

## Kerberos V5

Di

Max Giordano

[giomas@genie.it](mailto:giomas@genie.it)

Giuseppe Giongati

[giugio@tiscalinet.it](mailto:giugio@tiscalinet.it)



## Argomenti

- Cos'è KERBEROS
- Perché KERBEROS
- Funzionamento
- Installazione
- Configurazione



## Cos'è Kerberos

- sistema di autenticazione distribuito
- realizzato al MIT dall'ATHENA Group in alternativa al sistema di autenticazione tradizionale

La versione 4 fu ideata nel 1987 da Steve Miller e Clifford Neuman

La Version 5, John Kohl e Clifford Neuman, fu ideata nel 1990

## Lo Scenario

Nel mondo di kerberos valgono 3 assunzioni:



- la rete è insicura

- gli host sono sicuri

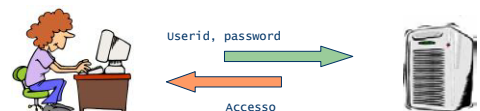
- le chiavi non sono banali

## Concetti base

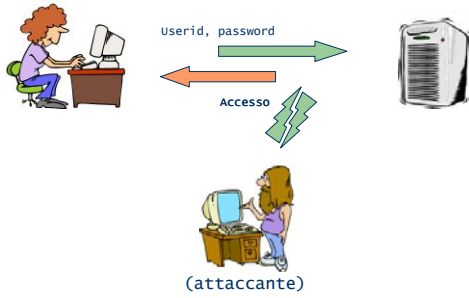
- non ci si basa sulle affermazioni degli utenti
- elimina la necessità di dimostrare il possesso di informazioni segrete (password, etc)
- un vigilante non si accontenta di ciò che affermiamo per accertare la nostra identità



