Securing Telehealth Applications in a Web-Based e-Health Portal

Qian Liu, Shuo Lu, Yuan Hong
Department of Computer Science
Concordia University
1455 de Maisonneuve Blvd. West,
Montreal , Quebec , Canada
{liu_qian,lu_shuo,y_hon}@cs.concordia.ca

Lingyu Wang, Rachida Dssouli
Concordia Institute for Information Systems Engineering
1455 de Maisonneuve Blvd. West,
Montreal , Quebec , Canada
{wang, dssouli} @ciise.concordia.ca

Abstract

Telehealth applications can deliver medical services to patients at remote locations using telecommunications technologies, such as the Internet. At the same time, such applications also pose unique security challenges. First, the trust issue becomes more severe due to the lack of visual proofs in telehealth applications. The public key infrastructure (PKI) is insufficient for providing the same kind of trust a patient may attain during a face-to-face service. Second, telehealth services, such as tele-monitoring or tele-consultant, naturally demand a systematic organization of users, roles, resources, and flows of information. Existing access control mechanisms in an e-health system are usually incapable of dealing with such workflow-based services. This paper provides cost-efficient solutions to those issues in the context of a Web-based e-health portal system. First, we propose a PKI-like infrastructure for establishing trust between users using biometrics-based authentication and hierarchies of trust. Second, we develop an access control method for workflow-based telehealth services using a rule-based module already available in the portal system.

1. Introduction

Telehealth applications are gaining momentum due to the increased popularity of Web-based e-health systems and a demand for remote and more convenient accesses to medical services. Through leveraging modern telecommunication technologies, such as the Internet, telehealth applications can provide much-needed medical services to patients at remote locations or even in different countries. At the same time, such applications also pose many unique challenges to their design and implementation. In particular, security is crucial to telehealth applications due to the fact that medical services may be critical to patients' health or even life. In this paper, we study two security issues in telehealth applications in the context of a Web-based e-health portal system. First, a unique trust issue arises due to the lack of visual proofs in telehealth applications. For example, a patient may have doubts in the identity of a doctor at the other end of a telehealth service provided via the Internet. The public key infrastructure (PKI) can enable a patient in establishing trust in the organization's website or telehealth applications, which is the very purpose of PKI by design. However, PKI is insufficient for providing the same kind of trust a patient may attain during a face-to-face service. Second, telehealth services, such as tele-monitoring or tele-consultant, usually involve a complex process that naturally demands a systematic organization of multiple users playing different roles in accessing shared resources and flows of information.

This paper provides solutions to the above issues in the context of a Web-based e-health portal system. First, we propose a PKI-like infrastructure for establishing trust between users using biometrics-based authentication and hierarchies of trust. By employing multimedia and biometric features, such as face recognition, the infrastructure can provide an increased degree of trust to users of telehealth applications. Second, to regulate accesses to workflow-based telehealth services in a cost-efficient way, we adopt an approach of re-using the rule-based access control module already available in the portal system. Specifically, the temporal dependency between events is expressed as partial orders and then enforced with a special *done* rule in the logic-based access control engine. In contrast to deploying a full-fledged workflow management system, our approach provides

0-7695-3102-4/08 $25.00 © 2008 IEEE
DOI 10.1109/ARES.2008.9

a light-weight and effective solution to existing telehealth applications.

2. Related work

As an expansion of telemedicine, telehealth refers to the delivery of health-related services and information via telecommunications technologies [1]. Telehealth services typically involve sets of coordinated activities for achieving a common business objective [2]. Such services are thus naturally workflows that separate various works of a specific process into a group of well-defined steps where each work contains many tasks as different logic steps [3]. The tasks may be executed manually by humans or automatically by applications relevant to the process represented by a workflow.

Access control is one unique security aspect of workflow systems [4]. The policies of security can be explained as rules or constraints on users or groups involved in a workflow system. Such constraints can be expressed with logic-based languages in three categories: static, dynamic, and hybrid, depending on the temporal order of their evaluation in comparison to the initiation of workflow execution or runtime of workflow [5]. The Workflow Authorization Model (WAM) specifies authorizations in such a way that the workflow execution goes in parallel with granting or revoking privilege on users or roles. Synchronizing authorization flows with workflow execution allows WAM to support dynamic constraints to ensure consistency of tasks at run time [6]. Another model for authorization constraint management in workflow systems is to use active rules implemented as triggers corresponding to workflow events in active databases [7].

