Federated, Secure Trust Networks for Distributed Healthcare IT Services

Alfred C. Weaver, Professor of Computer Science, weaver@virginia.edu
Samuel J. Dwyer, Professor of Radiology, dwyer@virginia.edu
University of Virginia

I. Goals

- Develop a GXA web services testbed that implements the security framework needed to support a distributed, trusted, secure healthcare IT system
- Implement a medical data portal that provides multi-device access to a medical record repository, medical image database, procedure scheduling, and an external (off-network) pharmacy
- Evaluate Microsoft security software solutions (Passport.NET, TrustBridge, Palladium) in our medical applications testbed
- Contribute to GXA specifications development, analyze the complex security interactions of a distributed, federated healthcare system, and examine generalizations of these systems
- Report lessons learned and provide system demonstrations at Faculty Summit 2003 and 2004

II. High Impact

Today's healthcare computer systems rely upon a disparate collection of legacy services, developed separately and independently for patient records, radiological images, scheduling, billing, and administration. Recent federal laws and healthcare trends have prompted industry-wide efforts to integrate these distributed systems securely, thereby increasing operating efficiency, workflow, and the quality of patient-centered care. Effective in 2003, the federal Health Insurance Portability and Accountability Act (HIPAA) subjects all medical data to stringent privacy and security regulations. Encryption services will be needed for the storage and transmission of patient information; authentication services will be needed to verify the identity of those who access healthcare records; authorization services will be needed to programmatically determine what data rights are granted to which individuals and IT subsystems.

The design of a distributed, federated security system for healthcare is a complex issue. Legitimate access to healthcare web portals and web services will occur from a variety of devices (desktops, laptops, Pocket PC, Tablet PC, cell phones) and the authentication service must handle multiple identification technologies (passwords, fingerprints, iris scans). The authorization rules must be programmable to respond to dynamic situations, and requires a rule engine that can implement context-dependent authorization based upon identity and the data requirements of the requested task. SOAP WS-Security and other GXA security implementations (including platform security for mobile devices using Windows CE .NET) must act in concert to enable a federated trust network across these disparate devices, individuals, and processes. Furthermore, to overcome the deficiencies of the existing patchwork system of healthcare systems, the entire medical IT enterprise needs to be accessed through a single portal that adapts itself to the needs of the doctor, technician, or patient who is engaged in authorized access.

III. Federated, Secure Trust Networks Based upon Microsoft's Global Web Service Architecture

Microsoft .NET XML web services offer a promising framework for developing next-generation distributed healthcare solutions that simultaneously fulfill HIPAA requirements and meet industry objectives. The GXA architecture provides a starting point for addressing multi-device access, multiple identification strategies, multi-level authorization, high-performance encryption, and the interplay among web services located both within and without the medical infrastructure.

Issues:

1. Today's healthcare IT infrastructure is fragmented. Doctors typically use a Hospital Information System (HIS) to view patient data; radiologists use a Radiological Information System (RIS) to store and retrieve diagnostic images; administrative staff use PCs for scheduling and billing. Although these systems are physically distinct, they need to be logically integrated to avoid lost data, improve workflow, enhance patient satisfaction, and reduce cost.
2. Today's medical professional uses multiple devices to access and record data. EKGs can be read on a Pocket PC. Tablet PCs can be used to capture hard-written case notes, and then transcribe them into the medical record. Prescriptions can be dictated on a cell phone, and voice recognition software can update the patient record and electronically transmit a prescription to a pharmacy.

3. Reliable authentication is essential. Biometric devices (e.g., fingerprint and iris scanners), smartcards, ID badges with radio transmitters, and similar techniques will be needed to achieve the level of privacy and security demanded by HIPAA. The authentication service of our federated security system, building upon Passport.NET, must be capable of working with multiple identification technologies.
4. Authorization rules must be dynamic and context-dependent. Staff come and go and get reassigned; their authorization privileges change as a result. A request to alter a medical record might be subjected to differing levels of trust depending upon whether it came from inside the hospital or from an external mobile device. Requests for data access come from programs as well as humans. To handle this complexity, we need a programmable rule engine that uses policies to determine what data accesses are permitted and under what circumstances, all following WS-Policy and other GXA security specifications.
5. Digital communications must be secured. All network transmissions and data storage must be encrypted if they are to be protected.
6. Encryption must be high performance. A typical MRI examination contains a thousand individual images. If each image is encrypted/decrypted each time it is stored or retrieved or transmitted, then a slow encryption service will have a dramatic negative impact on the workflow of the radiologist. Our medical center conducts 300,000 examinations and generates 9 TB of data annually, so high-performance encryption is an essential component of a realistic data service. There are performance concerns with SOAP communications when the data objects are this large. WS-Attachments may offer guidance on this issue.
7. External interfaces are required. The healthcare IT infrastructure must extend beyond the medical center into the real world of external participants, e.g., pharmacies and insurance companies.

