Монгол Улсын Их Сургууль
Мэдээлэл Технологийн Сургууль
Холбооны Технологын Тэнхим

Керберос-н талаар судалгаа хийх

Ангийн төсөл

Гүйцэтгэсэн_____[КСЗ Ч.Мягмарнаран]
Удирдсан багш _____[Г.Гандэмбэрэл]

Улаанбаатар 2010

Гарчиг

Оршил

Мэдээллийг нууцлах, найдвартай дамжуулал гэдэг нь маш чухал зүйл юм. Мэдээ мэдээллийг түргэн шуурхай ашиглах өнөөгийн нийгмийн маш чухал асуудал билээ. Үүнээс үүдэн тухайн мэдээ мэдээллийн аюулгүй дамжуулал гэдэг асуудал маш өндөр түвшинд хэлэлцэгдэх болсон билээ. Аюулгүй байдал хэмээх асуудлыг эхэн үедээ физик аргаар л хамгаалдаг байсан бол одоо үед мэдээллийг илүү логик түвшинд хамгаалдаг болсон билээ. Сүлжээгээр холбогдон аюулгүй холбоо үүсгэхийн тулд Kerberos хэмээх баталгаа хангах protocol ашигладаг болно.

Kerberos гэдэг нь эртний Creece-н домогт гардаг хаалга хамгаалагч гурван толгойтой нохойноос улбаалан нэрлэжээ. Тэгэхээр Kerberos маань тухайн хэрэглэгчидийн хооронд аюулгүй холбоог үүсгэх боломжыг олгож өгдөг сүлжээний оршины таны(бидний) хамгаалагч юм. Kerberos нь анх 1983 онд MIT-с анх гаргасан ба Windows2000 үйлдлийн системд анх Default-аар суугдаж байсан байнаа.

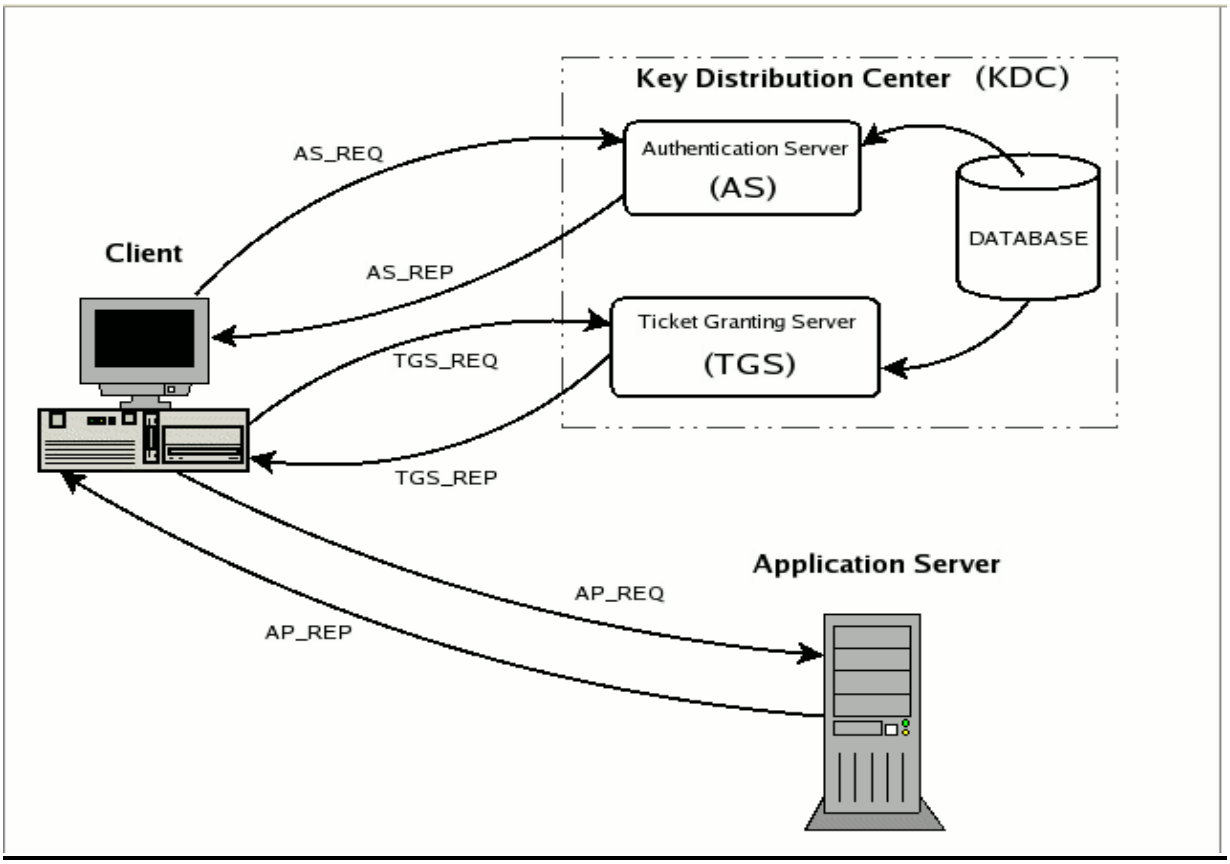
Зорилго

Зорилго нь гэвэл керберосын ажиллагааны талаар мэдэж авах, хэрхэн баталгааг хангаж байгаа, керберос яагаад хэрэглэгдэх болсон тухай мөн керберос-н хэрэглээний талаар судлан өөрийн судалгааны хэмжээнд гарын авлага бэлдэх гэсэн зорилттойгоор ангийн ажилаа хийх гэсэн зорилт гаргасан.

№1 Kerberos гэж юу вэ?

