The Hashed Token SASL Mechanism

draft-ietf-kitten-sasl-ht-00

2025-03-17

Florian Schmaus

IETF 122 Bangkok

Motivation

- application protocols using a persistent connection
- connection re-establishment becomes more frequent
- connection re-establishment takes a long time

Motivation

XMPP login takes too long...

Motivation

XMPP login takes too long...

- Note: Numbers are from my FOSDEM 2015 talk [4]
- Numbers are with 80ms round-trip

Phase	Time
TCP connect incl. DNS	60ms
Client-Server Initial Stream	80ms
TLS RFC 6120 § 9.1.1	420ms
SASL RFC 6120 § 9.1.2	470ms
Compression XEP-138	160ms
Stream Management XEP-198	190ms
Roster retrieval using versioning	80ms
Privacy List already set	80ms
Total (Real)	1750ms
Total (Sum. Parts)	1540ms

Suite of XMPP Extension Protocols (XEPs) to address this issue (and others)

Suite of XMPP Extension Protocols (XEPs) to address this issue (and others)

Extensible SASL Profile (XEP-0388) [1]

- SASL is now the outer layer
- see also the SASL 2 I-D [2]

Suite of XMPP Extension Protocols (XEPs) to address this issue (and others)

Extensible SASL Profile (XEP-0388) [1]

- SASL is now the outer layer
- see also the SASL 2 I-D [2]

Bind 2 (XEP-0386) [6]

single step feature negotiation

Suite of XMPP Extension Protocols (XEPs) to address this issue (and others)

Extensible SASL Profile (XEP-0388) [1]

- SASL is now the outer layer
- see also the SASL 2 I-D [2]

Bind 2 (XEP-0386) [6]

single step feature negotiation

Fast Authentication Streamlining Tokens (XEP-0483) [7]

Suite of XMPP Extension Protocols (XEPs) to address this issue (and others)

***Extensible SASL Profile* (XEP-0388) [1]**

- SASL is now the outer layer
- see also the SASL 2 I-D [2]

***Bind 2* (XEP-0386) [6]**

single step feature negotiation

SASL-HT [5]

SASL-HT token used to authenticate

***Fast Authentication Streamlining Tokens* (XEP-0483) [7]**

SASL-HT [5]

obtain token

The Hashed Token SASL Mechanism (SASL-HT)

Hashed **Token**

Token

- quick re-authentication using a token
- token is obtained after authentication via “strong” SASL mechanism
- token is required to
  - be generated by a cryptographically secure randon number generator
  - contain at least 128 bits of entropy
- application-protocol specific extension to obtain token required, for example the XMPP Extension Protocols (XEPs):
  - *Fast Authentication Streamlining Tokens* [7]
  - *Instant Stream Resumption* [3]

Hashed Token

Hash

- token is protected by cryptographically secure hash
- SASL-HT uses the TLS channel-binding data as key for the HMAC function
- additional benefit: *mutual authentication*
- even without channel-binding data, attacks based on pre-computed hash values seem not practical given that the token is at least a 16-byte number

Hashed Token

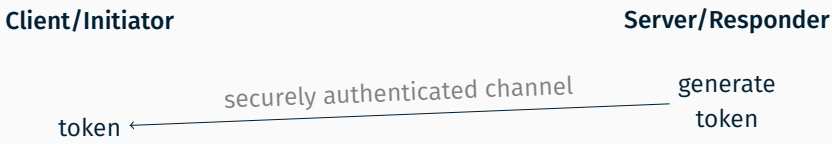
Hash

- token is protected by cryptographically secure hash
- SASL-HT uses the TLS channel-binding data as key for the HMAC function
- additional benefit: *mutual authentication*
- even without channel-binding data, attacks based on pre-computed hash values seem not practical given that the token is at least a 16-byte number

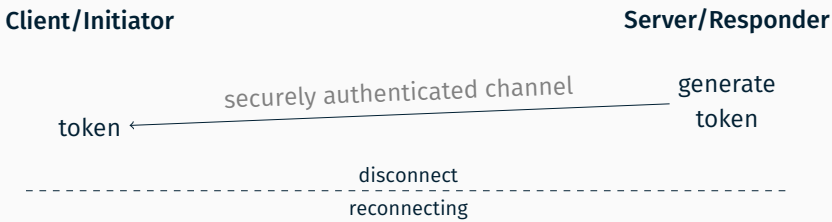
Channel Binding

- unfortunately not all environments support channel binding
- therefore, SASL-HT specifies the NONE channel-binding type

