Kerberos

Čo to je?

Sieťový protokol umožňujúci vzájomnú autentifikáciu klienta a servera. Je založený na symetrickej kryptografii a preto sa vyžaduje tretia dôveryhodná strana. Protokol je vhodné nasadiť na siete, ktoré sú nezabezpečené, pretože zabezpečuje integritu posielaných dát a bráni útokom **REPLAY**. Štandardne používa port 88.

Windows servery používajú Kerberos ako primárny autentizačný mechanizmus. Pracuje v spojení s Active Directory

Kerberos Tickets:

Kerberos používa ticket ako dôkaz, ktorý preukazuje identitu používateľa. Sú digitálne dokumenty, ktoré uchovávajú session key. Vydávajú sa zvyčajne počas prihlásenia a potom môže byť použité namiesto hesiel pre každé Kerberos služby. Počas priebehu overovania, klient dostáva dva lístky:

TGT – Ticket granting ticket, ako globálny identifikátor pre užívateľa

Service ticket – overuje požívateľa do konkrétnej služby

Tickety zahŕňajú aj časovú pečiatku, ktoré indikuje vypršanie platnosti.

Ako to funguje?

Je trojstranným protokolom, účastníkmi sú klient, server, a ďalší dôveryhodný server. Dôveryhodný server sa nazýva **Key Distribution Center (KDC)** a delí sa na 2 časti:

- **Authentication Server (AS)**
- **Ticket Granting Server (TGS)**

KDC pozná heslá všetkých užívateľov a služieb na spracovanie sieti.

Skratky:

Tiket: Základ autentizácie, posiela sa po sieti namiesto hesla. Obsahuje spravidla klientovú identifikáciu, session key(= dočasný šifrovací kľuč) a timestamp. Vždy zašifrovaný.

KDC: Server, ktorý autentizuje, resp. sada serverov – AS(authentication server), - TGS (ticket granting server) a hlavne databázu/ katalóg identít klienta a ich

údajov. Okrem šifrovania v záznamoch o heslách(hashoch) je celá databáza ešte šifrovaná pomocou tzv. Master key.

AS: Autentizačný server

TGS: Riadiaci server

TGT: Tiket oprávňujúci užívateľa ku komunikácií s riadiacim serverom

Autorizácia klienta

Klient sa autentifikuje voči KDC tak, že kontaktuje AS a vyžiada si nový **tiket**, ktorý ho v budúcnosti bude oprávňovať k získaniu tiketov pre jednotlivé služby.

AS pošle klientovi správy, ktoré obsahujú **Session Key**, ktorý je zašifrovaný hashovaným heslom z databázy KDC a **Ticket Granting Ticket (TGT)**, ktorý je zašifrovaný privátnym kľúčom TGS.

Ticket Granting Ticket sa skladá z ID klienta, jeho sieťovej adresy, session key a časovej platnosti tiketu.

Klient si pomocou svojho zahashovaného hesla (zadaného užívateľom) rozšifruje správu, ktorá obsahuje session key.

Autorizácia prístupu ku službe

V prípade, že chce klient pristúpiť k nejakej službe, tak kontaktuje **TGS** poslaním stále **zašifrovaného TGT**, ID služby, ktorej sa dožaduje a **svoje ID** aj s timestampom, zašifrovaný pomocou Session key.

TGS si môže prečítať **obsah TGT** pomocou svojho privátneho kľúča TGS. Pomocou Session key(ktorý bol v TGT) si odšifruje druhú správu.

Odošle klientovi Client/Server Ticket, ktorý obsahuje ID klienta, jeho adresu, dobu platnosti a session key client/servera všetko zašifrované pomocou tajného kľúča Session key služby. Tiež mu pošle client/server session key zašifrovaný pomocou pôvodného session key.

