Applying Kerberos to the Communication Environment for Information Appliances

Shoichi SAKANE and Nobuo OKABE (Yokogawa Electric Corporation)
Ken-ichi KAMADA and Hiroshi Esaki (The University of Tokyo)

Contents

- Background and our forcus
- Requirements
- Applying Kerberos to the environment
- Future study items
- Conclusions

Background and our forcus

- IPv6 technology can assign global addresses to lots of devices.
- Network capability will be implemented on the home appliances.
- This environment will challenge a set of new requirements.
- We focus on the security of the home appliances.

Requirements

- Access control between devices must be achieved.
- Secured IP address resolution should be needed.
- Setting up secured communication is mandatory.

Access control

- Access control is obviously required.
- It is not restricted by network topology.
- Access control should not depend on IP addresses.
- Restricted devices should access to the home appliances.

Secured IP address resolution

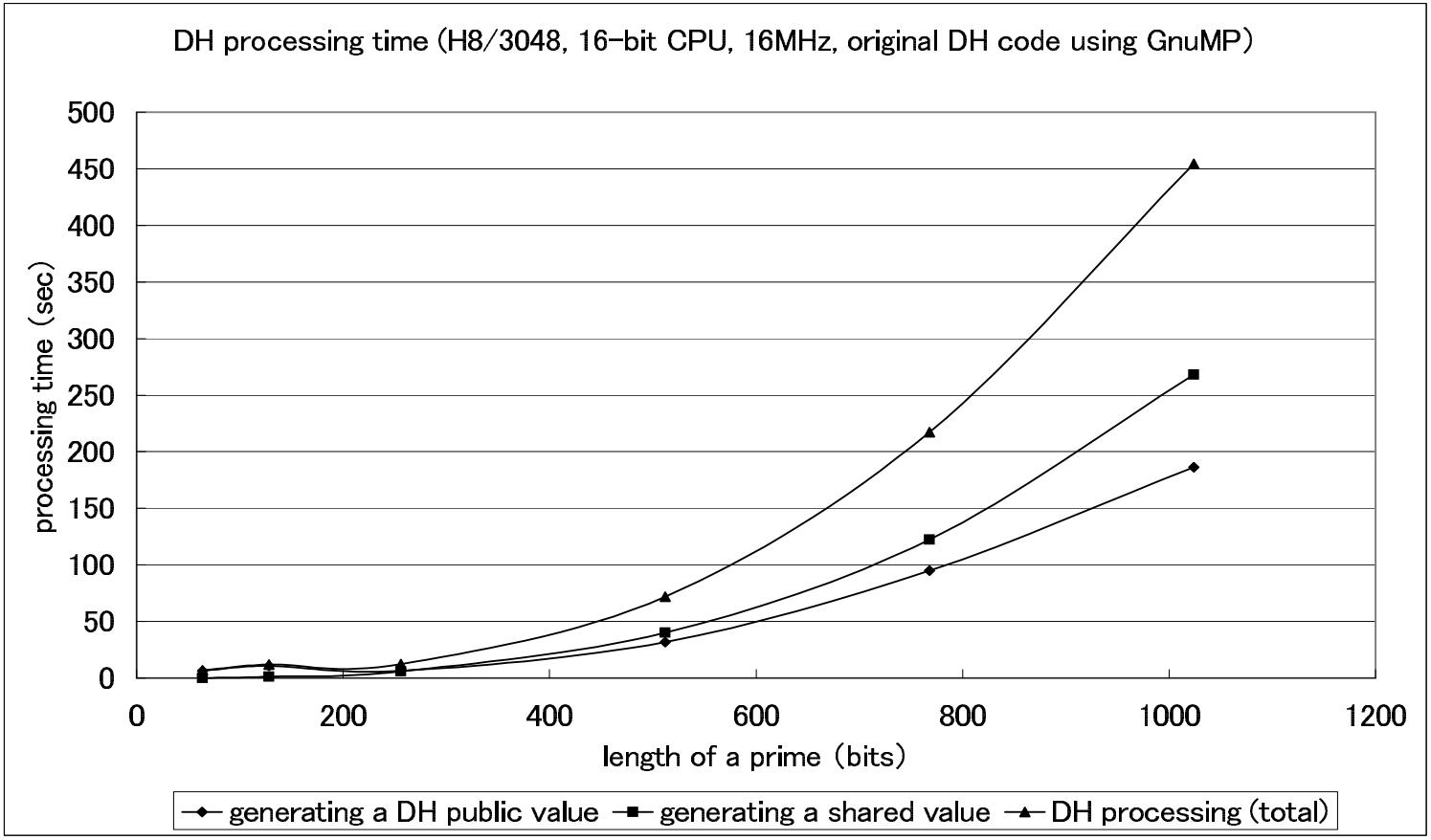
- IPv6 automatically generate the IP addresses of the devices.
- The device has to resolve the auto-configured IP addresses.
- This address resolution procedure must be performed securely.

