Kerberos V5

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-07/

- Kerberos V4 Issues
- ASN.1 and BER
- Names, Delegation of Rights
- Ticket Lifetimes
- Cryptographic Algorithms
- Hierarchy of Realms

Kerberos V4 Issues

1. Names, Instance, Realm (non standard)
1. Only DES encryption
2. Only IPv4 addresses
3. Byte ordering indicated in the message (ASN.1 better)
4. Maximum life time limited to 21 hours: 8 bit life time in units of 5 minutes
5. No delegation
6. Inter-realm authentication limited to pairs $\Rightarrow N^2$ pairs
7. Double encryption of the ticket: $K_{client}[K_{server}[...]]$
8. PCBC does not detect interchange of cipher blocks
9. No subsession keys for long sessions
10. Brute force password attack