Comparative Analysis of Trust and Security

Farookh Khadeer Hussain, Elizabeth Chang, *Member, IEEE* and Tharam S. Dillon, *Fellow, IEEE*

***Abstract*— In the literature, there is a lot of confusion regarding the relationship between the 'trust' and 'security'. Most of the times, these terms are regarded as being synonymous with each other. The existing literature does not draw a clear line how and when the terms of 'trust' and 'security' are synonymous and when they are not synonymous. In this paper we address this issue and discuss when the *distinct* terms of 'trust' and 'security' can be regarded as being synonymous with each other and when they could be regarded as not being synonymous with each other.**

***Index Terms*—Trust, Security, Business, Security Informatics**

I. Introduction

The advent of the Internet and the Web provide connectivity and information richness over great distances at any time. This has created a dynamic, open and convenient environment for social and business development. It not only provides the opportunity for new entrepreneurial endeavours utilizing the Web, but also opens up new opportunities for old, static, closed, locally based businesses to adopt new business paradigms and new organizational forms. The Internet has also opened up modes of interaction and dynamic organizational configurations that were previously inconceivable within a wide array of human and business activities. However, these have also introduced challenges. One of the most pressing of these arises from the fact that in a business or social interaction on the Internet, we cannot rely on the usual physical, facial and verbal cues that we might have relied on to reach a judgement as to whether or not the other party will fulfil the service which they are promising. In addition, in the case of the purchase of physical goods over the Internet, we have no direct physical, sensory contact with the specific product and are reliant solely on the promise of the seller. We are being put in the position of 'buying a pig in a poke', rather than being able to 'squeeze the tomatoes' to determine their firmness. There could, in some cases, be difficulties ensuring the purchaser pays for the goods. These factors and several others, which are proposed and discussed in [4], when taken together make it imperative for being able to make judgements within such an environment about the other parties' trustworthiness and capability to provide the service at a specific level of quality.

In this paper, we point out the role and importance of Trust and make clear distinctions between the concepts of trust and security. We point out when the terms 'trust' and 'security' could be synonymous and when they are not synonymous.

II. The Importance of Trust in Virtual Environments

In recent times, we have seen an increasing number of people carrying out a myriad of different activities on the Internet. These range from writing reports to looking at news, from selling a car to joining a club, from the purchase of goods (e.g. Amazon.com) to the purchase of services (e.g. Priceline.com for travel arrangements), from entertainment (music or games) to research and development (information surfing), from private resource utilization (Grid computing) to remote file sharing (peer to peer communication), from shopping at the mall (BizRate.com) to bargaining in virtual markets (eBay), from e-bill to e-pay, from the virtual community to virtual collaboration, from e-governance (e-administration) to mobile commerce (Stock Trading), from e-education (cyber-university) to e-learning (getting an MBA online), from e-manufacturers (remote control production) to e-factory (e-products), from off-shore development (business expansion) to outsourcing (such as IT), from e-warehouse (warehouse space booking) to e-logistics (goods shipping orders), and limitless other possibilities.

Transactions have moved away from less face-to-face encounters to being more on the Internet. The infrastructure for the above business and information exchange activities could be client-server, peer-to-peer (P2P), or mobile networks. In such distributed, open and often anonymous environments, *fraudulent* or *incomplete practice* could occur where the seller or business provider or buyer (in other terms the agents on the network) does not behave in a manner that is mutually agreed or understood, especially where terms and conditions exist. This could take several forms:

- The *seller* or *service provider* only delivers part of the service promised, or is inconsistent in delivering the goods or services e.g. sometimes delivers and sometimes does not deliver or cannot deliver or never delivers what was promised or advertised;
- The seller's *product* is not of a good quality
- The customer does not pay on receipt of the product.

Farookh Khadeer Hussain is with the Centre of Extended Enterprises, School of Information System, Curtin Business School, Perth, WA, Australia. (His contact details are as follows: phone: 0061-08-92662875; fax: 0061-08-92662861; e-mail: Farookh.Hussain@cbs.curtin.edu.au).

Professor Elizabeth Chang is the director of the Centre of Extended Enterprises, School of Information System, Curtin Business School, Perth, WA, Australia. (Her contact details are as follows: phone: 0061-08-92662875; fax: 0061-08-92662861; e-mail: Elizabeth.Chang@cbs.curtin.edu.au).

Professor Tharam S. Dillon is the dean of the Faculty of Information Technology, University of Technology, Sydney. Sydney, NSW, Australia. (His contact details are as follows: phone: 0061-02-95141800; e-mail: tharam@it.uts.edu.au).

