draft-sterman-aaa-sip-03

Wolfgang Beck
beckw@t-systems.com
Deutsche Telekom AG

RADIUS server generates nonces

- required for AKA
- 03 emulates an Access-Challenge

Proposal: use Access-Challenge

RADIUS server generates nonces

- Problem with Authentication-Info + qop=auth-int
- Body digest required to build rspauth

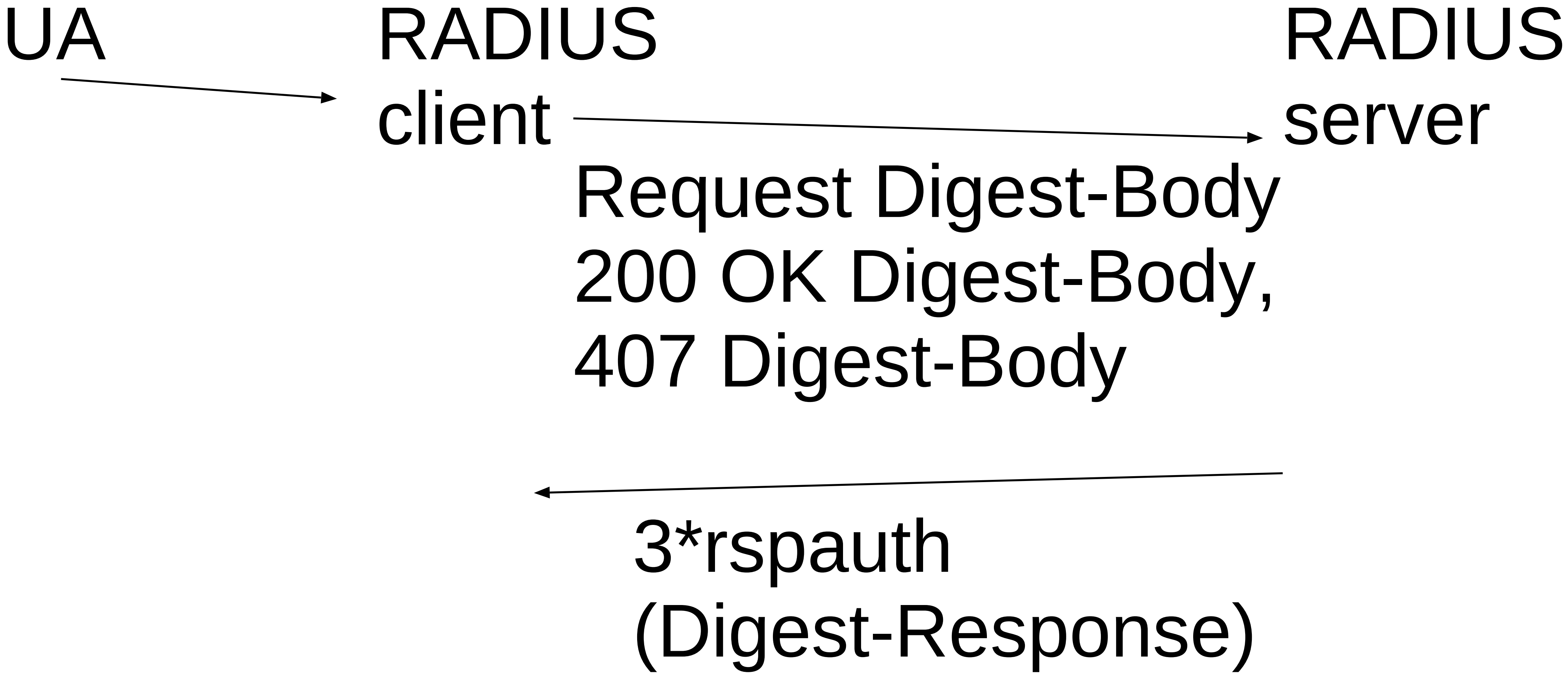
A2 = ":" digest-uri-value ":" H(entity-body)

Possible Solutions

my preference

1) don’t send Authentication-Info in problematic cases
2) client generates possible response-bodies and sends body digest attrs.
3) RADIUS server sends H(A1), client constructs rspauth

Three Digest-Body attributes



UA

RADIUS client

RADIUS server

Request Digest-Body
200 OK Digest-Body,
407 Digest-Body

3*rspauth
(Digest-Response)

Partial rspauth

- RADIUS server sends H(A1)
- RADIUS client constructs rspauth

is this secure? Replay attacks?

HTTP support

- Requested by 3GPP2
- HTTP should work
- HTTP example will be added

DIAMETER migration

M. Garcia’s preference

- Migration chapter in draft-sterman
or diameter-sip-app? ← my preference
- both documents are in Last Call,
would have to reference Work in Progress