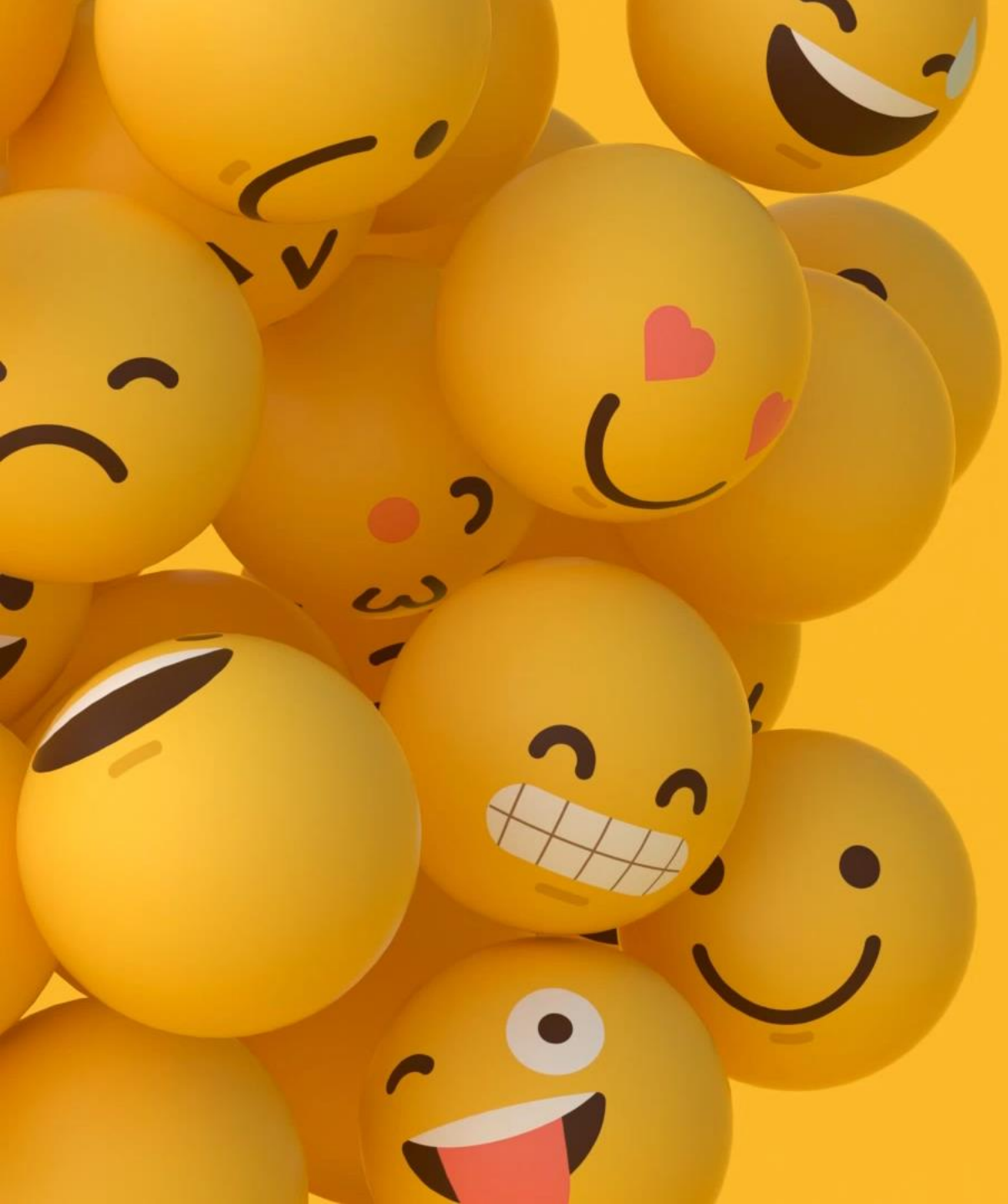


OHTTP Update

draft-ietf-ohai-ohttp @IETF113

Martin Thomson*, Chris Wood

Changes in draft-01

- Moved padding to binary messages
- Changed labels to "`message/bttp request`" and "`message/bhttp response`"
  - *Added text about repurposing this design*
- Text on resource mappings
- Draft text on anti-replay

Issue #66

Shadow Banning

Should we allow the proxy to signal to the oblivious request resource?

Privacy cost is that users can be split into groups by the proxy

How much signal?

One bit?

Issue #75

Streaming

Generic HTTP means streaming

OHTTP is currently atomic

Should we change that

Streaming Design Sketch

Apply HPKE or AEAD multiple times

AEAD needs a unique nonce

Can use a counter and XOR (as in TLS)

Prefix each chunk with a length

Cost: maybe 1 byte for atomic uses

Add something to the AAD to signal the end of a message

A counter or the length prefix would work

Distinguish last chunk with a 0 length

Issue #76 and #89 Anti-Replay

Text proposed in draft

This handles #76

Draft proposed to HTTPAPI WG

draft-thomson-httpapi-date-requests

This handles #89 (correction of bad clocks)

Anti-Replay Strategy

Some servers might not care

Easy answer, but not always the right one

Servers that care can remember every request they receive

If they have seen it before, reject it

Just need to save the **enc** *value*

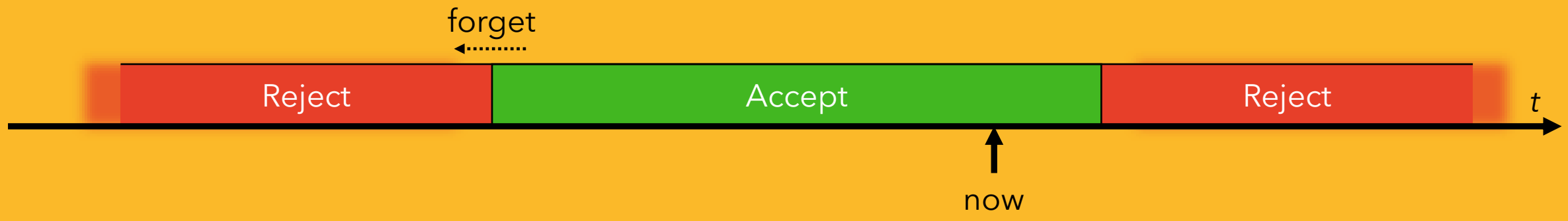
Problem: needs lots of state

Solution: include date in requests

- *HTTP Date header field recommended*

Server only remembers requests for a short period

- *Reject requests from before this period*
- *Reject requests from the future*
- *Forget requests as they age*



Problem: client clocks are bad

really bad

Solution: let the client retry

Use Date header field from server

Creates attack on incautious clients

if Date is used for more than just a retry

so don't do that

Covered by date-requests draft

Issues #58 and #19

#58: Should this be experimental?

Suggest: no

#19: Should we address discovery?

Reaffirm: not in this draft

Discuss with draft-pauly-ohai-svcb-config