Problem statements on cross-realm authentication

Shoichi Sakane

Shouichi.Sakane@jp.yokogawa.com

The 66th IETF meeting

Purpose of this presentation

- Not presentation of our extension.
  draft-zrelli-krb-xkdcp-00.txt

- We would like to share the problems on cross-realm authentication with everyone here.

- Next step, we can discuss to solve the problems.
  Our extension could be one of solutions.

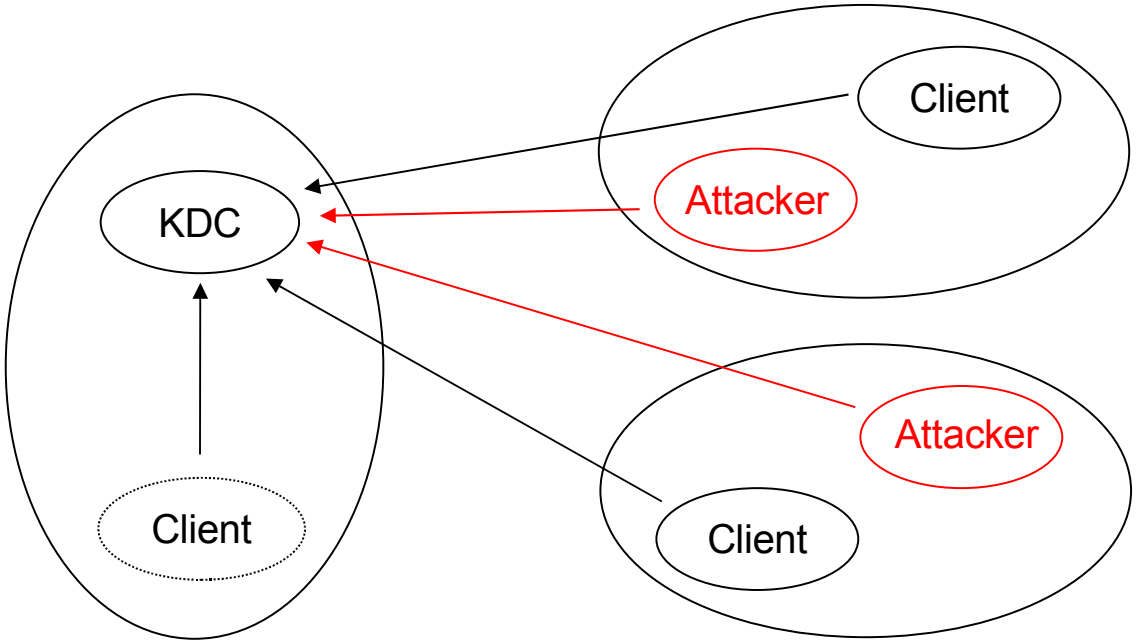
Problems

1. Security
2. Reliability
3. Performance
4. Applicability

Exposure to DoS attack

Not easy to set up filters to protect KDC.

