Cultural and Social Aspects of Security and Privacy - The Critical Elements of Trusted Online Service

Yinan Yang[1], Ed Lewis[2], and Lawrie Brown[2]

[1] IEEE Society on Social Implicatins of Technology, Australia
dr_yyang@ieee.org
[2] School of IT&EE, UNSW@ADFA, Canberra, Australia
ed.lewis@adfa.edu.au, lawrie.brown@adfa.edu.au

Abstract. The lack of trust is identified as the key concern for consumers in the eCommerce environment. Service providers attempt to address this concern by implementing Public Key Infrastructure (PKI) systems for online security and privacy and to enhance user confidence. Much research has focused on the technical implementation of online security and privacy systems. This paper discusses social and cultural influence as critical elements of a trusted online service environment. It suggests a mechanism for enhancing trust in e-commerce that takes account of these influences.

Keywords: Trust, social factors, PKI.

1 Introduction

The growth of eCommerce is being hampered by a lack of trust between providers and consumers of Web-based services. Both online service providers and consumers have been reluctant to establish new business relationships via open electronic networks like the Web. This lack of Web trust has a direct effect on user confidence in online services and is increasingly affecting the rate of growth of eCommerce [1].

Many researchers have tried to address multi-disciplinary trust issues [2, 3]. Electronic (Digital) security technology does play an important role in establishing trust in an eCommerce environment [4]. It also provides a tangible perception of trust for online consumers. Public Key Infrastructure (PKI) technology [5] uses digital certificates and a combination of public and private encryption keys for authenticating the legitimate parties before transactions. Public-key cryptography has been used for anti-spoofing, authentication, authorisation, non-repudiation, and secure data communications. Despite some technical issues with X509-compliant PKI [6], the use of PKI in the eCommerce environment is still rising.

However, with the increasing use of PKI technology for cross-border eCommerce transactions and delivery of services by various governments, there are challenging social, cultural and legal issues that require further research [7]. Shneiderman et al identified two principles and associated guidelines to enhance cooperative behaviours and win user/customer loyalty [8]. Several trust factors were identified such as

N. Aykin (Ed.): Usability and Internationalization, Part II, HCII 2007, LNCS 4560, pp. 546–553, 2007.

assurances, references, certifications from third parties, and guarantees of privacy and security. These identified trust factors are also referenced and more or less agreed among researchers of empirical trust studies and surveys [9, 10].

The proposed W3 trust-profiling framework [11] identifies a range of trust factors including professional association, reputation, policies and legal status in its trust categories [12]. This generic trust-profiling framework attempts to assist consumers to assess the trustworthiness of webcontent of service provider. Based on this trust profile [13], online consumers can make better-informed decisions and User Confidence is improved.

There is a need for enhancing user confidence through improving the organisational culture and consequently improve the reputation of the service provider [14]. Online service providers (or organisations) need to know how to increase cooperative behaviours and win customer trust by understanding the social and cultural elements that are embedded in online security and privacy systems.

2 Identified Gaps Between PKI Technology and Social and Culture Elements

Many researchers have identified the *Reputation* of a service provider as an important factor of trust [8, 9, 10]. To build online trust, service providers need to be able to demonstrate their reputation and credibility to online consumers. In other words, the reputation and credibility of an online service provider needs to be assessed and measured in a meaningful way [12].

For example, normally, a professional association logo is displayed on a service provider's website to symbolize its trustworthiness by showing its professional affiliation. However, a logo provides little tangible meaning of the Reputation of the service provider to online consumers. A GIF file can be easily copied, downloaded and created. For customers to be able to trust an organization, they must be able to establish that it has a trustworthy reputation, supported by sound governance of its use of PKI technologies.

To focus this discussion, the following is a simple way to describe implementation of an online security and privacy solution:

- *Governance with Embedded Social Values* represents the principles and standards that provide a sound basis for online security and privacy. This includes legal requirements, social factors, policy and architecture, such as the Gatekeeper PKI Framework in the Australian Government.
- *Development Approaches and W3TF Adoption* [14] represents the technologies and approaches that implement business solutions to create a trusted environment for online services.
- *Monitoring and Feedback Mechanism* to measure the outcomes of the above aspects and provides factual and measurable information that permits improvements and fine-tuning of the above two aspects.

To further complicate matters, social and cultural differences can play key roles with online security and privacy when dealing with each aspect above.

3 Challenges in Social and Cultural Aspects of PKI Implementation

PKI technologies have been developed and utilised by various groups and communities for a secure communication on the Internet to provide various trust models [13]. Many research works focus on the improvement of technical deficiencies of PKI. However, to achieve a trusted and credible online service environment, service providers should also examine their organisational culture that is influenced by its inhabited social environment. This self-assessment and self-regulation of Governance framework presents more challenges than technical improvement.