By employing unique features of human characters, biometrics technologies provide an alternative way over password or digital certificate-based authentication for verifying user identities. A web service has been used for the extraction and verification of biometrics across different organizations [8]. How to integrate biometrics with a PKI system is a growing concern in fields like e-Commerce, e-Banking, and e-Health, whereas it is particularly relevant to telehealth applications. Using biometrics features is a feasible way to establish private keys. However, there also exist potential risks related to biometrics, such as the threat to privacy of individuals [9]. Two-step authentications can be achieved through smart card authentication based on PKI and biometrics measures like fingerprint verification stored in an identical card. A combination of PKI and biometrics is believed as double protection for personal authentication [10].

3. Architecture design

Figure 1 illustrates the proposed architecture for e-Health portals. In our design, the e-Health portal is a web-based application that integrates various medical services provided by multiple hospitals and other medical organizations. An end user, such as a patient or doctor, directs a web browser to the portal server. The portal server displays a webpage, namely, *portal interface* to the user. The portlets inside each portal interface correspond to a collection of correlated services provided by medical organizations. The user may trigger various actions of a service by clicking on corresponding buttons encapsulated in a portlet (real-time applications, such as tele-consultant service, will bypass the portal server due to a more rigid performance constraint).

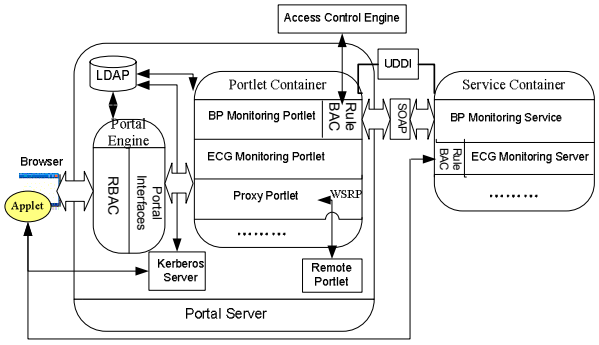

Figure 1. Architecture of e-Health portal

Our design provides a uniform and easy-to-use interface to users by hiding implementation details of services and their providers. It also enables single sign-on (SSO) for backend and remote services. Moreover, the design also simplifies the administration and maintenance of services at medical organizations, because the presentation layer (that is, the portal server) is separated from the implementation layer (that is, medical organizations).

Figure 2 shows the architecture of the telehealth subsystem with a focus on its security. The responsibility of the biometrics server is to provide the doctor's identify information including biometrics features to patients. Behind the portal server are application servers, named E-health server cluster, whose responsibilities are to define and manage workflows, to control and monitor multimedia streams, and to store data in databases. Not shown in the figure, the Certificate Authority (CA) server will issue digital certificate to every hospital and other members of the portal. Since our implementation is completely based on web service, patient's client-end application is

simply a Web browser and Java applet downloaded from the portal server.

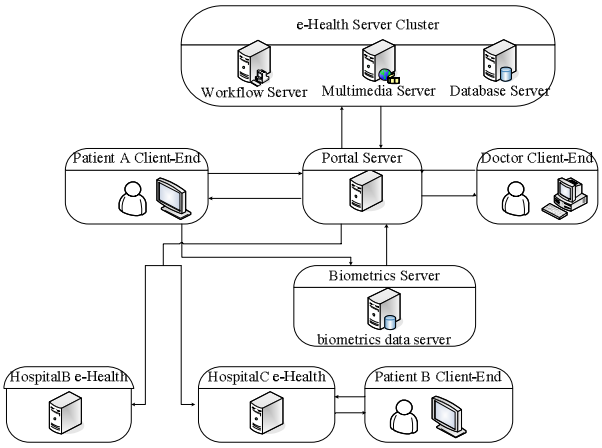

Figure 2. Architecture of telehealth subsystem

4. Trust management

Trust is a challenging issue in telehealth applications due to the lack of a visual contact between users. Our solution integrates PKI infrastructure, biometrics, and visible watermark for establishing sufficient trust.

