Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A survey of security solutions for distributed publish/subscribe systems

Anton V. Uzunov *

Defence Science and Technology Group (DST Group), West Ave., Edinburgh, SA 5111, Australia

ARTICLE INFO

Article history:
Received 4 July 2015
Received in revised form 1 February 2016
Accepted 27 April 2016
Available online 4 May 2016

Keywords:
Software security
Publish/subscribe
Distributed event-based systems
Software architecture
Security architecture
Survey

ABSTRACT

Over the last two decades, the need for loosely-coupled, asynchronous communications and distributed component interaction has made the *publish/subscribe* pattern increasingly popular in a variety of contexts. Despite their popularity, systems realizing this pattern are inherently susceptible to a wide variety of security threats, both of a general and specific nature. An increasing awareness of the importance of countering these threats has instigated a number of relevant proposals in the literature in the form of various types of *security solutions*. Having a broad knowledge of such security solutions is a prerequisite not only to proposing new solutions, but also to further advancing, re-using and adapting existing solutions to future publish/subscribe architectures. This paper seeks to contribute to the satisfaction of the latter prerequisite by presenting a comprehensive state-of-the-art survey of security solutions for distributed publish/subscribe systems, focusing on solutions taking the form of concrete security architectures. The solutions are reviewed "horizontally" from an architectural viewpoint, allowing their constituent parts to be seen in their original contexts. These "horizontal" reviews are augmented with brief analyses of constituent security patterns and pertinent threats addressed, thus providing a contextualized "vertical" dimension to each solution individually. In this way the paper provides a distinct perspective on a rapidly growing area of research, while complementing and consolidating the existing body of work concerned with surveying publish/subscribe security in general.

1. Introduction

Over the last two decades, the need for loosely-coupled, asynchronous communications and distributed component interaction has made the *publish/subscribe* pattern increasingly popular in a variety of contexts (Mühl et al., 2006; Opyrchal and Prakash, 2003; Tarkoma, 2013), ranging from complex event processing and status dissemination in cyber-physical infrastructures and health-care applications (Bakken et al., 2011; Cristea et al., 2011; Paschke et al., 2012; Singh and Bacon, 2009) to alert correlation in autonomous intrusion response systems (Docking et al., 2015; García et al., 2005). Being distributed systems in their own right, realizations of the publish/subscribe pattern are inherently susceptible to all the security threats faced by general distributed systems (network- and host-based), as well as a number of more specific threats (Aniello et al., 2014; Wang et al., 2002), which, as Savinov and Alencar (2014) and Fotiou et al. (2010a) point out, stem predominantly from the fact that attackers can leverage loosely-coupled publish/subscribe components as "entry points" for launching attacks. The inherent vulnerabilities in publish/subscribe systems become particularly noxious when requirements exist in a given system's context for sensitive

* Tel.: +618 7389 7252.
E-mail address: anton.uzunov@dsto.defence.gov.au.
http://dx.doi.org/10.1016/j.cose.2016.04.008

information to pass through untrusted, third-party networks or across disparate administrative domains (Bacon et al., 2009) – as is the case for all the contexts adduced as examples above; or when a given publish/subscribe system supports security and/or safety critical infrastructures, or is security and/or safety critical itself – as is also the case for most of the aforementioned systems.

An increasing awareness of the importance of security has instigated a number of relevant proposals in the literature in the form of various types of *security solutions*, such as the security architectures of concrete publish/subscribe systems, as well as generic, system-independent frameworks and isolated solutions, addressing one or more pertinent security threats. This trend has been so strong over the last nine years in particular, that a generally valid statement made by Corsaro et al. in 2006, namely, "security issues represent one major problem in pub/sub systems, only marginally addressed at present by both researchers and industry" (Corsaro et al., 2006) – and repeated in different forms in many topical security-related publications – is no longer true, with a significant body of research now attesting to the contrary. Having a broad knowledge of this research is a prerequisite not only to proposing new security solutions, but also to further advancing, reusing and adapting existing security solutions for future publish/subscribe architectures.

