Trust Negotiation for Authentication and Authorization in Healthcare Information Systems

David K. Vawdrey[1], Tore L. Sundelin[2], Kent E. Seamons[2], and Charles D. Knutson[1]
[1]Mobile Computing Laboratory
[2]Internet Security Research Laboratory
Department of Computer Science
Brigham Young University, Provo, Utah 84602
Correspondence Email: dkv@email.byu.edu

Abstract— **The expanding availability of health information in an electronic format is strategic for industry-wide efforts to improve the quality and reduce the cost of health care. The implementation of electronic medical record systems has been hindered by inadequate security provisions. This paper describes the use of *trust negotiation* as a framework for providing authentication and access control services in healthcare information systems. Trust negotiation enables two parties with no pre-existing relationship to establish the trust necessary to perform sensitive transactions via the mutual disclosure of attributes contained within digital credentials. An extension of this system, *surrogate trust negotiation* is introduced as a way to meet the security requirements of healthcare delivery systems based on mobile computing devices and wireless communication technologies. These innovative technologies have enormous potential to improve the current state of security in healthcare information systems.**

Keywords— **Security, Authentication, Access Control, Trust Negotiation, Surrogate Trust Negotiation**

I. Introduction

In modern healthcare delivery systems there is a critical need for timely access to accurate patient medical information. Comprehensive and cost-effective patient care depends on the provider's ability to readily access a patient's test results, prior treatment notes, current prescriptions, and so forth. The lack of access to this information may delay diagnosis and result in improper treatment and increased costs [1].

Electronic medical record (EMR) systems promise to solve many of the existing problems associated with information flow among healthcare providers. Advances in technology are enabling communication of medical record information among provider institutions, record repositories, and individual practitioners on a global scale [2] [3].

While global access to patient record information is necessary to the future of healthcare, strict legal and ethical responsibilities exist for protecting patient privacy. Specific security requirements include establishing protocols to guarantee confidentiality and integrity of identifiable patient information and implementing authentication and access control schemes to prevent unauthorized disclosures of sensitive information [4]. Unfortunately, while most facilities are equipped with up-to-date medical technology, many rely on antiquated communication networks lacking the security measures required to protect sensitive patient information [5].

This paper introduces *automated trust negotiation* to the healthcare environment. Trust negotiation addresses current authentication and authorization limitations in traditional security systems by creating a framework in which two unrelated parties may establish the trust sufficient to perform sensitive transactions. An extension of this technology, *surrogate trust negotiation*, provides dynamic authentication and authorization capabilities for resource-constrained devices in mobile ad hoc networks. Surrogate trust negotiation is useful for meeting the security requirements of systems in which patients use handheld devices (such as cellular phones and PDAs) to act as their digital representatives in the exchange of personal EMR data.

The remainder of this paper is outlined as follows. Section II describes the current state of EMR systems and associated security challenges and weaknesses. Section III explains how trust negotiation meets these challenges by providing a secure mechanism for exchanging EMR data. Section IV describes surrogate trust negotiation, which extends trust negotiation to mobile computing environments. Section V summarizes this research and provides conclusions.

II. Electronic Medical Record Systems

A. Advent of EMR Systems

Traditionally, patient medical records have consisted of data scattered among computerized and paper-based archives in various locations, referenced using inconsistent identifiers. Much of the information in these records tends to be obsolete, redundant, or indecipherable to the extent that it does not benefit the patient at the point of care [6]. Sharing information among various providers has historically been burdensome and inefficient, often requiring the physical duplication of paper-based material.

In response to this deficiency, the U.S. Department of Health and Human Services 2001 Report, *A Strategy for Building the National Health Information Infrastructure* suggests that the United States urgently needs a comprehensive health information infrastructure and that "ready access to relevant, reliable information would greatly improve everyone's ability to address personal and community health concerns" [7]. The

report further states that such a system is now technologically feasible, and its creation would have a marked impact on the effectiveness, efficiency, and quality of healthcare.