First, for users of a telehealth application to establish trust in the application running in the Web-based portal, we employ digital certificates and the PKI infrastructure in a standard way. More specifically, each provider of telehealth services holds a digital certificate issued by authorities, which can be trusted by a user's browser through trust chains. It is worth noting that such trust only indicates to the user that he/she is connected to a trusted service from a trusted organization, and the encrypted communication is secured from snooping. While such trust is typically regarded as enough for e-commerce applications, it is insufficient for telehealth services since a patient may still be wondering who is at the other end of the service. We can certainly extrapolate the PKI-based solution to user-level authentication by issuing a digital certificate to each user. This approach, however, may not be feasible in practice due to the implied cost (of issuing and maintaining a large number of certificates) and the fact that many users of a telehealth application may not possess the knowledge or skills required for using PKI. Moreover, unlike a digitally signed document or email, a real-time telehealth service requires continuous authentication. For example, a doctor may present his/her digital certificate at the beginning of a service and then ask someone else to replace him/her. By authenticating the doctor only once when the service begins, the patient will never detect such a change of identity.

Traditional walk-in medical services, such as consultant and diagnosis, are either within a hospital or in a very limited geographic range, so the uniqueness of facial character acts as the best evidence for a doctor's identity. Trust between patient and doctor can be easily established through implicit referrals and can be trivially achieved during face-to-face services. Although the geographical distance in a telehealth application renders direct visual contact between users infeasible, multimedia components of telehealth applications can provide a similar capability. Most telehealth applications have multimedia components for video capturing and transmission. Integrating such components with telehealth services will give patients an opportunity to see the doctor as if during a face-to-face visit to the organization. In the scenario of a tele-consultant, a patient can interact with a doctor via multimedia communication channels with both video and audio. The doctor's real-time video streams provide a constant authentication of his/her identity to the patient.

However, a challenging issue is to establish initial trust when the implicit authority in a physical organization is absent. For example, when a patient visits a hospital, he/she implicitly trusts each person during the whole process from registration to the interview with a doctor. Such trust is reasonably reliable in a physical organization, but it becomes suspicious when the organization only virtually exists at the other end of an Internet connection. For example, the trust established with PKI may allow a patient to believe that the service he/she is accessing is indeed from that medical organization. However, this does not mean that organization and everything on its website can be trusted. In particular, if a picture of the doctor posted on a clinic's website is used to establish initial trust in that doctor, then the patient will have to trust that clinic and its webmaster. Assuming such trust across the Internet for a clinic that only virtually exists is problematic considering abundant real-world examples of online frauds.

We propose to establish initial trust through hierarchies of trust, which is similar to PKI but applied to biometrics features. More specifically, biometrics features, such as facial characters, are provided by each organization for users to establish trust. Such biometric features act as digital certificates in PKI. Similar to chains of certificates in PKI, the biometrics features are certified by the organization that issues them, and the organization is certified by higher authorities, such as state or national medical associations. Like the built-in CAs in a Web browser, the client-side applet of telehealth applications includes a collection of

authorities that are trusted. Upon connecting to a telehealth service provided by an organization, the doctor's biometrics feature is delivered together with a chain of trust whose root is a higher authority. The patient's applet transparently verifies the root against its built-in collection of authorities, and then verifies the chain of trust attempting to establish trust in the biometrics feature. Figure 3 shows an example of such hierarchies of trust for medical organizations. The trust in a doctor's biometrics feature, such as picture, can be established if it is issued by a hospital that is certified by a provincial health organization, which is in turn certified by the national health organization built into the patient's applet. It is worth noting that we do not mean to invent new biometrics techniques but rather to build a PKI-like hierarchy using existing techniques.

