Problems with STUN Authentication for TURN

draft-reddy-behave-turn-auth-02

Aug 2013 IETF 87 Meeting

Authors : T.Reddy, Ram. R, Muthu.P, A.Yegin

Background

- Applications like WebRTC may choose to use TURN for privacy.
- NAT/Firewall traversal.
- TURN server could be deployed in Enterprise DMZ for Auditing etc
- Mobility.
- TURN includes IPv4-to-IPv6, IPv6-to-IPv6, and IPv6-to-IPv4 relaying.

Related proposals

- draft-thomson-mmusic-rtcweb-bw-consent proposes extensions to TURN for requesting bandwidth allocation at a TURN server.

- draft-ietf-rtcweb-use-cases-and-requirements refers to deploying a TURN server for auditing.

TURN Auth

TURN uses key derived from username and password to generate message integrity for TURN request/response.

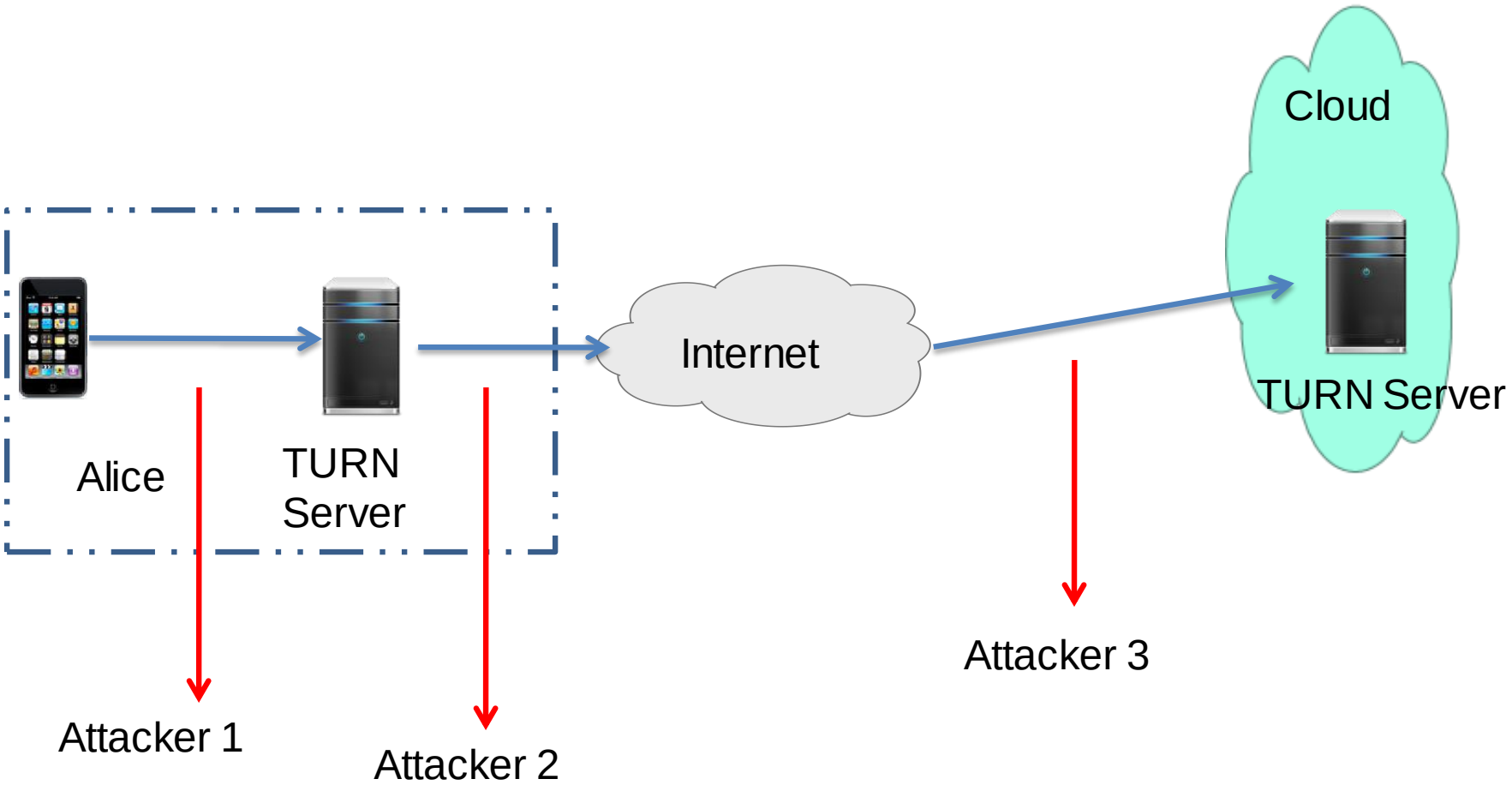
key = MD5(username ":" realm ":“ SASLprep(password))

Problems with STUN Auth

1. “log-in” username and password will not change for extended periods of time
    - Password susceptible to offline dictionary attacks
2. TURN server needs to be aware of username and password (management overhead).

Attackers verses TURN Servers

3. Adversary can learn USERNAME by snooping TURN messages. Attacker can learn USERNAME of the user.



Problems with STUN Authentication

4. TURN credential exposed to Java Script
   - TURN could be deployed in cloud and comes at a cost on SaaS provider.

5. No support for multiple realms

Problems with STUN Authentication

- This makes STUN authentication important to prevent un-authorized users from accessing the TURN Server.

Solutions

- draft-uberti-behave-turn-rest addresses the problem for third party authorization.
  - ➢ No revocation of temporary credential.
  - ➢ Could be misused by malicious Java Script
  - ➢ Static shared secret.

- There is still need to resolve first party authentication.
  - ➢ Auditing use case in Enterprise

Next steps

- Is the WG interested in documenting the problem ?
- Is the WG interested in solving the problem ?