Security Protocols

ALL YOU NEED TO KNOW

Brief Itrno

- SSL 1.0 – never publicly released due to security issues.
- SSL 2.0 – released in 1995. Deprecated in 2011. Has known security issues.
- SSL 3.0 – released in 1996. Deprecated in 2015. Has known security issues.
- TLS 1.0 – released in 1999 as an upgrade to SSL 3.0. Planned deprecation in 2020.
- TLS 1.1 – released in 2006. Planned deprecation in 2020.
- TLS 1.2 – released in 2008.
- TLS 1.3 – RELEASED IN 2018.

ankit pangasa

How they work

SSL/TLS certificate installed on web server.

Certificate includes public key & private key to authenticate & encrypt data

Client goes to site and does handshake to check validity of certificate and authenticate server

If certificate is invalid, client gets "your connection is not private"

If certificate is valid, encrypted line is established.

And now HTTPS comes in picture and data becomes less vulnerable

ankit pangasa

SSL vs TLS

ankit pangasa

Master Secret

SSL: Message Digest is used to create master secret

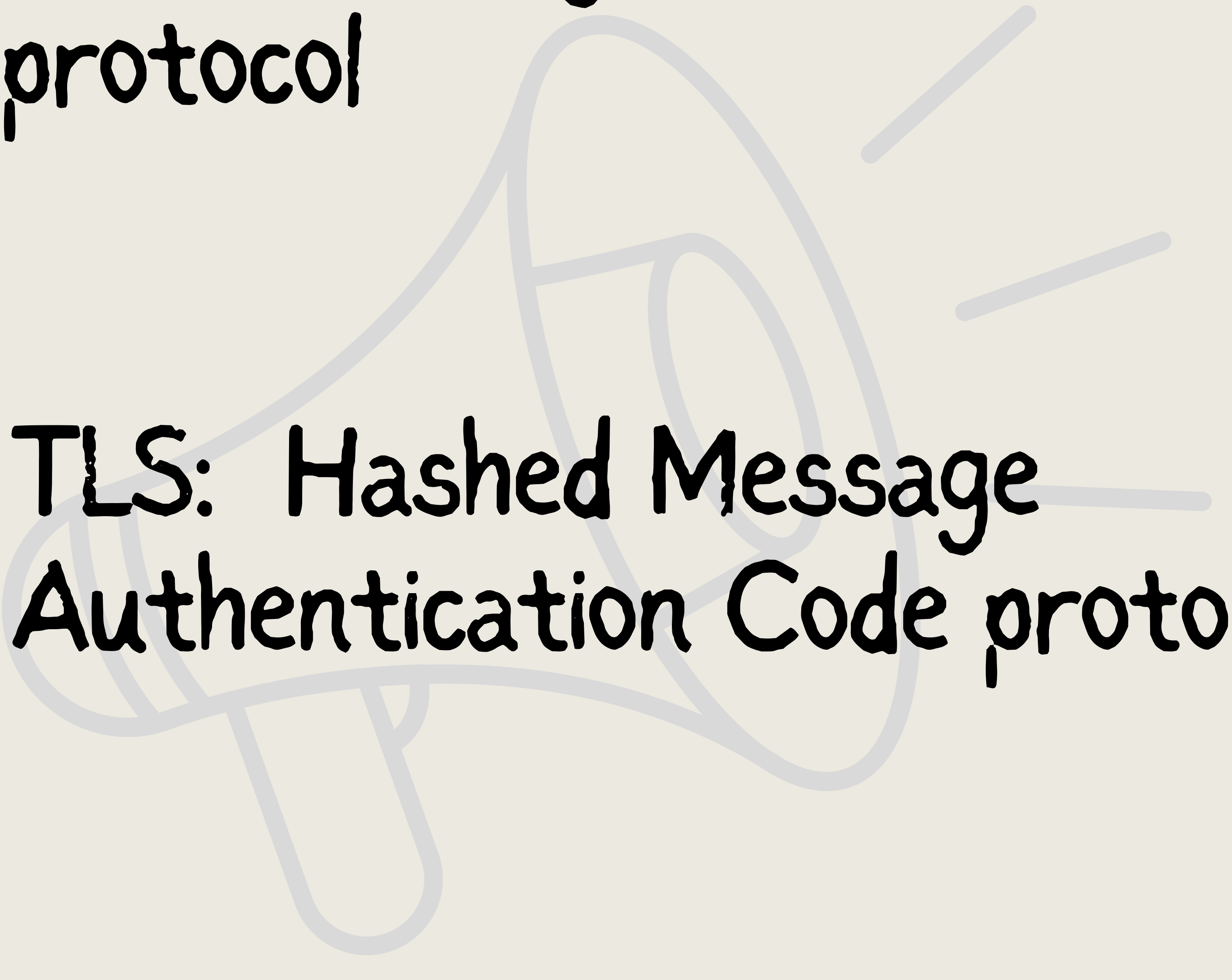
TLS: Pseudo-random function used to create a master secret

ankit pangasa

Protocol

SSL: Message Authentication Code protocol

TLS: Hashed Message Authentication Code protocol



ankit pangasa

Simplicity

SSL: More complex

TLS: Simple

Security

SSL: Less secured

TLS: More secured

ankit pangasa

Reliability

SSL: Less reliable and slower

TLS: More reliable and less latency

ankit pangasa

X-Compatibility

SSL: Doesn't support TLS

TLS: TLS 1.0 had SSL fallback mechanism for backward compability

ankit pangasa

was this helpful to you?

LIKE THE POST 👍

SHARE WITH YOUR FRIENDS ➤

BE SURE TO SAVE THIS POST FOR LATER READING 🔖

KEEP FOLLOWING ANKIT PANGASA FOR MORE SUCH USEFUL POSTS ⌄