Одоогоор MIT-нь Kerberos V5 дээр суурилсан Kerberos authentication system-г хөгжүүлж байгаа юм. Kerberos нь ерөнхийдөө client (хэрэглэгчээс) илгээсэн хүсэлт болон үйлчилгээний хариу өгөх үйлчилгээ буюу Key Distribution Center (KDC). KDC нь *ticket-granting ticket* (TGT) буюу хэрэглэгчийн талаарх мэдээллийг агуулах сервер, хэрэглэгчийн талаарх мэдээлэл үүнд тухайн хэрэглэгчийн нууц үг, ID зэргийг тусгай кодлолын аргаар кодлон хадгалах ба хэрэглэгчээс ирсэн хүсэлтийг шалган нууцлалыг тайлан, тухайн хэрэглэгч мөн эсэхийг тодорхойлж харилцах эрхийн тасалбар олгох процесс.

- Authentication Server ---KDC буюу баталгаа хангах үе гэж ойлгож болно
- Ticket Grantig Server ---AS-тэй харилцах эрхийг олгож өгч буй хэсэг
- Application Server ---Хандалт хийх гэж буй server



Зураг №1 Kerberos –н ажиллах зарчим

Дээрх зургийн тайлбар

1. AS_REQ -тухайн нэг хэрэглэгч Authentication server-рүү өөр нэг хэрэглэгчтэй холбогдох хүсэлтэй илгээх хэсэг. Үүнд: ip хаяг, lifetime зэргээс тогтсон байна
2. AS_REP – Тухайн хэрэглэгчид Ticket Granting Server-тэй холбогдох түлхүүрийг хариу болгох илгээнэ.
3. TGS_REQ- Олж авсан түлхүүрээ ашиглан Ticket Granting Server-с Application Server-тэй харилцах тасалбар авий гэсэн хүсэлт гаргана.
4. TGS_REP- Application server-тэй харилцах тасалбар болон Application Server-н талаарх мэдээллийг илгээнэ.
5. AP_REQ- Хэрэглэгч өөрийн олж авсан тасалбар болон бусад мэдээллээ(AP-н Key) ашиглан хандалт хийгдэнэ.
6. AP_REP- энэ хэсэгт харилцан бие биенээ мэдэлцлээ одоо харилцаж болно гэсэн мэдээллийг хариу болгон илгээж байна.

<u>Яагаад Kerberos хэрэглэх ёстой вэ?</u>

Интэрнет дэх хоёр хэрэглэгчийн хоорондох холбоосыг тухайн хэрэглэгчидийн тохиролцоо(нууц үг гэх мэт..) дээр тулгуурлан баталгаажуулах үйл ажиллагааг Kerberos хийдэг. Энэ нь Аюулгүй байдлыг хангах чухал түвшин болно гэхдээ хэрэглэгч дээр тодорхойлогдох Firewall-аас шал өөр ойлголт юм.

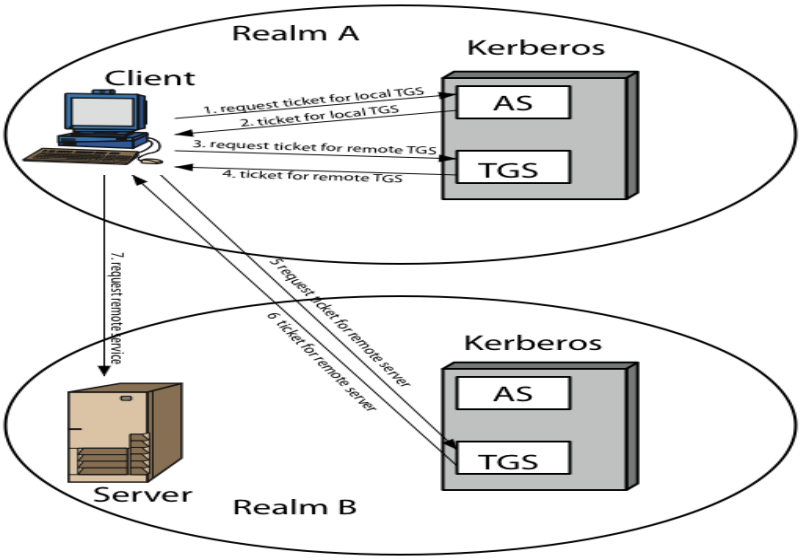
Kerberos Realms

Хэдийгээр Kerberos realm нь ASCII тэмдэгтийн нэг цуваа ба таны domain name-тэй ижилхэн нэртэйгээр энэхүү realm маань үүсдэг. Жишээ нь: таны host-н domain example.com байвал Kerberos realm маань EXAMPLE.COM байна.

1. Kerberos realms:

- Kerberos server
- Client-үүдийн тоо, бүх бүртгэгдсэн сервер
- application server-үүд, server-н sharing keys

2. ганцхан administrative домайн-тай байна.



Зураг 2 Kerberos realm

№2 KDC(Key Distribution Center)

Ports for the KDC and Admin Services

Kerberos-н default порт нь 88 ба Admin server KDC нь 749-р порт тус бүр дээр ажилладаг. Эдгээрээс өөр порт сонгон ажиллуулж болох ба host нь **/etc/services(krb5.conf)** гэсэн тохиргооны файлд Kerberos-н ажиллах портыг харин **(kdc.conf)** гэсэн тохиргооны файлд Admin server-н ажиллах портыг тохируулж өгч болно.

Key Distribution Centers (KDCs) –нь Kerberos tickets(тасалбар олгох) хэмээх гол асуудлыг хариуцдаг. KDC бүр өөрийн гэсэн Kerberos database байх ба түүнээсээ хэрэгтэй мэдээллээ авж ажиллуулах гэсэн хэлбэртэй байна. Master KDC нь өгөгдөлийн сангаасаа master файлаа хадгалдаг ба харин slave KDC нь өгөгдөлөө хадгалах шаардлага байдаггүй. Бүх өгөгдөлийн сангаа өөрчилдөг(password changes) Master KDC хийж өгч байх хэрэгтэй. Тэгэхээр Slave KDC маань Database administration(өгөгдөлийн сангийн удирдлага) хийдэггүй ба харин Kerberos Ticket-Granting Service(тасалбар түгээх үйлчилгээ) хариуцдаг.