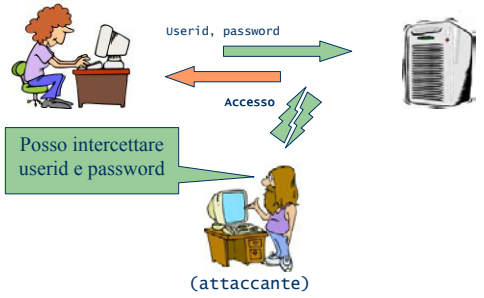
## Autenticazione Tradizionale



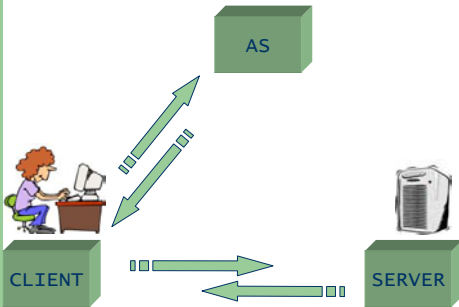
## Autenticazione Tradizionale



## Autenticazione Tradizionale



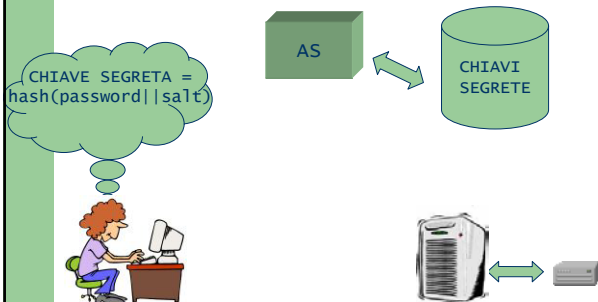
## Autenticazione con Kerberos



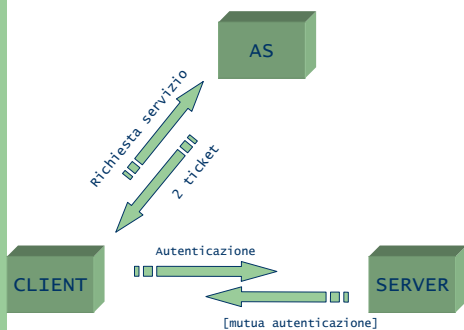
## Autenticazione con Kerberos

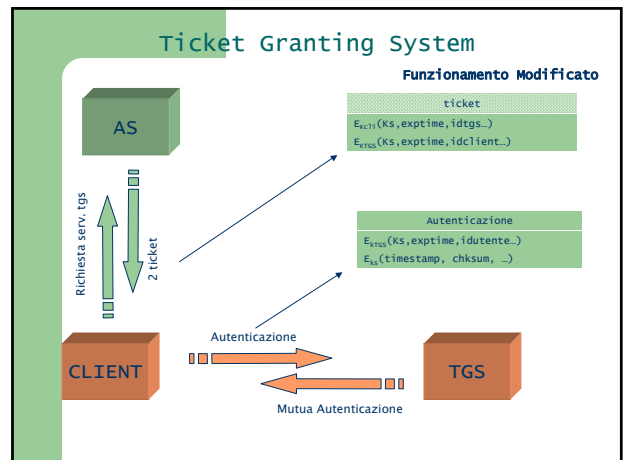
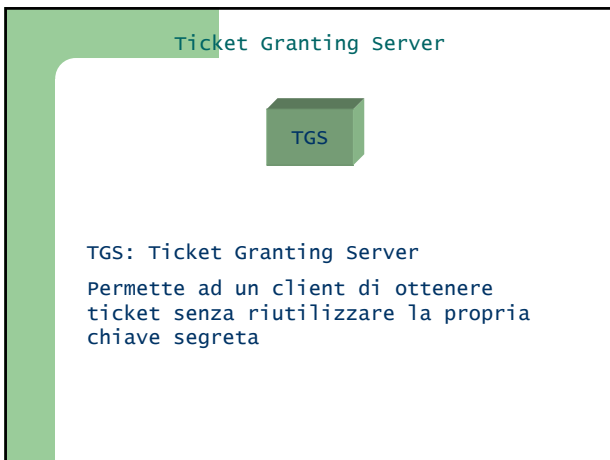
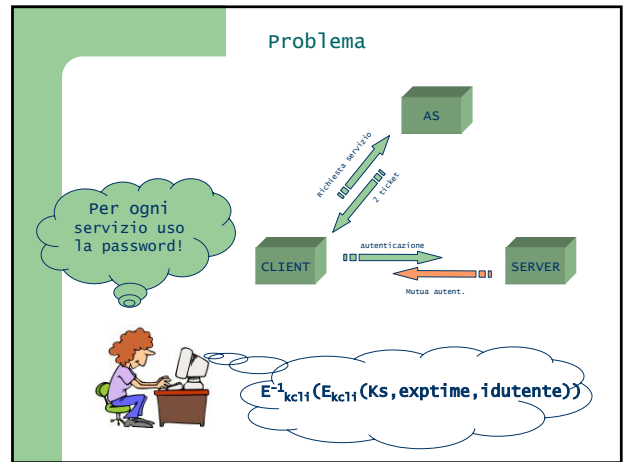
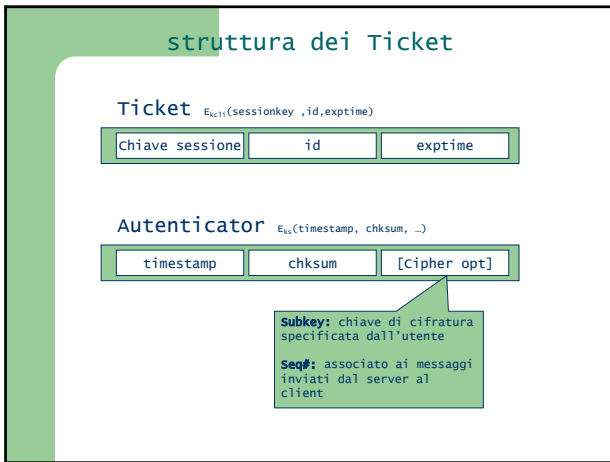
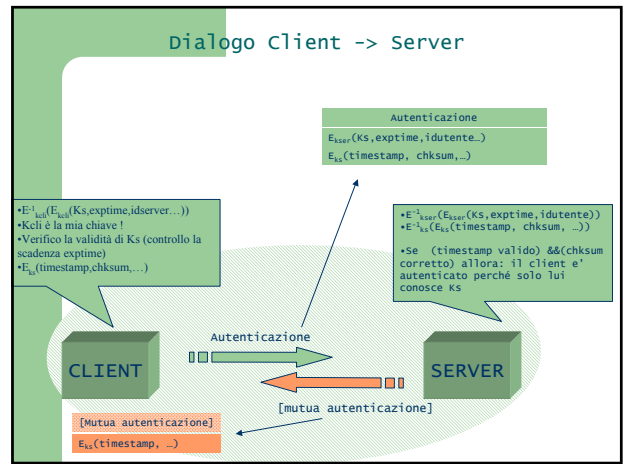
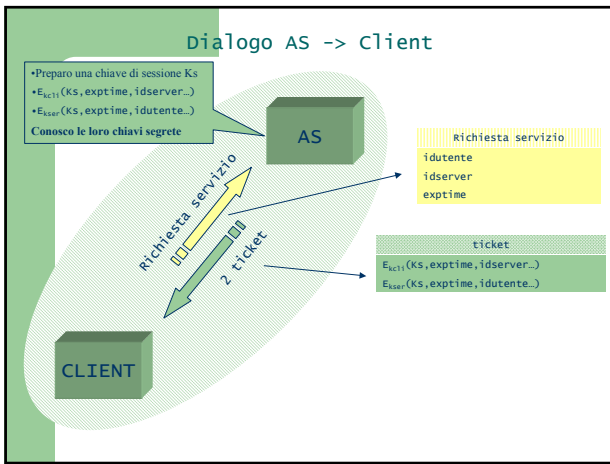
- AS: Authentication Server
- Conosce le chiavi segrete degli utenti e dei servizi
  - Rilascia le chiavi di sessione

