Kerberos

D. Leeuw

15 januari 2024
v.0.6.0

Over dit Document

0.1 Leerdoelen

De lezer van dit document heeft na bestudering van de inhoud kennis van:

- wat kerberos is
- welk probleem kerberos oplost
- een globaal idee hoe de verschillende onderdelen van kerberos in elkaar zitten

0.2 Voorkennis

Van de lezer wordt verwacht dat hij kennis heeft van:

- netwerken
- hoe gebruikers en hun wachtwoorden worden opgeslagen binnen een operating system
- symmetrische encryptie

Inhoudsopgave

Hoofdstuk 1

Inleiding

Kerberos is een client-server architectuur. Het maakt het mogelijk om op een veilige manier authenticatie te doen over onveilge netwerken. Kerberos gaat ervan uit dat de verbinding niet versteuteld is en dat informatie op het netwerk dus afgeluisterd kan worden. Met deze aannames zorgt kerberos voor een sterke authenticatie van gebruikers en diensten waarbij de integriteit (Integrity) en de vertrouwelijkheid (Confidentiality) gewaarborgd zijn.

Bij authenticatie is het belangrijk dat zowel de zender als de ontvanger geverifieerd kunnen worden. Beide moeten zogezegd hun paspoort laten zien. Daarnaast is het belangrijk dat de data die over het netwerk gaat aankomt zoals deze verzonden is, de integriteit moet gewaarborgd zijn. Tot slot moet de gevoelige data niet afgeluisterd kunnen worden.

Kerberos bestaat uit drie delen:

- AS - Authentication Service
- TGS - Ticket Granting Service
- Service - De dienst waartoe we toegang willen hebben

De AS en de TGS zijn onderdeel van de KDC (Key Distribution Center).

Hoofdstuk 2

Netwerk authenticatie

2.1 Inloggen over een netwerk en de gevaren

Om in te kunnen loggen op een remote server of service is het nodig dat een gebruiker zich authentiseerd, meestal gebeurt dat via een gebruikersnaam en wachtwoord. Het versturen van een gebruikersnaam en wachtwoord over het netwerk kan tot gevolg hebben dat dit wordt afgeluisterd en dat een hacker de veschikking krijgt over deze gegevens. De een onderdeel van een Man-In-The-Middle (MITM) attack.

Een oplossing voor dit probleem is dat we gebruikersnaam en het wachtwoord zouden kunnen encrypten en het dan over de lijn sturen. Een boefje zou dan wel mee kunnen luisteren, maar kan uit de verkregen data niet de gebruikersnaam en het wachtwoord halen. Hij kan echter wel deze hashes opnieuw versturen naar en server. De server kan het verschil niet maken en ziet de juiste gehashte credentials binnen komen en staat de login toe. Dit heet een Replay-Attack.

De enige veilige manier is om geen wachtwoord over de lijn te laten gaan. Niet in plain-text en niet in een encrypte vorm. En dit is waar Kerberos om de hoek komt kijken. Kerberos is een systeem waar wachtwoorden veilig worden opgeslagen, er geen wachtwoorden over de lijn gaan en er toch voor gezorgd wordt dat er controle op een door de gebruiker opgegeven wachtwoord plaats vindt.

2.2 Single Sign On

Naast het veilig inloggen probeert Kerberos nog een ander inlog probleem op te lossen, namelijk het feit dat er voor elke dienst op het netwerk opnieuw ingelogd moet worden. Het zou makkelijker zijn als je na één keer inloggen

automatisch geauthoriseerd wordt als je je aanmeldt bij een dienst op het netwerk. De mogelijkheid om na één keer inloggen bij meerdere diensten op het netwerk te kunnen heet Single Sign On (SSO).

Kerberos gebruikt hiervoor tickets, zoals op een vliegveld. Als je een ticket hebt voor een vlucht dan mag je je koffer mee laten vliegen in het ruim, dan mag je je melden bij de douane en heb je toegang tot de vertrekhallen. Dit alles kan alleen maar als je een geldig ticket hebt voor een vlucht. Kerberos werkt op dezelfde manier, wanneer je een geldig Ticket Granting Ticket (TGT) hebt mag je additionele service tickets aanvragen die toegang geven tot andere diensten op het netwerk. Een geldig TGT krijg je als je de eerste keer correct kan inloggen en wordt uigegeven door de KDC .

Hoofdstuk 3

Key Distribution Center

Het centrale punt binnen Kerberos is de KDC (Key Distribution Center). De KDC is de database waar de wachtwoorden van gebruikers in een encrypte vorm (als hash) worden opgeslagen. Het is ook het deel dat tickets uitdeelt om te gebruiken op het netwerk.

De diensten die de KDC aan het netwerk aanbiedt zijn de Authentication Service (AS) en de Ticket Granting Service (TGS).

3.1 Authentication Service

De AS neemt een vraag tot authenticatie van een systeem op het netwerk aan en geeft aan dat systeem terug dat goed of niet goed is. Zoals gezegd gebeurt dit zonder dat het wachtwoord of een hash van het wachtwoord over het netwerk gaat.

Als een gebruiker in wil loggen op een systeem geeft de persoon een gebruikersnaam en wachtwoord op. Dat systeem stuurt naar de AS een bericht met daarin de gebruikersnaam die wil inloggen. Dit is het zogenaamde AS_REQ bericht en het bevat dus niet het wachtwoord!

