Secure Socket Layer je široko uporabjen vendar sedaj skoraj zastarel protokol, ki ga je zamenjal **TLS**, RFC 2246. Ta varnostni protokol zagotavlja *zaupnost*, *celovitost*, *avtentikacijo* na višjih plasteh ISO/OSI modela.

Poenostavljeni SSL

SSL poenstavljeno deluje v 4 korakih: 1. **Rokovanje**: Oba udeleženca komunikacije se drug drugemu avtenticirata z uporabo *certifikatov* in izmenjata glavni ključ. ![[Pasted image 20230111213414.png]]

2. **Izpeljava ključev**: Izpeljeta množico ključev glede na glavni ključ (pogosto se lahko zamenjajo te ključi). ![[Pasted image 20230111213536.png]]
3. **Prenos Podatkov**: Podatki, ki se prenašajo, so zapisani in združeni v zapise. ![[Pasted image 20230111213753.png]] Razlika je, da je osnovna enota tok podatkov, ki ga razbijemo na zapise, ni nujno da je vsak zapis konec toka. Pri blokovnem šifriranju je vsak blok poslan posebaj. ![[Pasted image 20230111214017.png]]
4. **Zaključek povezave**: Za varen zaključek se uporabljajo posebna sporočila. ![[Pasted image 20230111214051.png]]

![[Pasted image 20230111214105.png]]

> Rokovanje je najšibekši člen SSL pogovora, tukaj se izmenjajo podatki o ključih in identitetah. Če bi bila ta faza na kakršenkoli način kompromizirana, bi lahko hudo vplivalo na slednje faze.

Torej, da lahko komunikacija steče, moramo zagotoviti, da rokovanje poskrbi da: - A res govori z B-jem in da B res govori z B-jem - Glavni ključ, iz katerega nato izpeljemo ključa za zakrivanje (A ->B in B -> A) ter ključa za preverjanja celovitosti (A -> B in B -> A). - Način računanja MAC-a (Hash funkcija) in Šifriranja (DES, 3DES)

> Napad na takšno komunikacijo lahko izvedemo, tako da: + Probamo ukrasti ključe ali šifriranja ali za celovitost + Probamo odkriti parametre šifriranja ali parametre računanja MAC-a + Lahko pa probamo ukrasti identiteto enega ali drugega ter se predstavimo, kot oni

Pravi SSL

SSL dejansko v fazi rokovanja izvede avtentikacijo strežnika, izbiro algoritmov, določanje ključev, avtentikacijo odjemalca (opcijsko). ![[Pasted image 20230112134955.png]]

> Certifikat vsebuje B-jev javni ključ, s katerim zašifrira nadaljni promet. PMS = Pre-Master Secret

V korakih 5 ni 6 se pošlje MAC, saj tako A in B zagotovita celovitost rokovanja, da napadalec in bil vmešan v 1. in 2. korak.

Preden se začne komunikacija, je potrebno ustvariti ključe, s pomočjo žetona odjemalca in PMS-ja se izračuna **Master Secret**. Ta MS in novi žeton se vstavijo v drugo funkcijo in dobimo nek BLOK, ta se razreže na 6 delov: - MAC ključ odjemalca - MAC ključ strežnika - Šifrirni ključ odjemalca - Šifirni ključ strežnika - Inicializacijski vektor (IV) odjemalca - Inicializacijski vektor (IV) strežnika

Na koncu pa se podatki pretvorijo še v dele, ki jih imenujemo zapise, preden jih šifriramo. Fragment je vedno enako dolg, neglede na podatke, saj recimo v simetričnem šifriranju uporabljamo blokovno šifriranje in le to ima določeno velikost podatkov, ki jih moramo imeti v bloku. ![[Pasted image 20230112140657.png]]