The proliferation of electronic medical record (EMR) systems in recent years assists in realizing this goal by enabling medical record information sharing among disparate entities involved in the treatment of patients [8]. Improvements in communication technologies (both wired and wireless) offer improved methods for transmitting EMR information, while standards developed within the medical informatics community provide consistency in formatting and storing data. For example, the Internet provides a growing medium for trading medical knowledge through distributed health services, and standards organizations such as Health Level Seven (HL7) are establishing a comprehensive framework to manage the exchange, integration, and retrieval of electronic health information [2] [9]. Many experts believe that Internet-based Electronic Patient Record systems will be common in the next several years, allowing remote access to a patient's entire medical record [1] [10].

B. Security Concerns

When it comes to personal medical records, patients have a high expectation of confidentiality and often an implicit belief that such information will be used exclusively to facilitate effective care. These records contain some of the most sensitive information about an individual, including data on fertility and abortions, emotional problems and psychiatric treatment, substance abuse, physical and sexual abuse, and genetic predispositions to certain diseases) [11]. Naturally, patients are inherently distrustful of storing and communicating such information electronically and making it available somewhere in "cyberspace" [12] [13]. While various delivery networks and legal jurisdictions have differing regulations regarding access rights to medical information, it is generally agreed that patients' care providers must be allowed consensual access to any information relevant to a patient's treatment [6].

The sensitive nature of medical record information is underscored by the legal obligations of healthcare providers worldwide, such as those outlined in the Data Protection Directive (95/46/EC) in Europe, the HPB 517 regulation in Japan, and the Health Insurance Portability and Accountability Act (HIPAA) in the United States [11]. HIPAA mandates that healthcare providers implement security procedures to protect the integrity and confidentiality of identifiable patient data and also to monitor access and protect against unauthorized uses and disclosures.

One of the fundamental obstacles in meeting legal requirements for privacy is the lack of a comprehensive security framework that addresses the need for authentication (i.e., mapping a party to its attributes) and authorization (i.e., mapping attributes to resource access) [10]. The most common threat to the security of electronic patient records does not come from outside attackers as some have supposed, but from the inappropriate accessing of information by "authorized" providers [1]. These internal security risks include accidental disclosures and poorly controlled secondary usage [11] [12]. One of the major implications of HIPPA is that healthcare institutions must track all instances of access to sensitive data, including who was involved, under what circumstances, and for what purpose [10]. Reliable authentication mechanisms are essential to make this feasible [13].

Traditional access-control methods describe access conditions in terms that only apply to parties within the local security domain. Within a security domain, communicating parties share a pre-existing relationship in which access criteria and permission levels are already defined prior to a transaction taking place. For example, protecting sensitive data with password and/or biometric schemes are popular security techniques but require foreknowledge of the communicating parties (e.g., the access-granting system must compare the requestor's password with a pre-established password list) [14]. Current Public Key Infrastructure (PKI) systems store the participants' certificates in a centralized repository and assume prior knowledge of the subject identity listed in each certificate.

A significant problem arises when no prior relationship exists between an access-granting service and a party requesting EMR data. For example, consider the common situation of healthcare provider *A* requesting a patient's EMR from hospital *B*, where *B* cannot authenticate *A's* request because they are strangers (i.e. they have no foreknowledge or pre-existing relationship).

III. Trust Negotiation

Trust negotiation solves the problems associated with classical authentication and authorization schemes by allowing individuals outside a local security domain to safely access sensitive data and services [15] [16]. It enables two parties to perform secure transactions through a bilateral, iterative process of requesting and disclosing *digital credentials* and *policies.* Credentials are digitally signed by an issuer and assert the veracity of certain attributes of the owner. Digital credentials are the electronic analogues of paper credentials, and may be used to verify such attributes as identifying information, licensing certifications, and association memberships. The properties of public key cryptography guarantee that these credentials are both unforgeable and verifiable.

