Distributed Authentication Through Kerberos Tickets: Problem statement and Requirements
draft-moustafa-krb-wg-ps-00.txt

Abstract

This document presents the problem of authentication and authorization in distributed environments constituted by several users communicating with application servers and communicating with each others. Each user in this environment can also play the role of an application provider.

Imagine a large music event where the provided network infrastructure is enhanced with network storage equipment to allow visitors to access content relating to the bands playing at the events, such as recorded video of previous performances, supplementary audio and video material relevant to the bands playing, etc. Certain content is, however, not necessarily available to everyone under the same conditions. Instead access control is applied before the full range of audio, and video material can be accessed. Other content, such as previews, might be offered for free. How can such authentication, and authorization infrastructure be made available with minimal configuration complexity for a temporary event like a music festival? This document describes a problem statement based on the attempt to use Kerberos and lists a couple of requirements for potentially needed Kerberos extensions.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
1. Specification Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

Authentication and authorization to services access is still an open problem in distributed environments in which several users would need to communicate to several application servers and also with each other, where each user could play the role of an application provider. The principle of using service tickets in Kerberos allows for credentials distribution which is suitable for distributed environments. However, the centralized approach in Kerberos (where each user should communicate with the authentication server each time he needs services credentials) restricts its usage for authentication in distributed environment.

Indeed, there is a need to control the authentication and access authorization among the different communicating users in a dynamic manner suitable for the dynamic network configuration.

3. Problem Statement

The problem of authentication and access authorization still presents an open issue for distributed environments. Employing symmetric cryptography using a secret (key) shared by all users constituting
the distributed environment network is a simple approach in terms of requiring lesser processing and consuming lesser resources. However, it has two main limitations: i) The possibility of key divulgation, where it is sufficient to attack only one user node for attacking the whole network and breaking its security, and ii) The difficulty of the key distribution process, where one should assume the existence of a mechanism assuring key distribution prior to the communication.

The Kerberos authentication model [RFC4120] uses a symmetric cryptography approach, however offering a high security level and allowing mutual authentication. However, Kerberos authentication could not be directly applied in distributed environments in which the communication between the different users can take place in a dynamic manner. Kerberos rather authenticates each node with respect to the authentication server and to the application server. The distributed credentials principle in Kerberos (through TGS tickets) is promising for allowing authentication in distributed environment between each user and the application server. However, the authentication between each two users that need to communicate together is still not covered by the TGS tickets, especially with the dynamic nature of distributed environments in which users connectivities change frequently with time.

4. Requirements

This section presents a number of requirements motivated by the problem statement defined in the previous section. These requirements are as follows:

- Providing authentication for each user participating in the distributed environment network by a trusted third party (as the Kerberos server).
- Providing access authorization of each user by a trusted third party in a way that corresponds to the user subscription type and profile.
- Providing mutual authentication between each pair of communicating users in a dynamic manner through attributing dynamic credentials to be distributed to each user.

5. Potential Use-cases

This section presents the potential use-cases for distributed environments requiring the distribution of the authentication and access authorization process. Two main use-cases are described:

- Temporary network infrastructure deployment for special events (sport events, music festivals, ..). Network operators deploy temporary low-cost infrastructure for such temporary events and
hence counts on the communication of users with the application servers that are locally deployed. Also the users themselves can play the role of application providers contributing to the diffusion of multimedia services (video snapshots on the event, video streams with inserted comments, video streaming for what was missed in the event, downloading an interactive audio-visual program for the event, ...). In such use-case, there is a need for dynamic credentials distribution on the different participating nodes and there is also a need of controlling the access of each user to the authorized service for a duration corresponding to his subscription.

- Community networks, where a user owns the home gateway to the Internet and allows other distributed users to have access to the Internet through passing by his home gateway. Users may need to pass by other users (in the community network) in order to reach the home gateway. In this use-case, there is a need for credentials distribution in a dynamic manner (adapting to the random configuration of the community network) to allow mutual authentication between each pair of communicating users and between each user and the home gateway providing the Internet access.

6. Security Considerations

This document focuses on the distributed authentication through the Kerberos protocol and presents the requirements to be considered.

7. IANA Considerations

This document does not require actions by IANA.

8. Acknowledgment

We would like to thank Hannes Tschofenig for his comments on this draft and for encouraging us to publish it.

We would also like to thank our colleague Estelle Transy for all the discussions during the use-cases definition.

9. Normative References


Authors’ Addresses

Hassnaa Moustafa
France Telecom - Orange
38-40 rue du General Leclerc
Issy Les Moulineaux, 92794 Cedex 9
France

Email: hassnaa.moustafa@orange-ftgroup.com

Gilles Bourdon
France Telecom
90 boulevard Kellermann
75013 Paris,
France

Email: gilles.bourdon@orange-ftgroup.com