Kerberos

1.1.Storia

Il Massachusetts Institute of Technology (MIT) sviluppò Kerberos per proteggere i servizi di rete forniti dal Project Athena. Il protocollo fu battezzato come il personaggio mitologico Cerbero, che nella mitologia greca era il cane a tre teste posto a guardia dell'Ade.

Le tre teste del Cerbero rappresentano le 3 funzionalità garantite da Kerberos: autenticazione, autorizzazione e cifratura.

Steve Miller e Clifford Neuman furono gli sviluppatori che lavorarono al’impleentaione delle versione 4 di Kerberos che però causò diversi problemi in particolare lagti agli algoritmi di cifratura a chiave simmetrica utilizzati all’interno del protocollo.

Il problema pricnipale di Kerberos v4 fu quello di non poter essere esportato in contesti di sicurezza globale in quanto utilizzava una versione di DES particolarmente vulnerabile detta “PCBC”.

La versione 5, progettata da John Kohl e Clifford Neuman, venne formalizzata nella RFC 1510 nel 1993 (resa obsoleta dalla RFC 4120 nel 2005), con l'intenzione di risolvere i limiti e i problemi di sicurezza della versione 4.

Nella versione 5 fu introdotta la possibilità di utilizzare algoritmi di cifratura a chiave simmetrica differenti e venne fornita un implementazione di DES detta CBC, in cui il controllo dell’integrità dei messaggi veniva svolto da un entit esterna rispetto all’algoritmo di cifratura stesso, andando a risolvere il problema delle vulnerabilità legate alla versione PCBC di DES.

Le autorità degli USA classificarono Kerberos come arma [senza fonte] e ne vietarono l'esportazione poiché utilizzava l'algoritmo di crittazione DES (con chiavi da 56 bit).

Una implementazione di Kerberos non statunitense, KTH-KRB sviluppata in Svezia, rese il sistema disponibile anche al di fuori degli Stati Uniti, prima che questi cambiassero la propria legge sull'esportazione degli algoritmi crittografici (attorno al 2000).

L'implementazione svedese del protocollo era basata su una versione di Kerberos detta eBones. eBones era basata sulla versione MIT Bones (in pratica una versione di Kerberos priva delle funzioni crittografiche e delle loro chiamate) ricavata da Kerberos 4 patchlevel 9.

L'australiano Eric Young, autore di diverse librerie crittografiche, reinserì le chiamate alle funzioni crittografiche utilizzando la propria libreria libdes. Questa versione limitata di Kerberos fu chiamata eBones. Una implementazione della versione 5 di Kerberos, Heimdal, fu rilasciata essenzialmente dallo stesso gruppo che creò KTH-KRB.

Windows 2000, Windows XP e Windows Server 2003 usano una variante di Kerberos come sistema predefinito di autenticazione.
Anche macOS di Apple utilizza Kerberos sia nella versione client sia in quella server.

1.2. Obiettivi e Funzionalità

L’obiettivo di Kerberos è quello di garantire comunicazioni sicure sulla rete tra più client e server tramite un sistema centralizzato.

Gli algoritmi crittografici, presi singolarmente, non sono in grado di garantire autenticazione, identificazione, confidenziaità ed integrita.

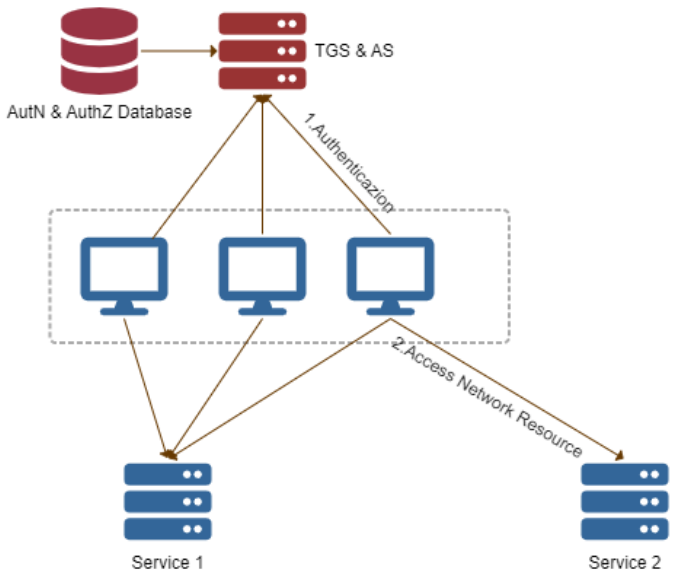
Bensì devono essere utilizzati come librerire all’interno di un protocollo che li sfrutta per ottenere una comuicazione sicura.

E’ di gran lunga importante considerare il peridodo storico in cui kerberos venne sviluppato: le aziende IT erano in massima espansione e si stava dirigendo tutto verso un organizzazione molto più strutturata dei sistemi interni alle aziende.