1-4244-0318-9/06/$20.00 ©2006 IEEE

- The *customer* or user may always be negative and disruptive of the business, or gives false or faulty credit details;
- The service provider provides a *service*, however it is not up to an acceptable standard;
- The interacting agent in an interaction does not deliver on the agreed terms.

Trust and *Trust Technology* have come into the picture for the virtual environment recently to give an online user the sensation of being able to 'squeeze the tomatoes before you buy'. As we will explain the later chapters, *trust and trust technology* provide a means to providing opinions and assessments about the product or service you have experienced. These opinions and assessments can be used by an agent to make a trust decision of whether or not interact with another agent. It boosts consumer confidence, in the sense that the customer feels more confident to purchase a product or take service, based on the assessments of others. Additionally these assessments and opinions expressed can help an agent to make judgements about products, service or other agents. In other words, you feel confident to pay for a service or product because you trust the seller's reputation for providing services of a given quality or the quality of products (goods). In other words based on the reputation of the *seller or service provider,* the consumer can determine the quality of the service (QoS) provided by the service provider. The consumer / customer can get an idea of the quality of the service that could be provided to it by the seller. This helps mitigate the risk in the business transaction.

Another advantage of *trust and trust technology* is that based on the feedback of the users about the products and the service, the product manufacturers and service providers respectively can come to know about the quality of product and the quality of service that is expected and desired by the user. The service providers and the product manufacturers can than tailor their products and services in order to satisfy the user demands and needs. Trust technology such as trustworthiness systems, or rating systems, or recommender systems already exist on the Web. For example e-Bay, Amazon, BizRate and CNet already have some rudimentary versions of trust technologies. Regardless of the fact that these examples of the use of the technology only provide some basic functions, the trust technologies being used by these online companies have been shown to be able to foster trust between the interacting entities. Trust and Trust Technology are becoming more and more popular and providing a convenient tool to simulate social trust and recommendation experience for online users. *Trust* is a crucial ingredient in any mutual relationship and where transactions are carried out in an distributed environment where the interacting entities may not have necessarily interacted with each other previously to provide the agreed to quality of service.

With trust technology supported web based e-business, one is able to respond to dynamic individual and business needs, thus achieving the targeted productivity improvement, lowered operational costs, enhanced customer service and most importantly customer satisfaction. On the consumer side, such system support will allow greater confidence to emerge, leading to greater willingness to participate in transactions on the Web. Trust and Trust Technology can as pointed before; facilitate judgements about products and services.

III. Trust and Security

Trust and security are not the same thing in the world of e-Commerce. Unfortunately a variety of uses, particularly of the term *'trust'*, could lead to some confusion. In this section, I clearly distinguish between trust and security and additionally determine when trust and security could be synonymous and when they are not.

Security focuses on protecting users and businesses from anonymous or non-anonymous intrusions, attacks, vulnerabilities etc., while ***Trust*** helps build consumer confidence and a stable environment for customers or businesses to carry out interactions and transactions with a reduction in the risk associated with doing these in a virtual world, thus allowing one to more fully reap the possible rewards of the increased connectivity, information richness and flexibility. In the next section, we discuss about the concept of security and the reason why it is used.

IV. Security

The dynamic, open and convenient Web environment not only boosts business potential and the economy but also creates concerns of security, trust, privacy and risks. If these issues are not dealt with in a timely fashion, they could hamper business in utilizing the Web. Security issues can affect communication, infrastructure, servers, client browsers, e-products, e-services, software, hardware, electronic documents, business transactions, and organizational backend databases. We need to prevent hackers, attackers, unauthorized individuals, and malicious users or servers from taking advantage of honest online users, from damaging private businesses and also from attacks on non-government and government organizations.

Security threats and attacks on the Internet include, but are not limited to, the following [1]:

- Eavesdropping - intercepting and reading messages intended for other users
- Masquerading - sending/receiving messages using another user's ID
- Message tampering - intercepting and altering messages intended for other users
- Replaying - using previously sent message to gain another user's privileges
- Infiltration - abusing a user's authority in order to run hostile or malicious programs
- Denial of service - preventing authorized users from accessing various resources
- Virus and worms - micro virus or attachment virus, Morris worm, cert/cc

Security Technologies that are widely available to address these include:

- Encryption (RSA encryption, algorithms, keys, encryption standards, etc.)
- Cryptography (hiding messages in text)
- Steganography (hiding messages in pictures or media)
- Secret information sharing (algorithms, symmetric keys)
- Digital signatures and standards
- Authentication (digital certificates, verifying identities, public keys)
- Authorization (controlling access to particular information and resources)
- Data integrity (a receiver can detect if the content of a message has been altered or a receiver can detect it)
- Intrusion detection

Currently, the above mentioned security technologies are sufficiently mature for e-commerce, and most of the technologies are already standardized [1].

