TLS-KDH

Project omschrijving
Het TLS-KDH project combineert het Transport Layer Security protocol, dat momenteel op het Internet het meest gebruikte protocol is voor end-to-end encryptie, met het Kerberos protocol, dat het meest gebruikte authenticatie protocol is. Daarnaast wordt er standaard gebruik gemaakt van het Diffie-Hellman key exchange algoritme, waardoor alle Kerberos sessies standaard voorzien zijn van perfect forward secrecy.

Impact
TLS-KDH breidt het TLS protocol uit met een nieuwe authenticatie methode, nl. Kerberos. Dat betekent dat TLS niet meer alleen afhankelijk is van een public-key infrastructuur (PKI) voor authenticatie (bijv. X.509) maar nu ook gebruik kan maken van een centraal beheerde (Kerberos) authenticatie service. Dit biedt meer flexibiliteit met betrekking tot de toepasbaarheid van het procotol en daarnaast een alternatief met betrekking tot het type security van het systeem dat wordt gebouwd op TLS (gedistribueerd / multiple attack surfaces vs gecentraliseerd / single attack surface). Daarnaast wordt Kerberos heel veel toegepast in corporate security systemen en wordt TLS veel gebruikt in consumer systemen. TLS-KDH verbindt deze twee werelden op een manier dat beiden van elkaars sterke punten kunnen profiteren en waarbij tevens een aantal zwakke punten worden aangepakt. TLS-KDH is verder gebouwd op GnuTLS, een van de grotere open-source TLS bilbiotheken, en hiermee is de nieuwe functionaliteit meteen toegankelijk voor de rest van de Internet gemeenschap. Een volledige lijst van voordelen van TLS-KDH is te vinden op http://tls-kdh.arpa2.net/

Mensen achter TLS-KDH
Het TLS-KDH project wordt gedreven door Rick van Rein en Tom Vrancken. Rick is de hoofd architect en initiatiefnemer van het project. Tom is afgestudeerd op het uiteindelijke ontwerp en prototype van TLS-KDH.

Toekomstplannen
Een proof-of-concept van het ontwerp is inmiddels gebouwd en getest. TLS-KDH is gebouwd op GnuTLS en wordt momenteel als een eigen fork gebruikt in het TLS Pool project van ARPA2. Daarnaast zijn we, samen met de head maintainer van GnuTLS, bezig om onze fork van GnuTLS samen te voegen met de hoofd ontwikkel tak van GnuTLS zodat de TLS-KDH functionaliteit beschikbaar komt voor de Internet gemeenschap over de hele wereld.