Chapter 3.17
Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems[1]

Himanshu Khurana
NCSA, University of Illinois, USA

Radostina K. Koleva
NCSA, University of Illinois, USA

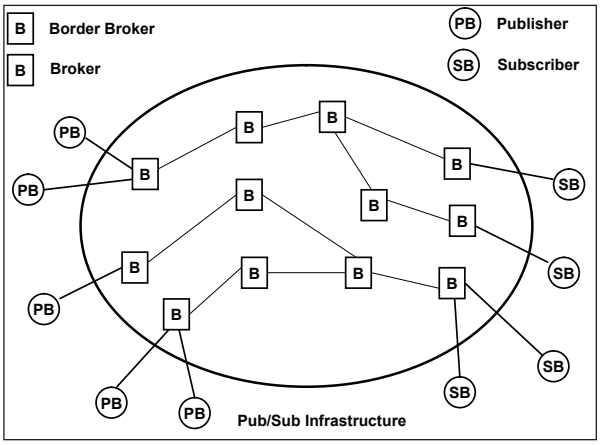
ABSTRACT

Content-based publish/subscribe systems offer an interaction scheme that is appropriate for a variety of large-scale dynamic applications. However, widespread use of these systems is hindered by a lack of suitable security services. In this paper, we present scalable solutions for confidentiality, integrity, and authentication for these systems. We also provide verifiable usage-based accounting services, which are required for e-commerce and e-business applications that use publish/subscribe systems. Our solutions are applicable in a setting where publishers and subscribers may not trust the publish/subscribe infrastructure.

INTRODUCTION

The publish/subscribe (pub/sub) interaction scheme provides a loose coupling between event generators (the *publishers*) and event consumers (the *subscribers*), which makes it ideally suited for a variety of dynamic applications such as software updates, location-based services for wireless networks, supply chain management, multiplayer online games, traffic control, and stock

Figure 1. Generic pub/sub model



quote dissemination. Publishers and subscribers are loosely coupled by a network of *brokers* who route events from the publishers to the subscribers. Different ways of expressing subscriber interest in events have led to different pub/sub schemes (Eugster, Felber, Guerraoui, & Kermarrec, 2003). Topic-based systems specify interest on certain topics or subjects, type-based systems specify interests in event types where all event types are organized in an inheritance hierarchy, and content-based systems specify interest via filters (using a subscription language) over the contents of the event. Content-based systems are considered to be the most general, and we focus on these systems in this paper.

One of the major hurdles to wide-scale deployment of content-based pub/sub systems (CBPS) is security. For example, ensuring that events are delivered only to authorized subscribers, preventing unauthorized modification to events, and guaranteeing that delivered events are authentic. In other words, ensuring confidentiality, integrity, and authentication of events (i.e., *event security*) as they traverse through the pub/sub infrastructure. A closely related problem to event security is that of accounting, which allows publishers to bill subscribers based on usage, for example, for applications such as stock quote dissemination. Challenges other than these event security ones include privacy of user subscriptions that would enable subscribers to receive events without revealing their subscriptions to the pub/sub infrastructure, and measures that would prevent against denial-of-service attacks. Wang, Carzaniga, Evans, and Wolf (2002) highlight many important security issues in pub/sub systems.

In this paper, we provide solutions to event security and accounting problems in CBPS systems with a very relaxed trust assumption, namely, one where the publishers and subscribers may not trust the broker network. That is, we assume the adversary will be able to access all communications in the pub/sub network, and can insert or modify communications as well. To solve the event confidentiality and accounting in this setting, we describe events in XML documents and use the secure XML document dissemination techniques of Bertino and Ferrari (2002) combined with the proxy reencryption scheme of Jakobsson (1999). We use digital signatures (Bartel, Boyer, Fox, LaMacchia, & Simon, 2002) to provide integrity and authentication. Our solution does not require any security associations (e.g., shared keys) between publishers and subscribers, or any modifications to existing matching and routing techniques. We analyze our solution and show that it scales to a large number of publishers and subscribers connected via an Internet-scale pub/sub infrastructure.