The field of security research is still very active in the following areas (though it is not limited to them):

- Electronic payment (electronic wallets, dual signatures etc)
- Digital money (blind signatures, coins, double spending, etc)
- Web security (HTTP messages, header leaks, SSL tunnelling etc)
- Server security (data and database security, copyright protection etc)
- Client security (privacy violation, anonymous communications)
- Mobile agent security (agent protection, malicious agents, attacking servers, sand box, cryptographic trace)
- Mobile commerce security (GSM security, subscriber ID authentication, etc)
- Smart card security (SIM card, biometrics, etc)
- Communication security (firewalls, security negotiations, virtual private networks, network layer securities)
- Data, database and information security (triple keys, Hippocratic databases)
- Security policies (international legislation and regulation, enforcement of security)
- Security management (infrastructure, network, application and database)
- Computer forensics (electronic evidence, expert witness, etc)
- Risks and emergency responses
- Privacy (protecting the identity of individuals and their information and allowing them to control access to their information)

As can be seen from above that the main objective of security it to provide defence against possible attacks, so that the communication between the interacting entities could be carried out without any obstruction or impediment. In general it can be inferred from the above discussion that the concept of security is used in an open and dynamic environment like the Internet to provide the needed infrastructure to enable sheltered communication between the consumer (end user or service consumer) and service provider.

In contrast however, trust is the belief or faith that a person or agent has in another person or agent with respect to certain activities at a given time. It can be regarded as the belief a person or agent has in another agent or person that its behaviour will be as per the mutually agreed behaviour. In order to acquire trust in another entity over the open network, security establishing mechanisms may be necessary to provide sheltered communication or information protection. In the next section, we will see the reason the scenario where in the concept of security may be treated synonymously with the concept of trust.

V. TRUST

The concept of trust, its use and semantics can be interpreted in two distinct domains, namely Business Domain and Security Domain. In the following section A, we discuss about the concept, semantics and use of the concept of trust in security domain. In section B, we discuss about the concept, semantics and use of the concept of trust in business domain

A. Trust in Security Context

The concept of 'Trusted Computing' known as Palladium technology was initiated by Microsoft around 2001, as a combined software and hardware solution and a tamper-proof computer environment for secure communication. Microsoft's 'trusted computing' known as the 'secure computation service' [2] claimed that 'this significant evolution of the personal computer platform will introduce a level of security that meets rising customer requirements for data protection, integrity and distributed collaboration' [3]. The significance of trusted computing (Palladium technology) is its potential to improve system integrity, personal privacy and data security. Reliability and security is achieved as the applications run in the protected communication environment provided by Palladium. This promising technology is only available in a beta version on the market, and its promises still need to be proved.

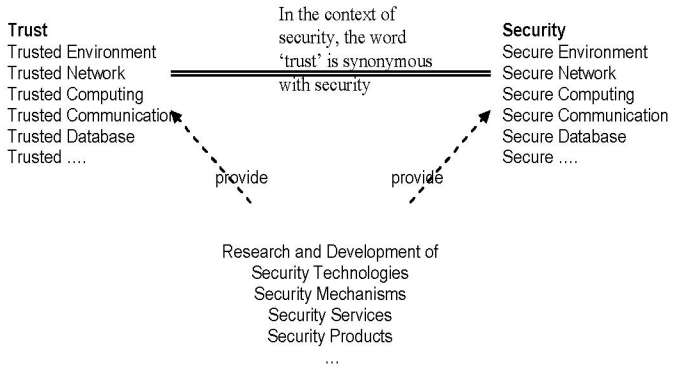

Figure 1. 'Trust' in Security Context

The concepts of Microsoft's 'Trusted Computing', 'Trusted Network', Trusted Communication', 'Trusted Agents', 'Trusted …' etc, are related to security issues, security mechanisms, security technology and security services. The main objective of 'Trusted Computing' as perceived by Microsoft is to enable data protection, data integrity, data security and data privacy. All topics of security study and research are directed towards providing a secure and tamper free environment, or network or communication. In this context, 'trust' is synonymous with 'secure', which is tied to 'security'. However, this is not the same as trust in the business paradigm, which is the subject of this thesis. In the security context, the term trust is synonymous with security.

