What are the problems of Cross-realm ?

Shoichi Sakane

Shouichi.Sakane@jp.yokogawa.com

The 69th IETF meeting

Purpose of this slot

- To introduce issues of cross-realm operation
- To review by the working group member
- To get a consensus of what is problems to be solved.

Current Problem statement

- draft-sakane-krb-cross-problem-statement-03.txt
- Introduced actual environments.
- Specified requirements and constraints.
- Defined issues.

Issues that are defined

1. Client's Performance
2. Unreliability of authentication chain
3. No PFS
4. Scalability of direct trust model
5. Exposure to DoS attacks
6. Applicability to roaming scenario

Client's performance

- Client must perform TGS exchange with each KDC until reaching the final KDC.
- TGS exchanges demands important processing time for a client.
- In particular, the overhead can not ignore for a resource limited device.

Processing time of Kerberos on embedded devices

CPU	DS5250 (8051 arch., 8-bit, 22MHz, w/ DES H/W)	H8 (16-bit, 20MHz) + Crypt H/W (AES, 3DES, SHA1, MD5)			
Krb lib	MIT-1.2.4	MIT-1.2.4		Original	
Crypt H/W	Enable	Enable	Disable	Enable	Disable
AS	4650ms	74ms	106ms	26ms	74ms
TGS	4579ms	195ms	294ms	49ms	178ms

Including waiting time

Excluding waiting time

measured by Yokogawa Electric Corporation 04 through 06

Unreliability of authentication chain

- Cross-realm operation allows to construct a chain or a hierarchical of trust.
- When an intermediary KDC downs, the authentication procedure will fail.
- The end-realms can not have responsibility.

No PFS

- Any KDC in the authentication path can learn the session key.
- The KDC is able to spoof the identity either of the server or the client.

Scalability of direct trust model

- Cross-realm operation allows to make a direct authentication path.
- KDCs need to maintain each inter-realm key.
- It obviously increases maintenance cost.

Exposure to DoS attack

KDC handles TGS exchanges with clients from different realms.

KDC is typically exposured.

An administrator has to configure proper filtering rules.

But, it is not easy to set up filters.

Applicability to roaming scenario

Client may need to access its home KDC.

The policy requires a client to have a credential before accessing to the outside of the realm.

Client can not access to home KDC from the visited realm due to chiken-and-egg problem.

Questions

- **Are they all of issues ?**
- **What is problem to be solved ?**
- **Can the problem statement be a working group document ?**

End of presentaion