Problem statement on the cross-realm operation of Kerberos in a specific system
draft-sakane-krb-cross-problem-statement-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft expires in October 29, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

There are some issues when the cross-realm operation of the Kerberos Version 5 [RFC4120] is employed into the specific systems. This document describes some manners of the real example, and lists requirements of the operation in such real system. Then it clarifies issues when we apply the cross-realm operation to such specific system.

Conventions used in this document

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 RFC 2119 [RFC2119].

It is assumed that the readers are familiar with the terms and concepts described in the Kerberos Version 5 [RFC4120].
Table of Contents

1. Introduction .................................................. 4
2. Kerberos system .............................................. 4
   2.1. Kerberos basic operation ................................ 4
   2.2. Cross-realm operation ................................. 5
3. The status of the industrial system .......................... 6
4. Requirements ................................................ 7
5. Issues ....................................................... 8
   5.1. Unreliability of authentication chain ................. 8
   5.2. No PFS in case of the indirect trust model .......... 8
   5.3. Scalability of the direct trust model ................. 9
   5.4. Exposure to DoS Attacks ................................ 9
   5.5. Client’s performance ................................... 9
   5.6. Pre-authentication problem in roaming scenarios ...... 10
6. Implementation consideration .................................. 10
7. IANA Considerations .......................................... 11
8. Security Considerations ....................................... 11
9. Acknowledgments ............................................... 11
10. References .................................................. 11
   10.1. Normative References ................................ 11
   10.2. Informative References ............................... 11
Authors’ Addresses ............................................... 12
Full Copyright Statement ........................................ 12
Intellectual Property Statement ................................. 13
1. Introduction

The Kerberos Version 5 is a widely deployed mechanism that a server can authenticate a client access. Each client belongs to a managed domain called realm. Kerberos supports the authentication in case of situation that a client and a server belong to different realms. This is called the cross-realm operation.

Meanwhile, there are lots of manners of operation in the real system, where Kerberos could be applied. Sometimes, there are several managed domain in such system. and it requires the authentication mechanism over the different managed domains. When the cross-realm operation of Kerberos is applied to such specific systems, some issues come out.

This document briefly describes the Kerberos Version 5 system and the cross-realm operation. Then, it describes two real systems that can be applied the Kerberos system, and describes nine requirements of those systems in term both of management and operation. Finally, it lists six issues of the cross-realm operation when it is applied to those system.

Note that it might not describe whole of issues of the cross-realm operation. It also does not propose any solution to solve issues described in this document. In further step, we have to analyze, and compare candidates of solutions. This work will be in another document.

This document is assumed that the readers are familiar with the terms and concepts described in the Kerberos Version 5 [RFC4120].

2. Kerberos system

2.1. Kerberos basic operation

Kerberos [RFC4120] is a widely deployed authentication system. The authentication process in Kerberos involves principals and a Key Distribution Center (KDC). The principals can be users or services. Each KDC maintains a principals database and shares a secret key with each registered principal.

The authentication process allows a user to acquire the needed credentials from the KDC. These credentials allow services to authenticate the users before granting them access to the resources. An important part of the credentials are called Tickets. There are two kind of tickets: Ticket Granting Ticket (TGT) and Service Ticket.
The TGT is obtained periodically from the KDC and has a limited limit after which it expires and the user must renew it. The TGT is used to obtain the other kind of tickets, Service Tickets. The user obtains a TGT from the Authentication Service (AS), a logical component of the KDC. The process of obtaining a TGT is referred to as 'AS exchange'. When a TGT request is issued by an user, the AS responds by sending a reply packet containing the credentials which consists of the TGT along with a random key called 'TGS Session Key'. The TGT contains a set of information encrypted using a secret key associated with a special service referred to as TGS (Ticket Granting Service). The TGS session key is encrypted using the user’s key so that the user can obtain the TGS session key only if she knows the secret key shared with the KDC. The TGT then is used to obtain Service Tickets from the Ticket Granting Service (TGS)- the second component of the KDC. The process of obtaining service tickets is referred to as 'TGS exchange'. The request for a service ticket consists on a packet containing a TGT and an ‘Authenticator’. The Authenticator is encrypted using the TGS session key and contains the identity of the user as well as time stamps (for protection against replay attacks). After decrypting the TGT (which was encrypted by the AS using the TGS’s secret key), the TGS extracts the TGS session key. Using that session key, it decrypts the Authenticator and authenticates the user. Then, the TGS issues credentials requested by the user. These credentials consist on a service ticket and a session key that will be used to authenticate the user with the desired application service.

2.2. Cross-realm operation

The Kerberos protocol provides the cross-realm authentication capabilities. This allows users to obtain service tickets to access services in foreign realms. In order to access such services, the users first contact their home KDC asking for a TGT that will be used with the TGS of the foreign realm. If the home realm and the foreign realm share keys and have an established trust relationship, the home KDC delivers the requested TGT.