2.1 Install the Master KDC

Тухайн нэг хэрэглэгчийн хэрэглэгчийн нууц үгийг өөрчлөхийн UDP-н 464 портоор хандан Master KDC-ээ өөрчилдөг. Kpasswd._udp 464- password өөрчилөх

Master KDC хийгдэх ёстой тохиргоонуудыг доор харуулав:

- krb5.conf
- kdc.conf
- Create the Database
- Add Administrators to the Acl File
- Add Administrators to the Kerberos Database
- Create a kadmind Keytab (optional)
- Start the Kerberos Daemons

/etc/krb5.conf тохиргооны файлд агуулагдах зарим тохиргооны командууд

- **libdefaults**

  Kerberos V5 default-аар байдаг тохиргооны хэсгийг хэлнэ

```
[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes
```

- **login**
  Kerberos V5-н login хийгдэх программуудыг агуулдаг хэсгийг хэлнэ
- **appdefaults**
  Kerberos V5 default-р өгөгдсөн application-г агуулсаныг хэлнэ
- **realms**
  Kerberos realm нэрнүүдийг агуулах ба тухай realm-д харгалзах мэдээллүүд realms хэсэгт байна.

```
[realms]
 EXAMPLE.COM = {
  kdc = kerberos.example.com:88
  admin_server = kerberos.example.com:749
  default_domain = example.com
 }
```

- **domain_realm**
  Kerberos realm нэр болон дэд домайн нэрнүүдийн хоорондох холбоо хамаарлыг тодорхойлсон байна..

```
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

- **logging**
  Kerberos program-н log файлуудын хянаж бүртгэх хэсэг

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
```

krb5.conf тохиргооны файлын жишээ:

```
[libdefaults]
   default_realm = ATHENA.MIT.EDU

[realms]
   ATHENA.MIT.EDU = {
            kdc = kerberos.mit.edu
            kdc = kerberos-1.mit.edu
            kdc = kerberos-2.mit.edu
            admin_server = kerberos.mit.edu
   {

[logging]
   kdc = FILE:/var/log/krb5kdc.log
   admin_server = FILE:/var/log/kadmin.log
   default = FILE:/var/log/krb5lib.log
```

kdc.conf

kdc.conf файлд KDC дэх тохиргоо болон , including defaults used when issuing Kerberos tickets түгээлтийн үед default-аар үүсгэгдсэн тохиргоонууд байна. Хэвийндээ бол kdc.conf файл маань /usr/local/var/krb5kdc директорт суусан байдаг.

kdc.conf file маань үндсэндээ krb5.conf file-тэй ижил агуулагтай, KDC.conf нь дараах 3н Section-уудыг агуулдаг.

- **kdcdefaults**

  KDC-н талаарх бүхий л зүйлийг агуулсан байдаг default утга
- **realms**

  Kerberos realm нэрнүүдийг агуулах ба тухай realm-д харгалзах мэдээллүүд realms хэсэгт байна
- **logging**

Kerberos program-н log файлуудын хэсэг

2.2 Install the Slave KDCs

Slave KDC-н тохиргоо маань аль хэдийнээ хийгдсэн байдаг. Нэг Master KDC ашиглан олон олон Slave хийдэг, үүний тулд Master KDC-ээ маш сайн тохируулсан байх хэрэгтэй. Slave KDC-г тохируулхад дараах зүйлсийг анхаарна:

- Create Host Keys for the Slave KDCs
- Extract Host Keytabs for the KDCs
- Set Up the Slave KDCs for Database Propagation

№3 Installing Configuring Unix Client Machines

Client-н UNIX дээр хэрхэн байгуулах түүний тохиргооны файл:

- Client programs
- Client Machine Configuration Files

3.1 Client Programs(Хэрэглэгчийн програм)

Client program-ууд нь гэвэл login.krb5, rlogin, telnet, ftp, rcp, rsh, kinit, klist, kdestroy, kpasswd, ksu, krb524init ашиглаж баталгаажуулалт хийдэг байна.

3.2 Client Machine Configuration Files

Тухайн хэрэглэгчийн машин(Laptop,pc) kerberos ажиллуулахдаа хамгийн нэн түрүүнд **/etc/krb5.conf** буюу KerberosV5-н тохиргооны файлаа уншиж ажиллуулах ёстой юм.

```
kerberos        88/udp    kdc     --- Kerberos V5 KDC
kerberos        88/tcp    kdc     --- Kerberos V5 KDC
klogin          543/tcp           ---Kerberos authenticated rlogin
kshell          544/tcp           ---  remote shell(тэкст горимоор remote-ээр shell-тэй ажиллах)
kerberos-adm    749/tcp           --- Kerberos 5 administrator хийх порт
kerberos-adm    749/udp           --- Kerberos 5 administrator хийх порт
krb5_prop       754/tcp           --- Kerberos slave propagation
eklogin         2105/tcp          ---Kerberos auth. & encrypted rlogin
krb524          4444/tcp          --- Kerberos V5-г KerverosV4 рүү хөрвүүлэгч
```

№4 Application Servers

Application server гэдэг Сүлжээний орчинд тухайн нэг Host-д зүй зохистой үйлчилгээ үзүүлж буй server юм. Application servers нь ерөнхийдөө "secure(баталгаатай)" болон "insecure(найдваргүй) гэсэн хоёр хэлбэртэй. "Secure" server нь хэрэглэгч холбогдохоос эхлээд холбоо төгсөх хүртэлх Host бүрийн баталгааг хангаж байдаг server гэж үзэж болно.

Харин "insecure" Host нь Kerberos authentication ашиглаагүй ба ямарч баталгаажуулалтгүй хэрэглэгчидийг ч холбогдохыг зөвшөөрдөг найдвартай бус Server-г хэлнэ.

Доор Application server-т хамаарах зүйлсийг жагсаав.

