Design of a Secure and Decentralized Location Service for Agent Platforms

Benno Overeinder¹, Michel Oey¹, Reinier Timmer¹, Reinout van Schouwen¹, Erik Rozendaal², and Frances Brazier¹

¹ IIDS Group, Department of Computer Science, Faculty of Sciences, VU University Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands
{bjo,michel,rjtimmer, reinout, frances}@cs.vu.nl
² NLnet Labs, Kruislaan 419, 1098 VA Amsterdam, The Netherlands
erik@NLnetLabs.nl

Abstract. Agent platforms designed for Internet-scale, open networks need scalable and secure location services for agents and services. The location service based on the Fonkey public key distribution infrastructure presented in this paper has been designed and implemented for this purpose. It is scalable in the total number of published identifier–contact address pairs, the number of updates/changes, and the number of agent platforms publishing and requesting contact addresses. This system also supports a signing mechanism to authenticate the publisher of an identifier–contact address pair. Experimental results show that the current implementation based on the Bunshin/Free Pastry overlay network exhibits good scaling behavior.

1 Introduction

Scalable location services are essential in distributed systems and, in particular, for multi-agent systems. The Domain Name System (DNS) is a very successful realization of a location service that resolves symbolic names to contact addresses (IP addresses). DNSSEC (Secure DNS) has been designed to support authentication preventing spoofing and man-in-the-middle attacks [1].

Both DNS and DNSSEC, however, are not designed to deal with highly dynamic entities such as mobile agents. The dynamic nature of mobile agents in Internet-scale, open network systems requires a different type of approach for registering, deregistering, and retrieving location information. Scalability and integrity are of utmost importance as (up-to-date) agent location information is a prerequisite of successful agent mobility.

This paper presents the design of a scalable and secure location service based on the Fonkey system. Fonkey is an infrastructure for global public key (optionally with a payload) distribution. The payload in our location service is agent location information, optionally signed by other public keys.

Section 2 discusses current technologies used in name resolution, such as DNS and LDAP, and location services for (mobile) agent systems. Section 3 presents the design of the Fonkey-based location service. Section 4 discusses security issues, and Sect. 5 reports on experimental scalability results. Finally, Sect. 6 concludes the paper with a discussion on future work.

© Springer-Verlag Berlin Heidelberg 2010
2 Background

The most widely used location service on the Internet today is Domain Name System (DNS) [2]. DNS defines a hierarchical name space used to map computer host names and other resources to IP addresses. DNS is a distributed database that allows for scalable operation by distributing the hierarchical name space over many servers, each responsible for a specific part of the name space. DNSSEC [3] is a security extension for DNS that cryptographically ensures DNS data is not forged or altered. The DNSSEC extensions provide data integrity and authentication through the use of digital signatures.

The Lightweight Directory Access Protocol (LDAP) [4] is a directory service that can also be used as a location service. The LDAP protocol is designed to provide access to directories supporting the X.500 models. The directory access protocol provides both read and update access. Update access requires secure authentication. LDAP organizes data in a hierarchy using the Distinguished Name (DN). Like DNS, LDAP allows distribution over multiple servers based on the hierarchical name.

Van Steen et al. [5] present a location service for mobile objects in a worldwide system named Globe. The mobile object location service strictly separates an object’s name from the location on which it resides. This is done by binding an object’s name to a location-independent object handle, which, in turn, is mapped to the location where the object resides. The location service is organized as a distributed search tree. To achieve scalability of the hierarchical location service, where potentially high-level nodes may become a bottleneck, location information is distributed such that the load is evenly balanced, while at the same time exploiting locality [6]. Name and location service NLS extends the Globe location service by using prefixes to aggregate location information and using a two-layer architecture with fat-trees at the global layer [7].

Locating mobile agents in worldwide distributed systems is also specifically addressed in a number of research papers. Di Stefano and Santoro [8] propose a naming scheme and location protocol with intended general validity for mobile agents able to effectively meet all the typical requirements of mobile agent environments and, thus, straightforward to integrate into different platforms. Functionality for authentication of hosts publishing location updates and information integrity is not, however, considered in their system. Roth and Peters [9] propose a global tracking service for mobile agents, designed to scale to the Internet, and to be secure. Their location information load sharing approach is similar to the Globe location service, but does not presuppose coherent mobile agent migration patterns to achieve scalability. The protocols presented by Roth and Peters have a number of advantageous security properties, in particular, malicious location updates by unauthorized hosts are prevented. A scalable hash-based mobile agent location mechanism is proposed by Kastidou et al. [10]. A mobile agent tracking mechanism based on hashing is presented, and dynamic rehashing is supported to allow the system to adapt to variable workloads.

The research reported in this paper has defined design goals similar to the global tracking system presented in [9], namely a scalable and secure location service for mobile agents. However, the location service system presented in this paper includes data integrity verification.