Context-aware disclosure of health sensor data

Jatinder Singh* Pedro Brandão*† and Jean Bacon*
* Computer Laboratory, University of Cambridge
Firstname.Lastname@cl.cam.ac.uk
† Comput. Science Dept., Univ. of Porto and Instituto de Telecomunicações
pbrandao@dcc.fc.up.pt

***Abstract*—Healthcare processes are driven by sensitive information. Access control technologies aimed at protecting health information tend to focus on patient records. However, it is also important to control access to live data streams, such as those from sensor devices—especially as healthcare becomes increasingly pervasive. As opposed to bespoke, scenario-specific access control regimes, the middleware enforcement of access policy enables application- and device-independent information governance. This paper illustrates how a data control middleware can regulate sensor data flows, controlling the information disclosed in accordance with circumstance.**

I. Introduction

As the population ages, there is a world-wide push to better manage health services. The movement is towards *preventative care*; ongoing care to limit the occurrence and severity of health incidents. Sensor technologies are integral to future care services [1], providing detailed information of a patient's physiological and environmental state. Such information enables alerts in situations of concern, is useful for treatment and early diagnoses, and empowers patients to engage in self-care [2]. This improves a patient's quality of life, increasing independence and lowering the time spent in institutions (e.g. hospitals), while reducing the burden on health resources.

Healthcare is highly collaborative. Care practitioners often share information to provide treatment [3]. However, health information is inherently sensitive. Those providing care services are responsible for protecting the confidentiality of the information they deal with as part of the care process. Information is best shared on a *need-to-know* basis [4]. While consent is the primary driver, there are situations where patient information may be shared without explicit consent [5]. Patients generally trust health professionals to act appropriately with their information. Care providers define *information sharing protocols* [5], detailing the situations in which particular information is shared. It follows that the appropriateness of sharing information depends on the circumstances.

Technical infrastructure supporting healthcare must enable those responsible for information to meet their data management obligations. In healthcare, access controls tend to consider health records; however, mechanisms are required for managing *information flows*—to control the dissemination and disclosure of 'live' data. In this paper we demonstrate, through an example implementation, how a context-sensitive middleware can be used to provide fine-grained control over sensor information, both in terms of the access to the stream and the information delivered.

PERVASIVEHEALTH 2010, March 22-25, Munchen, Germany

DOI 10.4108/ICST.PERVASIVEHEALTH2010.8788

II. Event-Based Middleware

Healthcare is a data-driven environment. Health processes react and respond to incidents, be they observations, diagnoses, results or treatments. As incidents reflect information, they must be communicated to the relevant care (and related) service providers.

Such an environment is amenable to an *event-based middleware* [6]. An *event* is a data-rich occurrence encapsulating information of a particular semantic. We use events to represent health incidents, including readings, observations and alerts. The role of an event-based middleware is to serve as a layer of indirection between applications and the network, to manage the distribution of events *as they occur:* from producers, applications that generate information; to consumers, applications that receive and process such information. All communication occurs through the middleware.

Publish/subscribe (pub/sub) is an asynchronous, many-to-many, push-based communication paradigm suited to scalable event dissemination [7]. The paradigm takes an *information-centric* approach to communication, where *brokers* interconnect and co-operate with other brokers to provide the middleware functionality. A *client* (software component, typically user driven) acts as an event *publisher* (producer) and/or *subscriber* (consumer), connecting to a broker to communicate. In type-based pub/sub, subscribers register their interest with a broker in receiving particular events (e.g. a `sensor_reading`), optionally qualified by a content-based filter (e.g. `temp > 40.5`). Publishers produce events independently of subscribers, where the middleware is responsible for routing the events to consumers with matching interests.

Such an approach is appropriate for highly-collaborative environments such as healthcare. A health incident is often relevant to a number of parties, perhaps in different administrative domains; information-centric delivery avoids burdening clients with maintaining the addressing details of every potential information source/sink. Push-based communication is important not only to alert those providing health services, but to ensure that they operate with the latest representation of state.

III. Middleware Access Control

Middleware is an appropriate point for the enforcement of disclosure policy. As all communication occurs through middleware infrastructure, client compliance with policy is ensured. Healthcare is a large-scale environment where many

users operate with a degree of autonomy; therefore it is impractical, if not dangerous, for each client application to deal with all access control specifics. The enforcement of policy by middleware, in addition to ensuring the consistent application of policy against clients, simplifies policy management with fewer definition and enforcement points.