B. Trust in the Business Context

Trust is a belief that signifies the confidence that a given entity (person or an agent) has in another entity (person or agent or product) that its behaviour would be the same as the *mutually agreed behaviour* [1]. Trust is a belief of confidence or a feeling of certainty that one person has in another person or thing that he/she is interacting with. Everyone or every organization wants assurance, certainty and confidence about what they do and what they will receive. In the business world, trust is especially tailored for ensuring honest dealings, quality of products or services and that is usually related to mutual agreements and understandings. Trust Technology motivates a seller to behave in a way as promised to the buyer. Additionally the trust technology motivates a buyer to behave in a way as the promised to the seller. It creates an environment in which both the buyer and seller are accountable for their behaviour and actions while carrying out business electronically.

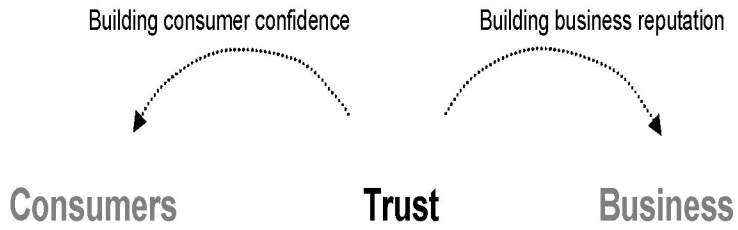

Figure 2. 'Trust' in Business Context

When we discuss trust in a social or economic or business context, there is a limited relationship with security. The motivation of trust technology is to help the business build their reputation, to aid business in ensuring that their customer would pay for their products, enable businesses to learn about the demands of the customer, to provide a means to businesses to tailor their products or services for as per the needs of the customers., for the consumers to trade with confidence with the business, enable fair trading, and to enable establishing mutual relationships between the business and consumer. As can be seen this interpretation of trust does not correlate with the notion of security. Hence in the context of business transactions trust is not synonymous to security.

However, Security can be used to support the process of *Trust Establishment,* through providing a secure environment for communication, secure network, so that trusted business transactions can take place.

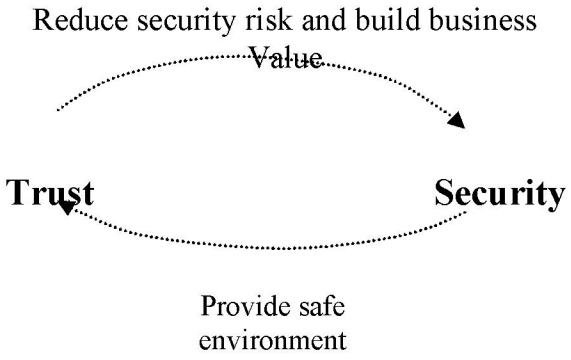

Figure 3. 'Trust' and 'Security': complementary technologies

Both Trust and Security are equally important in business, commerce and the world of technology. Trust and Security are complementary to each other. In the field of security, the word 'trust' is synonymous with 'security'. However, in business and social contexts and their support through the Internet they mean different things and both require complex studies, research and development.

VI. Conclusion

In this paper we have discussed the context in which the terms of 'trust' and 'security' could be synonymous with each other and when they could not be synonymous with each other. In security context the terms of trust and security are often synonymous with each other. However in business context the terms of trust and security are not synonymous with each other at all. In business contexts, trust is all about building and maintaining trust relationships. The purpose of building and maintaining trust relationships could be multifold like to increase consumer confidence, to expand business….etc in order to cerate a trusted business environment. In this context security can be regarded as a technology that aids in the process of establishing a trusted business environment by enabling and providing sheltered communication.

References

[1] Hassler, V., (2001), 'Security Fundamentals for e-Commerce', Artech House.

[2] Algesheimer, J., Cachin, C., Camenisch, J. & Karjoth, G., (2000), Cryptographic Security for Mobile Code, IBM Research, Zurich, Switzerland.

[3] Carrol, A., Juarez, M., Polk, J. & Leinger, T., (2002), 'Microsoft Palladium': A Business Overview, Microsoft whitepaper, June 2002. http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp.

[4] Chang, E., Dillon T, Hussain, F *"Trust and Reputation for Service Oriented Environment"*, John Wiley and Sons,, 2006.