However, if the home realm does not share cross-realm keys with the foreign realm, the home KDC will provide a TGT that can be used with an intermediary foreign realm that is likely to be sharing cross-realm keys with the target realm. The client can use this ‘intermediary TGT’ to communicate with the intermediary KDC which will iterate the actions taken by the home KDC: If the intermediary KDC does not share cross-realm keys with the target foreign realm it will point the user to another intermediary KDC (just as in the first exchange between the user and its home KDC). However, in the other case (when it shares cross-realm keys with the target realm), the
intermediary KDC will issue a TGT that can be used with the KDC of the target realm. After obtaining a TGT for the desired foreign realm, the client uses it to obtain service tickets from the TGS of the foreign realm. Finally, the user access the service using the service ticket.

When the realms belong to the same institution, a chain of trust can be determined by the client or the KDC by following the DNS domain hierarchy and supposing that the parent domains share keys with all its child sub-domains. However, because the inter-realm trust model is not necessarily constructing the hierarchic approach anytime, the trust path must be specified manually. When intermediary realms are involved, the success of the cross-realm operation completely depends on the realms that are part of the authentication path.

3. The status of the industrial system

This section describes the state in the industrial environment on which we focuses. It would be easier to understand the requirement and the restriction described after.

First, to understand the scale of the environment, we refers to a petrochemical company, Shell Petrochemical Company Limited. [SHELLCHEM]. It produces bulk petrochemicals and their delivery to large industrial customers. There are 43 typical plants of the company all over the world. They are managed by the operation sites placed in 35 countries. This section shows two examples of them.

One is the CSPC [CSPC], an example of the centralized plant. The CSPC is a joint enterprise of CNOOC and Shell. This plant is one of the hugest systems of a petrochemical industry in the world. This is placed in the area of 3.4 square kilo meters in the north coast of Daya Bay, Guangdong, which is at the southeast of China. 3,000 network segments are established in the system. 16,000 control devices are connected to the local area network. These devices belong to different 9 sub systems, A control device has some control points, which are controlled and monitored by other devices remotely. There are 200,000 control points in all. They are controlled by 3 different control center.

Another example is the NAM (Nederlandse Aardolie Maatschappij), an example of the distributed plant system. The NAM is a partnership enterprise of Shell and Exxon Mobil Corporation. It is a plant system group that geographically distributes to scatter in the area of 863 square kilo meters of Netherlands. 26 plants, each is named "cluster", are scattered in the area. They are connected each other by a private ATM WAN. Each cluster has approximately 500-1,000
control devices. These devices are managed by each local control center in each cluster. In the entire system of the NAM, there are one million control points.

In the both of the systems, the end devices are basically connected to a local network by a twisted pair cable, which is a low band-width of 32 kbps. Low clock CPU, for example H8 [RNSS-H8] and M16C [RNSS-M16C], are employed by many control devices. Furthermore, to suppress power consumption, these CPU may be lowered the number of clocks. Because there is a requirement of the explosion-proof. The requirement restricts the amount of total energy in the device.

A device on the network collects data from other devices which are monitoring condition of the system. The device uses the data to make a decision how to control another devices. And then the device gives more than one instruction that controls other devices. If it took time for data to reach, they could not be associated. The travel time of data from the device to the other device is demanded within 1 second at least.

A part of the operation, like control of these system, maintenance, and the environmental monitoring, is consigned to an external organization. Agents who are consigned walk around the plant to get their information, or watch the plant from a remote site.

4. Requirements

This section listed requirements derived from the previous section. R-1, R-2, R-3 and R-4 are related to the management of the divided system. R-5, R-6 and R-7 are related to the restriction to the industrial network.

R-1 It is necessary to partition a management domain into some domains. Or it is necessary to delegate a management authority to another independent management domain.

R-2 It is necessary to allow different independent management domains to coexist on the same network because two or more organizations need to enter into the system and to management it.

R-3 It is necessary that a device controls other devices that belong to a different domain.

R-4 It is necessary to consider that a device is not always geographically or network topologically close to the other
devices even when the devices belong to a same management domain.

R-5 It is demanded to reduce the management cost as much as possible.

R-6 It is necessary to consider the processing performance of the device. And, it is necessary to suppress the power consumption of the device.

R-7 It is necessary to consider bandwidth of the communication.

5. Issues

This section lists the issues in the cross-realm operation when we apply the Kerberos version 5 into the system described in the section 3, and consider the system applied the Kerberos with the requirements described in the section 4.

5.1. Unreliability of authentication chain

When the relationship of trust is constructed like a chain or hierarchical, the authentication path is not dependable since it strongly depends on intermediary realms that might not be under the same authority. If any of the realms in the authentication path is not available, then the principals of the end-realms can not perform the cross-realm operation.

The end-point realms do not have full control and responsibility of the success of the operations even if their respective KDCs are fully functional. Dependability of a system decreases if the system relies on uncontrolled components. We can not be sure at 100% about the result of the authentication since we do not know how is it going in intermediary realms.