Setting up secure communication

- The secured communication is required.
- IPsec provides confidentiality and integrity.
- The peering communicating devices have to share a symmetric key
- IPSEC-WG has standardized IKE based on asymmetric cryptography

Computational cost of asymmetric cryptography

- IKE is not suitable for the cost-sensitive devices.
- We need to define the other key exchange mechanism.



Applying Kerberos to the environment

What is Kerbros ?

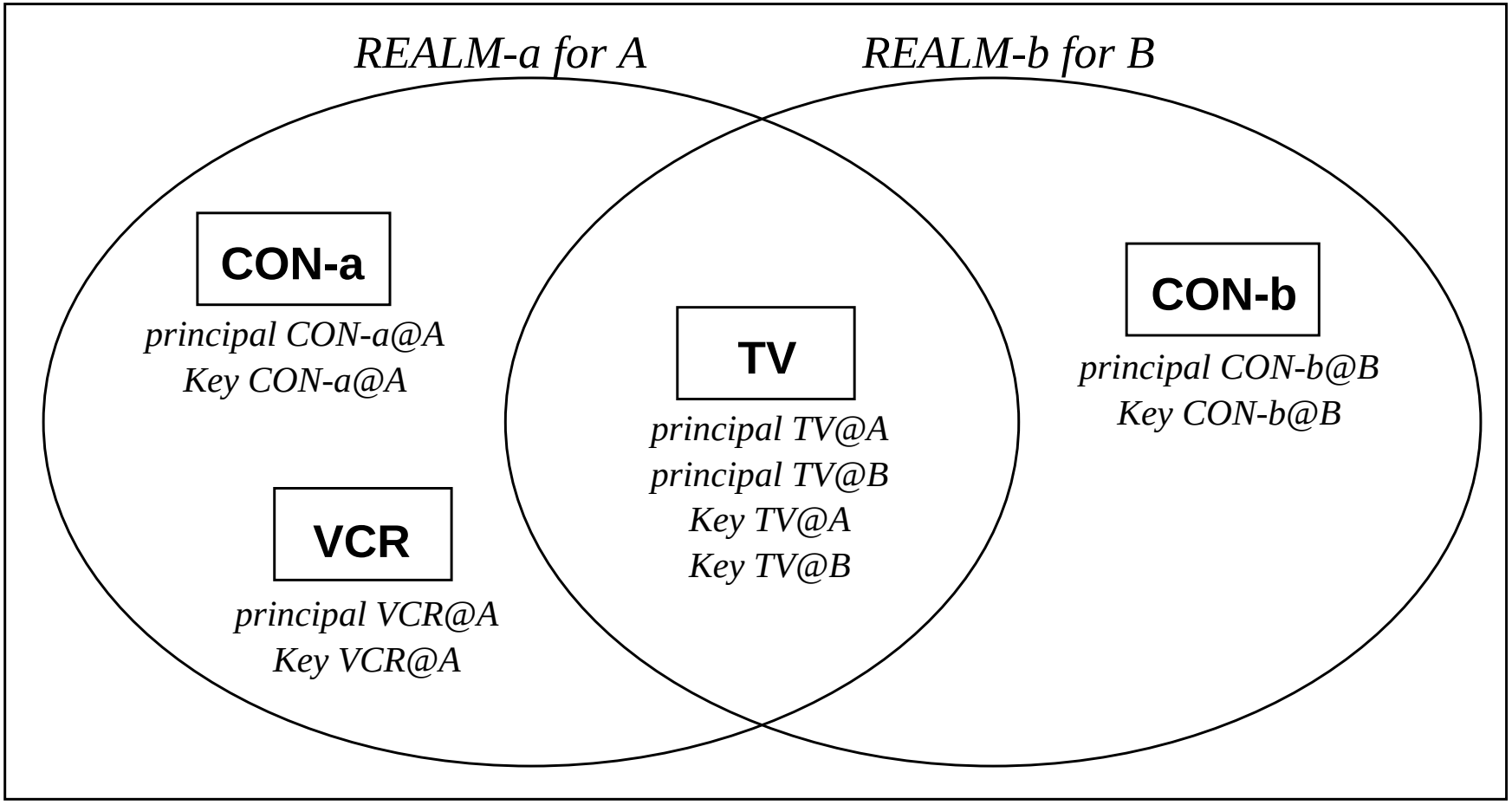
- Based on symmetric cryptography.
- Authenticating the nodes and to encrypt the communication between them.
  - Independent of the authentication system in the host OS.
  - Independent of IP addresses.
  - Independent of any network topology.
- Compatible with the cost-sensitive devices.