## Politica delle chiavi



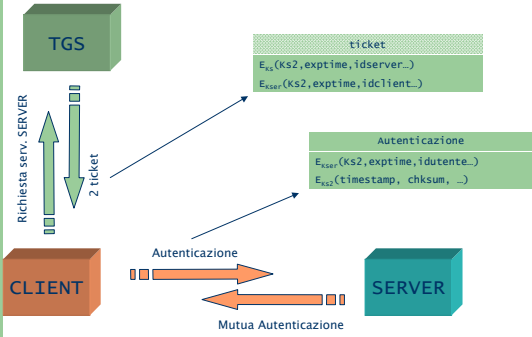
## Funzionamento semplificato





# Ticket Granting System

Funzionamento Modificato

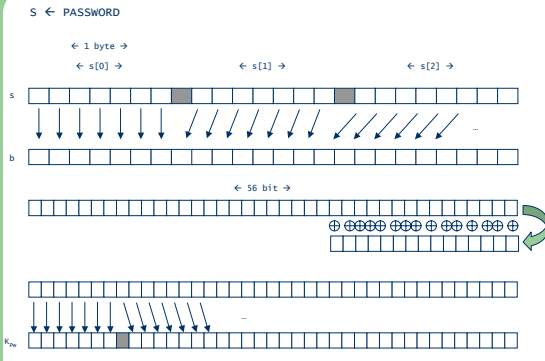


# Calcolo della chiave

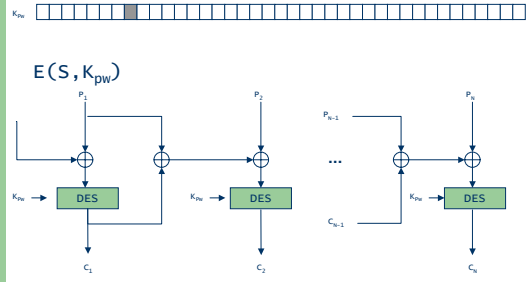
CHIAVE SEGRETA =  $hash(password || salt)$



