TLS results in AR mail header

Franck Martin

draft-martin-authentication-results-tls

Why?

- rDNS/SPF/DKIM/DMARC is already there
- TLS has a certificate and is also a form of authentication
- Facebook showed >90% of STARTTLS is not opportunistic anymore (1)
- Easier to read a mail header than the mail logs
- Abuse/Security handling made easier
- If header is trusted, MUA can use and abuse (eg. procmail)

(1) https://www.facebook.com/notes/protect-the-graph/massive-growth-in-smtp-starttls-deployment/1491049534468526

Example: no TLS

Authentication-Results: xxxxx.linkedin.com;

iprev=pass policy.iprev="204.232.133.74";

spf=pass
smtp.mailfrom=”xxxxx@messagesystems.com"
smtp.helo="b.mx.messagesystems.com";

dkim=pass header.d=messagesystems.com;
tls=none;

dmarc=pass (p=none; dis=none)
header.from=messagesystems.com

Example: TLS (no CA)

Authentication-Results: xxxxx.linkedin.com;

iprev=pass policy.iprev="2001:1900:3001:11::2c";

spf=pass smtp.mailfrom="dmarc-bounces@ietf.org" smtp.helo="mail.ietf.org";

dkim=pass header.d=ietf.org; dkim=fail (signature verification failed) header.d=gmail.com;

tls=fail (unverified) key.ciphersuite="TLS_RSA_WITH_AES_256_GCM_SHA384" key.length="256" tls.v="tlsv1.2" cert.client="" cert.clientissuer="";

dmarc=fail (p=none; dis=mailing_list) header.from=gmail.com

Example: TLS (CA)

Authentication-Results: xxxxxx.linkedin.com;

iprev=pass policy.iprev="2607:f8b0:4001:c03::232";

spf=pass smtp.mailfrom=”xxxxxx@gmail.com" smtp.helo="mail-ie0-x232.google.com";

dkim=pass header.d=gmail.com;

tls=pass (verified) key.ciphersuite="SSL_RSA_WITH_RC4_128_SHA" key.length="128" tls.v="tlsv1" cert.client="C=US,ST=California,L=Mountain View,O=Google Inc,CN=smtp.gmail.com" cert.clientissuer="C=US,O=Google Inc,CN=Google Internet Authority G2";

dmarc=pass (p=none; dis=none) header.from=gmail.com

Next steps

- WG adopts
- Review ptypes and results
- Write code

Questions?