Naturally, this prerequisite is best satisfied by a comprehensive survey of the given area. Yet in contrast to the relative profusion of surveys and related work considering the general functional and other non-functional features of publish/subscribe systems – e.g. Bellavista et al. (2014); Esposito et al. (2013); Eugster (2007); Eugster et al. (2003); Liu and Plale (2003); Martins and Duarte (2010); Tarkoma and Raatikainen (2006) – the current literature presents only a single survey on publish/subscribe security: that of Esposito and Ciampi (2015) from late 2014. Although Esposito and Ciampi's survey is comprehensive and covers much ground, its prevalent focus is on abstract, system-independent solutions – as opposed to the security architectures of concrete systems – which means that a number of solutions are not covered. Moreover, the solutions which are included are presented in a "vertical" fashion, with each solution divided across several security concerns – a presentation which certainly has advantages from the point of view of overviewing the area, but one which does not allow solutions to be seen in their original contexts, making it difficult to gain insight into how the solution parts fit together and hence how similar solutions should be realized in real-life systems (we explain the distinctions between Esposito and Ciampi (2015) and this paper in more detail later on).

The present paper aims to rectify the aforementioned omissions and complement the recent work of Esposito and Ciampi (2015) by providing a comprehensive, state-of-the-art survey of security solutions (understood as individual or groups of concrete countermeasures addressing one or more pertinent security threats – in essence security pattern instances (Fernandez, 2013; Uzunov et al., 2012a) or groups of such instances) for distributed publish/subscribe systems, focusing on the security architectures of concrete systems. The solutions are reviewed "horizontally" and from an architectural viewpoint, allowing their constituent parts to be seen in their original contexts. These "horizontal" reviews are augmented with brief analyses of constituent security patterns and pertinent threats addressed, thus providing a contextualized "vertical" dimension to each solution individually. In this way the survey aims to maximally contribute to the satisfaction of the prerequisite of creating a sound and holistic knowledge-base to support, above all, the design of future publish/subscribe security architectures as referred to above – while providing a distinct viewpoint on a rapidly growing area of research.

The rest of the paper has been structured as follows. Section 2 discusses related work in the form of surveys and taxonomies. Section 3 provides a brief overview and presents a conceptual reference model of publish/subscribe systems; describes relevant security threats via an abstract threat model; and defines our classification of security solutions. Section 4 presents a series of reviews of concrete security architectures in some detail; and Section 5 reviews several frameworks and isolated solutions that are not covered in Esposito and Ciampi (2015), in brief summary form. In all cases the aim is to foster some degree of appreciation and understanding of the specific features of the security solutions under review, as opposed to merely noting their existence in passing. We are firmly convinced more in-depth reviews (especially of security architectures, following our focus) are necessary to dispel the notion alluded to already that security for publish/subscribe systems has received little attention – a notion which continues to prevail in many publications appearing even close to the time of this writing.

As mentioned earlier, all security solutions can be seen as collections of security pattern instances, and throughout Sections 4 and 5 we make the latter relation explicit by indicating the main patterns (of those available at the time of this writing) constituting each solution, and which threats – from the threat model introduced in Section 2 – these patterns seek to address. Besides providing a "vertical" dimension to the reviews as mentioned already, these brief analyses serve the dual purpose of summaries and evaluations with respect to the threats the security solutions address (cf. (Dikanski et al., 2012; Fernandez et al., 2016)). Knowing which security patterns comprise a solution is also important when applying architectural analysis techniques such as those of Halkidis et al. (2008) or Heyman et al. (2008), not only for the analysis of particular solutions, but of whole publish/subscribe architectures implementing those solutions. The set of reviewed solutions is subsequently compared based on the threats they address in Section 6, where we also identify gaps and advance ideas for improving publish/subscribe security solutions in general. Finally, in Section 7 we conclude and discuss future research directions stemming from this survey.

2. Related work

As intimated in the preceding discussions, there are a number of surveys relating to the functional aspects of publish/subscribe systems or to their taxonomization. Some prominent examples include:

- Eugster et al. (2003), which places publish/subscribe in the context of other distributed system communication/