Along with attribute credentials, trust negotiation relies on *access control policies*, which protect sensitive resources such as services, data, credentials, and even other policies from unauthorized access. By specifying necessary credentials a party must possess in order to access a specific resource, policies provide a means by which any user may be granted or refused access to a resource in real-time. Associating policies with particular resources allows trust negotiation to thrive in a dynamic environment in which users and resources are constantly changing. As all parties in a given transaction may have sensitive resources protected by applicable policies, trust negotiation often occurs in a bilateral fashion with respective parties progressively fulfilling other parties' policies while

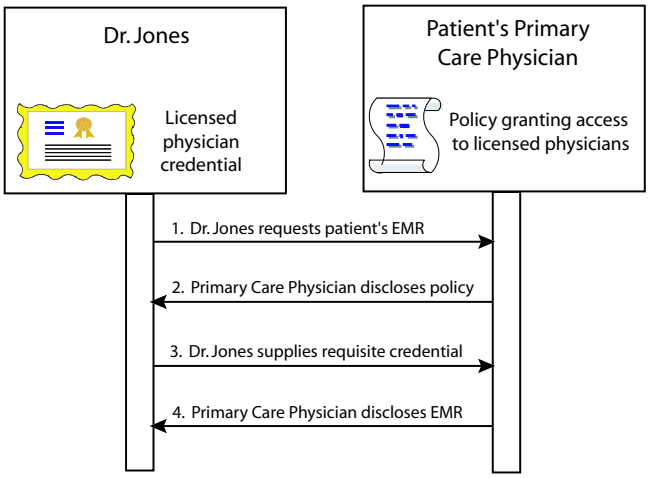

Fig. 1. Using trust negotiation to control access to EMR information.

iteratively making policy-based credential requests of their own.

For example, Fig. 1 describes a scenario where Dr. Jones wishes to access the EMR of a new patient, Ms. Sally White, who is visiting from out of town. He sends a request to the office of Ms. White's primary care physician, asking for her digitally signed medical record along with the credential containing the key used to sign it. To authenticate the requesting party, the primary care physician's trust negotiation system responds with a message containing a policy stating that records will only be disclosed to licensed medical doctors.

In order to satisfy this policy and establish adequate trust, Dr. Jones supplies a digital credential signed by the local medical association asserting his status as a licensed practicing physician. The primary care physician's server confirms Dr. Jones' digital credential by verifying its signature using a credential issued by a trusted third party (e.g., a national licensing association). This fulfills the primary care physician's policy, resulting in a sufficient level of trust to complete the transaction. The server then encrypts Ms. White's EMR using a unique shared session key and sends it via the Internet along with a credential asserting the primary care physician's status as a licensed medical doctor. Dr. Jones decrypts the EMR and verifies its legitimacy using the primary care physician's credential. The use of trust negotiation in this scenario provides a mechanism for the authorized, confidential transfer of Sally's medical record.

IV. Surrogate Trust Negotiation

Healthcare information systems that include handheld computing platforms and wireless communication technologies manifest numerous security challenges beyond those in conventional health information systems. These difficulties arise from both the broadcast nature of wireless transmission (i.e., data is transmitted in all directions simultaneously) as well as the resource limitations (including bandwidth, processing capability, battery life, and unreliable connections) of many devices that populate wireless networks. In spite of these obstacles, organizations such as the Mobile Healthcare Alliance (MoHCA) insist that wireless networks that transmit patient data meet the same security requirements established for their wired counterparts [17].

Ideally, the aforementioned techniques for negotiating trust in wired health information systems could be used to authenticate users and appropriately limit access in systems that include mobile computing devices. Unfortunately, many of the algorithms used in standard trust negotiation require computationally intensive cryptographic calculations and reliable access to the Internet that may not be possible for typical resource-limited mobile computing devices. A proposed solution to this problem is *surrogate trust negotiation*, a system which extends trust negotiation to mobile environments that rely on wireless communication technologies [18].

Surrogate trust negotiation (STN) provides a flexible model that effectively leverages the combined capabilities of network proxies, software agents, and modern cryptographic systems. Central to this solution are portable devices that are individually capable of acting as streamlined networking proxies in order to compensate for the topological idiosyncrasies and deficiencies often present in mobile networks. The STN protocol can perform dynamic, role-based authentication and authorization in mobile infrastructures as well as in the stationary environments addressed by previous research in automated trust negotiation systems.