IV. Fluency

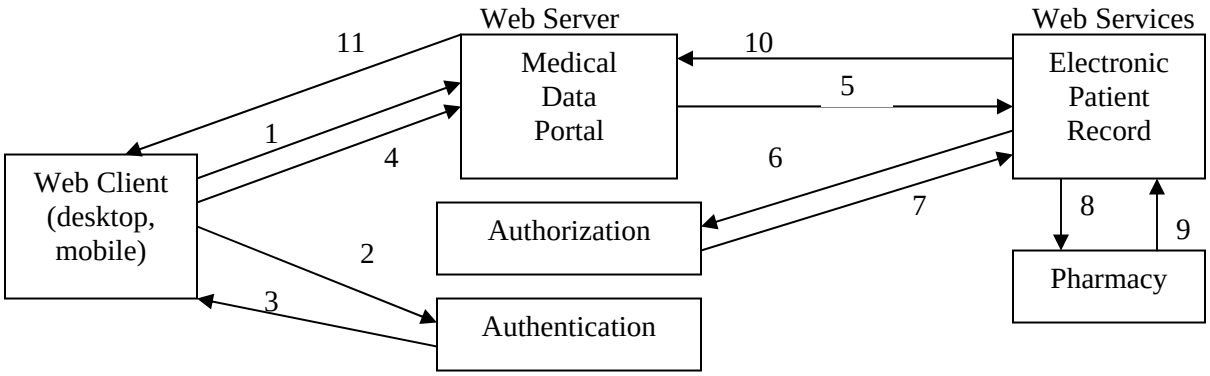
UVA's Department of Computer Science has enjoyed an established research relationship with the UVA Medical Center, the Department of Radiology, and the Office of Telemedicine since 1995. We have collaborated on the evaluation of compression algorithms to be used in telemedicine, the development of a telesonography (digital ultrasound) capability now in commercial use, and the creation of workflow models for an academic radiology department. Dr. Samuel J. Dwyer, Professor of Radiology, is a leading authority on telemedicine, teleradiology, and HIPAA requirements, and has agreed to be our medical partner in this project.

Utilizing previous Microsoft gifts, UVA CS has already developed a small-scale network running .NET and we have conducted some initial capability and performance studies on authentication, authorization, and encryption. We are confident that our faculty, students, and staff can enlarge the existing testbed to encompass the variety of issues soon to be encountered in protecting medical data. A closer collaboration with Microsoft will give our results legitimacy and promote industry acceptance.

V. Research Agenda

1. Acquire three high-performance PCs, two Pocket PCs, and two Tablet PCs (all running .NET); acquire fingerprint, iris scan, and active ID badge identification hardware.
2. Develop a central authentication service that utilizes passwords, fingerprints, iris scans, and RF tags to identify individuals by customizing Passport.NET for healthcare applications.
3. Develop an authorization service that works with the authentication service to associate data privileges (read, append, change) with personal identity and with data record types (patient records, diagnostic images, lab test results, data access logs). Authorization will use a programmable rule engine that implements multi-level access.
4. Ensure that all web services are capable of forming, maintaining, and sharing federated trust relationships.
5. Implement secure SOAP communications following WS-Security specifications.
6. Develop these .NET services: (a) patient medical record repository; (b) medical image database; (c) medical procedure scheduling; and (d) external pharmacy interface, including electronic prescription transmission.
7. Share with Microsoft the lessons learned in designing and implementing such a complex, dynamic security system based upon GXA services, and contribute to the development of WS-Authentication, Authorization, Policy, Security, Trust, and Secure Communications service definitions.
8. Provide system demonstrations at Faculty Summit 2003 and 2004.

VI. Example Service Interactions



A doctor using a mobile phone or PDA needs to order a new prescription for her patient; she makes her first entry of the day into the medical portal [1]. The portal requires authentication and redirects the client to the authentication service [2]. Authentication identifies the doctor and issues a security token to the client [3] who again contacts the portal [4], this time with the security token. (Alternatively, the portal could have contacted authentication directly on behalf of the client.) The portal processes the prescription request and attempts to write to the patient's medical record [5], but needs authorization to do so. This request is relayed to authorization [6], which uses a rule engine to determine if this access by this person (or web service) is authorized; it is, so authorization is granted [7]. The electronic patient record is updated with the new prescription data and the prescription is forwarded via secure transmission to an off-network pharmacy [8]. This pharmacy has already established a trust relationship with the hospital, and thus can share the trust relationships established by the hospital IT systems with its staff and web services. The pharmacy confirms [9] receipt of the prescription. The receipt is logged in the medical record and reported to the portal [10], which alerts the doctor [11] that the prescription has been received by the pharmacy.

VII. Participants

Dr. Alfred C. Weaver, Lucian Carr III Professor of Computer Science, U.Va., www.cs.virginia.edu/~acw and intercom.virginia.edu/people.html
Dr. Samuel J. Dwyer, Professor of Radiology, U.Va., www.healthsphere.org/Board_Bios/SamD-Bio.htm
Three graduate students, led by Andrew M. Snyder (www.cs.virginia.edu/~ams6x), who will use this topic for their master's theses
Three undergraduate students, led by James Van Dyke (intercom.virginia.edu/people.html), who will use this topic for their senior theses

VIII. Value, Deployment, and Dissemination

The HIPAA privacy and security regulations take effect in 2003, and significant penalties are associated with security breaches. As a classic unfunded mandate, hospitals and healthcare practitioners must adhere to HIPAA, although no federal funds are provided for its implementation; thus the solution must come from the commercial sector. The .NET framework with GXA services is the most promising candidate architecture available for building the federated trust networks that HIPAA will require.

In phase one (Nov. 2002-Sept. 2003) we will implement the research agenda above on our testbed physically located in Computer Science. In phase two (Oct. 2003-Nov. 2004) we will migrate our code into the medical center as a demonstration project of how to satisfy HIPAA using .NET and GXA.

All code developed in our testbed will be open source, maintained on our website, and freely and openly disseminated to other institutions for testing, improvement, and expansion. We will act as a clearinghouse and distribution center for medical .NET services.

IX. Budget

Hardware: three high-end workstations; two Pocket PCs; two Tablet PCs; biometric identification hardware
Software: all .NET components
Support: $200,000 over two years; includes all eight personnel above working during two academic years and two summers; includes travel to provide demos at Faculty Summit 2003 and 2004