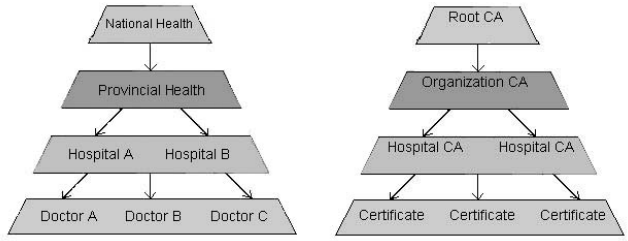

Figure 3.Trust hierarchy in organizations and PKI

A complementary mechanism for increasing trust is to embed visible watermarks (which is different from invisible watermarks used for protecting digital copyright) into biometrics features in the form of an image. For example, if a doctor's picture is used as the biometrics feature, then a higher authority such as the national health organization can assert the validity of this biometric feature by embedding its URLs or seals in the doctor's picture, as shown in Figure 4. The URL embedded in the doctor's picture is a word-form visible watermark indicating the issuer of the picture. The URL allows patients to visit the higher authority's website to verify the validity of the picture. It is worth noting that this mechanism is helpful only when the patient already trusts the authority appearing in the visible watermark. A malicious organization can certainly put up fake pictures embedding a URL that leads to itself or its alliances, and in this case the patient will distrust the picture together with the authority that issues it. This fact proves the needs for hierarchies of trust through authorities that patients initially trust (the counterpart of a root CA) and chains of authorities originating from those trusted ones.

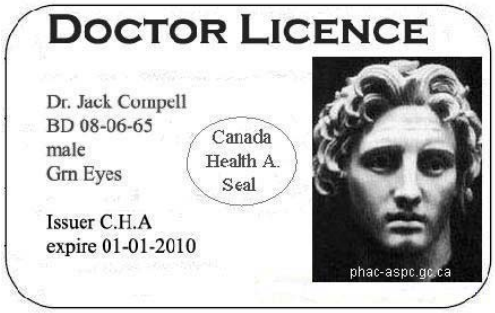

Figure 4. An example of visible watermarks

Similar to revocation of digital certificates, the biometrics features of users are not permanent, either. Biometrics features may change over time so they should have validity duration and will be revoked once they expire. Another issue is to establish trust using a model different from the hierarchical approach of PKI, that is, the web of trust. In traditional organizations, referrals between users such as doctors are a common way for establishing trust. A similar approach is possible in telehealth applications with the help of multimedia components. For example, a patient may be introduced to a new doctor by someone with whom he/she is familiar via a tele-referral service, as depicted in Figure 5.

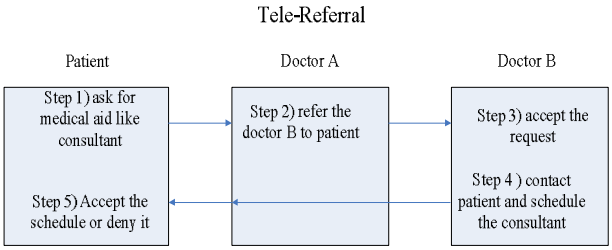

Figure 5. Tele-referral

5. Access control

The basic support for access control is usually a built in feature in the software platforms on which e-health systems are built. For example, the Web-based e-health portal system employs the built-in module of role-based access control (RBAC) in WebLogic, and supplements it with a rule-based module for finer-grained control and conflict resolution [11]. However, such access control mechanisms cannot deal with workflow-based telehealth services that involve a series of interdependent tasks organized as a complex process. Section 5.1 first presents an example of telehealth services, namely, tele-consultant. Section 5.2 represents this workflow as partially ordered conditions and then shows how to enforce such a partial order with the existing rule-based access control engine.

5.1 Example scenario of Tele-Consultant

Figure 6 shows an example scenario of tele-consultant. Suppose a patient needs to consult a doctor for help on treatments. The patient first makes an appointment through a coordinator (who is responsible for organizing and coordinating interactions between doctors and patients). The coordinator checks the patient's record for verifying his eligibility for making such a request. If the patient is registered with the medical organization and has appropriate privileges, the coordinator will send the appointment information to the corresponding doctor who is assigned to the patient. The doctor sets up a schedule for the consulting service and notifies the coordinator who in turn notifies the patient about the schedule. When scheduled time arrives, the coordinator notifies both the patient and doctor to start consulting service. The patient and doctor both need to authenticate to each other before the service starts, using techniques outlined in the previous section (the details are omitted in Figure 6). After the service completes, the doctor notifies the patient with results and recommendations and stores the analyses and diagnoses data to the EPR (Electronic Patient Records) server. The patient can then obtain further treatments according to the suggestion or diagnosis results.

