Controlled EHR access in secured health information systems

(paper submitted to the First IEEE International Conference on Digital Information Management (ICDIM 2006)

Saleh Al-zharani
Information Systems Department
Imam Mohammad Bin Saud University
Faculty of Computer & Information Science
Riyadh, Saudi Arabia
Dr_Saleh@hotmail.com
Sgzahrani@imamu.edu.sa

S.Chandrappa,
Tirigent Technologies Ltd
Bangalore. India
chandrappas@yahoo.com

Pit.Pichappan
Department of Information Science
Annamalai University
Annamalainagar 608002. TN
India
ppichappan@gmail.com

Abstract*: Health care systems are vulnerable to many possible attacks leading to challenge the data security. While designing information systems, this problem is addressed by proposing and testing various designs. Through this paper we describe two tier architecture to access EHR data with the use of interactive trust negotiation. The preliminary results suggest that security measures are not confined to systems alone but data correlations offer much promise for developing a secured health care information system.*

Introduction

Information systems are increasingly become more vulnerable in the light of attacks on data that is sharable and available at remote locations. Health care data need to be transferred across domain, places, networks and people. The core health care data is derived from the electronic health records (EHR) as trials and controlled studies largely depend on EHR data. EHR data like any other sensitive data is prone to unpredictable attacks.

Viruses and DoS employ malicious programmes to attack the data available in the web where EHR data is of no exception. The extent of usability of stored and processed health care information depends on how we secure and protect against possible attacks. Security unlike other nonfunctional requirements, such as reliability and performance, has not

been fully integrated within the development lifecycle and it is still mainly considered after the design of the system. (Haralambos Mouratidisa, et al 2005)

Ignoring security issues during the development process could lead to serious problems [R. Anderson], since security mechanisms would have to be fitted into a pre-existing design, therefore leading to design challenges that usually translate into software vulnerabilities [W. Stallings].

Some of the key issues that must be carefully considered prior to the design of the security architecture for interconnected EHR systems are the following

• The interconnection of EHR systems facilitates the collaboration of independent HCU, each unit remaining sovereign in its own domain and defining its own security policy. However, users in one domain may ask to access information in any other domain.
• The network of interconnected sites is not static. New HCU may join the network at any time.
• There is no central authority administrating or even enforcing a common policy to all interconnected sites.
• The fact that medical information can be accessed from some unknown remote location, possibly belonging to a different domain and thus exhibiting a different security policy, imposes the need to treat the data in accordance to specific security attributes (policies) attached to it.
• No predefined trust relations among individual health care units or groups of units can be assumed. Trust evaluations should be dynamic.([Blobel and Blobel, S. Katsikas]:

Problem for study

Through this paper we stress that security issues need to be considered while designing the systems rather than post-testing or post-issue stage. Health care data access is warranted from unspecified remote location, leading to transfer of data where authenticated users need to access and the failure if any is vulnerable. The use of different security policies, imposes the need to treat the data in accordance to specific security attributes (policies) attached to it.

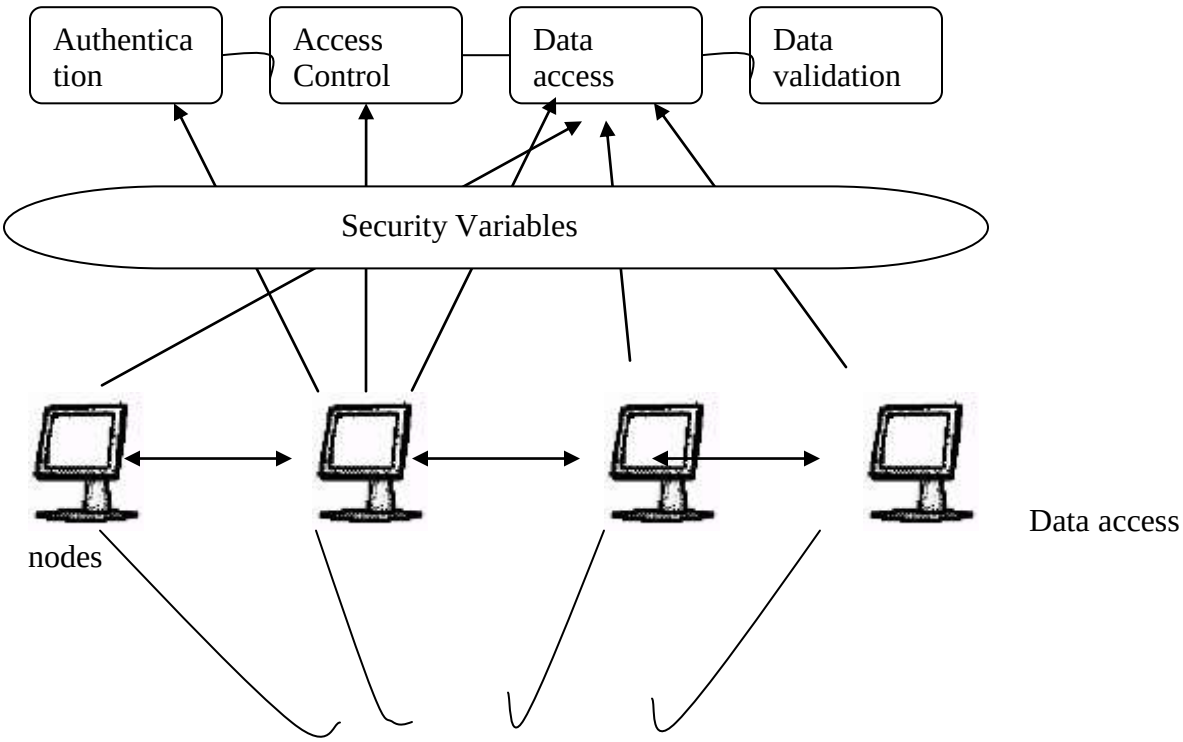
We through this work, address the security specification from two major components, viz., variables for *software design* and *application domain.* Many security issues ignore application domain as security is not independent of characteristics of domain

