Praktikum. Protokollid.

**Kerberose protokoll**



Joonis . http://www.kerberos.org/software/tutorial.html

Kasutades oma eesnime moodustage oma ID formaadis user@REALM, näide: joe@ORIONSPORTS.COM

|  |
| --- |
|  |

Olgu KUser võtmeks (sümmeetriline võti suhtlemiseks AS serveriga) Sinu perekonnanimi:

|  |
| --- |
|  |

Olgu vajalik teenus ftp@lin2.tlu.ee,

Sinu IP number (vaata ipconfig):

Klient saadab serverisse AS järgmised asjad: oma identifikaator (user ID), teenuse ID, teenuse IP number, kestvuse aeg. Andmed ei ole krüpteeritud.

1. **AS\_REQ** = ( PrincipalClient , PrincipalService , IP\_list , Lifetime )
2. **AS\_REP** = { PrincipalService , Timestamp , Lifetime , SKTGS }KUser { TGT }KTGS

TGT = ( PrincipalClient , krbtgt/REALM@REALM , IP\_list , Timestamp , Lifetime , SKTGS ), kus

SKTGS – sessiooni võti kliendi ja TGS suhtlemiseks, olgu selleks 128 bitine juhuarv:

|  |
| --- |
|  |

KTGS – sümmeetriline võti AS ja TGS serveritevaheliseks suhtlemiseks, olgu selleks sõnast Tallinna Ylikool moodustatud 128 bitine võti:

|  |
| --- |
|  |

Põhjalik spetsifikatsioon asub aadressil: <http://tools.ietf.org/html/rfc4121>

Olgu tegu versiooniga, mis kasutab krüpteerimiseks AES algoritmi.

Moodustame sõnumid ja krüpteerime neid kasutades online abivahendit <http://www.tools4noobs.com/online_tools/encrypt/>

TGT sõnum:

|  |
| --- |
|  |

TGT krüpteeritud kujul:

|  |
| --- |
|  |

Sõnum, mis on moodustatud andmetest PrincipalService , Timestamp , Lifetime , SKTGS:

|  |
| --- |
|  |

Krüpteeritud kujul:

|  |
| --- |
|  |

1. **TGS\_REQ**

Authenticator = { PrincipalClient , Timestamp }SKTGS

TGS\_REQ = ( PrincipalService , Lifetime , Authenticator) { TGT }KTGS

SõnumAuthenticator:

|  |
| --- |
|  |

Krüpteeritud kujul:

|  |
| --- |
|  |

Sõnum TGS\_REQ tervikuna:

|  |
| --- |
|  |

## TGS\_REP

TService = ( PrincipalClient , PrincipalService , IP\_list , Timestamp , Lifetime , SKService )

TGS\_REP = { PrincipalService , Timestamp , Lifetime , SKService }SKTGS { TService }KService

Kus SKService  on sessiooni võti, juhuarv, 128 bitine:

|  |
| --- |
|  |

Timestamp (date and time (of the KDC)):

|  |
| --- |
|  |

The timestamps used in Kerberos are encoded as GeneralizedTimes(<http://en.wikipedia.org/wiki/GeneralizedTime> ). An encoding shall specify the UTC time zone (Z) and shall not include any fractional portions of the seconds. It further shall not include any separators. Example: The only valid format for UTC time 6 minutes, 27 seconds after 9 pm on 6 November 1985 is 19851106210627Z.

## AP\_REQ

Authenticator = { PrincipalClient , Timestamp }SKService

AP\_REQ = Authenticator { TService }KService

Authenticator krüpteerimata:

|  |
| --- |
|  |

Krüpteeritud kujul

|  |
| --- |
|  |