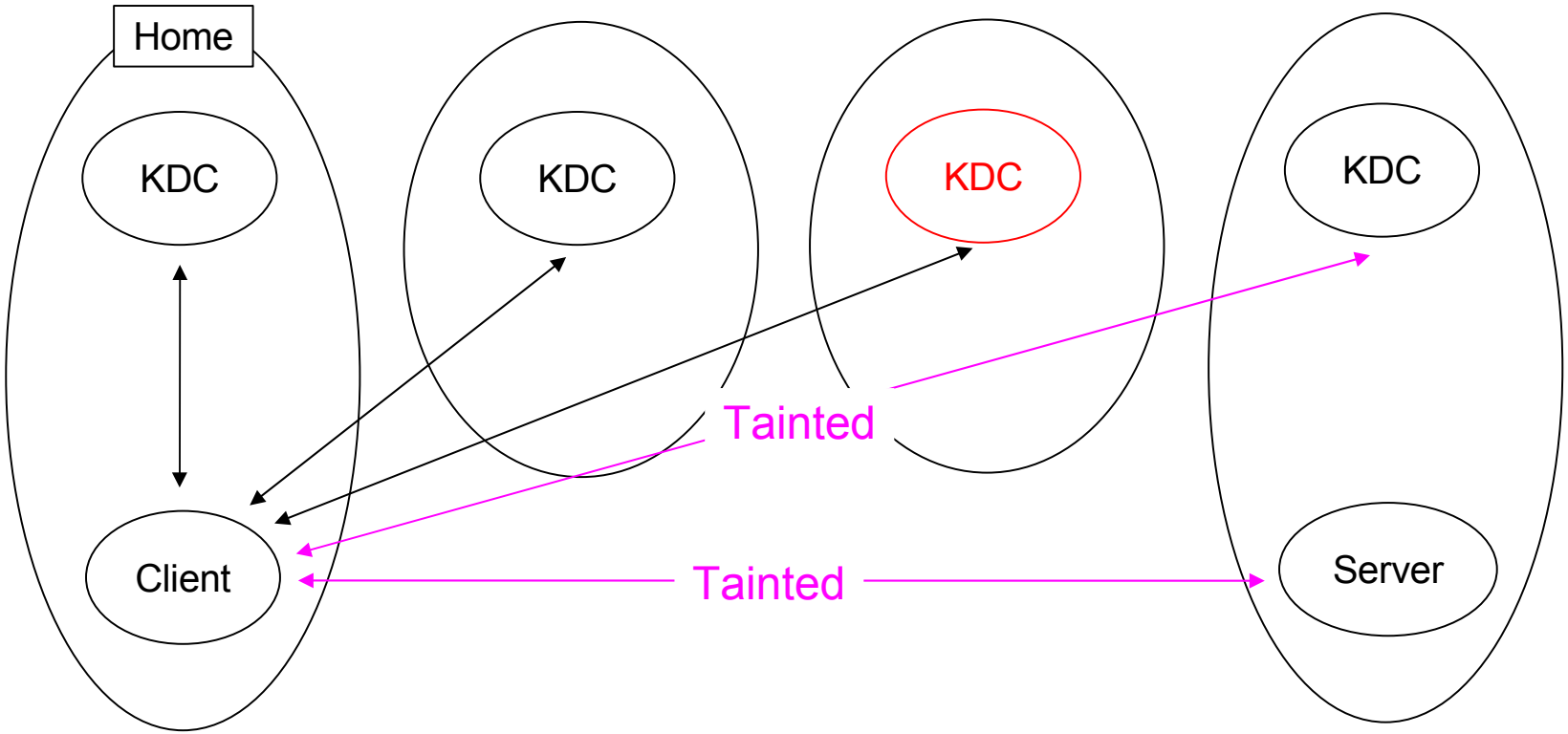
- KDC handles TGS exchanges with remote clients from different realms.



No PFS

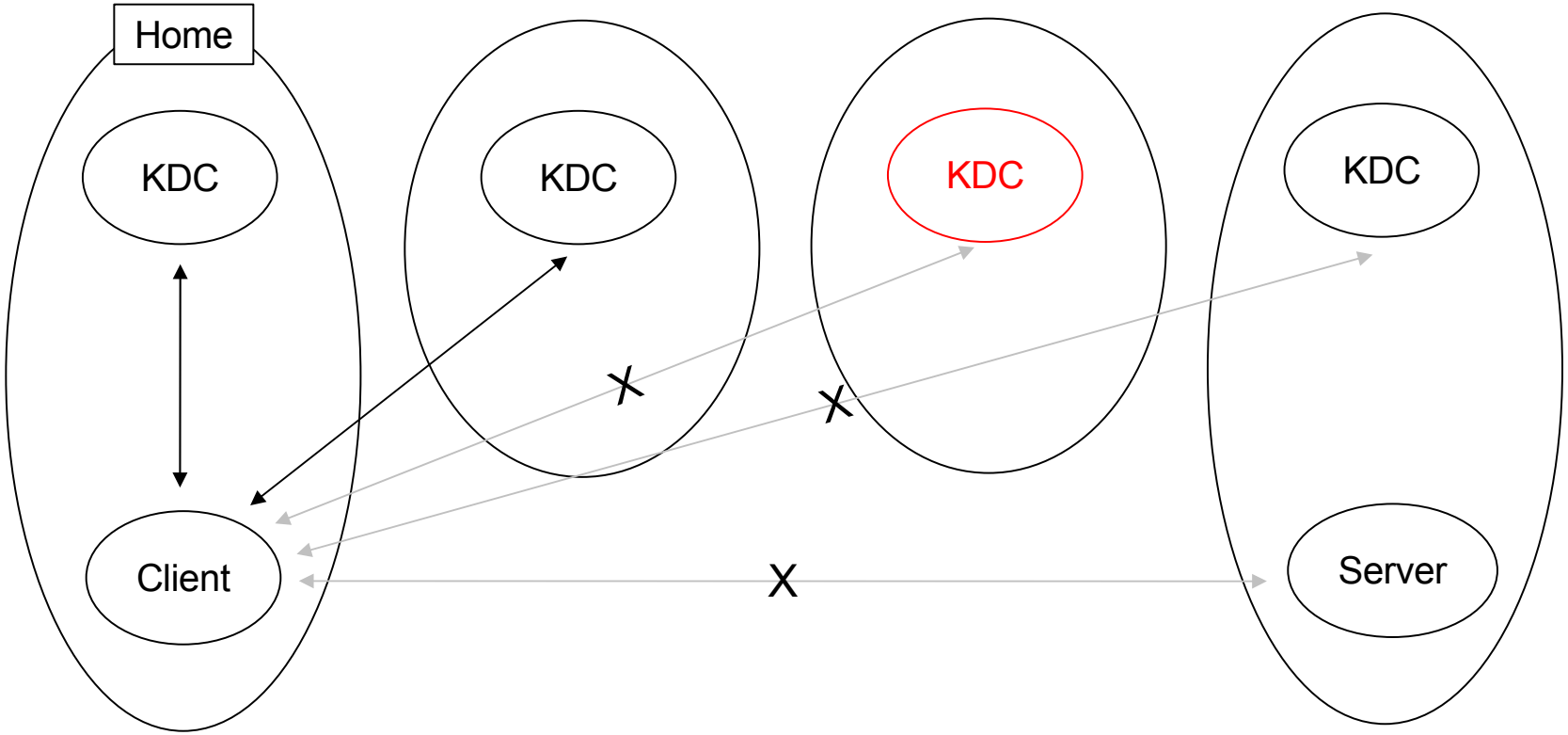
Intermediary KDCs can learn session keys.