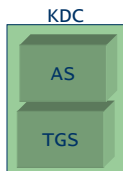
# "Password to key"



# "Password to key"



# Key Distribution Center



•KDC e' sinonimo di AS e TGS

# alcuni termini

- Client
- Host
- Keytab
- Principal
- Realm

E' un entità che puo' ottenere un "ticket" puo' essere sia un utente che un "host"

## alcuni termini

- Client
- Host **E' Un computer accessibile dalla rete**
- Keytab
- Principal
- Realm

## alcuni termini

- Client
- Host
- Keytab **Una tabella usata dagli host o dai servizi per memorizzare la loro chiave segreta**
- Principal
- Realm

## alcuni termini

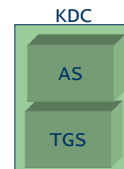
- Client
- Host
- Keytab
- Principal **Denota un utente o un servizio a cui assegnamo delle credenziali.**
  - E' una stringa del tipo: `primary/instance@REALM`
  - Primary equivale al nome dell'utente/servizio
  - Instance e' la qualifica di un utente
- Realm

## alcuni termini

- Client
- Host
- Keytab
- Principal **E' una rete "logica" che fa capo ad un unico database.**
- Realm **Definisce un area di validita' dei ticket**

# INSTALLAZIONE

## Obiettivo



CLIENT



SERVER

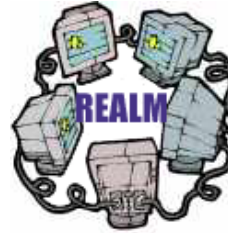
## Considerazioni Preliminari

- Scelta del/dei "kerberos Realm".
- Mapping hostnames → "kerberos Realm".
- Porte usate dal KDC e dal kadmin.
- KDC Secondari

## Scelta dei "Realm"

### Scelta dei "Realm"

Per convenzione utilizziamo i nomi di dominio in lettere MAIUSCOLE.



SPARTACO.IT

spartaco.it

## mapping hostname → Realm

Due possibilità:

- Tramite i files di configurazione
- Tramite il DNS

## mapping hostname → Realm

Primo approccio via file "krb5.conf":

Dal generale al particolare:

*dominio → sottodominio → eccezioni*

Esempio:

.it=IT

spartaco.it=SPARTACO.IT

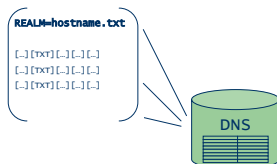
PROBLEMA: non è scalabile per ogni host va modificato un file di configurazione



## mapping hostname → Realm

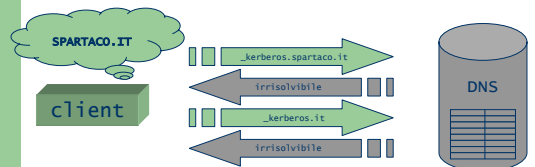
Secondo approccio via DNS:

- Nel DNS ogni hostname ha un record associato
- Usiamo il campo "TXT" di questo record per memorizzare il REALM associato all'Host



## mapping hostname → Realm

Secondo approccio via DNS:



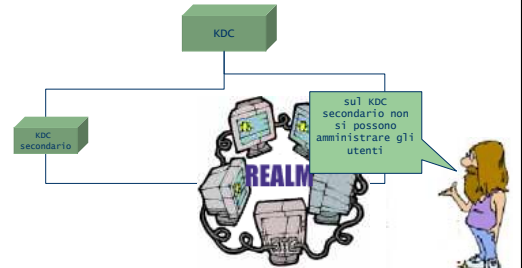
L'interrogazione si ferma quando il DNS risolve l'hostname

