Chapter 6
Securing Event-Based Systems

Jean Bacon
University of Cambridge, UK

David Eyers
University of Cambridge, UK

Jatinder Singh
University of Cambridge, UK

ABSTRACT
The scalability properties of event-based communication paradigms make them suitable for building large-scale distributed systems. For effective management at the application level, such systems often comprise multiple administrative domains, although their underlying communication infrastructure can be shared. Examples of such systems include those required by government and public bodies for domains such as healthcare, police, transport and environmental monitoring. We investigate how to build security into these systems. We outline point-to-point and publish/subscribe event-based communication, and examine security implications in each. Publish/subscribe decouples communicating entities. This allows for efficient event dissemination, however it makes controlling data visibility more difficult. Some data is sensitive and must be protected for personal and legal reasons. Large pub/sub systems distribute events using intermediate broker nodes. Some brokers may not be fully trusted. We discuss how selective encryption can effect security without impacting on content-based routing, and the implications of federated multi-domain systems. We discuss the specification of policy using role-based access control, and demonstrate how to enforce the security of the communications API and the broker network.

INTRODUCTION
This chapter examines techniques for securing various types of event-based systems. The first section discusses typical application requirements. The following section examines specific event dissemination approaches. Applying application-level security to event-based systems is introduced at first, along with an overview of Role-Based Access Control. Application-level security is a perimeter defence for an event-based system. The next section demonstrates mechanisms for implementing security within a large-scale distributed broker network, including discussion of

DOI: 10.4018/978-1-60566-697-6.ch006
distributed cryptographic key management. The following section explores a number of broker-specific policy enforcement mechanisms: where context-sensitive event processing allows more than binary (permit/deny) access control. The chapter conclusion highlights some of the open issues in this area of work.

APPLICATION REQUIREMENTS

Many large-scale distributed applications are best modelled as a federation of domains. A domain is defined as an independently administered unit in which a domain manager has, or may delegate, responsibility for naming and policy specification. Although most communication is likely to be within a domain, there is also a clear need for inter-domain communication. Some examples of application domains and communication requirements are as follows:

**Police infrastructure:** A number of regional (e.g. UK counties') police domains need support for intra- and inter-domain messages. Incident reports may be sent within and between domains for real-time response and may also be stored as part of an audit or record-keeping process. Databases for court records and the licensing of drivers of vehicles are accessible from all domains.

**Healthcare systems:** A national health service comprises many independently administered hospitals, clinics, primary-care practices, etc. The care of a patient may move from primary care to treatment in hospital. Specialists may be associated with more than one domain, such as hospitals and clinics. Caring for post-operative or elderly patients in their homes involves carers from many domains. This includes sharing information with various care providers (Singh, Vargas, & Bacon, 2008), making aspects of patient information persistent in centralised health record services (Moody, 2000), auditing data flows, to monitor compliance with procedures (Singh, Bacon, & Moody, 2007), and investigating anomalies. Communication within and between domains must therefore be supported but because of the sensitivity of the data must be strictly controlled.

**Environmental monitoring:** Traffic, noise, pollution, and weather conditions are monitored in a city to provide real-time information for citizens (Bacon, Beresford, et al., 2008). All data is recorded for historical analysis to aid prediction and for use by Local Government for planning purposes.

In such applications the need to communicate is driven by the actions of people, emergency situations, and the sensing and reporting of environmental conditions. Communication is naturally event-driven, requiring the transmission of data that captures the nature of some occurrence according to application-specific event-naming, specification and management, see Section 2.

Traditional access control mechanisms tend to focus on client authentication and authorisation specifics. In highly dynamic, distributed applications, context becomes increasingly important; that is, what are the circumstances in which access is appropriate. Often data is highly sensitive, and must be protected, yet must also be delivered in a timely manner to those parties that need-to-know. Data must be protected, not only from inappropriate clients, but also from other components of infrastructure (e.g. brokers). Policy must therefore be specified and enforced on how data is transmitted within and between domains, see Section 4.

EVENT DISSEMINATION INFRASTRUCTURE

As motivated above, events represent incidents. An event is a data-rich occurrence, encapsulating a particular semantic. Typically, an event instance consists of a set of (attribute, value) pairs, conforming to a named event type definition. A typical example of an event would be when a sensor device reports a reading from its sensor. Another often used example is each constituent update