Potom sa musí klient autentifikovať voči službe, teda pošle klient/server tiket zašifrovaný tajným kľúčom služby a svoje ID spolu s timestampom zašifrovaný

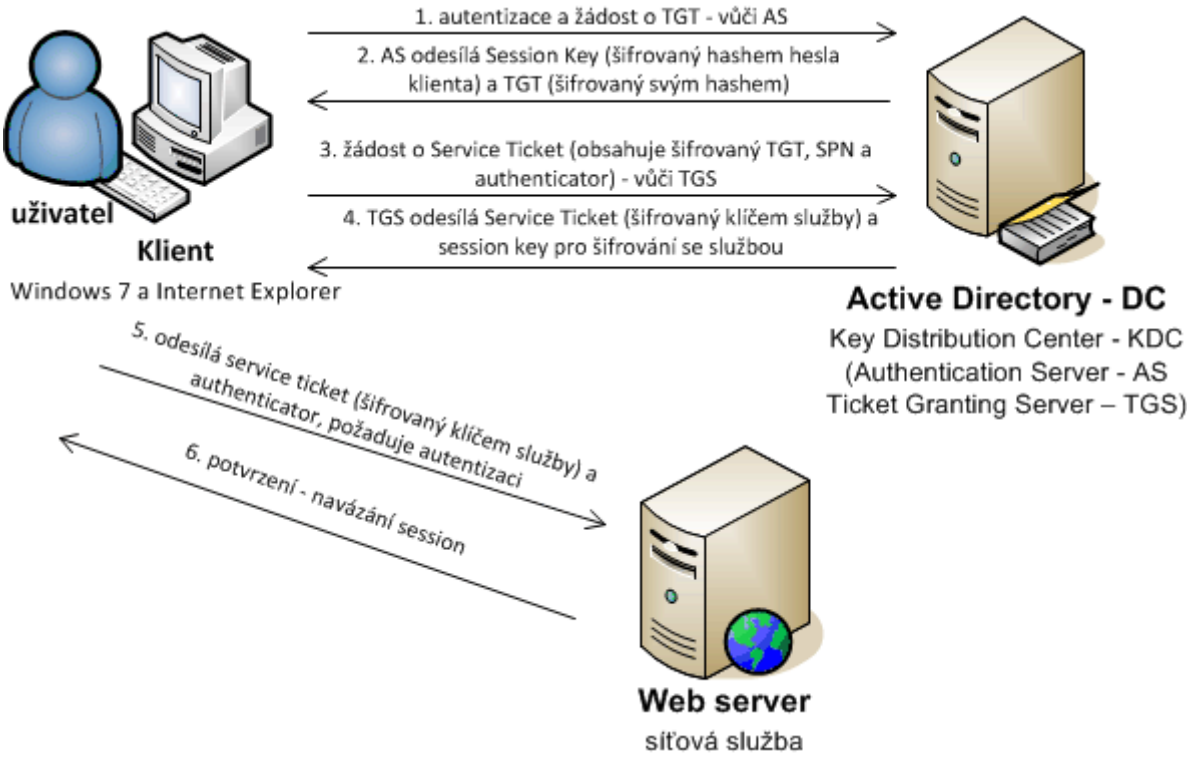
pomocou client-server session key. Tento key si dokázal prečítať pomocou Session key.

Služba si pomocou svojho privátneho kľúča prečíta tiket a pomocou informácií v ňom si pozrie aj druhú časť správy. Získa client/server key

Na záver pošle správu obsahujúcu timestamp+1 zašifrovanú pomocou klient-server key.

Klient skontroluje či je timestamp správne zväčšený o 1 a zaháji využívanie danej služby.

Zjednodušený obrázok:



Výhody :

- Je navrhnutý tak, aby bol bezpečný aj keď sa vykonáva cez nezabezpečenú sieť
- Každý prenos je šifrovaný pomocou vhodného tajného kľúča, útočník nemôže sfalšovať ticket na získanie prístupu k službe
- Ochrana pred replay útokmi kvôli časovej pečiatke, ticket môže obsahovať aj IP adresu, využíva replay cache(overuje predchádzajúce tokeny a detekuje opätovné používanie)

Riziká :

- Najväčšie riziko je v nutnosti nepretržitého behu centrálného server. Ak nebeží, nikto sa nemôže prihlásiť. Dá sa riziko odstrániť tým, že sa nasadia viac kerberos serveri a záložné autentizačné mechanizmy.

- Kerberos má prísne požiadavky na synchronizáciu času klientov a serverov. Tikety majú svoju životnosť a ak nie je čas klienta synchronizovaný s časom servera tak sa nedá autentizovať. Štandard je, že sa časy nemajú rozchádzať o viac ako 5 minút.

- Administračný protokol nie je štandardizovaný a líši sa podľa implementácie.

- Keďže je celá autentizácia riadená centrálne cez KDC, narušením tejto infraštruktúry dostane útočník možnosť vydávať sa za akéhokoľvek užívateľa.