What is Kerbros ?

- Maintain the information of devices on the central server (KDC).
- The number of devices in the home network could be small.
- The centralized management model is appropriate.

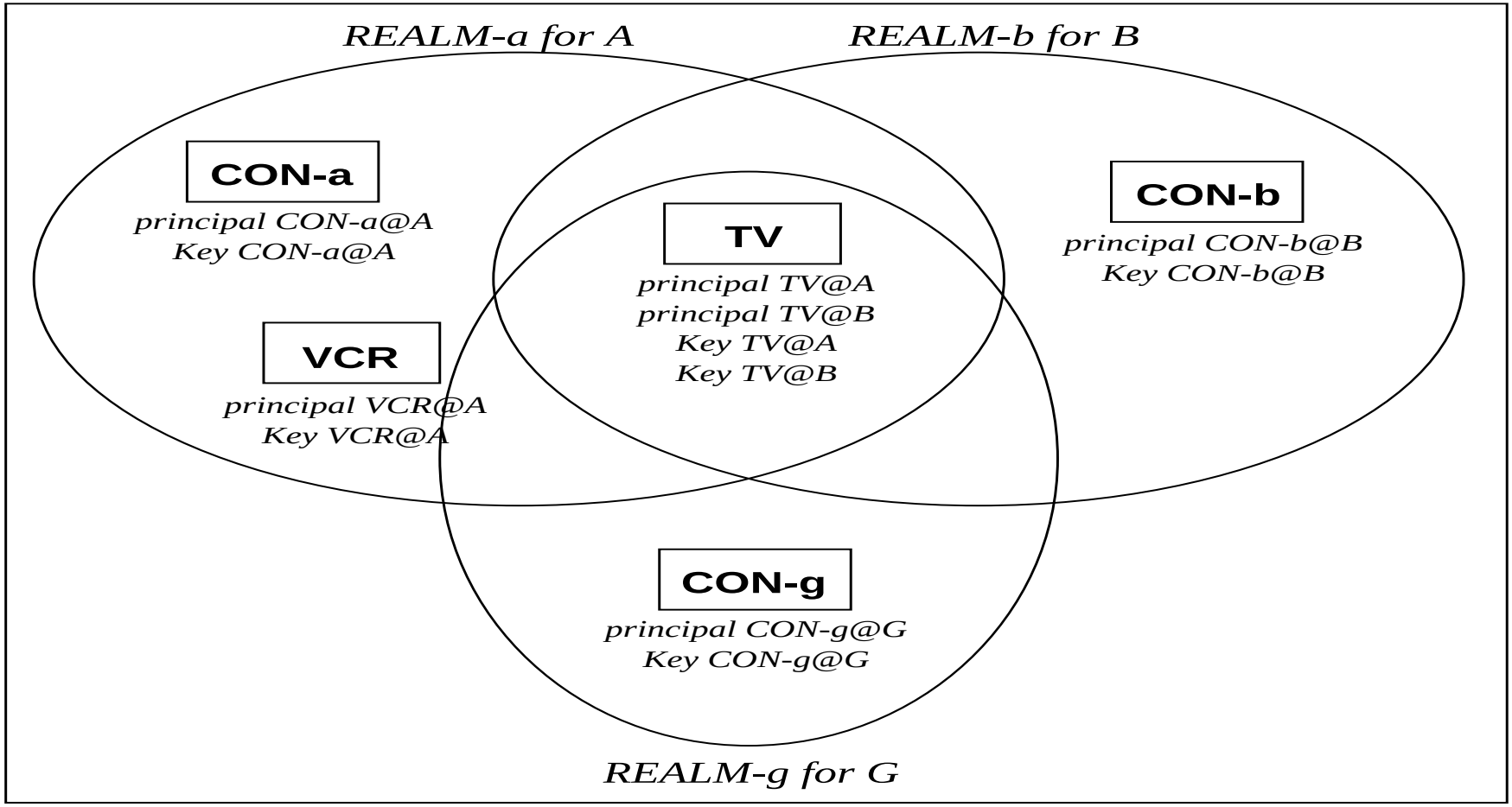
Access control

- Access control is achived by the fundamental function of Kerberos.



Access control of guest devices

- Access control of a guest is achived by the another realm.

