Data Security H3: Beveiligde toepassingsprotocollen

Inhoud

[Terminologie 3](#_Toc466206250)

[SSL, TLS, HTTPS 3](#_Toc466206251)

[SSH 3](#_Toc466206252)

[HSTS 4](#_Toc466206253)

[DKIM 4](#_Toc466206254)

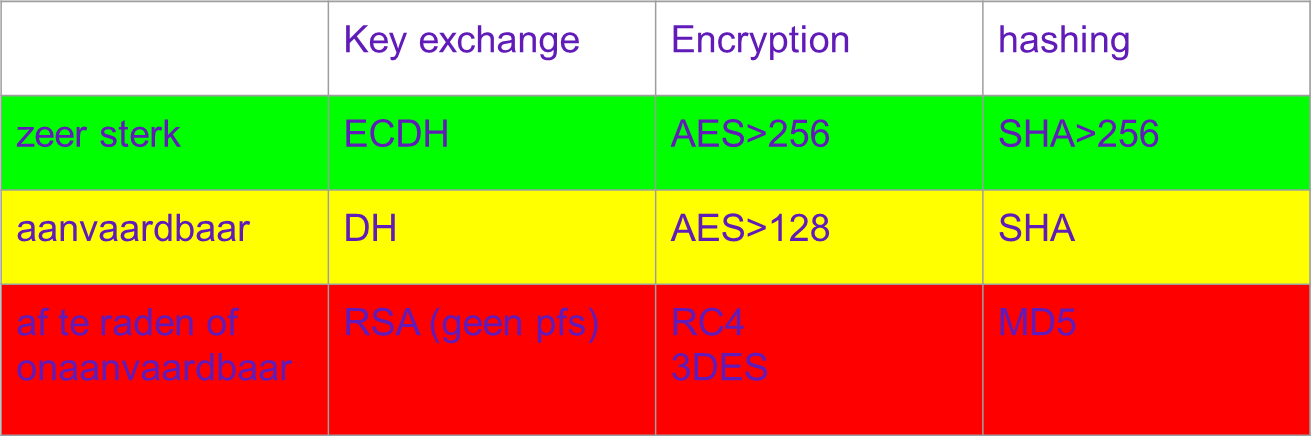
[SPF 4](#_Toc466206255)

[Andere beveiligde toepassingsprotocollen 4](#_Toc466206256)

# Terminologie

* Perfect forward secrecy: zelfs als de master key verloren gaan, dan nog kan je een gecapteerde conversatie niet vertalen

# SSL, TLS, HTTPS

* HTTPS: HTTP over een secure kanaal (SSL of TLS)
* SSL (Secure Sockets Layer)
* TLS (Transport Layer Security): opvolger van SSL
* Keuze van protocolsuite (voorbeeld)
  + ECDHE - ECDSA - AES128 - SHA256
  + ECDHE = key selection protocol
  + ECDSA = signing/certificates
  + AES128 = symmetrische encryptie
  + SHA256 = hashing protocol
  + 
* MITM: 2 sessies opzetten: 1 client<->aanvaller, 1 aanvaller<->server
* Poodle: CBC weakness in SSL3.0, MITM nodig om SSL versie te bepalen & pakketten te injecteren
* Beast: java applet om Same Origin Policy te omzeilen, CBC weakness uitbuiten
* HTTPS-problemen: concept blijft overeind
  + Aanvallen gericht op:
    - Onderhandeling
      * VB: degradation naar SSL3
      * VB: export keys
    - Implementatie
      * Bugs/zwaktes in openssl & andere SSL/TLS-bibliotheken
        + VB: Heartbleed
      * Slecht gekozen ciphers
        + VB: standaard Diffie-Hellman keys op veel servers

# SSH

* Public key encryption, in combinatie met cipher voor encryptie
* Kan gebruikt worden als tunnel met kanalen voor andere protocollen (VB: SFTP)

# HSTS

* HTTP Strict Transport Security
* Manier om SSLstrip-achtige aanvallen tegen te gaan
* Forceert HTTPS-connecties voor (sub)domeinen
* Ondersteund door alle recente browsers
* Werking: bij 1e request naar een site wordt een headerveld toegevoegd:
  + Strict-Transport-Security: max-age=15768000 ; includeSubDomains

# DKIM

* DomainKeys Identified Mail
* Laat een organisatie verantwoordelijkheid nemen voor een bericht in transit
* De organisatie is een afhandelaar van het bericht, hetzij als verzender of als tussenpersoon
* De reputatie van de organisatie is de basis om te evalueren of het bericht vertrouwd mag worden voor verdere stappen, zoals de levering
* DKIM voorziet een maniet om een domain name te valideren die met een bericht geassocieerd is via cryptografische authenticatie

# SPF

* Sender Policy Framework
* Email-validatiesysteem dat email spoofing detecteert
* Voorziet een mechanisme waardoor mail exchangers kunnen verifiëren of een binnenkomende email van een domein afkomstig is van een host die daar de bevoegdheid voor heeft
* De lijst van bevoegde hosts staan vermeld in de DNS-records voor een domein, als TXT-record
  + VB: v=spf1 a:mail.mijndomein.com -all
  + Uitleg:
    - v=spf1: de gebruikte versie is SPF 1
    - a: enkel de mailserver “mail.mijndomein.com” mag emails versturen
    - -all: alle andere emails zijn spam

# Andere beveiligde toepassingsprotocollen

* FTPS: FTP over TLS (niet te verwarren met SFTP: FTP over SSH)
* SMIME
* IMAP over SSL
* POP over SSL
* ...