Event-Based Data Control in Healthcare

Jatinder Singh and Jean Bacon
Computer Laboratory
University of Cambridge
{firstname.lastname}@cl.cam.ac.uk

ABSTRACT

Health services require appropriate information to provide proper care. At the same time, health information is sensitive, and thus its dissemination must be controlled. Health environments are becoming increasingly data driven, and thus are well supported by an event-based infrastructure.

We outline our work in building data control mechanisms into publish/subscribe middleware, to give those responsible for health data fine-grained control over the circumstances for its transmission.

Categories and Subject Descriptors

C.2.4 [**Computer-Communication Networks**]: Distributed Systems; H.3.4 [**Information Storage and Retrieval**]: Systems and Software

General Terms

Security, Management

Keywords

Data Control, Healthcare, Middleware, Publish/Subscribe

1. HEALTHCARE DIRECTIONS

Health services are typically reactive, dealing with *acute* (sudden, severe) episodes as they occur. Given the ageing population, such a care model is unsustainable. Therefore, there is a global push to reform health services, to improve the quality of care while reducing the burden on resources.

The movement is towards preventative care, through intermediate/telecare services that involve caring for patients outside of traditional care institutions (e.g. hospitals). That is, providing care services closer to the home. Less time in institutions improves the patient's quality of life, while reducing health expenditure. The goal is to better manage *chronic* (ongoing) conditions, in an attempt to lower the frequency and severity of costly acute episodes.

Technology is central to a remote care environment. Sensors provide monitoring capabilities to measure aspects of physiological and environmental state. Communications infrastructure must inform parties of incidents as they occur in this highly data-driven environment.

2. HEALTH INFORMATION

Healthcare providers require information to perform their tasks. However, personal health data is highly sensitive and thus must be controlled. Those who collect/hold data as part of the care process are responsible, through legislation and codes of practice, for maintaining its confidentiality.

The health space consists of many administrative domains, with varying degrees of autonomy, providing a range of care services. As such, the information requirements and sharing policies of each domain often differ.

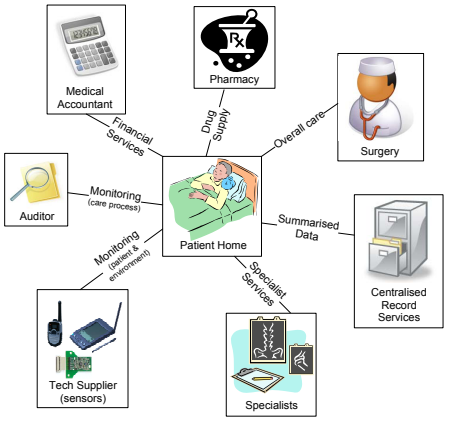

Figure 1: Healthcare is highly collaborative, involving interactions between professionals and service providers, often across administrative boundaries.

To meet their data management responsibilities, service providers must share information *appropriately*. This involves considering patient consent, general administrative policy and other aspects of context, such as the recipients (is this doctor treating this patient?) and environmental state (is this an emergency situation?).

3. EVENT-BASED MIDDLEWARE

An *event* is a data-rich encapsulation of a particular semantic. Middleware provides a layer of indirection between applications (users) and the network infrastructure. Event-based middleware serves to notify principals of relevant events as they occur within the system.

Federated environments, especially those of telecare, are highly data-driven. We use event-based middleware to effect communication while controlling data transmission in

accordance with disclosure policy.

3.1 Publish/Subscribe

Publish/subscribe is an asynchronous messaging paradigm, where a client (principal) takes the role of a publisher and/or a subscriber. Publishers produce events; subscribers register their interest in receiving particular events through a subscription, which may be optionally qualified by a filter. Clients communicate through brokers. Brokers provide the middleware functionality, cooperating to route published event instances to the relevant (interested) subscribers.

The decoupling of producers and consumers assists in supporting system scalability. Further, clients are not burdened with source/sink specifics. As all communication passes through the publish/subscribe middleware, it is an appropriate point for the enforcement of information control policies.

4. INTERACTION CONTROL

Interaction control [**?**] allows the data released by a broker to be customised to the current circumstances. Control is effected through context-aware policy rules enforced by middleware brokers [**?**]. Such rules allow the administrative domain controlling the broker to set the circumstances in which it is appropriate to transmit particular information; that is, they are able to release data on a *need-to-know* basis.

There are two categories of interaction control rules:

Restriction rules:

a) Subscription authorisation rules control who may subscribe to particular information.

b) Imposed conditions restrict particular event instances from being delivered to a particular subscriber.