ref. "Specifying Kerberos 5 Cross-Realm Authentication", Fifth Workshop on Issues in the Theory of Security, Jan 2005.



Reliability of chain

Intermediary KDC down cause authentication failed.



Client's performance

Client centralized exchanges causes unacceptable delay.

- Client must perform TGS exchange with each KDC of the trust path.

→Not scalable if number of realms increases especially for small/embedded devices.

Processing time of Kerberos on embedded devices

measured by Yokogawa Electric Corporation 04 through 06

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
TGT	4650ms	74ms	106ms	26ms	74ms
TGS	4579ms	195ms	294ms	49ms	178ms

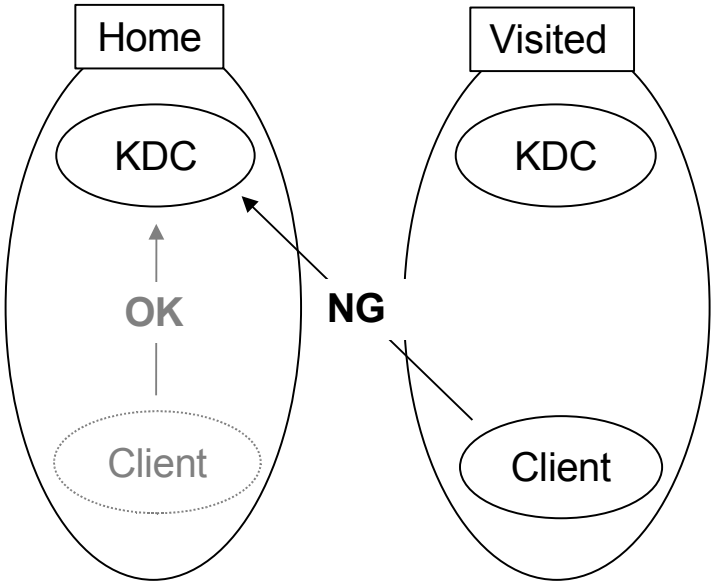
Including waiting time

Excluding waiting time

Applicability to roaming scenario

Roaming users can not access to home KDC from the visited realm.

- due to the policy of the realms.
- due to chiken-and-egg problem.



Summary of problems

1. Security issues
   - KDC is exposured to DoS attack from the Internet.
   - Intermediary KDCs can learn session keys.
2. Reliability of chain
   - Interealm KDC down causes authentication fails.
3. Client's Performance
   - client centralized exchanges cause unaccesptable delay.
4. Applicability to roaming scenario
   - Roaming users can not access to her home KDC.

Conclusion

- There are some problems to be solved in cross-realm environment.
- Let's consider real environment to more deploy Kerberos system.
  - What are the problems ?
  - What problems should be solved ?
  - What technologies do we need ?

End of presentaion