## Porte usate

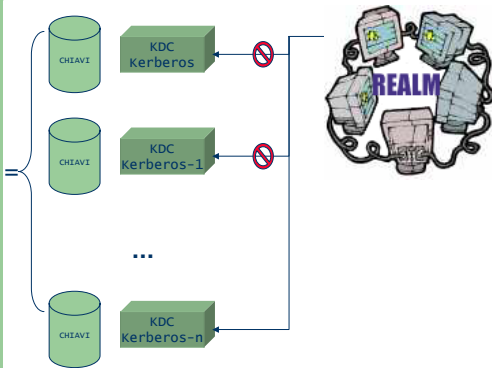
- 88 per il KDC
- 749 per il server di amministrazione.

## KDC Secondari

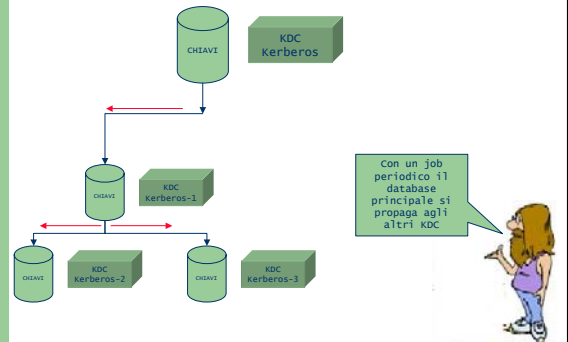
- Forniscono continuità al servizio "ticket-granting"



## Continuità del servizio



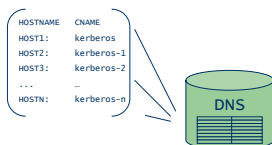
## Consistenza dei database



## Nomi per i KDC secondari

### Uso degli alias

DNS: ad ogni hostname sono associati uno o più alias detti "CNAME"



## Compilazione

**Requisiti:** Circa 70 mega byte di spazio su disco

Preleviamo il pacchetto da:

<http://www.crypto-pub.org/dist/mit-kerberos5/krb5-1.2.2.tar.gz>

## Compilazione

1. cd krb5-1.2/src
2. ./configure
3. make
4. make install

## “Configure”

personalizzare il pacchetto senza editare manualmente i Makefile

## “Configure”

### Alcune opzioni:

`--prefix=PREFIX`

Per impostare una radice diversa dal default, questo serve a:

- rendere piu' agevole una eventuale "de-kerberizzazione" e l'aggiornamento.
- separare i files Kerberizzati dalle versioni standard
- usare versioni non kerberizzate dei servizi (per compatibilita')

## “Configure”

### Alcune opzioni:

`--localstatedir=LOCALSTATEDIR`

Indica un percorso alternativo per i file di configurazione.

## “configure”

### esempio:

```
./configure --prefix=/opt/krb5 --localstatedir=/opt/krb5/var/krb5kdc
```

```
Spartaco# ./configure --prefix=/opt/krb5
...
Spartaco# make
...
Spartaco# make install
...
```

## Configurazione

### Comandi:

**Kdb5\_util:** che ci permette di gestire il db delle password (Creazione, cancellazione, ... di un db)

**Kadmin:** ci permette di amministrare i principal, le policies e le chiavi dei servizi (il file keytab).

• E' un tool remoto che si basa sull'autenticazione Kerberos e su una RPC

• Per autenticarsi usa il principal kadmin/admin che e' creato automaticamente quando creiamo il database

**Kadmin.local:** e' una versione che non usa l'autenticazione kerberos e che funziona solo in locale

## Passaggi

- Creazione file di configurazione
- Creazione del DB Principale
- Impostazione dei privilegi di amministrazione
- Creazione del keytab per gli host
- Aggiunta dei "Principal"
- Configurazione "application" server
- Avvio di Kadmin e del KDC