In surrogate trust negotiation, the highly sensitive and resource-intensive task of public key cryptography that is integral to credential-based systems is offloaded to *trust agents*. Trust agents are autonomous software modules on secure, offsite computers that act as "surrogates" for mobile devices, performing cryptographic operations and managing credentials, policies, and secret keys for use in trust negotiation. Thus, STN allows even computationally lightweight devices to effectively participate in data exchange scenarios using trust negotiation.

The application of an STN-based authentication and access control infrastructure in a healthcare information system enables many desirable usage models that are otherwise insecure or infeasible. The following scenarios illustrate the advantages of STN. The first depicts a novel STN application in a medical emergency (see Fig. 2). The second demonstrates how STN may be used to extend the capabilities of standard trust negotiation within the doctor's office scenario described in Section III.

A. STN in an Emergency Scenario

Emergency medical personnel arrive at the scene of an automobile accident where they discover an unconscious woman behind the wheel of her car. A paramedic's handheld computer wirelessly communicates with the victim's cellular phone which controls access to her EMR and directs emergency workers to authentication software on her home computer. The address of the victim's authentication software is then automatically forwarded to the computer system at the local hospital emergency room. Next, the emergency room system

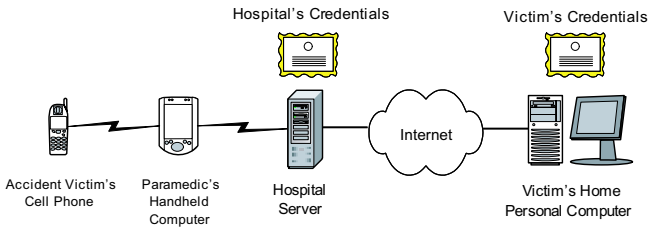

Fig. 2. Surrogate trust negotiation in an emergency medical situation.

contacts the victim's computer and provides the paramedic's security credentials in order to establish trust. In turn, the victim's computer supplies a credential issued by her physician asserting the accuracy and authenticity of her medical data. The on-site medical personnel are then granted access to the victim's critical EMR data, including her medical history, allergies, emergency contact information and potential drug interactions.

B. STN Used to Augment Standard Trust Negotiation

Recall the scenario from Section III, Fig. 1, where Sally White visits Dr. Jones while travelling. Noticeably absent from the example given is the notion of patient consent. A more accurate scenario might unfold as follows. Before providing care, Dr. Jones requires a waiver authorizing treatment and allowing access to Sally's EMR. To accomplish this, Dr. Jones' office computer sends a request to Sally's PDA for a digitally signed waiver expressing her consent. Sally's PDA communicates via the Internet with the trust agent on her home computer, which responds to Dr. Jones' request by disclosing a policy stating that the PDA will not sign a waiver without verifying the requestor's physician credential. Once Dr. Jones' respective trust agent supplies the necessary credential, Sally's PDA digitally signs the waiver.

Next, Dr. Jones' computer requests Sally's EMR from the office of her primary care physician. Before releasing the record, the primary care physician's record system must not only recognize Dr. Jones as a licensed physician, but also confirm his "need to know" [19]. In order to prove that the request for Sally's EMR is legitimate, Dr. Jones' computer submits the waiver Sally's PDA previously signed, and the primary care physician's system verifies the waiver and releases Sally's record.

V. Conclusion

The global expansion of EMR systems among healthcare institutions is absolutely essential for improving patient care, medical research, and public health. In the past, the implementation of EMR systems has been hindered by inadequate security mechanisms, including deficiencies in controlling access to sensitive data. Trust negotiation is a new approach for authentication and authorization among healthcare information systems with no pre-existing relationship. Surrogate trust negotiation extends these security benefits to systems involving resource-constrained mobile computing devices that may be used to store individual patient medical records. These innovative technologies have enormous potential to improve the current state of security in healthcare information systems.

Acknowledgment

This research was sponsored by DARPA through Space and Naval Warfare Systems Center San Diego grant number N66001-01-1-8908.

