Guidance for External PSK Usage in TLS

I-D: https://datatracker.ietf.org/doc/draft-dt-tls-external-psk-guidance/
Editor's Copy: https://github.com/tlswg/external-psk-design-team

IETF TLS Virtual Interim
April 27, 2020

Motivation

draft-ietf-tls-external-psk-importer merely fixes a “bug” in TLS 1.3, but:

- Lacked guidance for when applications should import PSKs.
- Under developed Selfie mitigation guidance.
- Omitted implications on PSK provisioning machinery.
- ...

External PSK (EPSK) Use Cases

Pairwise EPSK usage:

- Device-to-device communication with out-of-band synchronized keys.
- Intra-data-center communication.
- Certificateless server-to-server communication.
- Internet of Things (IoT) and devices with limited capabilities.
- The Generic Authentication Architecture (GAA) defined by 3GGP.
- Smart Cards.

Widely shared EPSKs also exist: group chats, IoT systems, etc.

Design Team Goals

Provide guidance for external PSK (EPSK) usage in TLS!

- Clarify EPSK security and privacy properties.
- Suggest “simple” recommendations for EPSK usage.
- Discuss provisioning processes and constraints (legacy systems, TLS stack interface limitations, etc.).

Security Properties

Fundamental EPSK authenticity assumption:

> *Each PSK is known to exactly one client and one server and these never switch roles.*

Problems if violated:

- Any (compromised or uncompromised) group member can impersonate any other group member.
- If PSK without DH is used, then compromise of any group member allows the attacker to passively read all traffic.

Recommendations

Each PSK SHOULD be derived from at least 128 bits of entropy, MUST be at least 128 bits long, and SHOULD be combined with a DH exchange. *Low-entropy PSKs SHOULD be used in conjunction with PAKEs*.*

Each PSK MUST NOT be shared between with more than two logical nodes *unless other accommodations are made*.*

**Changes proposed by Verisign review.*

Recommendations (cont’d)

Nodes SHOULD use external PSK importers.

Unimported PSKs SHOULD be deleted after import (where possible).

Next Steps

Seek further review before making additional changes

Adopt as WG document

Questions?

Thanks to the DT Members!

Benjamin Beurdouche, Bjoern Haase, Chris Wood, Colm MacCarthaigh, Eric Rescorla, Jonathan Hoyland, Martin Thomson, Mohamad Badra, Mohit Sethi, Oleg Pekar, Owen Friel, Russ Housley