## Configurazione

La configurazione e' basata su due files:

- **kdc.conf**
- **krb5.conf**

organizzati in sezioni

## File di configurazione

**Krb5.conf e' il file principale e contiene sette sezioni:**

- Libdefault:** impostazioni per la libreria
- Appdefault:** impostazioni per le applicazioni
- Realms:** impostazioni per i singoli realm
- Domain\_realm:** mapping domainname->realm
- Logging:** impostazioni funzioni di log
- Capaths:** path non gerarchico per l'autenticazione cross realm
- Kdc:** indica il file "kdc.conf"

## File di configurazione

**Kdc.conf contiene tre sezioni:**

- kdcdefaults:** impostazioni per il kdc
- Realms:** impostazioni per i singoli realm
- Logging:** impostazioni funzioni di log

## Configurazione

**In particolare le sezioni piu' significative sono:**

- **Libdefaults**
- **realms**
- **domain\_realm**

## Configurazione

```
[libdefaults]
ticket_lifetime = 24000
default_realm = SPARTACO.IT
default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
dns_lookup_realm = false
dns_lookup_kdc = false
```

Qui posso impostare l'alg. Di cifratura e la vita del ticket



## Configurazione

```
[realms]
SPARTACO.IT = {
kdc = spartaco.it:88
admin_server = spartaco.it:749
default_domain = it
}
```

Qui definisco i  
"REALM"



## Configurazione

```
[domain_realm]
.it = SPARTACO.IT
it = SPARTACO.IT
spartaco.it = SPARTACO.IT
spartaco = SPARTACO.IT
```

Qui definisco il  
mapping  
hostname → realm



## Creazione DB

Il database principale contiene le chiavi.  
Si crea con il comando:

kdb5\_util:

```
Spartaco# ./kdb5_util create -r SPARTACO.IT -s

Initializing database '/krb5/lvar/krb5kdc/principal' for realm
'spartaco.it',
master key name 'K/M@spartaco.it'
Enter KDC database master key:
your_master_key
Re-enter KDC database master key to verify:
your_master_key
```

l'opzione -r indica il dominio, -s crea un file  
"stash" usato dal KDC per "autenticarsi".

## Privilegi di amministrazione

I livelli di privilegio sul file della password  
sono memorizzati nel file kadm5.acl

```
spartaco# cat kadm5.acl
*/admin@SPARTACO.IT *
giugio@SPARTACO.IT ADMCIL
giugio/*@SPARTACO.IT 1
```

Quindi:

- giugio/admin puo' tutto
- giugio non puo niente
- giugio/qualsiasiosa puo solo listare il contenuto del db

a/A permette/vieta l'aggiunta di un principal  
d/D permette/vieta la rimozione di un principal  
m/M permette/vieta la modifica di un principal  
c/C permette/vieta changepw di un principal  
i/I permette/vieta query sul DB principale  
l/L permette/vieta l'elencazione dei principal

## Creazione keytab

Definiti i privilegi creiamo il file keytab  
Aggiungiamo almeno i due principal kadmin/admin e  
kadmin/changepw per poter usare kadmin

```
Spartaco# ./kadmin.local
kadmin.local: ktadd -k /opt/krb5/var/krb5kdc/kadm5.keytab kadmin/admin
kadmin/changepw
Entry for principal kadmin/admin with kvno 3, encryption type DES3-
SHA1-HMAC added to keytab WRFILE:/krb5/var/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES3-
SHA1-HMAC added to keytab WRFILE:/krb5/var/krb5kdc/kadm5.keytab.
kadmin.local: quit
```

Il comando ktadd aggiunge i principal indicati al  
file keytab

Quit chiude kadmin

## Creazione Principal

Sempre dal software kadmin.local possiamo creare  
un principal con addprinc:

```
Spartaco# ./kadmin.local
Kadmin: addprinc giomas@SPARTACO.IT -expire "10/05/2002 24.00"
Enter password for principal giomas@SPARTACO.IT:
Re-enter password for principal:
Principal giomas@SPARTACO.IT created.
Kadmin:
```

Altri comandi:

modprinc, listprinc, delprinc.