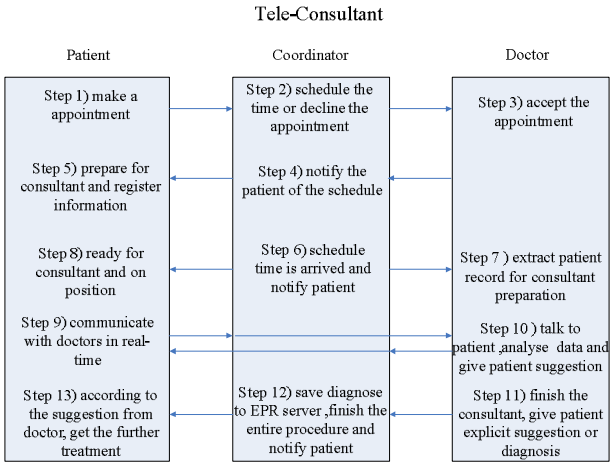

Figure 6. Scenario for tele-consultant

5.2 Enforcing task dependency

In the scenario shown in Figure 6, dependencies between different tasks clearly exist. Table 1 summarizes the tasks and their relationships in terms of pre-conditions. The tasks form a partial order as shown in Figure 7.

Table 1: Task and dependency between tasks

Role	Task	Task	Pre-condition
Patient	P1	Make a appointment	
	P2	Reset, if time conflict	C3
	P3	Talk to doctor real-time	C4
Coordinator	C1	Censor the appointment	P1
	C2	Schedule the time	P1
	C3	Reschedule if conflicting	P1
	C4	Notify others, when time arrive	P1, D1
	C5	Save to EPR server	D3
Doctor	D1	Accept the appointment	P1, C2, C3
	D2	Talk to patient, analysis	C4
	D3	End the consultant	C4

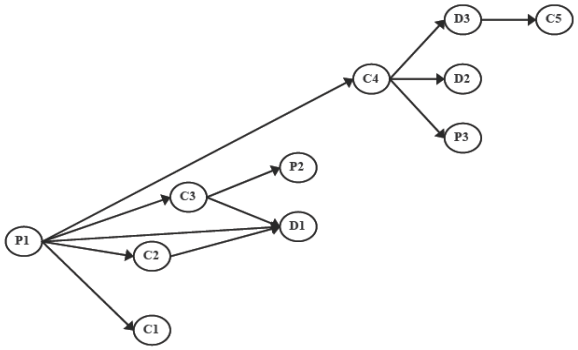

Figure 7. Tasks as partial order

The dependency between tasks should be enforced by access control mechanisms in order to prevent users from either mistakenly or deliberately executing tasks in a wrong order. To enforce the partial order, we leverage the existing rule-based access control engine in the Web-based portal system [11]. This access control engine is based on the classical Flexible Authorization Framework (FAF), which utilizes a logic-based language for authorization derivation, conflict resolution, and other advanced access control features. For our purpose, the *done* rule is sufficient for enforcing the partial order between different tasks. Each done rule specifies a past event, which can be a precondition of one or more other tasks. In Figure 7, the preconditions of the task D1 can be expressed as below:

cando(o, p, +make_apt) ← in (p, patient), typeof(o, appointment)

do(o, p, + make_ apt) ← cando(o, p, + make_ apt)

do(o, p, - make_ apt) ← ¬ do(o, p, + make_ apt)

Those rules mean only a patient, as indicated by the predicate *in (p, patient)*, can make an appointment.

cando(o, c, +schedule_apt) ← done(o, p, + make_apt), in (c, coordinator), in(p, patient), typeof(o, appointment)

do(o, c, + schedule_apt) ← cando(o, c, + schedule_apt)

do(o, c, - schedule_apt)←¬do (o, c, + schedule_apt)

Those rules indicate that only after the patient has made an appointment can a coordinator schedule a time for the appointment. The predicate of *typeof(o, appointment)* indicates object o to be an appointment.

cando(o, c, +reschedule_apt) ← done(o, p, + make_apt), in (s', coordinator), in(p, patient), typeof(o, appointment)

do(o,c,+reschedule_apt)←cando(o,c,+ reschedule_apt)

do(o,c,- reschedule_apt)←¬do (o,c, +reschedule_apt)

