DNA Authentication Alternatives

IETF 81

Eric Rescorla

ekr@rtfm.com

Problem Statement(per Richard Barnes)

- *XMPP outsourcing providers don't want to have to hold certificates with their clients' domain names in them.*
  - *Risk of key compromise, hijacking other services, masquerading, etc.*

- Note: this is absolutely standard practice for Web hosting

  ... but let's assume it's bad for XMPP

How To Provide a certificate that can only be used for XMPP

- Threat then limited to XMPP service
- Options:
  - XMPP URI in SAN
  - Certificate with special name in the SAN or CN
    - E.g., `__xmpp__.example.com`
    - Unlikely this will be confused with any other kind of cert
  - May need to modify XMPP clients to detect this kind of cert
    - But modification needed for DNSSEC in any case

Putting it Together

- Hosting provider server has multiple certs
  - His own cert, which he uses for most connections
  - One cert for each customer, which he used to validate the binding to his cert
- Certificate selection is by SNI