The following social and cultural aspects illustrate some challenges that face organisations as online service providers.

3.1 The Healthier the Organisational Culture, the Better the Reputation

Nowadays, most organisations have codes of conduct to regulate employees' behaviour. The company's reputation relies upon its employees for they are also the trust agents of organisation and carry the implementation of PKI.

Organisations that operate a trusted online service often ensure that staff associated with the trusted systems are required to have regular vigorous and intrusive security checks based on the level of information protection required by the organisation. Staff who pass background and character checks are considered to be trusted staff and have privileges to view and access the information that they are cleared to see. However, organisations sometimes find that major security and privacy breaches were carried out by these trusted staff, e.g. possible inside trading [15], and unauthorised access to personal information [16]. This indicates there can be a gap between an organizational culture and individual values.

These diverse individual values are often based on the varied cultural inheritances of individuals and groups. The cultural bases of privacy values are very difficult to regulate through a simple mechanism, such as the code of conduct of the organisation. Indeed, legal prosecution can be utilised for those serious cases of security and privacy breaches, but by that stage great damage may have been done to the organisation's reputation.

There are differences between individuals in their value systems, which can lead to tensions in decision-making. There are differences between organisations in their cultures – the sum of the value systems. These differences can lead to loss of collaboration and delays in action. These losses can, in turn, lead to loss of reputation. In which case, displaying a reputable logo on its website adds no value.

There are a number of possible ways to encourage and consolidate the positive organisational culture and sharing of common values.

- Building up various leadership groups at all levels of the organisation. Each group (or a business unit) acts as a trust agent to translate the organisational value into daily interactions and dealings among themselves and other stakeholders.
- Some organisations provide an induction session for new staff and ongoing training for existing staff. These induction sessions inculcate common values and state clearly the organisational values and expectations for individual of the company.

- Some organisations adopt an organisation maturity model [17] as a tool for attracting, developing, motivating, organising and retaining an outstanding workforce as well as bench-marking of the current state of the organisation with a desirable organizational culture and value ahead.
- Providing coaching to some senior executives to be a role model to lead the organisational change requirements.

Although common sense is probably the most important ingredient, persistence, resilience and commitment are required from the top executives to the lower ranking staff. With sufficient time, a desirable organisational culture may prevail, which will see organisational Reputation enhanced. The question now is, how does this reputetion translate into increased trust? How can the user of the organisation's e-commerce come to know if it has a trustworthy reputation?

3.2 Taking Social and Culture Elements into PKI Implementation

PKI technologies have been developed and utilised by various groups and communities for online security and privacy protection. Different PKI offers different trust models [18]. PKI technology is continuing to improve from its deficiencies because of many researchers and security communities' contributions. However, there is little research on how different cultural and social factors may influence implementation of PKI and various levels of trust.

According to Australian Standard 8015: 2005 *Corporate Governance of information and communication technology,* ICT governance is

> The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization.

The principles of ICT governance given in the Standard include Principle 5 (Ensure that ICT conforms with all external regulations and complies with all internal policies and practices) and Principle 6 (Ensure that ICT meets the current and evolving needs of all the 'people in the process'). That is, governance must incorporate social and cultural values in such as way as to show clearly that its use of ICT is acceptable to all stakeholders.

Gatekeeper PKI Framework (Gatekeeper) is the Australian Government's strategy for the use of Public Key Infrastructure (PKI) to enable the delivery of online government services. Gatekeeper Strategy governs the use of PKI in government for the authentication of external clients (organisations, individuals and other entities). Gatekeeper ensures a whole-of-government framework that delivers integrity, interoperability, authenticity and trust for Agencies and their clients [19]. The Gatekeeper PKI framework covers a range of areas, including policy documentation requirements, online authentication requirements, privacy impact assessments and risks and threats assessments and Gatekeeper accreditation requirements.

Gatekeeper has been in action since May 1999 and was developed through a comprehensive consultation process involving all Gatekeeper accredited service providers, Federal, State and Territory governments. The Australian Government led consultation process aimed to balance various stakeholder requirements including legal requirements, all levels of government responsibilities, and Australian public expectations. Through this consultation process, the Australian government sought to demonstrate its commitment [20] to the Australian public that culture and social values are reflected in its governance strategy.

