Kerberos Working Group
Internet-Draft
Intended status: Informational
Expires: April 19, 2012

H. Moustafa
France Telecom - Orange
G. Bourdon
France Telecom - Orange France
T. Yu
MIT Kerberos Consortium

October 17, 2011

Distributed Authentication in Wireless Mesh Networks Through Kerberos Tickets

draft-moustafa-krb-wg-mesh-nw-02.txt

Abstract

This document presents the problem of authentication and authorization in wireless mesh networks constituted by several users communicating with application servers and communicating with each other in a single or multi-hop fashion. 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 lists the requirements for a potentially needed Kerberos extension and presents a solution proposal based on the attempt to use a Kerberos extension for mutual authentication in wireless mesh networks.

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."

This Internet-Draft will expire on April 19, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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 and Problem Statement

Authentication and authorization to services access is still an open problem in wireless mesh network distributed environments in which several users would need to communicate to several application servers and with each other in a single or multi-hop fashion, and each user could play the role of an application provider.

The Kerberos authentication model [RFC4120] uses a symmetric cryptography approach, offering a high security level and allowing mutual authentication. The principle of using service tickets in Kerberos allows for credentials distribution which is suitable for wireless mesh networks 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 such distributed environments. Furthermore, Kerberos rather authenticates each node with respect to the authentication server and to the

application server. The distributed credentials principle in Kerberos (through Service tickets) is promising for allowing authentication between each user and the application. However, the authentication between each two users who communicate with each other is still not covered by Service tickets, especially with the dynamic nature of distributed environments in which users connectivity (that could be single or multi-hop) change frequently with time.

Although the multi-hop communication is transparent to the application, there is a need to handle the authentication and access control among the different multi-hop communicating nodes to prevent against malicious actions taken by the human users themselves. Based on this fact, this draft proposes to use a common key obtained by Kerberos for authentication among each two nodes who communicate together in a multi-hop fashion. This common key is dynamic (renewable with time) for security reasons in such dynamic and distributed wireless environment that is less secure.

3. Requirements

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

- Distributed environment consisting of fixed and mobile nodes.
- Dynamic neighbors and dynamic application providers (any node could be an application provider at any time providing applications to other nodes in the network, e.g. file sharing, sending special announcement concerning the surrounding environments, and sending alarms in case of problems).
- User Generated Content (UGC) application, in which each node could be a source of content (mainly multimedia contents) for other nodes in the network, e.g. transmitting video snapshots during festival events.
- Hundreds of nodes (indoor or outdoor environment).
- Personal devices (of low power) individually used by users.
- Multihop communication.
- Authentication and access control of each user node by a trusted third party.
- Access control of each user by a trusted third party in a way that corresponds to the user subscription type and profile.
- Mutual authentication between each pair of communicating users.
- Limited bandwidth: need for minimizing traffic (minimizing the communication with the KDC).
- Dynamic credentials (attributing dynamic credentials to be distributed to each user).

4. Kerberos Extension Solution Proposal

This section presents a solution proposal extending the Kerberos authentication model for authenticating each user node in wireless mesh networks with respect to the network operator and with respect to other users nodes participating in the network.

The Kerberos server resides in the local mesh network or in an external network and each user node needs to communicate firstly with this server in order to authenticate with respect to the operator and to obtain the necessary credentials (Kerberos tickets) for authentication with other users nodes and for accessing the offered services in the mesh network. The communication can take place in a single hop or through multi-hops (passing by intermediate users nodes) according to the proximity of each user node from the application providers nodes.

To prevent unreliable communication from taking place (intermediate nodes could do DoS, messages truncating,...), this solution proposal extends the classical Kerberos authentication model to adapt to the multi-hop communication through introducing a new shared secret for authentication and access control between intermediate nodes along the multi-hop communication. But, if this secret is the same for all the time, it could be compromised and the entire network would be compromised. It is then proposed in this draft to obtain several shared secrets during the service ticket request for the service for which the multihop communication is needed.

