An Architecture for a Secure Service Discovery Service

Steven E. Czerwinski, Ben Y. Zhao, Todd D. Hodes, Anthony D. Joseph, Randy H. Katz

University of California, Berkeley

{*czerwin, ravenben, hodes, adj, randy*}*@cs.berkeley.edu*

April 2, 2014

Overview

Outline

Introduction

- Large scale deployment of networks and devices
- Challenge: locate a service for a task out of thousands
- Secure and trusted services with minimum client intervention
- Ninja SDS: scalable, fault-tolerant and secure repository
- Repository: description of services and existing, running, services
- Hierarchical load-balancing and application level query routing

Outline

Announcement-based Information Dissemination

- Failure does not require a separate service
  It's sufficient to listen to the periodic multicast announcements to update the cache/database
- Bootstrapping
  Clients discover an SDS server by listening to a multicast address.
  Client can solicit asynchronous announcements
- Eventual Consistency
  Eventual consistency vs. transactional semantic

Announcement-based Information Dissemination

- Failure does not require a separate service
  It's sufficient to listen to the periodic multicast announcements to update the cache/database
- Bootstrapping
  Clients discover an SDS server by listening to a multicast address.
  Client can solicit asynchronous announcements
- Eventual Consistency
  Eventual consistency vs. transactional semantic

Announcement-based Information Dissemination

- Failure does not require a separate service
  It's sufficient to listen to the periodic multicast announcements to update the cache/database
- Bootstrapping
  Clients discover an SDS server by listening to a multicast address.
  Client can solicit asynchronous announcements
- Eventual Consistency
  Eventual consistency vs. transactional semantic

Hierarchical Organisation

SDS server hierarchy

- under heavy load, a child is spawned - shares load with parent
- the domain of an SDS server (fractional subnet, etc) is the network extent it covers

XML Service Descriptions

XML Service Descriptions

1. More flexible than ¡key,value¿ pairs
2. Service description validation against a set schema
3. Database schema vs. DTD: flexibility, backward-compatibility

Privacy and Authentication

Contents

- Hybrid symmetric and asymmetric cryptography used
- Each component has a public key and a principal name

Outline

SDS Server

- Global multicast channel to send authenticated messages
- Authenticated advertisements contain:
  - Certificate Authority and Capabilities Manager contact
  - Address for sending service announcements
  - Service annoucement rate
- Aggregate rate set by administrators
- Should several servers fail, recovery is cascading from the top
- Privacy and authentication assured by the *secure one-way service broadcast*

Services

1. Continously listen on the global multicast channel for SDS server announcements
2. Multicast its service descriptions to the proper channel/frequency
3. Set appropriate capabilities by contacting the Capabilities Manager

Services

1. Continously listen on the global multicast channel for SDS server announcements
2. Multicast its service descriptions to the proper channel/frequency
3. Set appropriate capabilities by contacting the Capabilities Manager

Services

1. Continously listen on the global multicast channel for SDS server announcements
2. Multicast its service descriptions to the proper channel/frequency
3. Set appropriate capabilities by contacting the Capabilities Manager

Capabilities Manager

1. Contacted by services
2. Specifies an access control list
3. Generates and stores appropriate capabilities

Capabilities Manager

1. Contacted by services
2. Specifies an access control list
3. Generates and stores appropriate capabilities

Capabilities Manager

1. Contacted by services
2. Specifies an access control list
3. Generates and stores appropriate capabilities

Secure Communications

Secure Communications

- Authenticated Server Annoucements

Secure Communications

- Authenticated Server Annoucements
- Secure One-Way Service Description Annoucements

Secure Communications

- Authenticated Server Annoucements
- Secure One-Way Service Description Annoucements
- Authenticated RMI

Outline

Wide Area Support

Wide Area Support

1. Lorem Ipsum

Wide Area Support

1. Lorem Ipsum
2. Lorem Ipsum

Wide Area Support

1. Lorem Ipsum
2. Lorem Ipsum
3. Lorem Ipsum

Alternatives

Questions ?