TRUST IN MOBILE HEALTHCARE: RESEARCH REVIEW AND IMPLICATIONS

Binshan Lin, Louisiana State University in Shreveport, blin@pilot.lsus.edu

ABSTRACT

The premise of this paper is that the effectiveness of wireless healthcare solutions will be a function of security with trust and the appropriateness of the wireless trust model to a particular healthcare environment. We review the most commonly advocated elements of trust. Then we review the research evidence on wireless trust in healthcare. Managerial implications and future research directions are discussed as well.

Keywords: healthcare, e-healthcare, mobile commerce, wireless solutions, mobile architecture, healthcare delivery system, trust, mobile trust model

INTRODUCTION

Mobile commerce represents a significant development in healthcare, offering accessibility, ubiquity, mobility, and localization to end users (10). In healthcare one of the advanced information technology solutions gaining popularity is the wireless access to patient records and other healthcare services. Such initiatives are becoming popular especially in many European countries. These solutions, in particular the mobile electronic patient record, have many advantages over their wired counter parts including significant cost advantages, higher levels of physician acceptance and more functionalities (9); however, they also bring with them challenges of their own. One such major obstacle in mobile adoption and development in healthcare is trust. Given that these systems will be transmitting highly sensitive information namely patient data, implicit in their use is a need for high level of end-to-end security, confidentiality and privacy.

Mobile trust model can be incorporated into any wireless healthcare initiative that will enable healthcare organizations to meet the necessary security standards. By utilizing a well designed trust model in the structuring of a mobile or wireless initiative, it will only then be possible for these organizations to maximize the benefits from wireless technologies as well as minimizing their risks; thereby, enabling the benefits of cost effective, quality healthcare to ensue to those who are most critical; namely the patient.

The premise of this paper is that the effectiveness of wireless healthcare solutions will be a function of security with trust and the appropriateness of the wireless trust model to a particular healthcare environment. We begin with a wireless solution in healthcare as an illustration. Then we review the most commonly advocated elements of trust. Third, we review the research evidence on wireless trust in healthcare. Managerial implications and future research directions are discussed as well.

MOBILE TRUST MODEL

Literature review shows that customers simply do not trust most wired and wireless commercial sites enough to engage in "relationship exchanges" that involves providing credit card and/or personal information about them (5). As business marketers place greater emphasis on building long-term relationships with their customers, trust has assumed a central role (1, 3, 12).

Trust is a complex social phenomenon that reflects technological, behavioral, social, psychological, as well as organizational aspects of interactions among various human and non-human agents. Trust represents customers' confidence to engage in a relationship exchange with a company (6). Two key ingredients of an online trust environment come from security and privacy (8).

Privacy has been defined traditionally as the right of an individual to be left alone and to be able to control the flow of information about him or herself (13). According to the fair information practice proposed by Federal Trade Communications (2), privacy has four dimensions:

- Notice - where appropriate, prior to collection of data;
- Access - allowing people access to data collected about them;
- Choice - providing people a choice to share or use their information;
- Data security - keeping the data secure both internally and externally.

In order to effectively address consumers' privacy concerns, privacy advocates promote adherence to the FTC four dimensions. Mobile healthcare solutions need to cover all four privacy dimensions in their information gathering process.

Mobile healthcare needs security. It is impossible to translate the potential business applications of the wireless technology into viable business ventures without first setting up secure wireless environment. Consumers would shy away from paying goods or services over the wireless medium, if financial and personal information could not be securely transmitted. In other word, wireless trust environment closely relates to individual intention to adopt wireless technology. Mobile healthcare security embraces confidentiality, authentication, and message integrity, and must also be seen in the broader context of e-healthcare systems (7).