Even we confine our discussions on the data access system, many discussions were initiated about the effectiveness of the formal security measures. Among them, encryption is found to be effective in security agents applications. (Dimitris Gritzalis)

Basic premises

The basic premise underlying the proposed two level architecture lies on the following principles.

For a secured health care system two components are required. First is the software design than includes the formal security variables such as concepts, mechanism, algorithms, data and services. In the second level we have the application domain that includes the factors such as authentication, access control, data access and data validation. The system security modules are the protocols in the security architecture and they not be explicitly addressed in any system specifically.



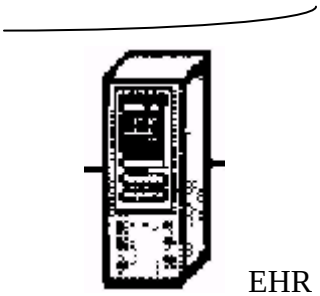


Figure 1. Generic Level architecture for EHR data access and security

Security Environment in EHR data

The encryption, fire walls, authentication and other formal factors are required in any security system. However we limit to our discussions by excluding such formal security measures. However despite the availability and use of these formal measures much intrusion takes place across health cares system. Hence besides the systems control data access control could be enabled when the middle agents such as brokers authenticate and control the data access. Based on this premise, we propose a two-tired architecture for the health care data access.

Proposed Two tier Architecture

The proposed two tier architecture as illustrated in the figure 1, includes two levels, security variables and application domain, data access nodes and the EHR server. As said earlier we limit our discussions to the application domain and data access rather than the security variables. The application domain is based on the four components, viz., authentication, access control, data access and data validation.

The authentication comes after the security testing and approval by the system, but it goes beyond as the data authentication is introduced in the architecture. The proposed four components thus first under go security testing initially and then data is extracted from the database. The architecture works on the concept interactive trust negotiation which is incremental than the automated trust negotiation. (David K. Vawdrey et al)

Trust Negotiation

Trust negotiation scores over the basic authentication and authorization schemes particularly the access comes beyond the local security domain (Winsborough etal, M. Winslet et al) Trust negotiation works in the interactive environment where the requester and server exchange the bilateral way disclosing digital credentials and policies.

Two components in our architecture the access control and data access warrant the attribute credentials, which is ensured by the trust negotiation, which protect important resources such as services, data, credentials, and prevent the unauthorized access. By producing the necessary credentials a node should have order to access a specific resource, the conditions provide a way by which any node gets data access or refused access to the required data. As the data requirement is routed through many intermediate servers and across different users who are not confined to specific sets, trust negotiation is more effective and suitable.

The users who involve in a given transaction may have secured data protected against any possible intrusion, trust negotiation often occurs in an interactive way with all involved users progressively fulfilling other user's' policies while iteratively making policy-based credential requests of their own.