Different countries may embed different social and cultural values in their Governance models. To illustrate variations in regulatory environments in countries, ASIA Public Key Infrastructure (PKI) Forum [7] reported:

> Laws and regulations in Australia have had federal privacy legislation since 1988 that applies to government conduct. In 2000, Australian federal law was extended to private sector (in an attempt to come into line with European Union law). Most Australian has passed mirror legislation. The 2000 Australian Law is broadly based on the OECD principles. It was intended to harmonise Australian Private Sector regulations with those of the European Unit. However, most commentators agree here that the Australian federal privacy law is not as stringent as Europe's. Some states have adopted somewhat tougher health privacy law (page 8).

ASIA PKI Forum [7] found some differences in laws and regulations among the participant countries. These differences may cause some technical difficulties such as interoperability as well as the legal status of digital signatures across various countries. Given that the 2000 Australian Law is broadly based on OECD countries, the Gatekeeper-compliant PKI in Australia may offer acceptable levels of trust to OECD countries when they deal with Australian government service providers.

The Gatekeeper PKI framework is the governance model for PKI implementations adopted by Australian government agencies for their online services. The development of this governance model continues, based on extensive consultation with other Gatekeeper-compliant PKI stakeholders, including State and Territory governments and industries. This ongoing redevelopment of the governance framework often requires regular updating to meet new business and consumers expectations and demands. These changes in Governance can result in technical implementation changes. At the same time, technical advances can also force Governance to catch-up. Therefore, an ability to develop a strategy and sufficient resources around PKI implementation become critical for an organisation.

The Gatekeeper PKI framework is developed based on Australia's culture and social values, which are also deeply embedded in Australian organisations' culture and practice. This broader social context dictates individual's thinking and interprettation of government policies (i.e. Gatekeeper PKI Framework), legal requirements (e.g. Privacy Act) and how to implement the online security and privacy solutions to meet Australian consumers' expectations.

3.3 Development Approaches and W3TF Adoption

Although Australia's use of PKI does meet the governance principles, how is this made known to the users of its certificates so they can trust this use? PKI technologies have been developed and adopted world wide on various platforms and devices by individuals, small and medium service providers to large government organisations.

However, there are different approaches to implementing it, which may offer different levels of trust to consumers.

Some organisations require implementing PKI with a well-developed governance strategy, while others just simply install the technology. The Australian government requires federal government agencies to comply with the Gatekeeper PKI Framework when implementing PKI technology. This requirement increases User Confidence through alignment of the PKI technological component with the Gatekeeper policy and strategy framework.

In contrast, some companies could easily ignore their obligations to their customers by implementing a system without adequate security and privacy protection. So it can be difficult for consumers to differentiate the reputable ones from disreputable ones. To address this issue, a conceptual W3 trust-profiling framework (W3TF) was developed by Web trust researchers [14]. W3TF has proposed a trust metadata mechanism for online service providers to implement and to improve trustworthiness as described in its trust categories.

W3TF provides a means of establishing Web trust and indicates where to start to assess the trustworthiness of online service information before committing to business dealings on the Web. W3TF is also capable of providing a generic framework to integrate different trust requirements and factors into a coherent but flexible framework to allow it to grow. As shown, W3TF is based on various trust principles and incorporates important trustworthiness factors and trust requirements from various empirical studies. In addition, the simplicity and practicability of W3TF offers a sensible and a logical way to perform trust assessments on both standalone and hyperlinked webcontents.

In a heterogeneous Web environment, transitivity of trust can be achieved through a combination of various trustworthiness assessments using the proposed trust categories of the W3TF. This mechanism brings hidden information into its trust categories that communicate with the end-user and enable consumers to find out more about the potential service providers. Consumers can make the right choice about using a service, after checking what might be artificial or spoofed certification. The system based on the trusted information provided by W3TF [16] shall assist consumers to determine the acceptable level of trust.

3.4 Monitoring and Feedback Mechanism

Ongoing monitoring is important to maintain the trusted online service environment. Any glitch will hinder user confidence in the system and the organisation that operates the system. PKI offers online authentication and privacy protection to online consumers.

Often, the cost of the ongoing monitoring of the PKI system is very high including resources, disaster contingency plan, updated equipment, software components, knowledge and skills. It can be difficult to convince management to budget for ongoing monitoring of the trusted systems to prevent undesirable events. Many organisations do not see the importance of a sufficient budget for ongoing monitoring activities. In some cases, there could be a tension between a technical team and a non-technical team as to whom is responsible when things go wrong.

Continuing monitoring can improve PKI environment over time. The proposed W3TF mechanism provides factual and measurable operational information that indicates the health status of the existing PKI operational environment.

