TLS-KDH

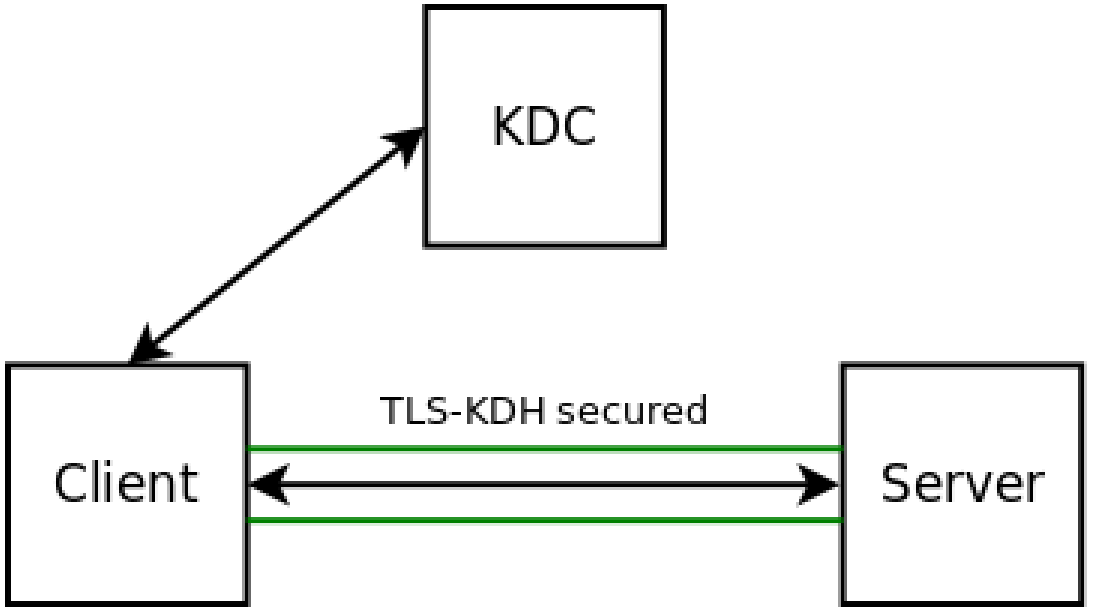
Tom Vrancken
ARPA2.net

Agenda

- What is TLS-KDH?
- What are its use cases?
- Where should it land?

What is TLS-KDH?

- Kerberos-based authentication mechanism for TLS
- Kerberized Diffie-Hellman KX
- Combine / connect the worlds of Kerberos and TLS



What is TLS-KDH?

- Two modes of operation:
  - KDH-only
  - KDH-enhanced
- KDH-only
  - Only Kerberos-based authentication
  - Mutual authentication based on client ticket
- KDH-enhanced
  - Regular certificate-based (e.g., X.509) auth enhanced with Krb auth
  - Based on server certificate and client ticket

TLS-KDH use cases

- Alternative strong auth mechanism for TLS
  - Next to PSK and PKIX
  - Serves different usage scenarios
- Quantum hardening TLS KX
- TLS-protected Kerberos sessions
  - Perfect forward secrecy
- SPNEGO alternative / replacement

Where should it land?

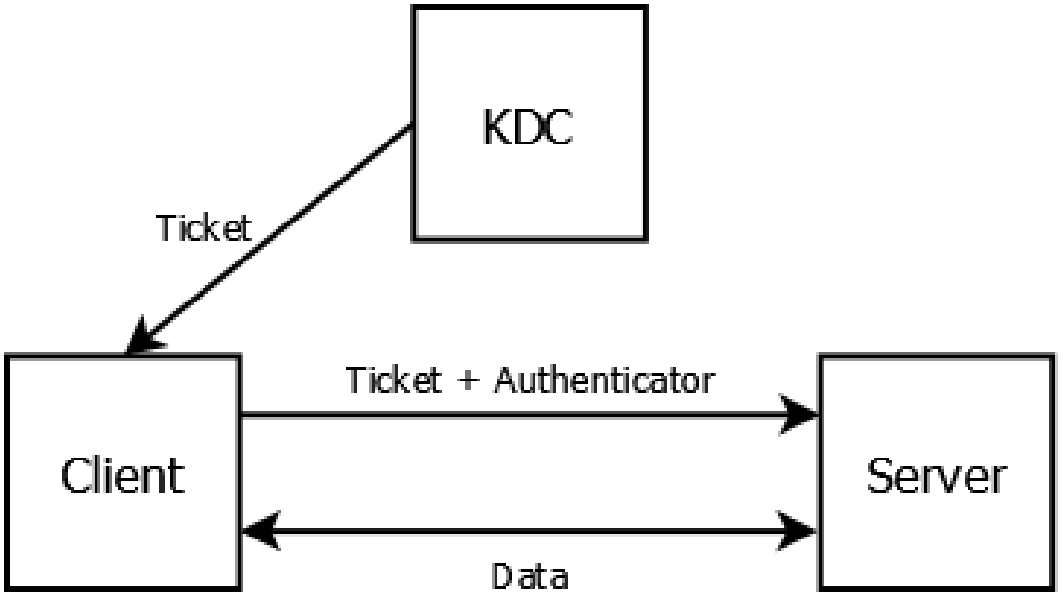
- Is TLS-KDH
  - Viable?
  - Feasible?
  - Applicable?

- Go / no go?
  - If yes, where should we go?
    - TLS wg, Kitten wg?

Draft spec

- https://datatracker.ietf.org/doc/html/draft-vanrein-tls-kdh

Krb auth



What realm owns the host(name)?

- `_kerberos.hostname IN TXT “EXAMPLE.COM”`
- draft-vanrein-dnstxt-krb1
  - https://datatracker.ietf.org/doc/html/draft-vanrein-dnstxt-krb1-11