Providing an Additional Factor for Patient Identification Based on Digital Fingerprint

Guy C. Hembroff Xinli Wang
School of Technology
Michigan Technological University
Houghton, MI 49931, USA
hembroff@mtu.edu, xinlwang@mtu.edu

Sead Muftic
Computer Science
KTH – Royal Institute of Technology
Stockholm, Sweden
sead@kth.se

Abstract

Implementing a comprehensive healthcare security model is a difficult task due to the many complexities in the medical environment. Accurate patient identification is often overlooked in the areas of security and privacy. We have used our own architecture and experiences to bring forward this problem and offer suggestive solutions of incorporating biometric fingerprints and photographs of patients in a strategic manner to help strengthen our healthcare security model.

1 Introduction

The importance of securing and controlling sensitive healthcare data is paramount. Medical staff require systems to permit secure authentication and authorization to patients' medical records to assist in patient diagnosis and treatment. Patients benefit from an architecture permitting heightened security to protect their sensitive information, yet also demonstrates functionality in allowing the patient to view, update or make changes to electronic personal health records (PHRs).

Developing a secure and scalable architecture for accurate information exchange is difficult due to the complexities within the healthcare environment. Trust may not be established or incorrectly defined between different healthcare domains. Policies often conflict between entities discouraging data being evaluated from the implemented security mechanisms, resulting in data not able to be retrieved successfully. Also, the use of different message standards, such as varying HL7 versions, add to the barriers of exchanging information. While each of these reasons are critical in contributing to the difficulties in achieving secure and scalable information exchange in healthcare, there has been research and testing through implementation in recent times to validate the reduction of these complexities. Rather, we argue in this paper the inaccuracies of identifying the patient create a significant barrier to produce a comprehensive and scalable healthcare security model. We investigate general healthcare security architectures to document this occurrence, however and more importantly, we call on our own health information exchange to validate this claim, provide additional details to better understand all variables affected by this issue, and justify the actions we are currently taking to strengthen security and privacy within our network.

2. General Healthcare Security Architectures

Typical healthcare security architectures regulate authorization through role-based access control [6] and policy storage to coincide with authentication and authorization engines proceeding access to data. The integration of standards such as Extensible Access Markup Language (XACML) and Security Assertion Markup Language (SAML) have helped extend healthcare's security model over distributed systems [1].

This extended security model brings new challenges to identify the patient accurately and securely. Patient identification and record linkage is often conducted with preset identifier categories. Often these identifiers are not accurately recorded and patients' identification becomes flawed [4]. The result weakens the healthcare security model.

3. Healthcare Security Model Example

We have developed a security HIE for a region that consists of 13 hospitals and one Regional Center. A *federated* environment was established in the form of multiple autonomous domains. The developed architecture utilizes the following security standards to help ensure compliancy and scalability [3]:

- Public Key Infrastructure (PKI) components, protocols and services handling X.509 certificates
- Web Security Services (WSS) , World Wide Web Consortium (W3C), Organization for the Advanced of Structured Standards (OASIS), Internet Engineering Task Force (IETF), secure Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), SAML, and XACML policies
- Secure transactions based on Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), and SAML standards
- Smart Cards Management Services (CMS, Federal Information Processing Standard (FIPS) 201 standard

3.1 Resulting Security and Privacy Issues

Within our architecture, we have noticed several important points of interest contributing to weakening the security and privacy of our system. First, the matching algorithm keying in on patient variables such as first name, last name, social security number, gender, etc. have proven to be inaccurate. As a result of these deficiencies, multiple records have merged incorrectly into a consolidated record to display not only inaccurate information to this patient, but also sensitive information that is not their own. Second, the evaluation has shown that local policies within each of the hospitals are becoming less secure due to security personnel modifying security policies based on medical staff requests that they are not able to access the correct patient record when individuals are being evaluated or consulted. A review of XACML policies have shown security personnel are granting medical staff additional rights to increase patient search capabilities. This has led to conflicting policies and produced cases allowing medical staff to view patient information which should be restricted. Third, test results have been found to be placed into the incorrect patient record, due to human error, inaccuracies on gathering patient information, or similarities in patient's name, date-of-birth, city, etc. As a result, each of the above examples have weakened the security and privacy of our implemented healthcare model, while simultaneously jeopardizing patient safety.