References

[1] D. M. Rind, I. S. Kohane, P. Szolovits, C. Safran, H. C. Chueh, and G. O. Barnett, "Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web," *Ann. Int. Med.*, vol. 127, no. 2, pp. 138–141, July 1997.

[2] I. S. Kohane, P. Greenspun, J. Fackler, C. Cimino, and P. Szolovits, "Building national electronic medical record systems via the World Wide Web," *JAMIA*, vol. 3, no. 3, pp. 191–207, 1996.

[3] J. van der Lei, "Closing the loop between clinical practice, research, and education: The potential of electronic patient records," *Meth. Inf. Med.*, vol. 41, no. 1, pp. 51–54, 2002.

[4] R. C. Barrows, Jr. and P. D. Clayton, "Privacy, confidentiality, and electronic medical records," *JAMIA*, vol. 3, no. 2, pp. 139–148, 1996.

[5] NetMotion Wireless, Inc., "HIPAA security for wireless networks," White Paper, 2001. [Online]. Available: http://www.netmotionwireless.com/assets/netmotion_security_hipaa.pdf

[6] R. Schoenberg and C. Safran, "Internet based repository of medical records that retains patient confidentiality," *BMJ*, vol. 321, pp. 1199–1203, Nov. 2000.

[7] "Information for health: A strategy for building the national health information infrastructure," National Committee on Vital and Health Statistics, Tech. Rep., Dec. 2001.

[8] R. S. Dick, E. B. Steen, and D. E. Detmer, *The computer-based patient record: An essential technology for health care.* Washington, DC: National Academy Press, 1997.

[9] J. van Wingerde, J. Schindler, P. Kilbridge, P. Szolovits, and C. Safran, "Using HL7 and the World Wide Web for unifying patient data from remote databases," in *Proc. American Medical Informatics Association Annu. Fall Symposium*, J. J. Cimino, Ed., 1996, pp. 643–647.

[10] A. Dwivedi, R. K. Bali, M. A. Belsis, R. N. G. Naguib, P. Every, and N. S. Nassar, "Towards a practical healthcare information security model for healthcare institutions," in *Proc. 4th Conf. Information Technology Applications in Biomedicine (ITAB'03)*, Birmingham, UK, pp. 114–117.

[11] T. C. Rindfleisch, "Privacy, information technology, and health care," *Comm. ACM*, vol. 40, no. 8, pp. 92–100, 1997.

[12] T. Huston, "Security issues for implementation of e-medical records," *Comm. ACM*, vol. 44, no. 9, pp. 89–94, 2001.

[13] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patient control: How to keep electronic medical records accessible but private," *BMJ*, vol. 322, pp. 283–287, Feb. 2001.

[14] H. M. Chao, S. H. Twu, and C. M. Hsu, "A secure identification access control scheme for accessing healthcare information systems," in *Proc. 4th Conf. Information Technology Applications in Biomedicine (ITAB'03)*, Birmingham, UK, pp. 122–125.

[15] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated Trust Negotiation," in *Proc. DARPA Information Survivability Conference and Exposition*, Hilton Head, SC, Jan. 2000.

[16] M. Winslett, T. Yu, K. E. Seamons, A. Hess, J. Jacobson, R. Jarvis, B. Smith, and L. Yu, "Negotiating trust on the Web," *IEEE Internet Comput.*, vol. 6, no. 6, pp. 30–37, Nov./Dec. 2002.

[17] Mobile Healthcare Alliance (MoHCA), "Are there HIPPA recommendations regarding patient data transfer over wireless networks?" White Paper, 2002.

[18] T. Sundelin, A. Hess, J. Holt, R. Bradshaw, K. E. Seamons, and C. D. Knutson, "Surrogate trust negotiation: Authentication and authorization in dynamic mobile networks," unpublished.

[19] M. A. Epstein, M. S. Pasieka, W. P. Lord, S. T. Wong, and N. J. Mankovich, "Security for the digital information age of medicine: Issues, applications, and implementation," *J. Dig. Imag.*, vol. 11, no. 1, pp. 33–44, Feb. 1998.