The solution proposal takes the following sequence:

- Each user node wishing to access the services offered by the mesh network starts by sending a first request to the KDC (TGT part) in order to authenticate with respect to the operator and to obtain the TGT ticket. The process is similar to the classical Kerberos authentication approach, and the user, if legitimate, obtains the corresponding TGT ticket.
- After obtaining the TGT, the user node re-contacts the KDC (TGS part), through sending a TGS request, in order to obtain the necessary credentials (including the service ticket for the service for which multihop communication will be employed in addition to the shared secrets for authentication during the multihop communication) while presenting the obtained TGT ticket as a proof of authenticity. The classical Kerberos TGS request should be extended to illustrate the need of extra credentials for authentication with intermediate nodes along the multi-hop communication. The following figure illustrates this extension, where a new flag is defined in the flags field in the reserved bits between bits 12 and 25 taking the value 1 to indicate the case of Kerberos in the multi-hop mode.

o

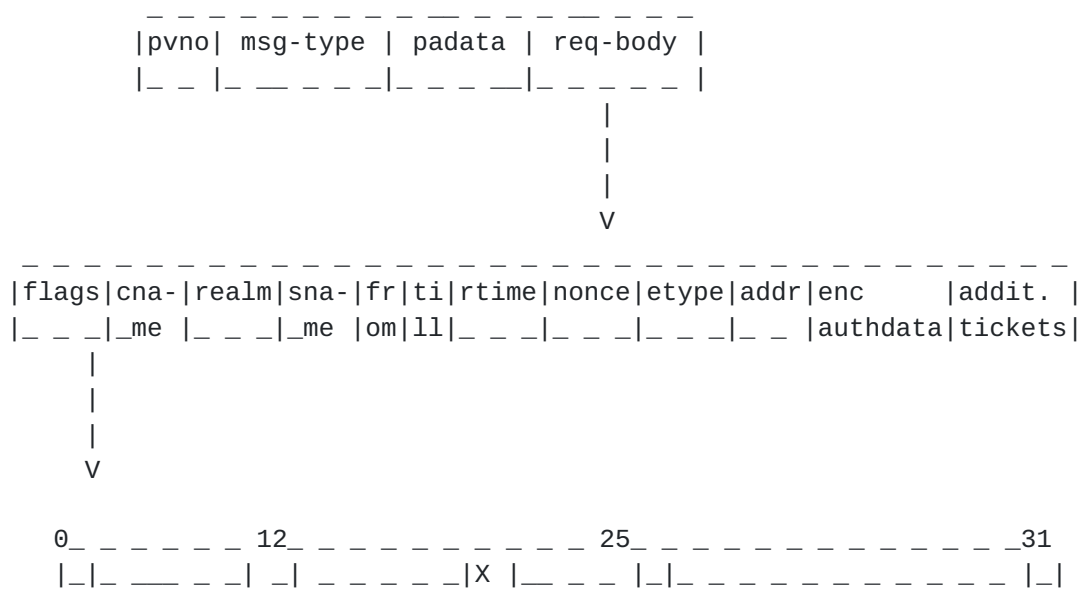

Figure 1: Extended TGS-REQ

o Once the KDC (TGS part), receiving the TGS request from the user, verifies the TGT ticket and the user authenticity, it sends to the user the Kerberos TGS reply message extended to contain the necessary credentials according to the user profile and according to the required service.
o The extended Kerberos TGS reply message includes the service ticket for the service for which the multihop wommunication will be employed as well as the shared secrets.
o To avoid the shared secret compromise, several shared secrets are obtained, where each shared secret is valid for a given time interval. However, the shared secret distributions should be done in a mean that would not compromise the security of the whole network:
  * If the shared secrets are required by each mesh node at each time interval, this would generate lot of traffic during the communication with the KDC.
  * If the shared secrets for future time intervals are pre-generated by the KDC and given in batch to each user, this would optimize traffic, but if a node is compromised at an

interval of time, all the shared secrets would be known and the network would be compromised.

- Then, the KDC sends to each mesh node in the extended TGS reply message the current interval shared secret and the pre-generated ones for the future, while each pre-generated shared secret is encrypted with a key corresponding to the its related time interval. This encryption key should be sent to each mesh node in the corresponding time interval either through Kerberos protocol or through a multicast routing protocol. The following figure illustrates the extended TGS reply message. In this extended message: i) a new flag is defined in the flags field in the reserved bits between bits 14 and 31 taking the value 1 to indicate the case of Kerberos in the multi-hop mode. ii) a new field authorized-data is added which is identical to the authorization data field existing in the service ticket and containing elements, where the first element contains the current time interval in its (type) part and the corresponding shared key to this interval in its (data part). The other elements contains the upcoming time intervals and the corresponding shared keys in an encrypted form as explained above.
-

