Problems with STUN Authentication for TURN

draft-reddy-behave-turn-auth-04

Mar 2013 IETF 89 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-ietf-rtcweb-use-cases-and-requirements refers to deploying a TURN server for auditing and FW traversal.

STUN Auth

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

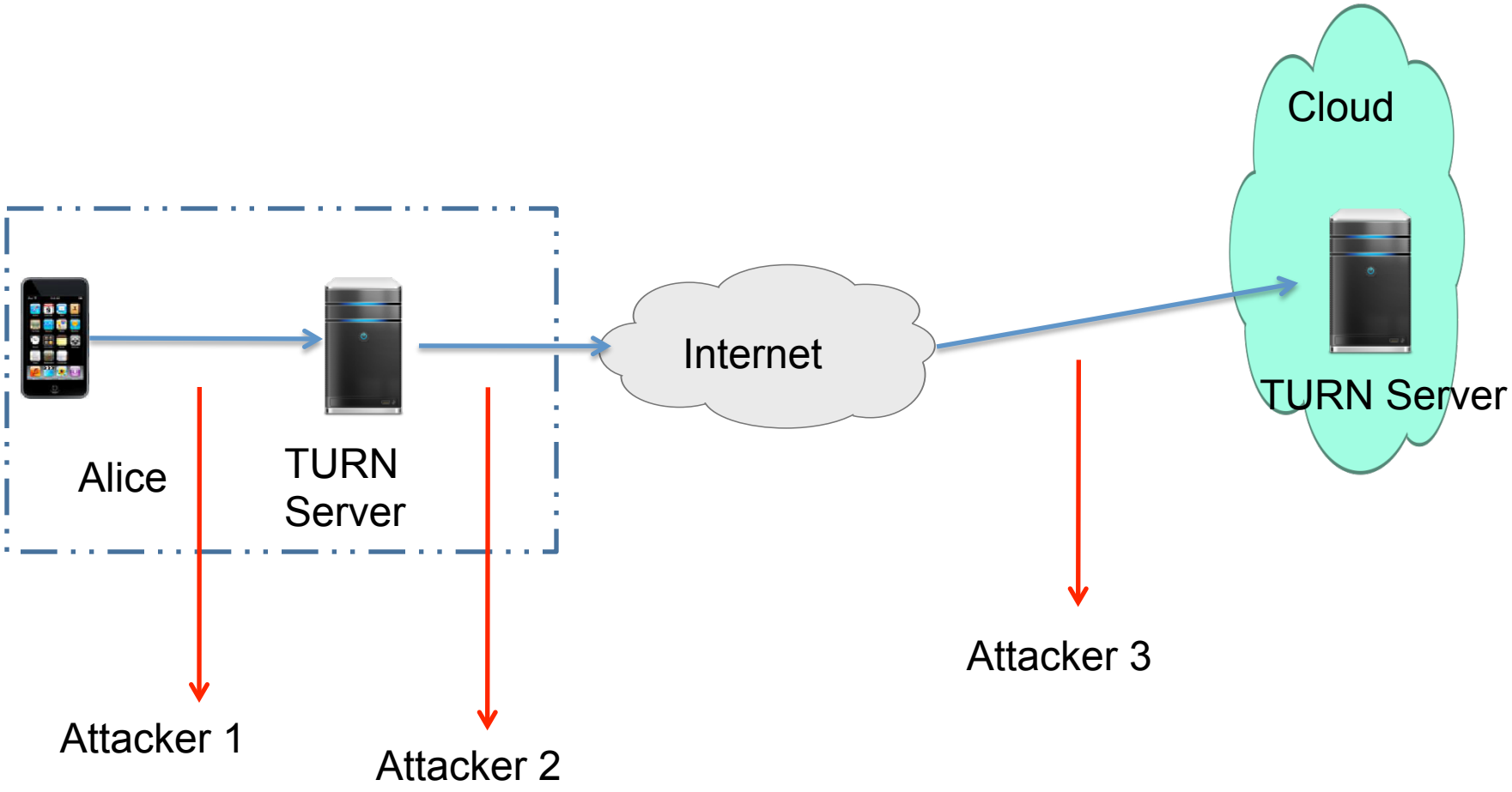
key = MD5(username ":" realm ":“ SASLprep(password))

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) or store the key (MD5 hash).

Attackers verses TURN Servers

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



Problems contd..

4. TURN credential exposed to JavaScript.

5. TURN could be deployed in cloud and comes at a cost on SaaS provider.

6. No support for multiple realms.

Problems contd..

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

Solutions

- draft-johnston-tram-stun-origin-01 addresses the realm problem
- draft-petithuguenin-tram-stun-dtls-00 addresses some of the problems
- draft-reddy-tram-turn-third-party-authz-00 addresses the problem for third party authorization.

Solutions contd..

- There may be a need to resolve first party authentication.
  - Auditing and FW traversal use case in Enterprise
  - ISP deploying TURN Server

Next steps ?