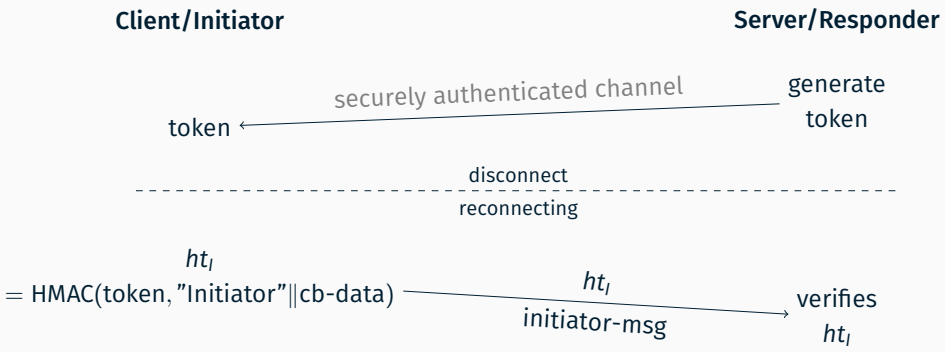
SASL-HT Authentication Sequence



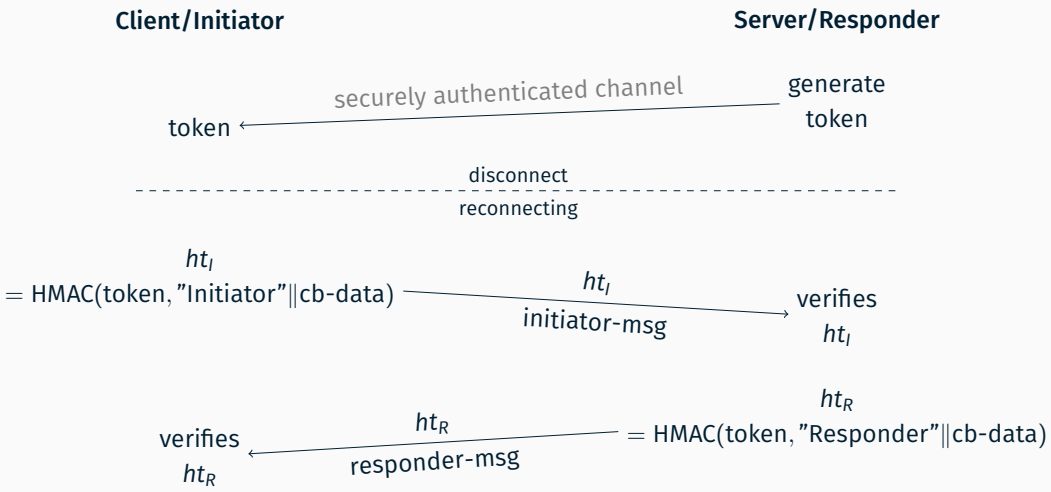
SASL-HT Authentication Sequence



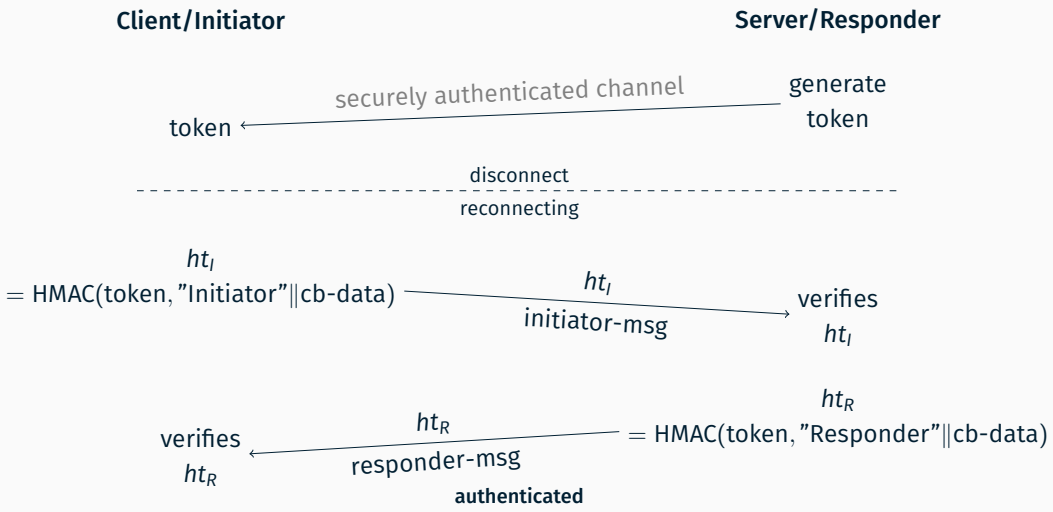
SASL-HT Authentication Sequence



SASL-HT Authentication Sequence



SASL-HT Authentication Sequence



Current Status

Deployments

- XEP-FAST [7] gained a lot of traction within the XMPP ecosystem
- XEP-FAST uses SASL-HT
- therefore, SASL-HT has been implemented by various XMPP software

- responder message can now signal an error condition

- responder message can now signal an error condition
- how to deal with the wire format change, given that there are already deployments of the previous wire format?
  - Rename mechanism to HT2-*?
  - Ignore?
  - ...

Open Questions

- not many open questions
- even during the phase of adoption, there where not many

Open Questions

- not many open questions
- even during the phase of adoption, there where not many
- but...

Open Questions

- not many open questions
- even during the phase of adoption, there where not many
- but…

TLS 0-RTT Data

- SASL-HT [5] and XEP-ISR [3] require the TLS 0-RTT data to exclusively contain the authentication data
- XEP-FAST [7] requires the TLS 0-RTT data to also contain further data (like feature negotiation or commands)

Thanks for your attention

Thanks for your attention

Questions?

References

[1] Dave Cridland, Thilo Molitor, and Matthew Wild. ***Extensible SASL Profile.*** XEP 0388. Version 1.0.2. XMPP Standards Foundation, Feb. 7, 2017–Aug. 6, 2024. URL: https://xmpp.org/extensions/xep-0388.html.