Il principale obiettivo di Kerberos era quello di fornire accesso sicuro alle risorse distribuite su una rete insicure e vi eran 2 modi per implementarlo:

- con algoritmo di cifratura a chiave asimmetrica
- con algoritmo di cifratura a chiave simmetrica coadiuvato da una TTP (Thrusted Third Party) di cui si fidano gli utenti della organizzazione e che possiderà una chiave per ognuno di essi e per ogni servizio.

Ora, immaginiamo uno scenario aziendale per il quale Kerberos rappresenta la solzuione ideale:



Abbiamo un’organizzazione con vari servizi di rete offerti internamente e varie workstation alle quali accederà ciascun utente dell’organizzazione.

Ciascuna workstation , prima di accedere ai vari servizi di rete offerti dall’organizzazione, dovrà ricevere autenticazione ed autorizzazione da server interno che implementerà il protocollo Kerberos e poi successivamente accedere ai servizi desiderati tramite le credenziali (ticket) ottenute da Kerberos.

In questo modo ciascun utente non dovrà necessitare di credenziali diverse per ogni servizio e Kerberos si occuperà di creare un canale sicuro tra client e servizi.

In questa ottica, come scelta progettuale è stato adottato un algoritmo di cifratura a chiave simmetrica coadiuvato da un TTP che svolgerà il ruolo di AS (Authentication Server) e che immagazzinerà tutte le chiavi segrete d ciascun
servizio e di ciascun client.

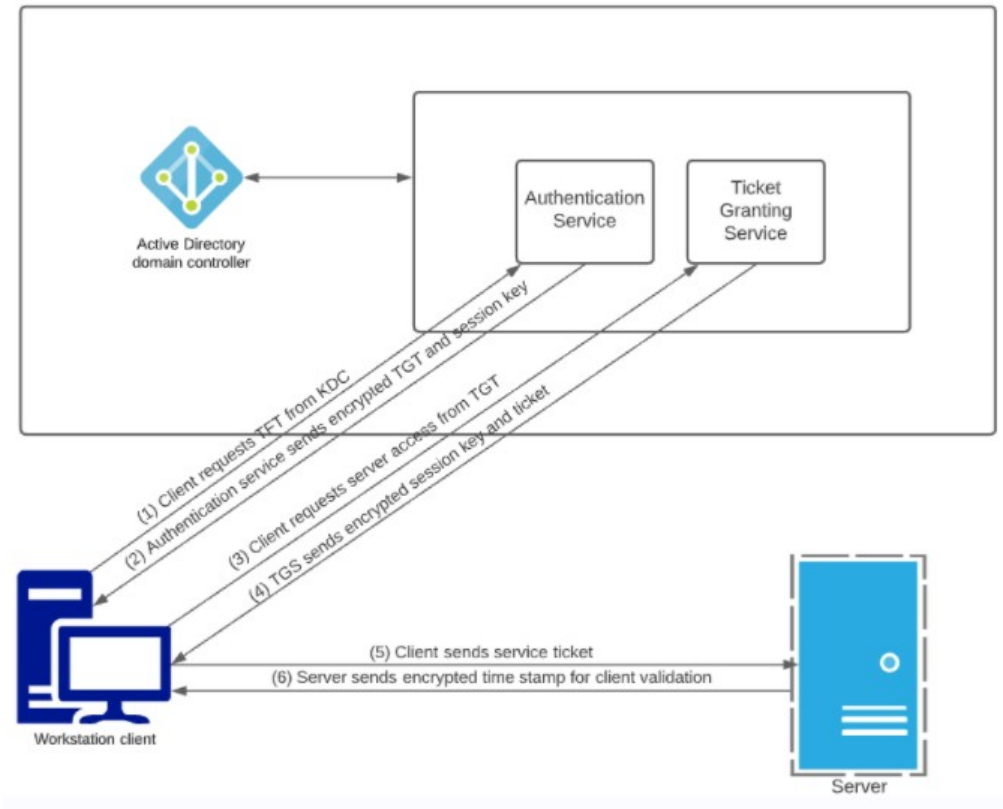
Un breve riassunto delle caratteristiche fondamentali di Kerberos può essere racchiuso in questi 3 punti:

- attraverso un unico sistema di autenticazione e memorizzazione delle credenziali permette a vari utenti del realm di accedere alle risorse/servizi offerti tramite un unico set di credenziali
- è basata sulla fiducia di una TTP che si occupa di autenticare utenti e servizi ed è garantita dall'organizzazione stessa
- sicurezza: le comunicazioni tra utenti e servizi sono sicure e non viene trasmessa nessuna password in chiaro sulla rete

E' importante notare come Kerberos svolga un ruolo fondamentale all'interno di un Realm: insieme di utenti suddivisi in gruppi, di servizi e di sistemi di autenticazione ed autorizzazione per garantire agli utenti un accesso sicuro e centralizzato ai servizi.

Di conseguenza, Kerberos è diventato il prtocllo di sicurezza più utilizzato all'interno di un dominio Realm diventando anche parte costituente del servizio di organizzazione aziendale più diffuso al mondo: Active Directory.

Ecco uno schema che illustra comeKerberos sia diventato parte costituente di Active Directory:



1.3.Autenticazione ad Autorizzazione Prima di Kerberos