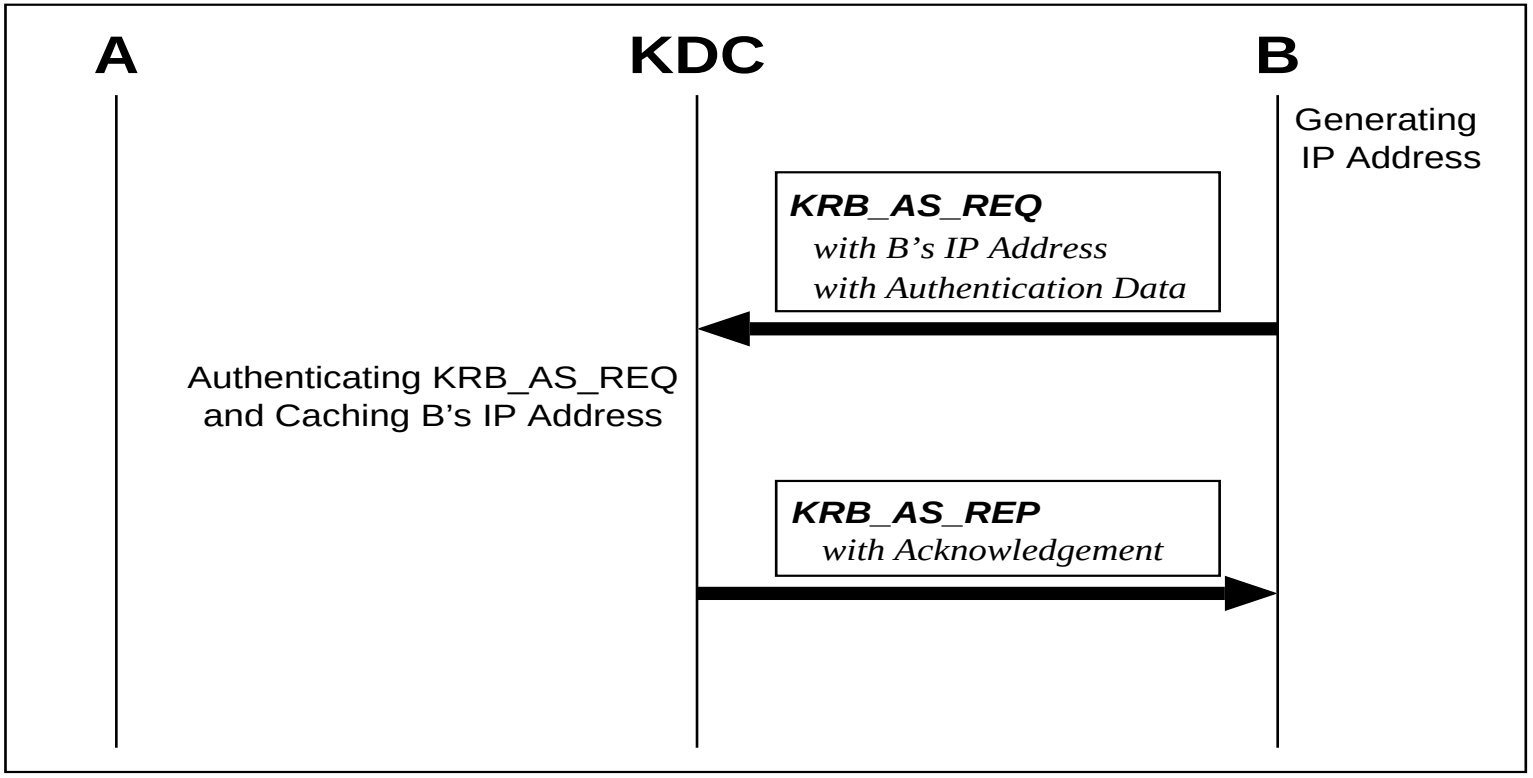


Secured IP address resolution

- The KDC could replace the name server.
- KRB_AS_REQ is sent to the KDC when the devices connect to the network.
  - It could be used to register the IP address to the KDC.
- KRB_TGS_REQ is sent to the KDC when the devices initiate a communication with the other.
  - It could be used to resolve IP addresses.

