Distributed Data Authentication (System Demonstration)

Michael T. Goodrich
Department of Computer Science
University of California, Irvine
goodrich@acm.org

Michael Shin Christian D. Straub Roberto Tamassia
Department of Computer Science
Brown University
{mys,cstraub,rt}@cs.brown.edu

Abstract

We demonstrate the functionality of a distributed system that supports the wide-scale deployment of an authenticated map. The system can be easily extended to support applications that use authenticated maps, including certificate revocation, document integrity, and digital rights management.

1. Introduction

The *Lightweight Authenticated Information Repository* (*LAIR*) [2] is a distributed system that implements an authenticated map. LAIR has significant performance, scalability and security advantages over traditional authentication systems, such as OCSP and certificate revocation lists.

LAIR can integrate smoothly with a Web services model using a type of XML signature. Indeed, several Web-based applications of LAIR have been developed, including end-to-end integrity of Web content, certificate revocation, and SSH host authentication.

The development of LAIR was supported in part by the Dynamic Coalitions Program of the Defense Advanced Research Projects Agency (DARPA) under DARPA/AFRL agreement F30602–00–2–0509.

2 Architecture

LAIR involves the interaction of four primary parties: a *publisher* of data, a trusted *source*, untrusted *responders*, and *clients*. The *source* maintains a set S of key-value pairs that evolves over time. A *publisher* is a trusted entity who is given the authority to insert and delete elements in the set S. A *responder* maintains a copy of set S and answers queries from *clients* of the form "is element e in set S?" and "what is the value associated with element e?". Figure 1 shows the high-level architecture of LAIR.

The source and responder components have been implemented in Java. Various clients and publisher components have been implemented in Java, C++ and C#. Also, we have developed toolkits for building Java and C# clients.

The implementation of the LAIR system is fully resistant against compromised responders and active adversaries on the network. These security properties rely on standard cryptographic assumptions about one-way collision-resistant hash functions and digital signatures.

3 Applications

The following applications have been implemented using LAIR.

- Certificate revocation
- XML signature validation [3]
- End-to-end document integrity [4]
- Personal digital media library
- SSH host authentication [1]

References

[1] M. T. Goodrich, J. Lentini, and R. Tamassia. JSSH: A secure shell client. Technical report, Center for Geometric Computing, Brown University, 2002.

[2] M. T. Goodrich, M. Shin, R. Tamassia, and R. Cohen. LAIR: A lightweight authenticated information repository system. Technical report, Center for Geometric Computing, Brown University, 2002. http://www.cs.brown.edu/cgc/stms/papers/lair.pdf.

[3] D. J. Polivy and R. Tamassia. Authenticating distributed data using Web services and XML signatures. In *Proc. ACM Workshop on XML Security*, 2002.

[4] M. Shin, C. Straub, R. Tamassia, and D. J. Polivy. Authenticating Web content with prooflets. Technical report, Center for Geometric Computing, Brown University, 2002.

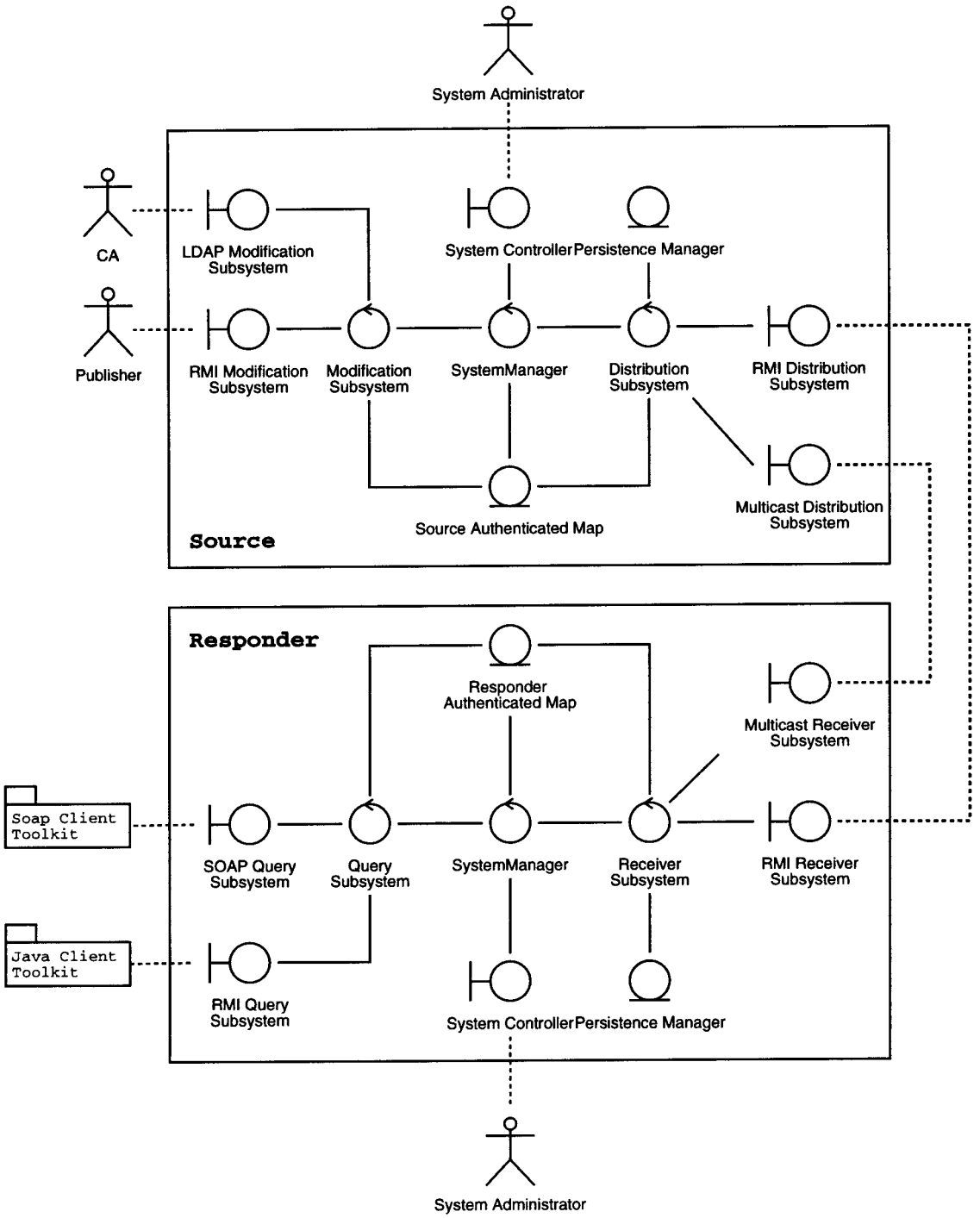

Figure 1. High-level architectural overview of the LAIR system for distributed data authentication.