Kerberos

System Design in V5

Data Presentation

- V4 has fixed layout, variable length fields
- V5 uses ISO Standard ASN.1 syntax with Basic Encoding Rules
- ASN.1 gives flexibility at cost of overhead
- e.g. V4 address 4 octets, V5 address 11 octets

Names

- V4 { Name, Instance, Realm} 40 characters
- V5 {Name, Realm} V5 name contains instance
- V4 names are DNS (Domain Naming Service from Internet)
- V5 Names are DNS or X.500

Delegation of Rights (I)

- Not permitted in V4
- V5 allows KDCs to issue TGTs to resources with addresses which differ from requester's address or with no specified addresses
- TGT can then be passed to delegates with specified addresses
- Issuing/accepting *no address* TGTs is policy decision for KDC and servers

Delegation of Rights (II)

- V5 TGTs have flags for delegation permissions
- A *forwardable* TGT may be exchanged for a TGT with different network address and it may allow new TGT to be forwarded further
- A *proxiable* TGT may be used to obtain tickets with different network address – tickets are *proxy* tickets
- Applications may refuse delegated tickets

Ticket Lifetimes

- V4 ticket lifetime ≤ 21 hours (1 octet in units of 5 minutes)
- V5 timestamp 17 octets – virtually unlimited lifetime in units of s
- Tickets contain
  -Start-time
  -End-time
  -Authtime (time of initial login)
  -Renew-till

Renewable Tickets

- Renewable tickets are potentially longlasting but require regular renewal from KDC
- Late tickets cannot be renewed
- Tickets may be renewed up until Renew-till time- latest legal end-time

Postdated Tickets

- Postdated tickets become valid at start-time
- Validity is confirmed by KDC which removes *Invalid* flag on ticket
- A *postdated* flag in TGT allows KDC to postdate

Key Versions

- Similar in principle to V4
- V5 KDCs need to remember multiple key versions to allow for renewable and postdated tickets

Other Features of V5

- A user may be registered in several realms with same password but different master keys (Realm name used in password hash)
- Double encryption and redundant fields removed
- Many cryptographic algorithms supported
- Cryptographic weaknesses repaired

Integrity – Only Algorithms (I)

- V5 offers choice of algorithms (3 required and 2 optional)
- Security as strong as weakest algorithm
- Algorithms are not negotiated – compatibility could be an issue
- Choice today would probably be
  HMAC-SHA-1

Integrity Only Algorithms (II)

- Required
  - rsa-md5-des - a combination of MD5 and DES
  - des-mac - based entirely on DES
  - des-mac-k - based on DES but using the same key twice (undesirable but required for backward compatibility)
- Optional – two based on MD4 and DES of which one uses the same key twice

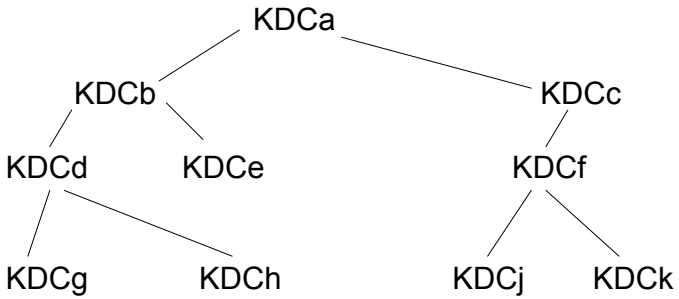
Encryption for Privacy and Integrity

- Employs checksum followed by encryption
- Checksum may be MD4, MD5 or CRC-32
- Encryption is DES CBC, IV = 0

Hierarchy of Realms (I)

- V4 inter realm comms requires each KDC to have all other KDCs as principals
- V5 supports realm hierarchy
- Each V5 realm shares keys with children and parent
- May be possible to identify path from syntax of names

Hierarchy of Names (II)



Path from KDCs g-k is g-d-b-a-c-f-k

Hierarchy of Names (III)

- Some KDCs in path may be untrustworthy
- V5 requires path KDCs to be named in transited field
- Normally shortest path is safest
- Each network user/resource must exercise policy in regard to transited realms

PKINIT – Public Keys for Users

- Provides bridge between future public keys for users and legacy private key systems
- PKINIT allows public key authentication for tickets or TGTs obtained from a KDC
- User's public key replaces master key in KDC database

V5 KDC Database

- name (principal)
- key (principal master)
- p_kvno (prpl key vn)
- max_life (prpl tickets)
- max_renewable_life
- k_kvno (KDC key vn)
- expiration (data)
- mod_date (data)
- mod_name (prcpl dat)
- flags (KDC policy)
- password expiration
- last_pwd_change
- last_success (login)