- Server Programs
- Server Configuration Files
- The Keytab File
- Some Advice about Secure Hosts

4.1 Server Programs

Kerberos V5 нь UNIX хэрэглэгчидийн сүлжээний програмчлалд зориулагдсан Kerberos-н илүү сайжруулсан хувилбар ба Kerberos-оос server-т зориулсан deamon-уудтай KerberosV5 нь харилцан UNIX server дээр ашиглагддаг. Эдгээр deamon-д ftpd, klogind, kshd, telnetd зэрэг ордог. Эдгээр программууд **/usr/local/sbin** дотор сууж өгдөг ба хэрвээ та хүсвэл root's path директордоо нэмж суулгаж болох юм..

4.2 Server Configuration Files

Secure server /etc/inetd.conf доторхи өөрлөлтийг доор харуулав

ftp, telnet, shell, login, exec зэрэг service-үүдийн хэлбэржилтийг харуулав.

- klogin stream tcp nowait root /usr/local/sbin/klogind -k -c
- eklogin stream tcp nowait root /usr/local/sbin/klogind -k -c -e
- kshell stream tcp nowait root /usr/local/sbin/kshd -k -c -A
- ftp stream tcp nowait root /usr/local/sbin/ftpd -a
- telnet stream tcp nowait root /usr/local/sbin/telnetd -a valid

Insecure server-н **etc/inetd.conf** доторхи өөрлөлт

ftp болон telnet service-үүдийг тохиргоог хэлбэржилтийг харуулав

- klogin stream tcp nowait root /usr/local/sbin/klogind -k -c
- eklogin stream tcp nowait root /usr/local/sbin/klogind -k -c -e
- kshell stream tcp nowait root /usr/local/sbin/kshd -k -c -A
- ftp stream tcp nowait root /usr/local/sbin/ftpd
- telnet stream tcp nowait root /usr/local/sbin/telnetd -a none

4.3 The Keytab File

Бүх Kerberos server-үүдэд *keytab* файл маш хэрэгтэй, энэ нь тухайн хэрэглэгчийн local disk дээрх /etc/krb5.keytab файлыг ачаалдаг ба KDC дээрх баталгаажуулалтыг хийдэг. Keytab file зөвхөн унших эрхтэй root директорид байрласан байдаг энэ файл нь зөвхөн таны өөрийн local disk-нд байрлуулсан байна. Таны keytab file ямарваа нэг халдлагад өртөх хулгайлагдах боломж өндөр байдаг учир та BACKUP machine-н нэг хэсэг болгож болохгүй юм.

№5 Upgrading to Triple-DES Encryption Keys(*Сайжруулсан 3DES түлхүүр кодлолын арга)*

Triple-DES with Two-Keys

Энэ нь тухайн түлхүүрээ кодлохдоо хоёр удаа DES алгоритм хэрэглэнэ гэсэн үг юм. Block тус бүрээ хоёр удаа DES-ээр кодлоно. Ер нь практик дээр хоёр түлхүүртэй Triple-DES-г өргөн ашигладаг.

- 2 DES encrypts on each block

$$C = E_{K2}(E_{K1}(P))$$

Triple-DES with Three-Keys

Энэ нь тухайн түлхүүрээ Key1 ашиглан Encode хийчээд, Key2 ашиглан Decode хийгээд, Key3 ашиглан эх түлхүүрээ Encode хийх үйлдэл хийдэг алгоритм юм.

- Triple-DES with Three-Keys :

  Encryption:

  ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

Үйлдэмж: DES encrypt with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.

Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

Үйлдэмж: decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

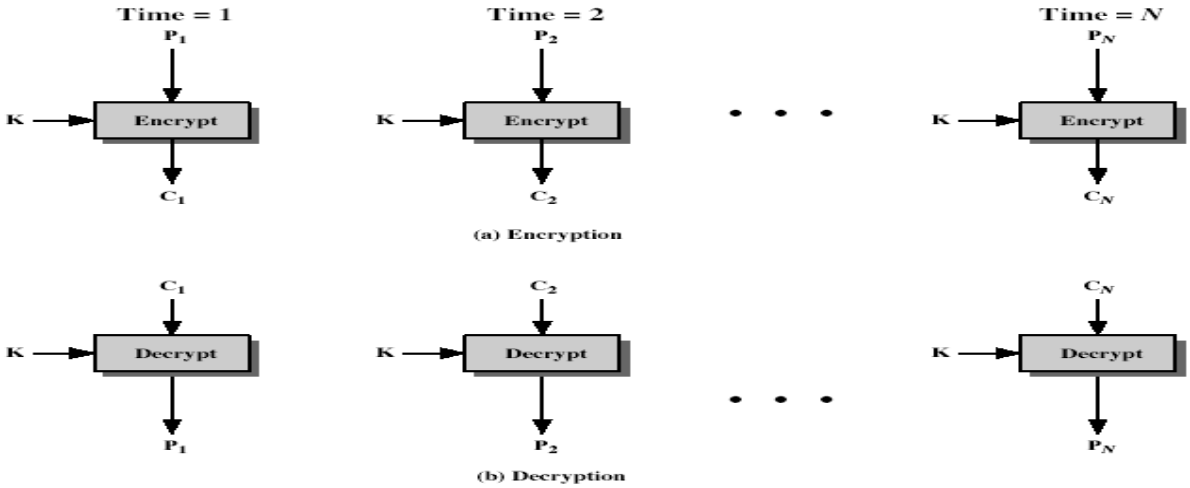
AES(Advenced Encryption Standard)

- DES нууцлалын дараагийн хувилбар 128 битийн өгөгдөл дээр 128/256/512 битийн түлхүүр ашигладаг.
- C, Java хэл дээр хөгжүүлсэн хувилбар бий
- Ойрын 10-20 жилдээ эвдэх боломжгүй гэж үздэг
- Triple DES- с давуу

