = \frac{1}{e(g2\ , g1)^s}$$

The ability to use identities as a public key avoids the need to distribute the public key certificates. It can simplify many applications of public key encryption.

D. Biometric Trust Authentication

Cryptographic secret keys are long, random and expensive to maintain, hence difficult to memorize and must be stored somewhere. Fingerprint scanners can be used for authentication of trusted individuals. The method resists the threats of stolen-verifier, many logged in users with the same login identify, guessing, replay and impersonation. They have a unique design which represents just the person at the fingertips hence ensuring the trusted person gains authentication. The tiny ridges of skin on a person's fingers are used in biometric to form patterns. These ridges form through a combination of genetic and environmental factors. A fingerprint scanner needs to get an image of a finger and to determine whether the pattern and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

Minutiae-based fingerprint matching algorithm

We introduce the minutiae-based fingerprint matching algorithm as follows [18]. Let *T* and *I* be a fingerprint template and an input fingerprint sample. Each of them is a set of minutiae. A minutia is a vector (p, θ) , where $p = (x, y)$ represents the location coordinate and θ denotes the orientation angles of the minutia. Then

$$T = \{m_1, m_2, \ldots m_n\}, m_i = (p_i, \theta_i), p_i = (x_i, y_i), i = 1, 2, \ldots, n$$

$$I = \{m_1', m_2', \ldots m_n'\}, m_j' = (p_j', \theta_j'), p_j' = (x_j', y_j'), j = 1, 2, \ldots, n'$$

Where n and n' are the numbers of minutiae in T and I, respectively. Deciding whether T matches I depend in the number of matched minutiae. A minutia m_i in T matches a minutia m_j' in I if the following formulae hold:

$$\overline{p_i p_j'} = \sqrt{(x_i - x_j')^2 + (y_i - y_j')} \le r_0$$

$$\min(|\theta_i - \theta_j'|, 360^0 - |\theta_i - \theta_j'|) \le \theta_0$$, Where r_0 and θ_0 are the numbers of minutiae in T and I respectively.

The biometric methods have advantages over other methods i.e. keys are extremely hard to be guessed, keys are not easy to be lost or forgotten, keys are very difficult to copy or share, keys cannot be forged or distributed easily. In summary Authentication based on biometric keys is more reliable than traditional authentication based on passwords.

IV. ENCRYPTION AND SECURE SOCKETS LAYER TRUST

The incredible growth of the internet has excited businesses and consumers alike with its promise of changing the way we live and work based on trust to each other. It's extremely easy to buy and sell goods all over the world online[16]. Security and trust is a major concern on the internet,

businesses need to incorporate SSL Certificates and the encryption technology in their websites. Encryption is the basis of trust, data integrity, and privacy necessary for e-commerce. In the paper we highlight a method in which we can be able to ensure the transaction is secure according to SSL as in figure 4.

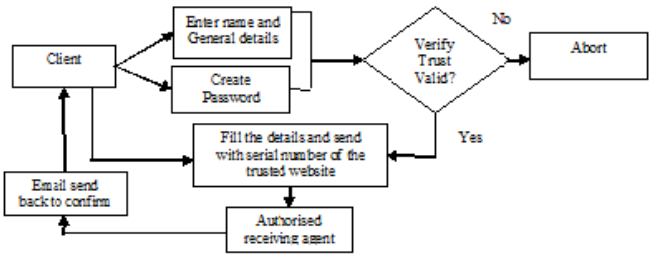

Figure 3: Authentication of website by SSL

After the security is confirmed a user can now fill his details and post information i.e. payment. If the SSL server is set to use two-way SSL authentication, it then asks the SSL client to verify and prove its identity, and the same process described above is used to verify the identity of the SSL client to the SSL server through an internet connection[19]. SSL is used to exchange cryptographic key which encrypts all data sent between client and server. SSL certificates are high assurance if they provide three security services confidentiality, authentication and integrity. According to [20] with the help of the server certification and client-side certification, SSL provide access route way for HTTP security. Its basic processing includes three steps: PKI-based secret key conversation agreement, ensuring the conversation confidentiality with symmetric cryptogram, Verifying the integrity with HASH function.

V. TRUST IN WEBSECURE

These are software which used to protect hackers from entering into ones computers. It encrypts all the data before sending it out to the proxy server. The software protection architecture is as shown in Figure 9.