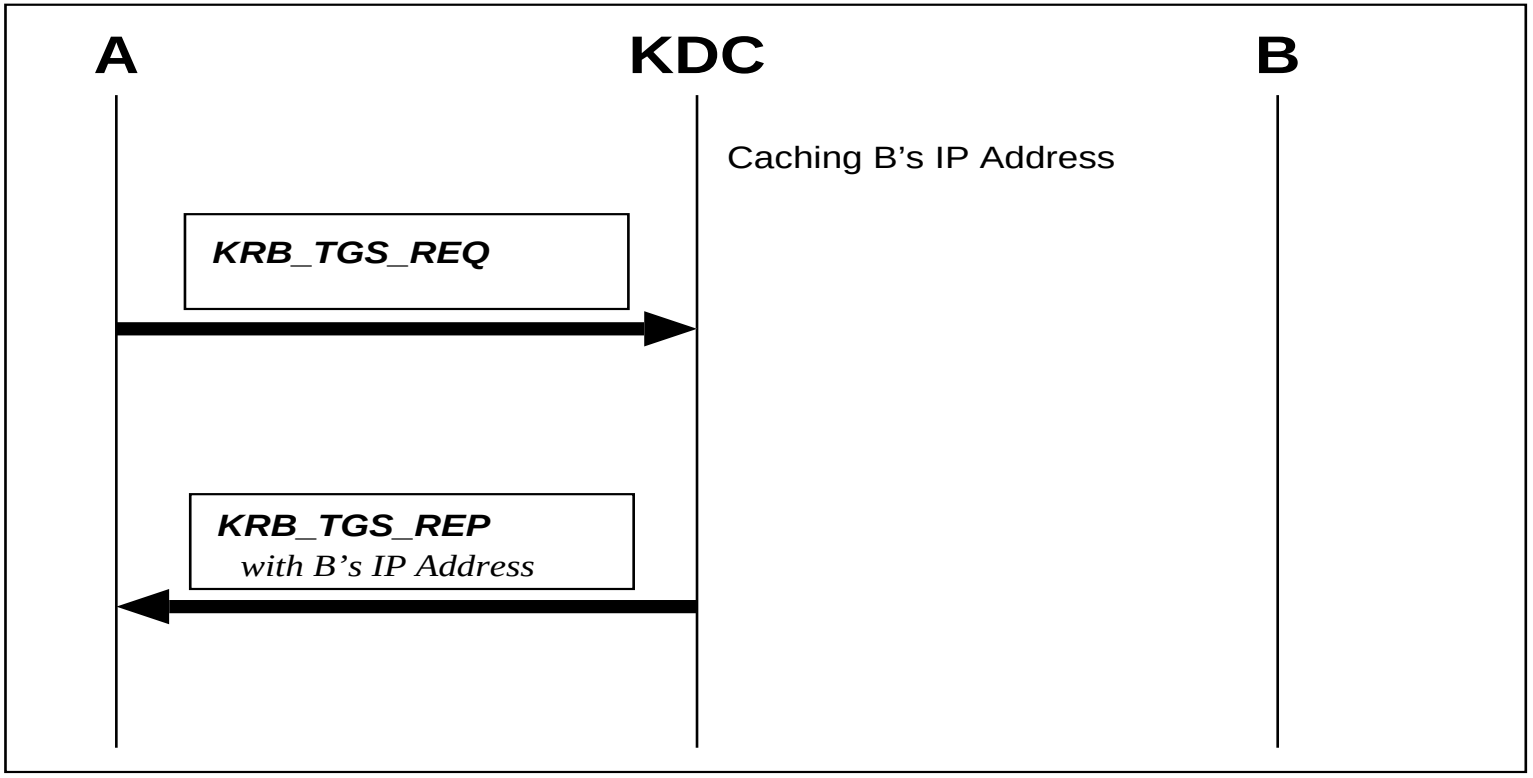
Registering IP address

- There is a message called KRB_AS_REQ when the devices connect to the network.



Resolving IP address

- There is a message called KRB_TGS_REQ when the device start to communicate with the other.