1. **Electronic Codebook Book (ECB)**

   Block тус бүрийг DES алгоритмаар кодлодог

$$C_i = DES_{K1}(P_i)$$

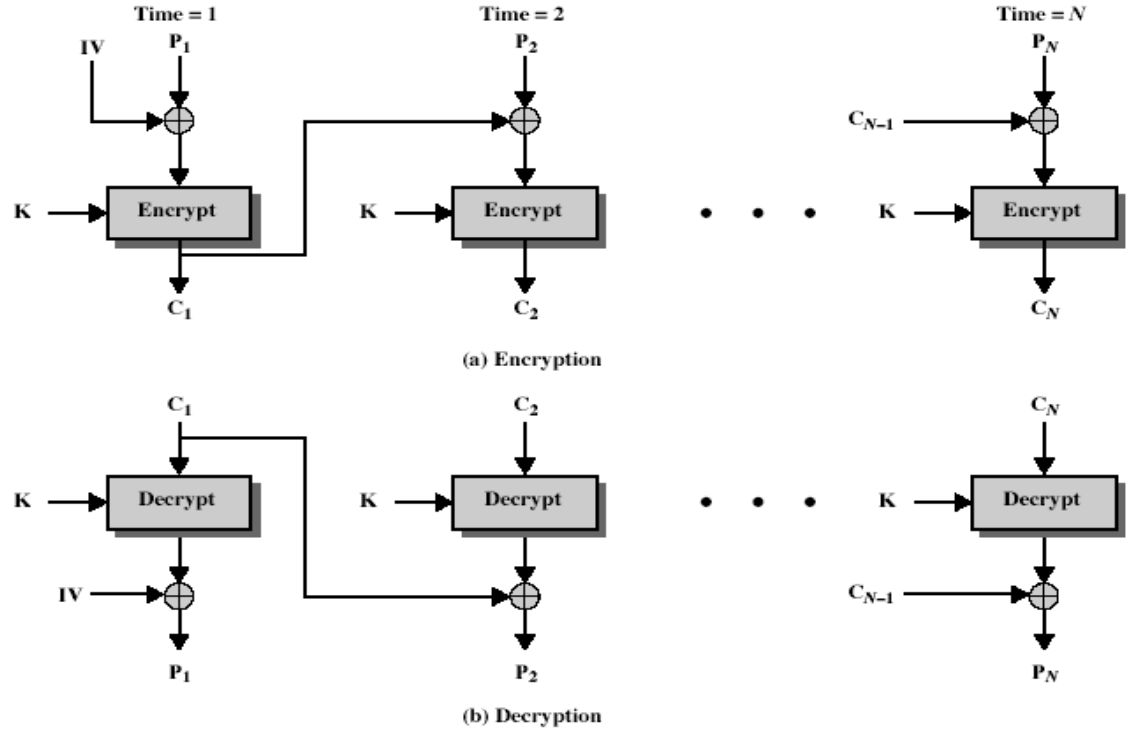


Зураг3 ECB кодлолын зураг

2. Cipher Block Chaining (CBC)

Initial Vector (IV) ашиглан кодлох процессоо эхлүүлдэг

$C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$ $C_{-1} = IV$

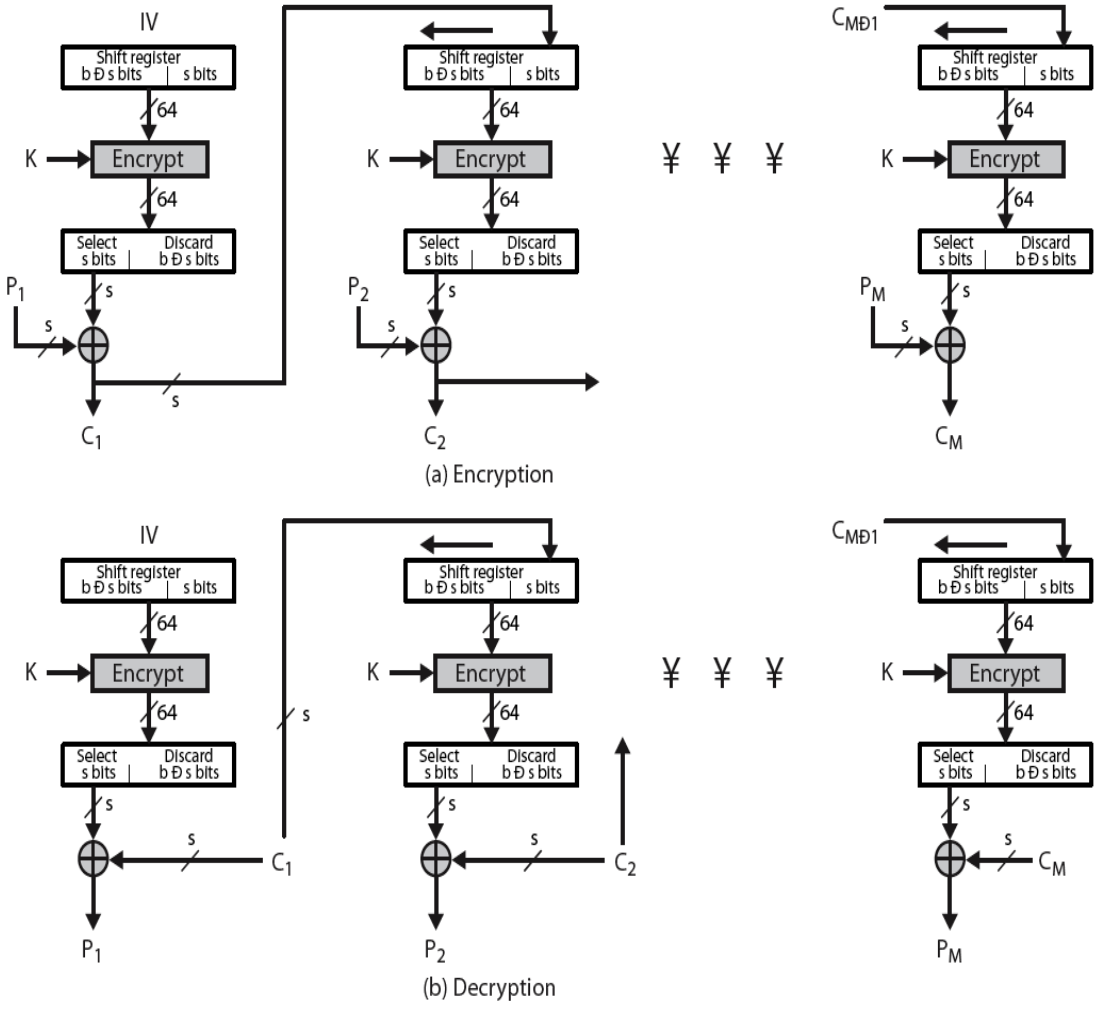


Зураг4 CBC кодлолын зураг

3. Cipher FeedBack (CFB)

Энэ нь мөн эхлэхдээ IV хэрэглэх ба эхний block-с гарсан кодлогдсон мэдээллээ дараагийн block-н Plaintext-тэй XOR-дох үйлдэл хийн кодлолоо хийдэг.

$$C_i = P_i \text{ XOR } DES_{K1}(C_{i-1}) \qquad C_{-1} = IV$$

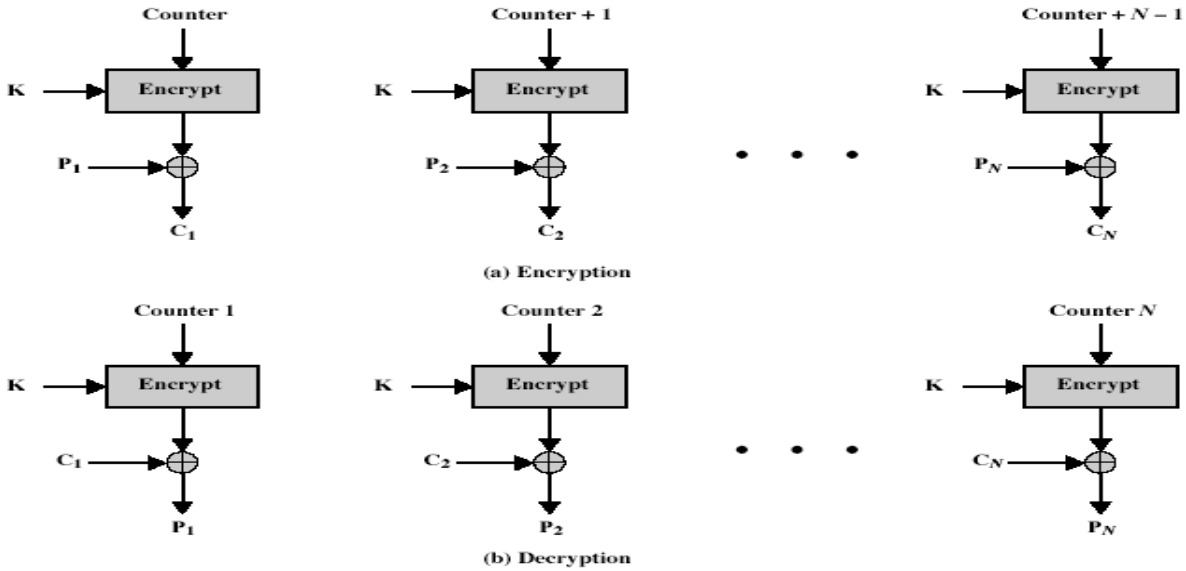


Зураг5 CFB кодлолын зураг

4. **Counter (CTR)**

Plaintext бүрээ block тус бүр дээр нь өөр өөр түлхүүр ашиглах ба тусгай тоолуурын хувьсагч ашиглан кодлодог.

$C_i = P_i$ XOR O_i $O_i = DES_{K1}(i)$



Зураг6 CTR кодлолын зураг

№6 Operation system and Kerberos

Kerberos нь тухайн тухайн нэг хэрэглэгчийн хувьд(баталгаа хангах) бус олон олон чухал үүргийг гүйцэтгэж байдаг. Бүхий л үйлдлийн системд түлхүү ашиглаж баталгааг нь хангаж өгдөгийг мэдлээ.

6.1 Cisco IOS

Cisco төхөөрөмжид зориулж гаргасан Cisco IOS хүртэл KerberosV5 –г хэрэглэдэг. Cisco router дээр KerberosV5 маань хэрхэн ажиллаж,тохируулдагыг судалж үзлээ.