## Aggiunta Servizi

I servizi sono considerati come principal e come tali vanno aggiunti:

```
nerone# ./kadmin
Kadmin: addprinc host/nerone.it@SPARTACO.IT
Enter password for principal host/nerone.it@SPARTACO.IT:
Re-enter password for principal:
Principal host/nerone.it@SPARTACO.IT created.
Kadmin:
```

La parola "host" indica un tipo di servizio che e' l'accesso via rlogin o telnet. Altri servizi hanno altri nomi, es. ftp, pop..

Naturalmente vanno aggiunti al keytab locale

```
nerone# ./kadmin
kadmin.local: ktadd host/nerone.it@SPARTACO.IT
Entry for principal host/nerone.it with kvno 3, encryption type DES3-SHA1-HMAC added to keytab WRFILE:/etc/kadm5.keytab.
kadmin.local: quit
```

## Avviamo i server

modifichiamo il file /etc/services e il file /etc/inetd.conf

```
Spartaco# vi /etc/inetd.conf
klogind stream tcp nowait root /krb5/sbin/klogind klogind -ki
eklogind stream tcp nowait root /krb5/sbin/klogind klogind -eki
kshell stream tcp nowait root /krb5/sbin/kshd kshd -ki
ktelnet stream tcp nowait root /krb5/sbin/telnetd telnetd -a user
kftpd stream tcp nowait root /krb5/sbin/ftpd -a
~
~
```

## Avviamo i server

Non ci resta che avviare i due server e riavviare i servizi:

```
spartaco# /opt/krb5/sbin/krb5kdc
spartaco# /opt/krb5/sbin/kadmin
Spartaco# /etc/rc.d/init.d/inetd restart
```

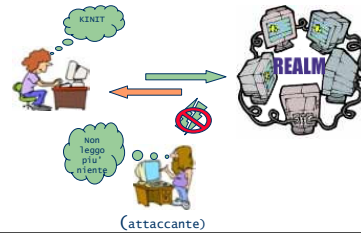
Con uno script posso rendere effettivi questi due comandi



## Lato Utente

Con il comando kinit inizia la sessione di lavoro

```
giomas@spartaco$ kinit
Password for giomas@SPARTACO.IT:
```



## Lato Utente

L'utente ha a disposizione altri comandi per gestire la sua cache di "ticket":

Klist: ci mostra i ticket acquisiti  
kdestroy: li distrugge

```
giomas@spartaco$ rlogin nerone
Welcome to nerone!
You've mail !
giomas@nerone$ ^d
```

Nessuna password  
Anche le comunicazioni si possono cifrare



## Pregi e difetti

Le limitazioni possono essere riassunte nei seguenti punti:

- Non protegge dalla possibilità di scoperta della password dell'utente
- Richiede in genere una macchina dedicata e sicura come Authentication server
- Le applicazioni devono essere in parte riscritte
- Superato il DES sussistono ancora conflitti con la legislazione degli USA
- l'installazione e' molto "intrusiva"

## Pregi e difetti

Tuttavia Kerberos ha anche dei pregi:

- E' scalabile
- La gestione centralizzata delle chiavi e degli utenti (revoca, rinnovo, cancellazione, ecc, ecc) è più semplice ed efficiente che in altri sistemi come SSL.
- E' un sistema FREE cioè aperto a tutte le modifiche e contributi.
- E' sicuro perché la chiave non circola sulla rete e non e' memorizzata in nessun posto oltre che la testa dell'utente e il KDC.
- E' flessibile, volendo usare una nuova tecnologia di autenticazione (per esempio un nuovo tipo di Smart Card con il proprio algoritmo), basta "solo" modificare il KDC.

## Kerberos V5

F I N E !