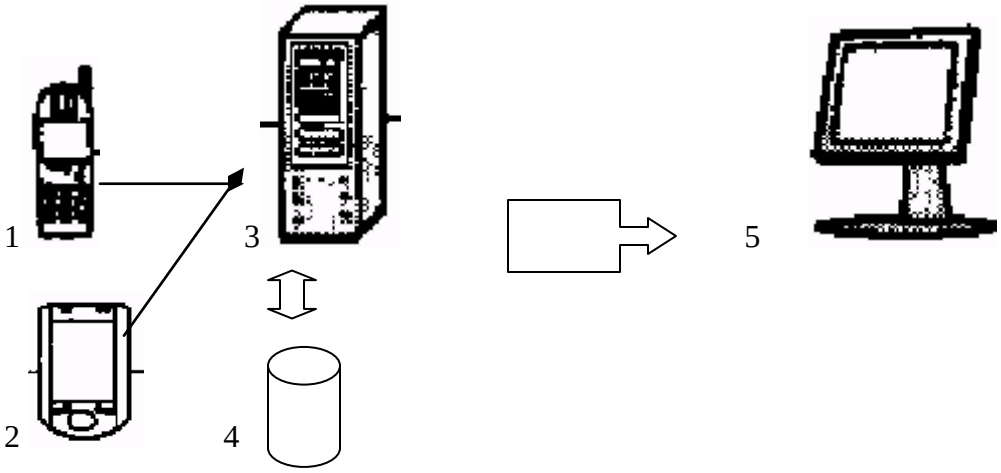
Surrogate trust negotiation

Healthcare information systems often involves data access stream from varied users and intermediaries that include handheld computing platforms and wireless communication technologies manifest unpredictable security challenges. The difficulties in the resource-limited mobile computing devices make it difficult to use the trust negotiation as the algorithms used in it often is complex. To delimit the difficulties, surrogate trust negotiation is proposed initially in (David K. Vawdrey)

In surrogate trust negotiation, trust agents depend the pubic cryptography for highly sensitive and resource task where the credential based systems get offloaded. Trust agents are independent programmes on secure, offsite computers that act as better alternatives for mobile devices, performing cryptographic operations and managing credentials, policies, and secret keys for use in trust negotiation. The deployment of surrogate trust negotiation ensures the healthcare information system for securing the data modules.

Interactive trust negotiation

The cryptographic credentials are verified with the help of the trust agents stored in the EHR server which secure the previously recorded data in the database and authenticate the credentials. Otherwise the interactive trust negotiation is similar to the surrogate negotiation as the surrogate negotiation ensures better cryptography. Requests often arise from handheld mobile devices where authentication needs to be credential managed. The interactive trust negotiation works by correlating the basic data in a problem environment with the basic data already stored in the database. The validity of this security is increased as the base data is compared empirically.



1/2 Mobile and hand held devices
3. Authentication server
4. Database
5. Authenticated system

Figure 2. Illustrated interactive trust negotiation

The interactive trust negotiation is illustrated in a following situation. Health care professionals record a particular patient for treatment. The handheld device is used basically to report the case to the treatment. The preliminary investigation and clinical data is transferred to the database with the authentication request. The authentication request is first analysed for security using formal mechanisms of security and then in order to ensure trust, the basic data is verified in the database. The database has inbuilt preliminary authentication questions for each patient which are directed to the health care professionals who sought data. Correlation between the health care professionals feed data and the patient data stored in the database is based on the concept interactive trust. The basic data observed from a patient by health care professional describe a variety of environments such as physical features, early symptoms that get correlated in a problem situation and biophysical conditions. Such a system ensures access to protected data from remote locations with security.

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.

Architecture of the broker server

In this section we describe the EHR data flow architecture with the help of the broker server. The broker server was introduced in (Chao-Hung Lin) which discussed the data flow between the remote-monitoring devices and the in-home PCs.

Broker server operates based on the following premises.

a) authenticate only designated requests and services
b) adheres to all formal security variables
c) monitoring regularities in data access pattern

