IK2206 – Internet Security and Privacy
Chapter 14 – Kerberos V5

14.1 ASN.1

- What is ASN.1, and why was it introduced In Kerberos V5?

  ASN.1 is a data representation language standardized by ISO. It is popular among spec writers and standards bodies because it gives people a way to precisely define data structures without worrying about different data representations, such as bit and octet order, on different machines

  Kerberos V5 uses ASN.1 in order to make it easier for fields to be optional, of varying length, and tagged with type information to allow future versions to include additional encodings.

14.2 Names

- What is the difference between V4 and V5 names?

  Data representation: Kerberos V5 uses ASN.1 where Kerberos V4 uses fixed layouts. V5 is therefore more flexible but creates the disadvantage of resource overheads.

  V4: principal is named by the three fields NAME, INSTANCE, REALM, which is a text string up to 40 characters. → size of these fields is too short for some environments.

  V5: two components REALM and the NAME (contains a type and a varying number of arbitrary strings)

  In V4 Realms are DNS standard names, whereas in V5 they can be DNS standard names or X.500 names.

  Integrity protection: Kerberos V4 uses mathematically questionable checksum functions whereas Kerberos V5 uses MD4, MD5, DES-MAC…

  Kerberos V5 introduces identity impersonation and delegation of rights.

  Kerberos V5 tickets can live longer than in V4. (Is this preferable? – I don't think so…)

14.3 Delegation of Rights

- What are the benefits of allowing delegation?

  Delegation of rights is the ability to give someone else access to things you are authorized to access.

Delegation is a feature of Kerberos authentication that allows a server to obtain a Kerberos ticket on behalf of a user without ever having access to the end user's password. This functionality allows Kerberos to solve typical "double-hop" authentication problems where a user's credentials need to flow through multiple levels in an n-tier architecture (Web Server → Domain Controller → SQL Server)

http://www.adopenstatic.com/cs/blogs/ken/archive/2007/01/28/1282.aspx

- What are the potential problems of allowing delegation?

  If we delegate too many rights another account is able to misuse our rights.

- Is it possible to delegate rights in Kerberos v4, and if so, how?

  It is not possible, because the ticket contains a network layer address.

- How can rights be delegated in Kerberos v5

  It allows Alice to ask for a TGT with a network layer address different from hers.

14.4 Ticket Lifetimes

- What's the difference in ticket lifetimes between v4 and v5?

  In V4, the maximum lifetime of a ticket is 21 hours. In Kerberos V5, tickets can be issued with virtually unlimited lifetimes.

- Is there a problem with allowing long lifetimes?

  Yes, because once created they cannot be revoked.

- Why would you make a ticket renewable, instead of just giving it a long lifetime?

  Renewing a ticket involves giving the ticket to the KDC and having the KDC reissue it.

- What can postdated tickets be used for?

  Postdated tickets are used to run a batch job at some time in the future. Kerberos V5 allows a ticket to become valid at some point in the future (using START-TIME timestamp).

14.5 Key Versions (SKIP)

14.6 Making Master Keys in Different Realms Different (SKIP)

14.7 Optimizations (SKIP)

14.8 Cryptographic Algorithms (BRIEFLY)

14.8.1.1-5 Details not important.

- Why are multiple algorithms used in V5?

  DES is not secure enough for high-security environments. U.S. government does not allow exporting DES because it is too secure.

14.9 Hierarchy of Realms (BRIEFLY)

- Why is a hierarchy desirable?

  If realm names were just unstructured strings, it would be difficult to find a path. It is possible to take the shortest path through the tree, you only have to find the lowest common ancestor.

14.10 Evading Password-Guessing Attacks (BRIEFLY)

- How can a password-guessing attack be imposed in V4?

  There is no authentication of the request to the KDC for a TGT. Anyone can send a cleartext message to the KDC requesting a TGT. Since the function that maps a password string to a DES key is publicly known, an intruder can use the encrypted credentials for an off-line password guessing attack to find the password (of the finally recipient of our initial request)

- How can it be thwarted in V5?

  Information known as preauthentication-data can be sent along with the request for a TGT for user Pope which proves that the request knew user Pope's master key. The preauthentication data consists of a current timestamp encrypted with user Pope's master key.

14.11-14.14 (SKIP)

14.15 KerberosV5 Messages (VERY BRIEFLY)

You should have an idea of what the messages are, and what goes into these messages, but you need not remember the exact formats