As well, the organisation should use monitoring within the guidelines established in AS 8015 to enable it to improve and fine-tune its strategy and development approaches. Monitoring also can be a timely sensing of any deficiencies in the environment before disaster occurs and causes political embarrassment. Any disaster in business services will certainly damage the reputation of the organisation as well as consumers' confidence.

To address this issue, organisations should follow the AS8015 principles to build a trustworthy reputation that is obvious to its customers. In order to do so, it should encourage an organisational culture of collaboration, cooperation and coordination.

4 Summary

This paper identifies social and cultural influences as critical elements for a trusted online service environment. The ability to incorporate diverse cultural and social values into online service implementation should enhance user confidence through the demonstrable reputation of the service providers. Some issues in Governance include roles and responsibilities, the maturity of security architectures and implementation of standards.

This paper also identifies a number of issues and potential options to improve online trust, including the adoption of W3TF and the use of sound governance principles. Through collaboration between the research and practitioner communities, the identified issues can be narrowed and more user-centric online security and privacy systems can be achieved.

References

1. Princeton Survey Research Associates: A Matter of Trust: What Users Want From Web sites (January 2002), http://www.consumerwebwatch.org/news/report1.pdf
2. Belanger, F., Sridhar, V., Slyke, C.V.: Comparing the Influence of Perceived Innovation Characteristics and Trustworthiness Across Countries. In: Proceeding of the International Conference on Electronic Commerce Research (ICECR-5) (November 2002)
3. Hoffman, D.L, Noyak, T.P., Peralta, M.: Building Consumer Trust Online. Communications of ACM 42(4), 80–85 (1999) ISSN: 0001-0782
4. Yang, Y., Brown, L., Newmarch, J.: Tokens of Trust: Different Certificates for Different Trust Models. In: Proceedings the UniForum New Zealand Conference (April 1999)
5. ITU-T Recommendation X.509, Information Technology - Open Systems Interconnection - the Directory: Authentication Framework, International Telecommunication Union, (June 1997)
6. Gutmann, P.: PKI: It's Not Dead, Just Resting. Computer 35(8), 41–49 (2002) ISSN: 0018-9162
7. Legal Infrastructure Working Group, Asia PKI Forum. Legal Issues on New Security Technologies and CA's Risk Management (July 2006)

8. Shneiderman, B.: Designing trust into Online Experiences. Communications of the ACM 43(12), 57–59 (2000) ISSN: 0001-0782
9. Cheskin & Studio Archetype/Sapient, San Francisco, eCommerce Trust Study (January 1999), www.cheskin.com/think/studies/ecomtrust.html
10. Grandison, T., Sloman, M.: A Survey of Trust in Internet Applications, IEEE Communications Surveys, 4th quarter, IEEE (2000)
11. Yang, Y., Brown, L., Newmarch, J., Lewis, E.: IWSM 2000. LNCS, vol. 3841. Springer, Heidelberg (2006)
12. Yang, Y., Brown, L., Lewis, E., Newmarch, J.: W3 Trust Model: a Way to Evaluate Trust and Transitivity of Trust of Online Services. In: Proceedings Internet Computing Conference, Las Vegas, USA (June 2002)
13. Yang, Y., Brown, L., Newmarch, J., Lewis, E.: A Trusted W3 Model: Transitivity of Trust in a Heterogeneous Web Environment. In: Proceedings of the Fifth Australian World Wide Web Conference, Queensland, pp. 59–73 (April 1999)
14. Yang, Y.: W3 Trust-Profiling Framework (W3TF) to assess Trust and Transitivity of trust of Web-based services in a heterogeneous Web environment, PhD Thesis, School of Information Technology and Electrical Engineering, University of New South Wales, ADFA, Canberra, Australia (August 2004)
15. 06-025 NAB Forex trader pleads guilty to ASIC charges, (February 7, 2006) URL at http://www.asic.gov.au
16. Shanahan, D., Karvelas, P.: Welfare Spies Sacked, Australian (February 5, 2007)
17. Curtis, B.: Capability Maturity Model, (2001), at http://www.gartner.com/measurement
18. Yang, Y., Brown, L., Newmarch, J., Lewis, E.: Trust Metadata: Enabling Trust and a Counterweight to Risks of E-Commerce. In: Proceedings Asia Pacific World Wide Web Conference, pp. 197–203 (1999)
19. Australian Government Information Management Office. Gatekeeper Public Key Infrastructure (PKI) Framework, (September 2006), URL at http://www.agimo.gov.au/infrastructure/gatekeeper
20. Office of the Federal Privacy Commissioner. Office of the Federal Privacy commissioner Consultation paper. (accessed on December 2006), URL at http://www.privacy.gov.au/publications/dpki.html