draft-radext-digest-auth

65. IETF Wolfgang Beck beckw@t-systems.com

Client configuration

- HTTP Digest uses challenge/response as capability exchange
- This does not work with RADIUS client nonce generation

Solution in -07: manual configuration

Nonce Replay

- RADIUS client gets hijacked
- Attacker logs successful authentications
- Attacker replays successful authentications
- Victim might get charged

Nonce Replay, Option 1

remove RADIUS client nonce generation

Nonce Replay, Option 2: Do Nothing!

- Charging per authentication?
- SIP servers are often part of a ‚chain of trust‘.

Nonce Replay, Option 3: embed time-stamp into nonce

- nonce = r + ts + hn(r + ts, secret) + nonce-opt

  r: random string (28 byte)
  ts: time-stamp (4 bytes, seconds since epoch)
  secret: shared secret between client and server
  nonce-opt: optional nonce characters

- Requests with large clock difference will be rejected

Nonce Replay, Option 3: embed time-stamp into nonce

- What is a large clock difference?
- What is a large network delay?
- What about retransmissions?
  - not exactly a retransmission, as the Digest-Nonce attribute has to be updated

severe problems

Nonce Replay, Option 3: embed time-stamp into nonce

- Allow large clock differences?
  - open the window for attacks
- Allow only smaller clock differences?
  - Reject with ‚stale‘, initiate more RADIUS/HTTP-style round trips, more packets, more congestion, more delay, reject with ‚stale‘, initiate ...

severe problems

Nonce Replay, Option 4: embed sequence number into nonce

- nonce = r + seq + hn(r + seq, secret) + nonce-opt
- Server maintains sequence number per NAS
- Server only accepts a sequence number higher than the previous
  - does not protect the first packet
  - clients need to store the sequence number

Nonce Replay, Option 4: embed sequence number into nonce

- Server accepts sequence numbers that fall into a window [previous + 1, previous + 101]
  - client has some leeway to store the sequence number permanently

Nonce Replay

- Option 1 (rm client nonce gen.): rejected
- Option 2 (do nothing): rejected
- Option 3 (time-stamp): severe problems
- Option 4 (seq. no): selected for -07, window size?