Modification to Kerberos

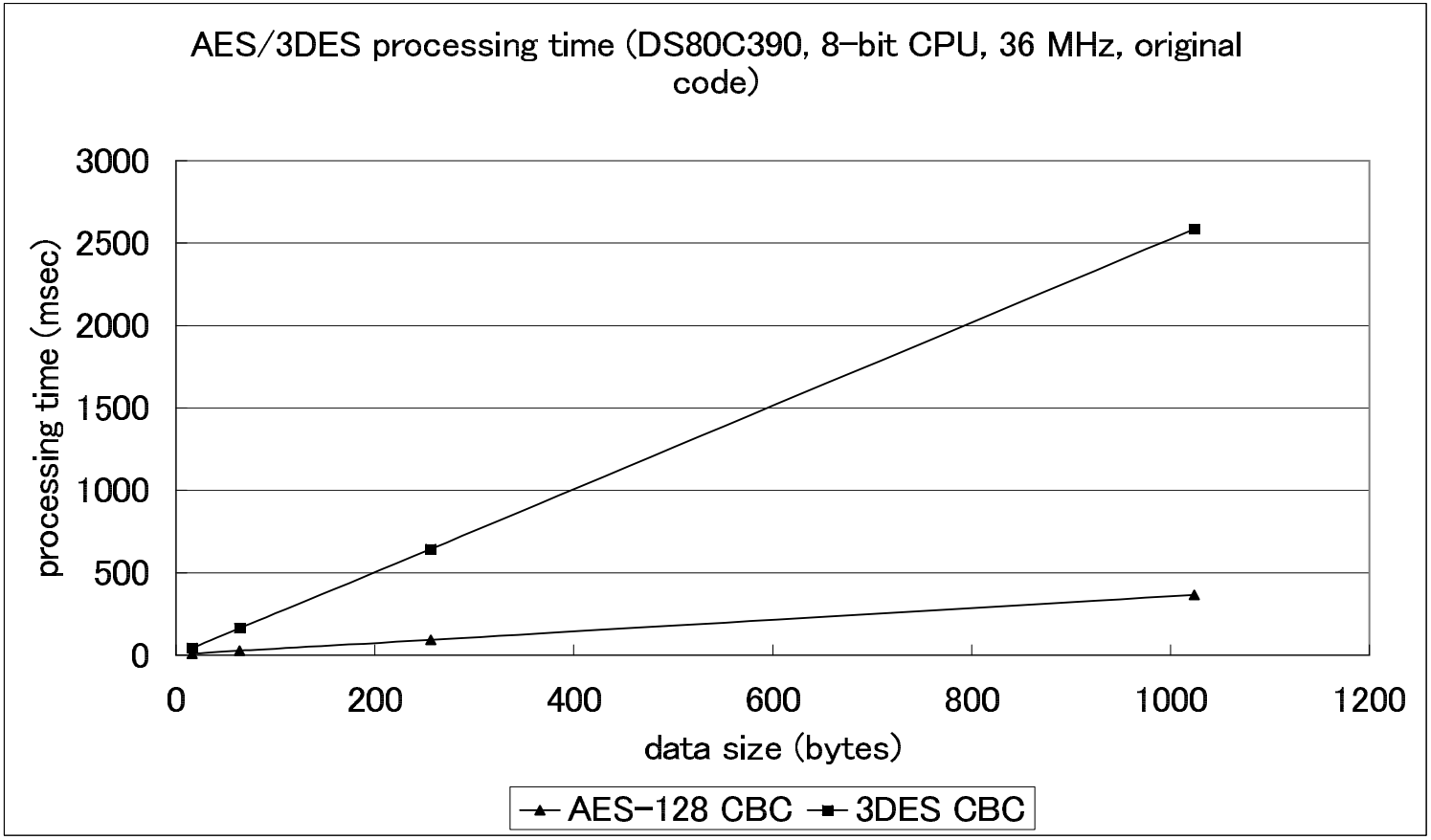
- The optional field containing IP addresses in KRB_AS_REQ must be used.
- The field containing IP addresses in KRB_TGS_REP must be added.
  - There is no address field defined in KRB_TGS_REP message.