Router дээрээ үндсэн тохиргооны горимд ороод команд ашиглан тохиргоо хийдэг.

KerberosV5 Configuration File and Commands	
krb5.conf File	**Cisco IOS Configuration Command**
[libdefaults] default_realm = *DOMAIN.COM*	(in configuration mode) **kerberos local-realm** *DOMAIN.COM*
[domain_realm] .domain.com = *DOMAIN.COM* domain.com = *DOMAIN.COM*	(in configuration mode) **kerberos realm**.*domain.com DOMAIN.COM* **kerberos realm** *domain.com DOMAIN.COM*

Зураг7 Cisco IOS дээр хийгдэх тохиргооны команд

[realms] kdc = *DOMAIN.PIL.COM:750* admin_server = *DOMAIN.PIL.COM* default_domain = *DOMAIN.COM*	(in configuration mode) **kerberos server** *DOMAIN.COM 172.65.44.2* (*172.65.44.2* is the example IP address for *DOMAIN.PIL.COM*)

Cisco router дээрх Kerberos-н командууд:
Cisco# **show Kerberos Credentials**-энэ нь Cisco IOS дээрх хийгдсэн ажилуудыг харуулна.
Cisco(config)#**kerberos** realm.*domain.com DOMAIN.COM* –энэ нь Realm үүсгэх команд

Cisco(config)#**kerberos local-realm** *DOMAIN.COM*
Cisco(config)#**kerberos server** *DOMAIN.COM 172.65.44.2*
Cisco# **ank** *username@REALM* –энэ нь Router-с KDC-н өгөгдөлийн санд шинэ хэрэглэгчийн нэр password зэргийг агуулсан Key-г нэмж өгч байна.