This issue will happen as a by-product of a result meeting the requirements R-1 and R-2.

5.2. No PFS in case of the indirect trust model

In [SPECCROSS], any KDC in the authentication path can learn the session key that will be used between the client and the desired service. This means that any intermediary realm is able to spoof the identity either of the service or the client as well as to eavesdrop on the communication between the client and the server.
This issue will happen as a by-product of a result meeting the requirements R-1 and R-2.

5.3. Scalability of the direct trust model

In the direct relationship of trust between each realm, the realms involved in the cross-realm operation share keys and their respective TGS principals are registered in each other’s KDC. When direct trust relationships are used, the KDC of each realm must maintain keys with all foreign realms. This can become a cumbersome task when the number of realms increase. This also increases maintenance cost.

This issue will happen as a by-product of a result meeting the requirements R-1, R-2 and R-5.

5.4. Exposure to DoS Attacks

One of the assumptions made when allowing the cross-realm operation in Kerberos is that users can communicate with KDCs located in remote realms. This practice introduces security threats because KDCs are open to the public network. Administrators may think of restricting the access to the KDC to the trusted realms only. However, this approach is not scalable and does not really protect the KDC. Indeed, when the remote realms have several IP prefixes (e.g. control centers or outsourcing companies, located worldwide), then the administrator of the local KDC must collect the list of prefixes that belong to these organizations. The filtering rules must then explicitly allow the incoming traffic from any host that belongs to one of these prefixes. This makes the administrator’s tasks more complicated and prone to human errors. And also, the maintenance cost increases. On the other hand, when ranges of external IP addresses are allowed to communicate with the KDC, the risk of becoming the target of attacks from remote malicious users increases.

5.5. Client’s performance

In the cross-realm operation, Kerberos clients have to perform TGS exchanges with all the KDCs in the trust path, including the home KDC and the target KDC. TGS exchange requires cryptographic operations. This exchange demands important processing time especially when the client has limited computational capabilities. The overhead of these cross-realm exchanges grows into unacceptable delays.

We ported the MIT Kerberos library (version 1.2.4), implemented a Kerberos client on our original board with H8 (16-bit, 20MHz), and
measured the process time of each Kerberos message [KRBIMPL]. It takes 195 milliseconds to perform a TGS exchange with the on-board H/W crypto engine. Indeed, this result seems reasonable to the requirement of the response time for the control network. However, we did not modify the clock speed of the H8 during our measurement. The processing time must be slower in a real environment because H8 is used with lowered clock speed in such system. Also, the delays can grow to unacceptable delays when the number of intermediary realms increases.

This issue will happen as a by-product of a result meeting the requirements R-1, R-2, R-6 and R-7.

5.6. Pre-authentication problem in roaming scenarios

In roaming scenarios, the client needs to contact her home KDC to obtain a cross-realm TGT for the local (or visited) realm. However, the policy of the network access providers or the gateway in the local network usually does not allow clients to communicate with hosts in the Internet unless they provide valid authentication credentials. In this manner, the client encounters a chicken-and-egg problem where two resources are interdependent; the Internet connection is needed to contact the home KDC and for obtaining credentials, and on the other hand, the Internet connection is only granted for clients who have valid credentials. As a result, the Kerberos protocol can not be used as it is for authenticating roaming clients requesting network access.

This issue will happen as a result meeting the requirements R-3 and R-4.

6. Implementation consideration

This document just describes issues of the cross-realm operation in the specific systems. However, there are important matters to be considered, when we solve these issues and implement solution. Solution must not introduce new problem. Solution should use existing components or protocols as much as possible, should not introduce any definition of new component. Solution must not require a KDC to have any additional process. You must not forget that there would be a trade-off matter anytime. So an implementation may not solve all of the problems stated in this document.
7. IANA Considerations

This document makes no request of IANA.

8. Security Considerations

This document just clarifies some issues of the cross-realm operation of the Kerberos V system. There is especially not describing security. Some troubles might be caused to your system by malicious user who misuses the description of this document if it dares to say.

9. Acknowledgments

The authors are very grateful to Nobuo Okabe, Kazunori Miyazawa, Ken’ichi Kamada and Atsushi Inoue. They gave us lots of comments and input for this document.

10. References

10.1. Normative References


10.2. Informative References


S.Sakane, et al. [Page 11]
[SHELLCHEM]  http://www.shellchemicals.com/home/1,1098,-1,00.html


Authors' Addresses

Shoichi Sakane
Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi,
Tokyo  180-8750 Japan
E-mail: Shouichi.Sakane@jp.yokogawa.com,

Saber Zrelli
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi,
Ishikawa  923-1292 Japan
E-mail: zrelli@jaist.ac.jp

Masahiro Ishiyama
Toshiba Corporation
1, komukai-toshiba-cho, Saiwai-ku,
Kawasaki  212-8582 Japan
E-mail: masahiro@isl.rdc.toshiba.co.jp

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.