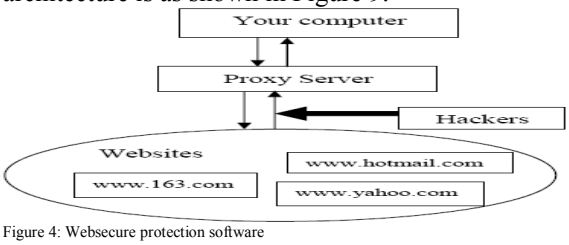

Figure 4: Websecure protection software

The proxy server and its software hides IP address, blocks malicious privacy and security threats .The software also safeguards the personal information, and encrypts the passwords. Businesses that succeed in today's privacy-conscious climate will do so by building privacy into their infrastructure and operations. The hackers cannot put invasive files or scripts on your PC. The websites cannot track and monitor your personal data and online activities [20]. The websecure software blocks any unauthorized files online. This is due to the fact that the hackers send files across the internet inform of .exe. The dot exe file which have not been requested are not allowed to bypass the software. The hackers also are not able to see the hidden IP addresses.

VI. CONCLUSION

The key factors influencing customers' decision to buy goods via Internet are the wide assortment, the reliability of the retailer, the safety of the transaction with the security of personal data and clear information about products. As businesses expose their internal process to customers and suppliers, today's security is being rendered ineffective. A new model is needed to save companies from security's crippling complexity and to enable increased openness based on trust. Security methods ought to be trustworthy in order to generate confidence in the use of information and communication systems. This paper talks about public key infrastructures, SSL, and different authentication methods. More research is needed to enable the trustor and trustee to be able to identify worthy business partners.

REFERENCES

[1] Khare R. and Rifkin A., Trust Management on the World Wide Web, Peer-reviewed Journal on the Internet , Elsevier,1998.
[2] Jacques Bus ,Building Trust and Security in Information Society: A Strategic Challenge for European R&D,2005, http://www.ercim.eu/publication/Ercim_News/enw63/bus.html.
[3] TNS Research Surveys, http://www.researchsurveys.co.za/
[4]D. Gefen, Reflections on the dimensions of trust and trustworthiness among online consumers, ACM SIGMIS Database 33 (3) (2002) 38–53.
[5]S.L. Jarvenpaa, N. Tractinsky, L. Saarinen, M. Vitale, Consumer trust in an Internet store: a cross-cultural validation, Journal of Computer Mediated Communication 5 (2) (1999).
[6]D.J. Kim,Y.I. Song, S.B. Braynov,H.R. Rao,Amulti-dimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspective, Decision Support Systems 40 (2) (2005) 143–165.
[7]Secure Internet Transactions At Internet Cafes Possible With Tiny Security Device, 6th March 2010 http://www.sciencedaily.com/releases/2008/02/080219093009.htm
[8]C. Moorman, R. Deshpande, G. Zaltman, "Factors affecting trust in market research relationship", Journal of Marketing, pp. 5781–101, 1993.
[9] R. M. Morgan and S. D. Hunt, "The commitment and trust theory in relationship marketing", Journal of Marketing 58, pp. 20–38, 1994.
[10] Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. Academy of Management Journal, 20, 379-403.
[11] Aberer, K., and Despotovic, Z., 2001, Managing trust in a peer-2-peer information system, CIKM'01, Atlanta, Georgia.)
[12]Peter G.W. Keen, Steve Schrump, Electronic Commerce Relationships: Trust by Design,1999
[13]Liikanen E. (2000): Trust and security in electronic communications: The European contribution, Speech/00/344, Information Security Solution European Conference "ISSE 2000", Barcelona 29.09.2000.
[14] A josang, Nam Tran,Trust management in ecommerce,2000.
[15]Gavin Longmuir, Privacy and Digital Authentication - Personal (or Individual) Privacy concerns verses the Community needs for Authentication in an increasingly Digital world,2000)
[19]How Encryption Works http://computer.howstuffworks.com/encryption.htm, 2010
[17]B. Waters: Efficient Identity-based Encryption without Random Oracles. Proc. Eurocrypt(Cramer R. Ed.), LNCS 3494, pp. 114-127(2005).
[18]Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer London (2009).
[19] Wei Feifei,Trust and Security Research of the C2C E-Commerce System Based on third part payment Platform,IEEE, 2009.
[20]New Security for Windows, http://www.radialpoint.net/home/