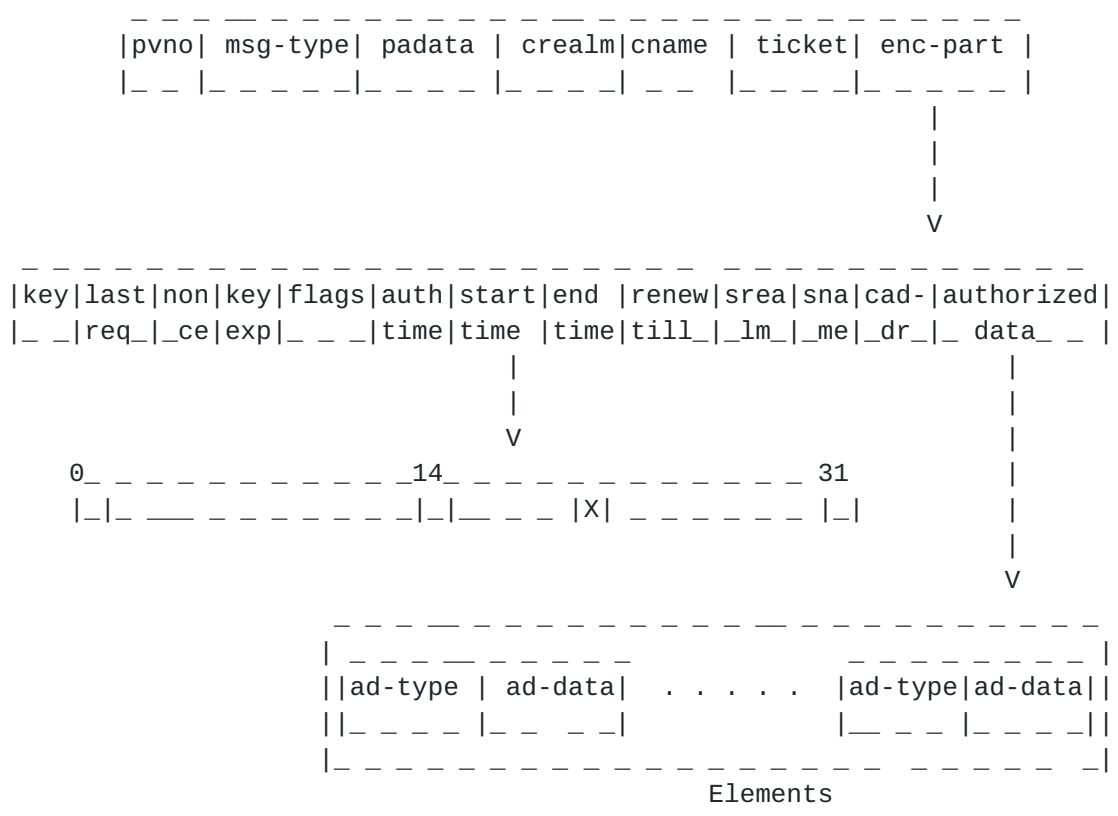

Figure 2: Extended TGS-REP

- Group keys can be also considered allowing to have a shared secret for each group of mesh nodes and allowing each mesh node to participate to more than one group and hence to have several group keys. If one group key is compromised it could be deleted by the KDC. Mesh nodes sharing the same group key are mesh nodes sharing some common characteristics (making a cluster, hierarchal group keys for example, ...).

5. Potential Use-cases

This section presents the potential use-cases for distributed environments of wireless mesh networks having multi-hop communication and requiring distributed authentication authorization.

- Temporary network infrastructure deployment for special events (sport events, music festivals, ..). Network operators deploy temporary low-cost infrastructure for temporary events and hence counts on the communication of users with 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.

Many thanks for Sam Hartman for all his useful comments and feedbacks on this draft.

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

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", August 2002.

[RFC4120] Neumann, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", July 2005.

Authors' Addresses

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

Email: hassnaa.moustafa@orange.com

Gilles Bourdon
France Telecom - Orange France
Immeuble Central 1, clos de la courtine
93162 Noisy le Grand,
France

Email: gilles.bourdon@orange.com

Tom Yu
MIT Kerberos Consortium

Email: tlyu@mit.edu