[2] Dave Cridland et al. ***Extensible Simple Authentication and Security Layer (SASL).*** Internet-Draft draft-melnikov-sasl2-02. Work in Progress. Internet Engineering Task Force, Dec. 2, 2024. 10 pp. URL: https://datatracker.ietf.org/doc/draft-melnikov-sasl2/02/.

[3] Florian Schmaus. ***Instant Stream Resumption.*** XEP 0397. Version 0.1.1. XMPP Standards Foundation, Feb. 12, 2016–Nov. 3, 2018. URL: https://xmpp.org/extensions/xep-0397.html.

[4] Florian Schmaus. **“XMPP and Android. Creating stable, reliable, push-enabled and battery friendly XMPP connections on Android”.** Talk. Free and Open source Softare Developers’ European Meeting (FOSDEM) 2015 (Université Libre de Bruxelles, Jan. 31–Feb. 1, 2015). Jan. 31, 2015. URL: https://archive.fosdem.org/2015/schedule/event/xmpp_and_android/.

[5] Florian Schmaus and Christoph Egger. ***The Hashed Token SASL Mechanism.*** Internet-Draft draft-ietf-kitten-sasl-ht-00. Work in Progress. Internet Engineering Task Force, Feb. 21, 2025. 11 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-kitten-sasl-ht/00/.

[6] Kevin Smith and Matthew Wild. ***Bind 2.*** XEP 0386. Version 1.0.1. XMPP Standards Foundation, Feb. 8, 2017–July 2, 2024. URL: https://xmpp.org/extensions/xep-0386.html.

[7] Matthew Wild. ***Fast Authentication Streamlining Tokens.*** XEP 0484. Version 0.2.0. XMPP Standards Foundation, Oct. 19, 2022–June 30, 2024. URL: https://xmpp.org/extensions/xep-0484.html.