3.2 Improving Security and Privacy

We are currently developing and testing an enhanced patient identification process in hopes to strengthen the security and privacy of our healthcare model. To achieve this we have implemented two distinct changes. The first alteration which is routine and has been implemented in other healthcare architectures was to add photo identification of the patient to all medical records [7]. Second, we developed a fingerprint to Personal Identification Number (PIN) algorithm to identify patients. Although this concept has received past research [2,5,8], our implementation is different in terms of accuracy and the scalability it provides. Patients fingerprint images are captured during enrollment and then matched for verification. The unique biometric PIN generated serves at the Master Patient Identifier (MPI) and becomes the primary key when conducting a record locater service (RLS) querying for the patient's consolidated electronic medical record. Any conflicts in identification are resolved with a one-to-one minutia analysis from the fingerprint image to the given template(s) of those chosen identified as conflicting. Photo identification and other descriptive variables are then used as an additional security provision to ensure correct patient records are being utilized. Patients unable or unwilling to submit fingerprints, are permitted traditional identification methods.

Having accurate fingerprint images of the patient also provides additional functionality that supports security and privacy, along with increasing patient safety. Patient tests incorporate the electric fingerprint of the patient, and results are added to electronic records only if they match the patient's biometric template. Additionally, patients will be able to digitally sign results or other sensitive information with their electronic fingerprint. Also, the fingerprint generated PIN and matching techniques has proven to be beneficial when patients are admitted to the Emergency Department (ED) and do not possess identification and are perhaps unconscious or unable to provide information of their medical history. Fingerprints are scanned and PIN generation confirmed with one-to-one minutia matching permit RLS to return patient's electronic medical records.

4. Conclusion

Implementing a comprehensive healthcare security model is a difficult task due to the many complexities in the medical environment. Often accurate patient identification is overlooked in the areas of security and privacy. We have used our own architecture and experiences to bring forward this problem and offer suggestive solutions of incorporating biometric fingerprint and photograph of the patient in a strategic manner to help strengthen our healthcare security model. Our data has shown improved security and privacy of our system, but has also increased patient safety while decreasing healthcare costs associated with reconciling electronic records and possible misdiagnosis or treatments due to incorrect information populating patient records.

References

[1] A. Dwivedi, R.K. Bali, M.A. Belsis, R.N.G. Naguib, P. Every, N.S. Nassar. Towards a practical healthcare information security model for healthcare institutions. *Information Technology Applications in Biomedicine 4th Annual EMBS Special Topic Conference,* IEEE, 2003.

[2] F. Han, J. Hu, L. HE, Y. Wang. Generation of Reliable PINs from Fingerprints, In ICC '07: *Proceedings of the IEEE's ICC symposium.* IEEE. 2007.

[3] G. Hembroff and S. Muftic. Secure Healthcare Information Exchange for Local Domains. *International Conference on Pervasive Health.* IEEE. 2009.

[4] Y. Hyser and E. Evans. Cross-system data linkage for treatment outcome evaluation: Lessons learned from the California Treatment Outcome Project. *Evaluation and Program Planning*, 31:2:125-135. 2008.

[5] T. Liu, C. Zhang, P. Hao. Fingerprint Indexing Based on LAS Registration. *IEEE International Conference on Image Processing*. IEEE. Pages 301-304. 2006.

[6] Z. Longhua, A. Gail-Joon, C. Bei-Tseng. A role-based delegation framework for healthcare information systems. In SACMAT '02, New York, NY, USA. ACM. 2002.

[7] A. Naszlady, J. Naszlady. Patient health record on a smart card. *International Journal of Medical Informatics*. 48:3:191-194. AMIA. 1998.

[8] Y. Zhang, J. Tian, K, Cao, P. Li, X. Yang. Improving efficiency of fingerprint matching by minutiae indexing. *Pattern Recognition, ICPR 2008 . 19th International Conference,* IEEE. Pages 1-4. 2008.