Arguably, a secure transaction begins with the establishment of identities of both the provider and the hospital involved in a transaction so that both parties can be verified as who they say they are. The need to identify and authenticate the provider is significant for obvious reasons:

Since mobile devices can be lost or stolen more easily than their fixed counterparts and a guaranteed physical protection of mobile devices such as PDAs is not very practical, a systemic solution is needed to establish identity of the provider even if the provider is using a preauthorized device. A provider interested in engaging in a trusted transaction thus needs to meet two tests irrespective of access location: (1) The provider must be able to identify his or her identity; and (2) The provider must be able to demonstrate the ownership of the mobile device being used for the transaction. Mobile Device: Mobile devices carry hardware-based Subscriber Identification Modules (SIM) that can be used to authenticate the device. However, this authentication does not offer a complete solution to the identity and device ownership problem even though the threshold against committing a fraud is increased. A possible solution to this problem may be to require the provider to enter some form of identification before he or she can complete a transaction using a mobile device. This identification should be distinct from any used to authenticate the SIM in the mobile device. The identification can be a password, or a PIN, or if technology becomes available, biometric.

Mobile devices must perform a series of tasks including initiating a transaction request, communicating the provider's identity to the hospitals' wireless application gateway, and ascertaining the hospital's identity before a secure transaction link is established. In addition to these functions, mobile devices must also carry mechanisms to protect data stored in the device from any form of malicious attack.

Wireless and communication protocols used to connect a mobile device to a base station can be encrypted on demand. Some of the wireless communication technologies such as GSM (4, 11) also provide a built in mechanism of challenge and response to authenticate the wireless device. These security features of wireless technologies offer a partial solution for the open-air portion of a transaction. These standards do not extend to the fixed part of the Internet or intranet where data is transmitted in the clear. However, wireless standards do not provide any mechanism for ascertaining the identity of the parties involved in a transaction.

Incidence of virus attack for mobile devices such as Mobile Phones and PDAs is at present uncommon even though many expect this threat to grow in the not so distant future. Portable computers are more susceptible to viruses and other forms of malicious code. However, portable computers can be protected using a number of virus detection software currently available in the market. Virus protection software for mobile phones and PDAs are beginning to appear in the market and hopefully these and future generation virus protection software will provide adequate safeguard in this respect.

Any security planning must also include application level policies. For example, should all providers have unrestricted access to a medical record? Should we allow a physician’s mobile device to engage in non-medical activities such as sending and receiving email with attachments? Should different providers have different level of access? Other application level policies may include the following:

End-to-end security of a mobile transaction requires intervention at multiple points since none of the individual technologies and devices offer a complete security solution. A comprehensive security strategy must therefore guarantee confidentiality, authenticity, content integrity and non-repudiability. Confidentiality in a mobile transaction is possible if the content of the transaction can be protected through end-to-end encryption. Not only the content must be encrypted in the mobile device itself, it must be transmitted in an encrypted form to the hospital's application gateway and vice versa. This requirement should not be confused with the radio path encryption since the content of a transaction uses media beyond the radio path.

End-to-end encryption can be implemented using symmetric encryption algorithms but would require both provider and hospital to agree on a key as well as the algorithm. This should not be a problem in a healthcare setting since hospitals do not allow unknown providers to interact with its patient and therefore, patient record. However, key distribution problem must be overcome by instituting policies within the organization. For example, mobile devices may be periodically recalled for changing encryption algorithms and keys. The hospital can also implement key distribution using the concepts of asymmetric encryption with public and private key pairs. Authentication of the provider or the hospital is not accomplished through encryption alone since authentication requires origin verification. Wireless standards use a challenge-response mechanism to verify the authenticity of the device. Since the device may not be in the possession of the true provider, other techniques are required to verify authenticity.

Digital signatures are perhaps the best techniques for the authentication of a provider. So long as the signature is generated with part information coming from the provider and part from the mobile device, it can go a long way to satisfy the authenticity need.
Digital signatures can also be used to satisfy the non-repudiability requirements of a transaction. Digital certificates can also be used for this purpose. Message integrity can be achieved through hashing and computing a hash digest. Hospitals can act as their own certificate authority and generate necessary certificate based on level of access allowed for a provider.

The preceding analysis suggests the need for an infrastructure within hospitals that can support both symmetric and asymmetric encryption, digital signatures and digests, as well as the use of digital certificates. Elements of this infrastructure, if developed, should include the following: (1) Handsets that can store private keys of the client in the smart chip in a tamper proof manner. (2) Handsets that include processors capable of supporting encryption algorithms. (3) In house (or public) certificate agencies that can issue digital certificates for mobile transactions as well as provide hosting site for public key look up.

