Ssl

ssl is een techniek om internet verkeer te beveiligen tussen de server en de cliënt. Inmiddels zijn alle versies van ssl verboden geworden omdat ze niet voldoende beveiligd zijn tegen inbreuken, de opvolger van ssl heet tls. Ondanks dat ssl niet meer wordt gebruikt word het nogsteeds vaak zo genoemed maar eigenlijk hebben mensen het dan over tls. In de basis is ssl een tegniek om websites te versleutelen zodat aanvallers het internet verkeer niet kunnen afluisteren. Het gebruikt een asymetrise sleutel, dat betekend dat er twee sleutels zijn, een voor de host en een voor de cliant, deze twee samen worden combineert tot een symmetrische sleutel, deze is voor iedere cliant/host combinatie anders.

Chifer

er is niet een ssl manier, er zijn meerdere soorten encryptie algoritme en deze kunnen allemaal gebruikt worden. Per ssl transactie zijn drie algoritmes nodig: het algoritme dat zorgt voor het uitwisselen van de sleutels, het algoritme om de html massages te versleutelen en een algoritme om de web pagina te versleutelen. Deze drie algoritmes samen noem je de chifer. Sommige chifers zijn zeer zwak en heel makkelijk te breken door derde, daarom is het afgeraden om deze chifers te gebruiken. De chifers van ssl zijn per definitie allemaal zwak, daarom mag ssl niet meer gebruikt worden. De chifers van tls verschillen in sterke sommigen zijn goed anderen zijn zeer zwak. Hier onder een lijstje van ssl/tls chifers, Yes betekend dat het nog niet gebroken is, no betekend dat de chifer al gebroken is door aanvallers. De onderste twee chifers zijn nog niet gebroken maar ze zijn wel per defenietie niet veilig.

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (Draft)
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
DH-DSS	No	Yes	Yes	Yes	Yes	No
DHE-DSS (forward secrecy)	No	Yes	Yes	Yes	Yes	No[40]
ECDH-ECDSA	No	No	Yes	Yes	Yes	No
ECDHE-ECDSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
PSK	No	No	Yes	Yes	Yes	
PSK-RSA	No	No	Yes	Yes	Yes	
DHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	
ECDHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	
SRP	No	No	Yes	Yes	Yes	
SRP-DSS	No	No	Yes	Yes	Yes	
SRP-RSA	No	No	Yes	Yes	Yes	

Kerberos	No	No	Yes	Yes	Yes
DH-ANON (insecure)	No	Yes	Yes	Yes	Yes
ECDH-ANON (insecure)	No	No	Yes	Yes	Yes