De AS haalt op basis van de gebruikersnaam de hash van het wachtwoord van deze gebruiker uit de database. Ook wordt de hash van de Ticket Granting Service uit de database gehaald. Op basis van deze hashes worden twee nieuwe hashes gemaakt:

- Een Session Key, SK1, wordt versleuteld met de hash van de gebruiker.
- De SK1, de gebruikers IP-adres en de geldigheidsduur van SK1 worden versleuteld met de hash van het Ticket Granting System. Dit is het zogenaamde Ticket Granting Ticket (TGT)

Beide hashes worden terug gestuurd in de AS_REP naar de client.

De client ontvangt de hashes en kan door een hash te maken van het wachtwoord de SK1 ontsleutelen. Hiermee weet de client dat het wachtwoord correct was zonder dat het wachtwoord over de lijn is gegaan, dankzij symmetrische encryptie. Kan de client de hash niet ontsleutelen dan was of het opgegeven wachtwoord niet goed, of de AS is niet de juiste AS. Het kan natuurlijk zo zijn dat iemand probeert om met een valse AS de sessie te hijacken.

Met het TGT kan de gebruiker (client) additionele diensten aanvragen op het netwerk, zolang als de TGT niet verlopen is. De TGT toont aan dat de gebruiker correct is ingelogd. De gebruiker kan de TGT niet decrypten, omdat het versleuteld is met de key van de TGS, dus de enige die er iets mee kan is de TGS.

3.2 Tickt Granting Service

De Ticket Granting Service (TGS) is de dienst die door de KDC van kerberos aangeboden wordt om toegang te verlenen tot diensten en systemen. De gebruiker neemt met zijn TGT contact op met de TGS en vraagt daarbij toegang tot een bepaalde dienst. De TGS kan de TGT ontsleutelen omdat de TGT versleuteld is met de password hash van de TGS. De TGS controleert alle gegevens in de TGT en als het allemaal okee is dan wordt er een Service Ticket naar de gebruiker gestuurd. Het Service Ticket is versleuteld met de hash van de service, dus ook hier kan de gebruiker niets mee. De gebruiker stuurt het Service Ticket door naar de service, die kan met zijn eigen wachtwoord hash het Servive Ticket ontsleutelen en als dit lukt kent de service de gebruiksnaam en weet het dat de gebruiker geauthenticeerd is door de TGS.

Om dit allemaal op een juiste manier te laten verlopen maakt de gebruiker een aanvraag aan voor de TGS. Dit wordt de zogenaamde TGS_REQ. In deze TGS_REQ zit de naam van de service zoals kerberos die kent (principal name), de TGT en een zogenaamde Authenticator die versleuteld is met de Session Key die de gebruiker heeft.

Dit bericht komt aan bij de TGS. Deze kan met zijn hash de TGT ontsleutelen. Daarmee heeft de TGS de Session Key en kan dus de Authenticator ontsleutelen. Een ander ding dat uit het ontsleutelde bericht komt is het IP-adres van de aanvrager. De TGS kan dit adres vergelijken met het adres waarvan het het packet heeft verkregen. Is dit niet hetzelfde IP-adres dan probeert iemand waarschijnlijk een Replay-Attack uit te voeren. Is de Authenticator correct (time-stamp) en het IP-adres dan kan de TGS de aanvraag van de gebruiker vertrouwen.

De TGS maakt nu een bericht voor de gebruiker, de zogenaamde TGS_REP. De TGS encrypts een generated session key (SK2) voor de principal en de server met de Session Key en het encrypts een Service Ticket (ST2) voor de service met de hash van de service. Beide gaan in de TGS_REP en deze wordt verstuurd naar de gebruiker.

Met de Session Key kan de gebruiker de generated session key (SK2) van de TGS in de TGS_REP ontsleutelen. De gebruiker genereerd een nieuwe Authenticator (AUTH2) en encrypt deze met SK2. Deze nieuwe hash en de ontvangen ST2 hash worden doorgestuurd naar de service (AP_REQ).

De service ontvangt de AP_REQ. Met zijn eigen hash kan hij ST2 ontsleutelen en vindt daarin de SK2. Met de gevonden SK2 kan de service de AUTH2 hash ontsleutelen. Daarmee is de authenticatie van de principal tegen de service rond.

Hoofdstuk 4

Tot slot

Binnen kerberos is het noodzakelijk dat elke computer, gebruiker en dienst een hash heeft in de database van de KDC. Als je contact wil opnemen met een dienst die niet in de KDC staat dan gaat Single Sign On met kerberos niet werken.

Met het gebruik van kerberos gaan er geen wachtwoorden over de lijn, een encrypte verbinding is in theorie dan ook niet nodig. Afluisteren van het verkeer heeft niet zo veel zin.

Tickets hebben een levensduur en gaan kort mee (TGT een paar uur). Ook de berichten over het netwerk zijn voorzien van een time-stamp en hebben een beperkte geldigheid (5 minuten). Alles is voorzien van een time-stamp zodat replay attacks buitengewoon moeilijk worden. Omdat tijd zo'n belangrijk onderdeel is van het goed functioneren van kerberos is het van cruciaal belang dat de klokken in een netwerk gesyncroniseerd zijn. Dus NTP is meestal van cruciaal belang.

Meer informatie:

- https://web.mit.edu/kerberos/www/papers.html

Index