Event transformation rules convert an event instance into another. A transformation function changes the attribute values and/or type of an event to enrich, degrade, perturb or create some other, loosely-related instance. This provides more than binary access control, allowing data to be tailored to circumstance. For example, a prescribe event may be converted to a prescription, by removing certain details; or, for reasons of privacy, data from body sensors can be summarised/fuzzified except in emergency situations.

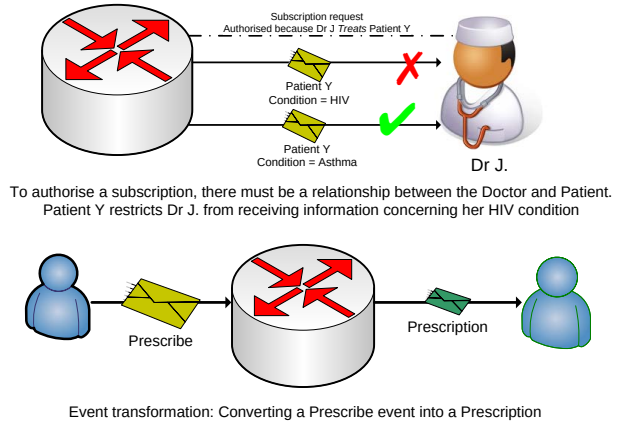

Figure 2: An illustration of data control rules.

4.1 Context

To meet their data management responsibilities, service providers require fine-grained control over the data they transmit. As such, context is crucial. Interaction control rules are context-aware, referencing:

1) Messaging information — e.g. event content, timestamps.

2) Credentials of the principals — e.g. job-role, employer.

3) Environmental state — e.g. emergency, carer present.

4) Stored data, external services, etc.

We have built publish/subscribe middleware functionality into the PostgreSQL database management system [**?**]. This allows a database instance to function as a broker: routing messages, storing data and enforcing interaction control policies. This coupling brings a common interface for managing data storage and transmission; and also provides data control rules access to a rich representation of context.

5. SCENARIO — DRUG CONTROL

A nurse, when visiting a patient in their home, may prescribe a drug. The managing doctor must be notified of this, as it may indicate a complication. The pharmacy service requires information in the form of a prescription in order to dispense a drug; however a prescription should not include details of the reasons (notes/observations). The auditor requires notification when certain drugs are prescribed. As this audit is prescriber focused, the auditor does not (generally) receive any patient details. The surgery defines a combination of restriction and transformation rules on `Prescribe` events to release information to providers on a *need to know* basis.

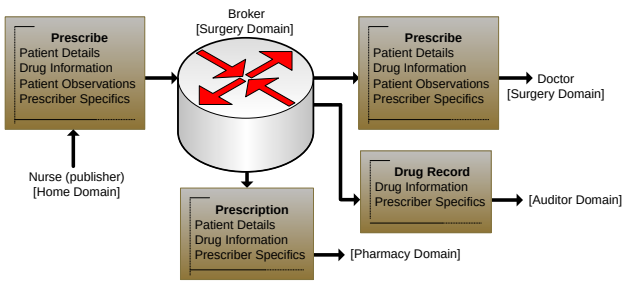

Figure 3: While a single event is relevant to multiple providers, each receives only the information appropriate to their role in the care process.

6. APPLICATION TO HEALTHCARE

As care models move towards a preventative care paradigm, health provisioning is becoming increasingly data-driven. Event-based middleware provides a suitable supporting infrastructure, facilitating interoperability between systems and administrative domains.

Data control policies are defined and enforced within the network infrastructure. This ensures policy adherence. Clients also benefit from this indirection, as they need not be concerned with data management details—leaving source/sink specifics and data control policy management to the middleware. Policy definitions are simplified, while fewer enforcement points reduce the risk of error. Policy changes are modelled as events, which allows automatic and immediate updates through the existing event-based infrastructure.

This approach facilitates information governance in an environment of federated administrative control. Those responsible for health information are given fine-grained control over the circumstances for data disclosure. Auditing mechanisms not only record the data transmitted, but the rules and circumstances that authorised the disclosure. This

improves accountability, promoting the safe-handling of sensitive health information.

7. REFERENCES

[1] J. Bacon, D. M. Eyers, J. Singh, and P. R. Pietzuch. Access Control in Publish/Subscribe Systems. In *Distributed Event Based Systems*, pages 23–34, 2008.

[2] J. Singh, L. Vargas, J. Bacon, and K. Moody. Policy-based information sharing in publish/subscribe middleware. In *POLICY*, pages 137–144, 2008.

[3] L. Vargas, J. Bacon, and K. Moody. Event-Driven Database Information Sharing. In *British National Conference on Databases*, pages 113–125, 2008.