Those rules indicate that only after the patient has made an appointment can a coordinator give the patient another amendable time for the appointment. The predicate *done(o, p, + make_apt)* indicates the patient *p* had already made an appointment.

cando(o, d, +accept) ← done (consultant, c, +schedule), done (consultant, c, +re-schedule), done (appointment, p, +make), in (c, coordinator) ,in (p, patient), in (d, doctor), typeof(o, appointment)

do(o,d,+ accept)←cando(o,d, + accept)

do(o,d,- accept)←¬do (o,d, + accept)

The expression indicate that a doctor can only execute the accepting appointment task if a patient has already made that appointment via the coordinator, and the coordinator has sent over a schedule for the appointment. In this case, a task has more than one pre-condition.

6. Implementation

We have implemented a prototype based on the proposed techniques. We use OpenLDAP server to store self-signed X.509 digital certificates for health organizations. The Doctors' pictures are certified by a fictitious higher authority. When the patient's browser connects to the Web-based e-Health portal, it will download a Java applet that will handle all client-side operations, such as verifying the doctor's picture through a chain of trust. For tele-consulting services, we have implemented a video/audio application based on the RTP (Real time protocol) and the Java Media Framework (JMF), which can capture, transfer, save, and playback video and audio streams. We will integrate this application in the tele-consultant workflow based on the SIP (Session Initiation Protocol) and SIP Servlet. The Web-based e-health portal has been implemented based on WebLogic. We complement the existing RBAC capability with a rule-based access control engine implemented on top of SICStus Prolog. The rules are stored in databases and extracted through an interface written in C into Prolog.

7. Conclusion

We have studied two security issues of telehealth applications in the context of a Web-based e-health portal. First, for establishing trust in the lack of visual contacts, we proposed a PKI-like hierarchical approach to provide users with additional trust established through biometrics techniques. The established trust can be verified during a telehealth service using multimedia components. Second, for telehealth services that involve workflow-like complex processes, we proposed a method for representing the dependency between tasks as partial orders, and then enforcing such partial orders using logic rules. This approach was cost-efficient since it reused the existing rule-based access control engine in the Web-based e-Health portal.

8. REFERENCES

[1] A.C. Norris, "Essentials of Telemedicine and Telecare," ISBN 0-471-53151-0, John Wiley & Sons, West Sussex, England, 2002

[2] *Workflow Management Coalition (WfMC)*, Workflow Security Considerations – White Paper, Document Number WFMC-TC-1019, Document Status-Issue 1.0

[3] Rohit Valia and Yahya AI-Salqan, "Secure Workflow Environment". *Proceedings of the 6th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises*, June 18-20 1997

[4] Vijar Atluri, *Security for Workflow systems*, Information Security Technical Report, 2001

[5] Elisa Bertino, Elena Ferrari and Vijar Atluri, "The specification and enforcement of Authorization constraints in workflow management systems", *ACM Transactions on Information and System Security (TISSEC)*, Volume 2, Issue 1, Page 65 - 104, ISSN:1094-9224, 1999

[6] Vijayalakshmi Atluri and Wei-Kuang Huang, "An Authorization Model for Workflow", *Proceedings of the 4th European Symposium on Research in Computer Security: Computer Security,* Pages 44 – 64*,* 1996

[7] Rabio Casati, Silvana Castano and MariaGrazia Fugini, "Managing Workflow Authorization Constraints through Active Database Technology", *Journal of Information Systems Frontiers,* 2002

[8] Andrew Joseph Marshall, *A Comparative Study of Biometrics and Their Application In A Web Based Healthcare Environment*, Technical Report, 2004

[9] Mark Gasson, Martin Meints and Kevin Warwick, *A study on PKI and biometrics*, the FIDIS NoE Technical Report, 2005

[10] Youchi Seto, "Development of Personal Authentication System using Fingerprint with Smart card and Digital signature technologies", *Proceedings of the 34th Annual Hawaii International Conference on System Sciences,* ISBN: 0-7695-0981-9, 2001

[11] Shuo Lu, Yuan Hong, Qian Liu, Lingyu Wang, Rachida Dssouli, "Access Control in e-Health Portal Systems," *Proc. 4th International Conference on Innovations in Information Technology (Innovations'07)*, IEEE Press