Operationally, asymmetric encryption based on public and private key pair tends to be computing intensive and may pose difficulties for lightweight mobile devices. This problem can be solved by using the asymmetric key system only for the establishment of a secure connection between the physician and hospital. Once such a connection is established, a session specific symmetric key can be exchanged and further communication can be encrypted using the symmetric key.

CONCLUSIONS

Because research on trust in mobile healthcare is relatively new, numerous challenges remain in the area of improvements to IS/IT management and healthcare research community, many of which require efforts from IS/IT researchers interested in mobile healthcare environments. Several areas in need of research present themselves and are briefly discussed below.

The key elements of trust in mobile healthcare were identified in this paper: (1) provider, (2) mobile device, (3) encryption. Each of these components in turn highlighting the particular security issues at each point and how these respective security issues can be addressed and thereby enabling better end-to-end security could be explored. It is suggested the need to explore empirically the important role of trust in any mobile healthcare environment and the need to ensure patient/healthcare providers have adequate access to, and lines of, communication with other players in the mobile healthcare environment.

This paper also set out to underscore the necessity of adopting an appropriate trust model for wireless security in health care in order to address this key challenge. We have then tried to go inside the black box of security as it relates to mobile transactions.

One area of future research that should prove especially interesting is the role of trust model in mobile healthcare. It is recommended that healthcare information systems designers should counter these tendencies by designing and encouraging opportunities for their mobile healthcare applications to form trust model in cyberspace. The benefits of trust model would not only serve to improve security in mobile healthcare; it would also heighten patient's interest and involvement in the mobile healthcare environments. What is required in trust model can include an end-to-end mobile transaction security. Future research is needed to develop trust model and discussed development stages of model in terms of its vulnerabilities and possible safeguards as well.

REFERENCES

1. Doney, P.M., and Cannon, J.P. (1997). "An Examination of the Nature of Trust in Buyer-Seller Relationships," Journal of Marketing, 61(2), 35-31.
2. FTC Report to Congress (2000). "Privacy online: fair information practices in the electronic marketplace," May 2000, Retrieved from http://www.ftc.gov/os/2000/05/index.htm#22.
3. Garbarino, E., and Johnson., M.S. (1999). "The Different Roles of Satisfaction, Trust, and Commitment in Customer Relationships, Journal of Marketing, 63(2), 70-87.
4. GSM (and PCN) Security and Encryption, Charles Brookson - http://www.brookson.com/gsm/contents.htm
5. Hoffman, D.L., and Novak, T. (1999). "Building consumer Trust Online," Communications of the ACM, 42(4), 80-85.
6. Jarvenppa, S.L., Knoll, K., and Leidner, D. E. (1998). "Is Anybody Out there? Antecedents of Trust in Global Virtual Teams," Journal of Management Information Systems, 14(4), 29-64.
7. Lin, B. and Umoh, D. (2002). "e-Healthcare: A Vehicle of Change, " American Business Review, XX(2), June 2002, 27-32.
8. McKnight, D. and Chervancy, N. (2001). Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model, in Proceedings of Hawaii International Conference on System Sciences, 7022.
9. Siau, K and Shen, Z. (2002). "Mobile Commerce Applications in Supply Chain Management," Journal of Internet Commerce, 1(3), 3-14.
10. Siau, K, Sheng, H., Nah, Fiona, and Davis, S. (2004). "Trust in Mobile Commerce: A Study Using the Value-Focused Thinking Approach," International Journal of Electronic Business, forthcoming.
11. The TDMA Operator Path to GSM: A Successful Transition to GSM & Evolution of TDMA - a white paper from Ericsson, September 2001 - http://www.gsmworld.com/technology/index.shtml

12. Viega, J., Kohno, T., and Potter, B. (2001). “Trust (and mistrust) in secure applications,” Communications of the ACM, 44(2), 31-36.
13. Warren, S.D., & Brandeis, L.D. (1890). “The Right to Privacy, “ Harvard Law Review, 4(5), 193-220.