KDC Database-д хэрхэн хэрэглэгч нэмэх

	Command	Purpose
Step 1	Router# **ank** *username@REALM*	**ank** (add new key) команд хэрэглэн KDC-д хэрэглэгч

		нэмдэг.
Step 2	Router# **ank** *username/instance@REALM*	**ank** команд хэрэглэн command to add a privileged instance of a user.

Зураг8 Cisco IOS-с KDC Database-д хэрхэн хэрэглэгч нэмэх

Жишээ нь: *Miigaa* гэсэн хэрэглэгчийг REALM нь CISCO.COM :

Cisco**#ank** miigaa@CISCO.COM

Creating SRVTABs on the KDC

All routers that you want to authenticate to use the Kerberos protocol must have an SRVTAB.

SRVTAB нь router-с KDC-рүү дамжигдах мэдээллийг нэмж тэмдэглэж байдаг:

Command	Purpose
Router# **ark** *SERVICE/HOSTNAME@REALM*	**ark** (add random key) командаар сүлжээгээр үйлчилгээ авч буй Host болон Router-ээ KDC-д нэмж өгдөг.

Kerberos command: **Cisco#ark** host/router1.cisco.com@CISCO.COM – энэ нь router1 host-н мэдээллээ KDC дээр үүсгэж байна.

Extracting SRVTABs

Command	Purpose
Router# **xst** *router-name host*	Use the kdb5_edit command **xst** to write an SRVTAB entry to a file.

Жишээ нь:

Cisco**#xst** router1.cisco.com@CISCO.COM **host –** энэ нь Router1 –н host-н мэдээллийг KDC-с router өөр дээрээ Extract хийж байна.

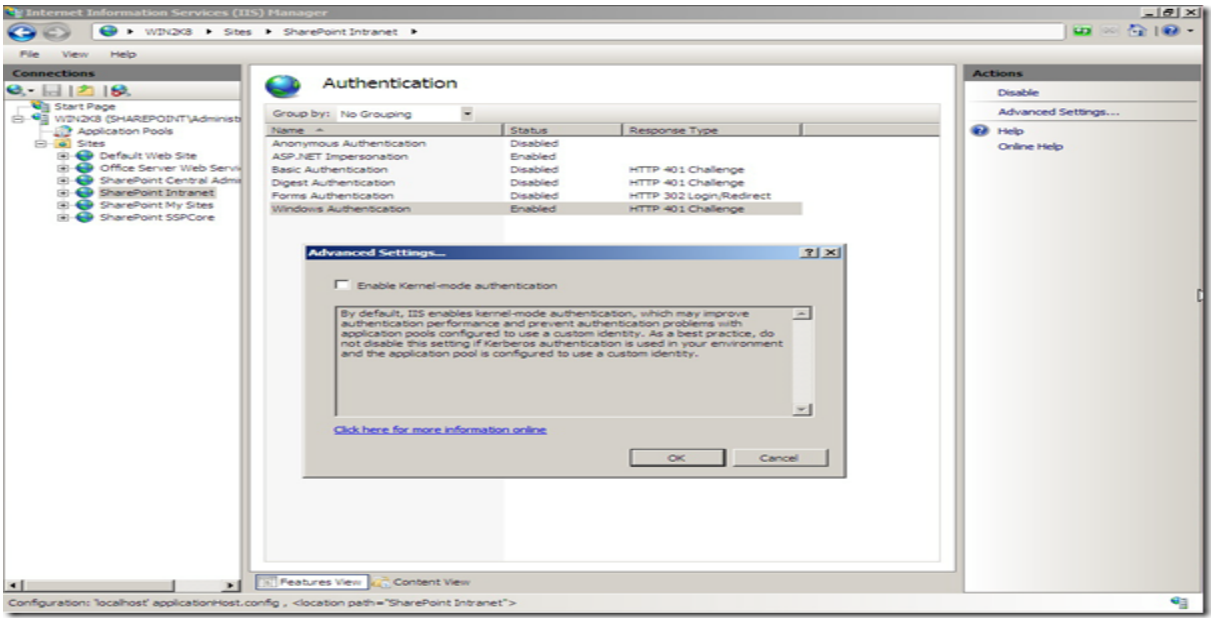
SRVTAB file - энэ нь router болон KDC хоорондын тусгай мэдээлэл солилцох нууц file гэж ойлгож болно. Тухайн router-н үүсгэгдэх KDC дээрх файл.

6.2 Windows Server 2008

Server дээрх ажиллагаа гэдэг бол мэдээж маш чухал зүйл юм.
Дээр би Kerberos-г Unix,Linux системд хэрхэн зохицдог мөн тохиргооны файл нь хаана хэрхэн байдаг талаар дурдсан билээ. Харин одоо Windows тэр дундаа Windows Server үйлдлийн системд хэрхэн ашигладаг мөн хэрэглэдэг эсэхийг судаллаа. Миний судалсанаар Kerberos-г Windows Server 2000, Windows Server 2003, Windows Server 2008 зэрэг server талын Windows үйлдлийн систем дээр ихээхэн ашигладаг юм байна. Ер нь бүхий л үйлдлийн систем KerberosV5-г түлхүү ашиглаж байна.

Configure the useAppPoolCredentials attribute in system.webServer/security/authentication/Windows-Authentication configuration section to true.
Жишээ нь:

<windowsAuthentication enabled="true" useKernelMode="true" useAppPoolCredentials="true" />



Зураг 9 Windows Server 2008 Share Points use Kerberos

6.3 Linux

Доор Linux дээрх KerberosV5-н тохиргооны файлыг тайлбарлав.

etc/krb5.conf тохиргооны файлд агуулагдах зарим тохиргооны команд.