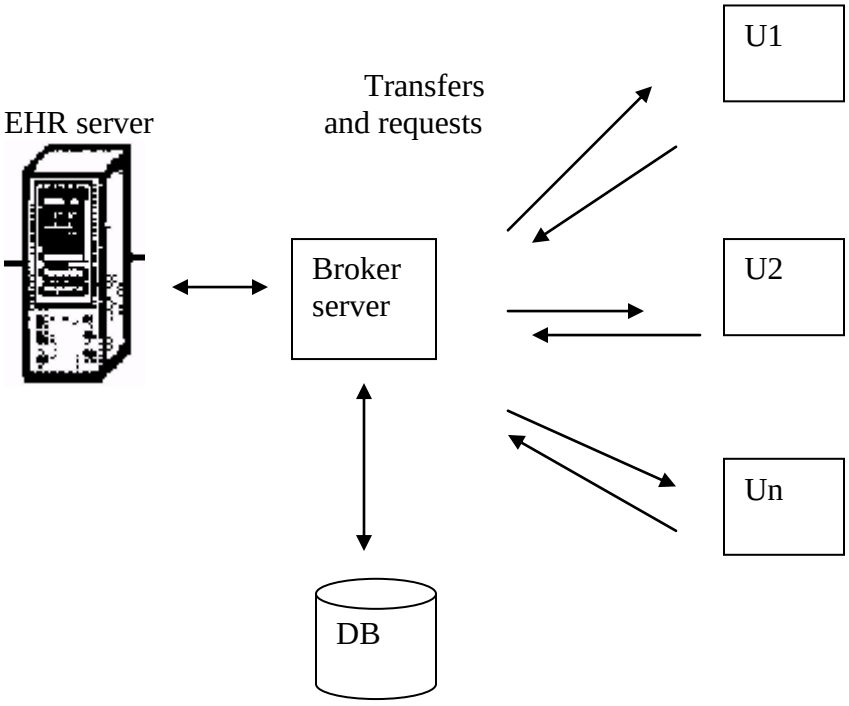


Figure 3. Broker server operation

The broker server acts as a controlling device which has a database of the users' description and the access data. It has the user control description where each user is permitted to enter into specific operation circles. Each user visit after authentication by the broker server is correlated by it for http description, the extent of the use of permissible rights etc. If a specific user when tries to exceed the right and when it happens with more threshold the broker server monitors and control it.

The broker server validates the request (including professional credentials check) and transmits the authentication to the EHR server. The EHR server then approves and delivers the digital certificate to the node. Once the formal security mechanisms validate the node user the node user can enter the user ID and password to log into the data server. The data such as http, ip, user id and other similar description about the computer programs and the accounts of remote-monitoring users are stored in the database.

Results

The proposed security design is validated in a stimulated environment. The random trial of 257 requests was routed through broker server with a mean frequency of 25 access attempts. The nodes used in the operations include remote location mobile and other related hand held devices. Out of the 25 nodes 17 are designated and the remaining are intruders. Each of the nodes tries to enter into the EHR data server including intruders. The security measures as well as broker validation is tested for the efficiency of the proposed design.

Over the evaluation period, 257 requests from the 25 nodes have applied for data access. In the first level that is at the formal security measures all the 17 valid users and two intruders were successful to get validated. The intruders' access is planned in an optimized way that they can break the security measures.

The 17 nodes were successful in each of the broker validation system. The 8 intruders requested for access by possessing false claims with the optimized authentication. It was found that two highly powerful intruders are able to break the firewall and encryption security.

Our preliminary employment of stimulated evaluation results is promising leading to a more penetrated analysis of the proposed interactive trust negotiation.

Conclusion

Advanced and enhanced architectural paradigms would enable to improve not only the security, but the scalability, interoperability and flexibility in electronic health care systems. Currently, developers employ varied architectures for functional health care system in a distributed environment. The health care systems do follow different schema, employ different formats, and use repositories with both fully secured to unsecured data. Architecture construction processes proceeds in multi-directions employing heterogeneous and unconnected architecture underlying different technologies. Fusing the different architectures is essential in order to construct federated health care system. While doing so, the platforms, repositories and interfaces play major role. This paper has addressed an enhanced architecture, identify the components and elements and suggest a fused architecture. The testing of the designs and improving the validity will enable to bring solid electronic health care system.

References

[1]. Haralambos Mouratidisa, Paolo Giorginib, Gordon Manson, “When security meets software engineering: a case of modeling secure information systems”, *Information Systems* 30 (2005) 609–6290

[2] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Computer Publishing, New York, 2001.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, second Ed., Prentice-Hall, Englewood, Cliffs, NJ, 1999.

[4] B. Blobel, ‘‘Security requirements and solutions in distributed Electronic Health Records’’, in: Proceedings of the 13th IFIP International Information Security Conference (SEC-1997), 1997.

[5] B. Blobel, S. Katsikas, ‘‘Patient Data and the Internet: Security Issues’’, Proceedings of the IMIA Conference on Common Security Solutions for Communicating Patient Data, 1997.

[6] David K. Vawdrey, Tore L. Sundelin’, Kent E. Seamons’, and Charles D. Knutson. Trust Negotiation for Authentication and Authorization in Healthcare Information Systems “Proceedings of the 25’ Annual Inlematianal Conference of the IEEE EMBS, Cancun. Mexico *September 17-21,2003*

[7] Dimitris Gritzalis and Costas Lambrinoudakis, “A security architecture for interconnecting health information systems, International Journal of Medical Informatics, Volume 73, Issue 3 , 31 March 2004, Pages 305-309.

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

[9]. M. Winslett, T. Yu, K. E. Seamans, A. Hess, 1. Jacobson, R. Jarvis, B. Smith, and L. Yu, "Negotiating trust on the Web:' IEEE lnternet Computation., vol. 6. no. 6, pp. 3&37. Nov.Dec. 2002.

[9] David K. Vawdrey’, Tore L. Sundelin’, Kent E. Seamons’, and Charles D. Knutson, op.cit

[10]. Chao-Hung Lin , Shuenn-Tsong Young , Te-Son Kuo, A remote data access architecture for home-monitoring health-care applications, Medical Engineering & Physics 2006.