Sharing a symmetric key by KINK

- KINK is based on Kerbros.
- It means that KINK is based on symmetric cryptography.
- The required computational cost will be significantly lower than asymmetric cryptography.

Computational cost of symmetric cryptography

- KINK can be suitable for the cost-sensitive devices.
- We propose KINK to share a symmetric key for network appliances.



Future study items

The inter-realm communication of Kerberos.

- Some devices belong to only each individual.
- For example, IP phones belong the different realms
- However an IP phone needs to communicate with the other phones.
- The inter-realm communication of Kerberos is required in this case.

Achieving integirty depends on the internal clock.

- The authentication method of some Kerberos messages should be improved.
- Because it depends on accuracy of the internal clock of the devices.
- We can not trust the clock of the cost-sensitive or physically-restricted devices.
- We need to improvement the method of achieving integrity.

Consider IP addressses to be registered

- A node can have several IP addresses.
- There are some scopes in IPv6 address architecture.
- There is a possibility that the communication will be impossible.
- We must consider which address to be registered to the KDC.

Conclusions

- The requirements for Information appliances
  - Access control
  - Plug and play
  - Secure communication
- Kerberos proposed in order to achieve above requirements
  - Access control by using separated realms.
  - The address resolution mechanism with modified messages of Kerbero
  - KINK as the method to establish secure communication.
- We described some future study items
  - The inter-realm communication of Kerberos is required in this case.
  - We need to improvement the method of achieving integrity.
  - Consider IP addressses to be registered to KDC.

That’it.

Why IPsec ?

- Why we have choiced IPsec for securing the end-end communication.
- IPsec has been choiced by elimination.

Why IPsec ?

- proprietary methods should not used.
  - we should choice an open standard.
  - it is not easy to design security protocols for each application.
  - some closed environments might choice this way.
- SSL, SSH might not be used.
  - these methods only protect the communication on TCP.
  - asymmetric cryptography could not be suitable for home appliances.
- IPsec
  - it could protect the communication on IP.
  - however it requires some light key configuration methods for home appliances.
  - other protection method could be used on IPsec or without using IPsec.