A. Interaction Control

Interaction Control (IC) [8], [9] enables control over a pub/sub service. IC introduces the following types of context-aware policy rules into brokers to control event dissemination:

- **Request Authorisation Rules:** Authorise the establishment of *event channels*, through which individual events flow. These rules control access to particular types of information.
- **Imposed Condition Rules:** Impose conditional (contextual) filters on an event channel to restrict certain events from propagating through it.
- **Transformation Rules:** Alter the content/type of an event instance as it moves through an event channel. Transformations enable more than binary access control (permit/deny) decisions, as information can be customised as appropriate to the circumstances.

Health incidents must be communicated to the appropriate clients, and often stored and audited [10]. IC integrates control mechanisms into brokers consisting of database systems providing pub/sub functionality [11]. A coupled pub/sub-database infrastructure is more efficient than separate storage and messaging substrates [12]. From a data control perspective, such an integration enables fine-grained, context aware policy rules; as rules have access to a rich representation of state: anything accessible from the database system. This is important in healthcare as the appropriate level of access is circumstantial, e.g. restrictions may be relaxed in an emergency situation.

IV. Remote Monitoring Scenario

Pervasive healthcare involves the use of sensor technologies to measure physiological and environmental state. This data provides care staff, who may not be physically present, with insight as to a patient's well-being [13], and can indicate situations of concern. Such information enables carers to respond appropriately to the patient's situation.

We consider a scenario where patients are monitored, measuring several aspects of their physiological state, and recording their present location. This information is published to a broker, which forwards the events to the relevant connected clients and records data for subsequent query/analysis. Carers may subscribe to the event streams of their patients, to obtain information of a patient's current state of health and to be alerted of situations of concern.

This scenario concerns the propagation of patient information, captured by sensors, to subscribers as appropriate to the circumstances. In the general case, summary information is transmitted at regular intervals. When a patient is in a (perceived) emergency situation, access controls are relaxed to allow subscriptions to raw sensor streams, and restrictions on location information are removed. This provides more detailed information to assist in emergency response. We present this scenario as a practical demonstration of how context-sensitive access policies can control information flows according to changes in context.

A. Sensor Technology and Events

Our implementation uses the Equivital sensor module [14], which provides the Electro-CardioGram (ECG), respiration details, heart and breathing rate, skin temperature, acceleration and orientation of the wearer. Using proprietary algorithms, the device can provide a general assessment of the patient's physiological status. The device transmits information at regular intervals, or in some cases, on a change in value.

We developed a *sensor adaptor* layer that interfaces with the device to manage the data it provides. These data flows are then converted into events that are sent (published) to the (pub/sub) broker. Table I summarises the events produced by the adaptor from the underlying data streams. As shown, the `movement` event is based on orientation (prone, upright, etc.) and the indication of movement (stationary, moving). The event also encapsulates location information, which is at room-level granularity for the patient's home, recorded through indoor positioning sensors, and also globally via a GPS receiver. Location data was simulated in our implementation, though such technology is available (e.g. [15]). A `sensor_snapshot` event consists of heart rate, respiration rate and temperature measurements. A buffer of 16 ECG values is sent in an `ecg_reading` event. As mentioned, the device's algorithms include an indication of perceived warnings, propagated in `status` events.

Table I also presents the event types used in this scenario, and the infrastructure that creates them. The `vitalsigns` event is generated by the broker *transforming* (see next section) a received `sensor_snapshot` event. The `panic` event is published on the press of a *panic* button. As described, the other events are generated by the *sensor adaptor* using data from the sensor module.

B. Patient Status—Emergencies

To enable appropriate responses, a patient's state—whether normal or in an emergency—will be relevant to a number of clients. From an information governance perspective, data concerning a patient in an emergency situation may be less tightly controlled, providing more information to assist emergency response. Given that brokers enforce disclosure rules, they must be able to determine the current state of a patient. Here, the emergency state of the patient is maintained by the broker itself.[1]

In this scenario, there are two ways in which a patient's emergency state is set. The first is through the sensor middleware publishing a `status` event, warning that a measurement lies outside of the (safe) range defined for the

[1] In some circumstances, certain contextual conditions may be represented in external services rather than individual brokers. An example is a nationwide service recording the relationships between carers and patients [16].

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2010.8788
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2010.8788

TABLE I
EVENTS ENCAPSULATING SENSOR DATA.