- **libdefaults**

  Kerberos V5 default-аар байдаг тохиргооны хэсгийг хэлнэ

```
[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes
```

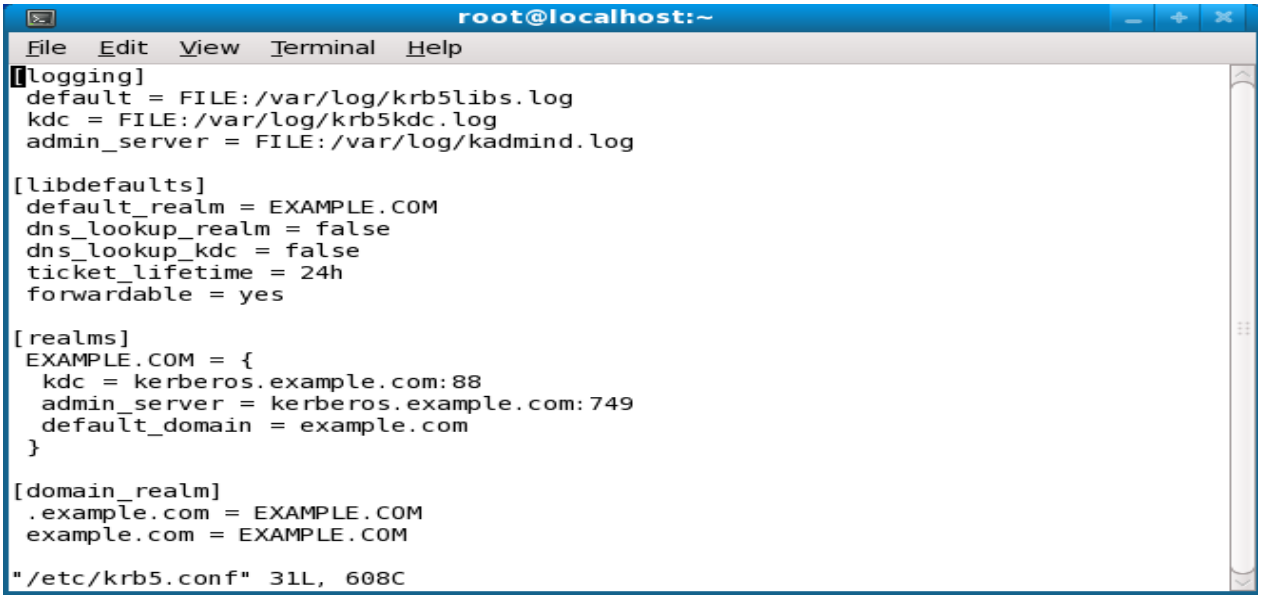
- **login**
  Kerberos V5-н login хийгдэх программуудыг агуулдаг хэсгийг хэлнэ
- **appdefaults**
  Kerberos V5 default-р өгөгдсөн application-г агуулсаныг хэлнэ
- **realms**
  Kerberos realm нэрнүүдийг агуулах ба тухай realm-д харгалзах мэдээллүүд realms хэсэгт байна.

```
[realms]
 EXAMPLE.COM = {
  kdc = kerberos.example.com:88
  admin_server = kerberos.example.com:749
  default_domain = example.com
 }
```

- **domain_realm**
  Kerberos realm нэр болон дэд домайн нэрнүүдийн хоорондох холбоо хамаарлыг тодорхойлсон байна..

```
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

- **logging**
  Kerberos program-н log файлуудын хянаж бүртгэх хэсэг



Зураг 10 Linux-н тохиргооны файл krb5.conf

kdc.conf

kdc.conf file:

```
[kdcdefaults]
   kdc_ports = 88,750

[realms]
```

```
ATHENA.MIT.EDU = {
    database_name = /usr/local/var/krb5kdc/principal
    admin_keytab = /usr/local/var/krb5kdc/kadm5.keytab
    acl_file = /usr/local/var/krb5kdc/kadm5.acl
    dict_file = /usr/local/var/krb5kdc/kadm5.dict
    key_stash_file = /usr/local/var/krb5kdc/.k5.ATHENA.MIT.EDU
    kadmind_port = 749
    max_life = 10h 0m 0s
    max_renewable_life = 7d 0h 0m 0s
    master_key_type = des3-hmac-sha1
    supported_enctypes = des3-hmac-sha1:normal des-cbc-crc:normal
}
```

Дүгнэлт

Kerberos-г судалсанаар өөрийн хэмжээнд баталгаа хангах процесс-г танин мэдэж чадлаа. Kerberos бол Сүлжээний орчинд баталгаа хангах protocol юм KerbeosV4 V5 өргөн ашигладаг ба Kerberos V5 –г анх 1990-д оны дунд үеэс хэрэглэж эхэлсэн байдаг. Version 5 нь RFC 1510 гэсэн интернет стандардтай. Kerberos V5 нь DES болон Triple DES нууцлалын алгоритмыг л зөвхөн дэмждэг. Мөн ажиллагааны зарчимуудыг танин мэдлээ. Kerberos-г ашиглах хэрэглэх тохиолдолд та өөрийн сүлжээний аюулгүй байдал, хэрэглээ таны host ямарваа нэгэн attack-д орох зэрэг асуудлыг оновчтой тодорхойлох хэрэгтэй бөгөөд Kerberos талаар тодорхой хэмжээний guide-тай танилцсан байх хэрэгтэй бөгөөд маш сайн судалсан байх хэрэгтэй юм.

Ашигласан материал:

C.Neuman T.Yu, S. Hartman, K. Raeburn, The Kerberos authentication system(RFC 4210) July 2005.
<URL: http://web.mit.edu/kerberos.htm>
<URL: http://kerberos.info/doc/tutorial.html>
<URL: http://theworldjournal.com/special/kerberos.html>