Sensor Data Type	Event Produced	Publication Rate	Producer	Description
Orientation	movement	on change or every 5s	Sensor Adaptor	Informs of the detection of a change in patient state concerning movement, orientation or location. Events are delivered on a change in state, or every 5secs if no change is detected. Publication rate is approx. 1 event per second in situations of constant change.
Movement				
Location			(simulated location)	
Heart Rate[a]	sensor_snapshot	every 2s[a]	Sensor Adaptor	A periodic event providing a snapshot of the patient's current physiological state.
Respiration Rate[a]				
Skin Temperature				
ECG values	ecg_reading	every 62.5ms	Sensor Adaptor	This encapsulates the live ECG stream. An event containing a buffer of 16 ECG readings. Timestamps account for messaging delays.
Respiration Warning	status	on change or every 15s	Sensor Adaptor	Records patient status. Indicates the start/cessation of perceived emergencies, where readings exceed a safe threshold. This event affects the emergency state representation. If after 15s there is no change in status, a heartbeat (Status OK) message is sent.
ECG Warning				
EDR Warning				
Apnea Warning				
n/a	panic	on press	Panic Button	Alerts of a patient-issued emergency situation.
(various)	vitalsigns	on sensor_snapshot	Broker	A combination (mashup) of sensor data, aggregating the last received snapshot, movement and status data for the patient, executed through a transformation function.

[a] The device transmits a 60s rolling average of the rates every 15s. However, these can also be calculated directly from the ECG stream for a higher sampling frequency.

patient. The second is through the patient raising a `panic` event by pressing the panic button. The emergency status can be reset (to normal) directly through a (carer-driven) application acknowledging that the emergency situation has been rectified. If the emergency state was set as a result of some sensor readings, it may also be reset if the sensor device detects the emergency as averted. Again this occurs through an appropriate `status` event.

V. DATA CONTROL

As described, the sensor adaptor publishes events to the broker that manages the patient. The broker stores such data to enable subsequent query and analysis, and for auditing and accountability purposes [17]. Carers require current patient information, and thus subscribe to (some or all of) the events presented in Table I. The broker is responsible for distributing information to those interested, while enforcing the access control rules as appropriate to the particular circumstances.

Fig. 1 presents the rule definitions to effect the data flow restrictions for this scenario.

Carers can generally subscribe to `vitalsigns` events, which provide a summary of the patient's current state; and `status` events, which inform of perceived emergency situations. As shown in Figs. 1(a) and 1(b), subscriptions are only authorised if the subscriber has a treating relationship with the patient whose data they request. *Permission attributes* force a subscription request to include additional information; in this case, the ID of the patient that the subscriber is interested in. This is used to determine the necessary relationship. A *monitored condition* is one that must continue to be true for the event channel to remain active.[2] Here, the condition representing the treating relationship is monitored to ensure that an event channel is closed should the relationship cease.

In situations where the panic button is pressed, or readings fall outside particular ranges, the event infrastructure is used to alert the relevant parties of potential emergencies through `status` events.

[2]Monitored conditions are only relevant to authorisation rules, as event channels are durative—persisting over time. Transformations and imposed condition predicates are evaluated in the context of each event instance.

```
<request_authorisation>
        <rule_name>ecgsub</rule_name>
        <event_type>ecg_reading</event_type>
        <request_type>s</request_type>
        <credentials>NHSCred(usernm,'doctor')</credentials>
        <permission_attributes>patient_id:int8</permission_attributes>
        <mon_conditions>treatsPatient(usernm, att.patient_id)</mon_conditions>
        <conditions>emergency(att.patient_id)</condition>
        <notes>A doctor can subscribe to their patient's ECG Stream
                in an emergency</notes>
</request_authorisation>
```

(a) `ecg_reading` **authorisation** rule. The rule is similar for the `movement` event type.

```
<request_authorisation>
        <rule_name>vitalsignssub</rule_name>
        <event_type>vitalsigns</event_type>
        <request_type>s</request_type>
        <credentials>NHSCred(usernm,'doctor')</credentials>
        <permission_attributes>patient_id:int8</permission_attributes>
        <mon_conditions>treatsPatient(usernm, att.patient_id)</mon_conditions>
        <notes>A doctor must treat the patient to subscribe</notes>
</request_authorisation>
```

(b) `vitalsigns` **authorisation** rule. The rule is similar for the `status` event type.

```
<transformation>
        <rule_name>perturbvitalsigns</rule_name>
        <event_type>vitalsigns</event_type>
        <output_event>vitalsigns</output_event>
        <stage>n</stage>
        <consumable>t</consumable>
        <function>removesensitivedata</function>
        <conditions>not emergency(vitalsigns.patient_id)</conditions>
        <notes>Perturb location details in non-emergency situations</notes>
</transformation>
```

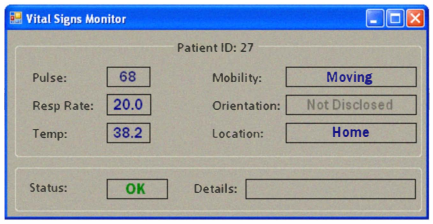
(c) `vitalsigns` **transformation** rule for perturbing the location.

Fig. 1. IC rules for the sensor scenario.

As mentioned, a perceived emergency represents a significant change in context that affects the applicability of the access control rules. Carers can subscribe to the other event streams to obtain more detailed information, but only in emergencies. Note that in Fig. 1(a) unlike `treatsPatient`, `emergency` is *not* a monitored condition because it may be useful to continue monitoring the ECG stream for some period after an emergency is considered resolved.

Fig. 1(c) presents a transformation rule controlling disclosure. The `vitalsigns` event acts as a summary. Location is useful for interpreting readings; if a patient is at home, they are less likely to be subject to external stimuli, and thus should

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2010.8788
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2010.8788



(a) Non-Emergency Patient Stream

(b) Emergency Patient Stream

Fig. 2. Screen-shots from the monitoring application.

be more relaxed/stable. In non-emergency situations, the rule in Fig. 1(c) removes orientation details and perturbs location data (into home/not home). However, in an emergency the location is relevant to assist emergency response, and thus the perturbation does not apply (as the `not emergency` condition fails to hold).

The data control rules of this scenario ensure a level of privacy appropriate to the current context. In the general case, only a certain amount of information is required to evaluate the status of the patient. However, in an emergency situation, it is important that detailed information is made available.

A. Client application

We demonstrate the enforcement of data control policy through a client application that functions as a *dashboard*, representing the state of a particular patient. The application subscribes, based on the user's credentials, to the sensor readings of a patient (`vitalsigns` events). In an emergency situation, the application subscribes to the patient's `ecg_readings` to display the cardiogram. The screen-shots of Fig. 2 show that the data received and displayed varies according to context. Fig. 2(a) presents the general dashboard, where some information is restricted and perturbed. Fig. 2(b) shows the application for an emergency patient, displaying complete location data as well as a plot of the ECG.

VI. Conclusion

Healthcare information must be both shared and protected; thus is best disclosed on a *need-to-know* basis. As healthcare becomes increasingly pervasive, more technologies are being added into the interaction-mix. By enforcing access policy in middleware, it can apply across specific applications and scenarios, controlling live information streams as appropriate to context. This paper shows, through an example implementation, how event streams pertaining to sensor information can be controlled according to the severity of a patient's situation.

Acknowledgments

We acknowledge the Technology Strategy Board and EPSRC for their funding. Pedro Brandão is partially funded by Fundação Ciência e Tecnologia from Portugal.

References

[1] European Commission, "Personal health systems (conference report)," http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=323, 2007.
[2] Department of Health, "Supporting People with Long Term Conditions. A NHS and Social Care Model to support local innovation and integration," http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4100252, 2005.
[3] General Medical Council UK, "Good Medical Practice," 2006.
[4] NHS Information Authority in conjunction with the Consumers Association and Health Which?, "Share with Care! people's views on consent confidentiality of patient information," 2002.
[5] Department of Health, "Confidentiality: NHS Code of Practice," http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253, Nov 2003.
[6] G. Mühl, L. Fiege, and P. Pietzuch, *Distributed Event-Based Systems*. Springer, 2006.
[7] P. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys*, vol. 35, no. 2, pp. 114–131, 2003.
[8] J. Singh and J. Bacon, "Event-based data control in healthcare," in *Middleware '08: Proceedings of the ACM/IFIP/USENIX Middleware '08 Conference Companion*. New York, NY, USA: ACM, 2008, pp. 84–86.
[9] J. Singh, L. Vargas, J. Bacon, and K. Moody, "Policy-Based Information Sharing in Publish/Subscribe Middleware," in *Proceedings of the 9th International Workshop on Policies for Distributed Systems and Networks (Policy'08)*. IEEE Computer Society, 2008, pp. 137–144.
[10] NHS Care Record Development Board, "The care record guarantee—our guarantee for NHS Care Records in England," http://www.nigb.nhs.uk/guarantee, 2007.
[11] L. Vargas, J. Bacon, and K. Moody, "Event-Driven Database Information Sharing," in *Proceedings of the 25th British National Conference on Databases (BNCOD'08)*, ser. Lecture Notes in Computer Science (LNCS), vol. 5071. Springer, 2008, pp. 113–125.
[12] L. Vargas, "Integrating Databases and Publish/Subscribe," Ph.D. dissertation, University of Cambridge, 2009.
[13] G. J. McNeal, *AACN Guide to Acute Care Procedures in the Home*. Philadelphia, PA, 19106: Lippincott Williams & Wilkins, 2000.
[14] Hidalgo Ltd., "Equivital," http://www.equivital.co.uk/, 2009.
[15] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2000, pp. 32–43.
[16] NHS Connecting For Health, "An introduction to Legitimate Relationships and Workgroups," July 2006, nPfIT Information Governance.
[17] Department of Health, "The statement of NHS accountability for England," http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_093422, Jan 2009.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2010.8788
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2010.8788