Address Settlement by Peer to Peer (ASP)

Jonathan Rosenberg

Cullen Jennings

Eric Rescorla

Key Ideas

- Security Framework
- NAT Traversal
- Extensibility
- Usage Models
- Pluggable DHT
- Forwarding Layer
- Multiple P2P Networks

Security Framework

- Two types of threats
  - Storage
    - Attackers discard, modify, or alter data
    - Attackers fill up the network with data
    - Attackers overwrite data from other users
  - Routing
    - Attackers discard messages
    - Attackers misroute messages

Storage Security

- Authorization
  - Each locus/type pair is bound to a set of certificates valid for writing to that pair
  - Binding is defined by the usage
- Distributed Quota
  - Defined by usage
- Correctness
  - Integrity protection via signature
  - Timestamps for replay attacks

Routing Security

- Central Enrollment Server
  - Peer ID selected by enrollment server
    - Help mitigate Eclipse
  - Rate limiting at enrollment server
    - Help mitigate Sybil
  - Public/Private keys selected by UA, only public key disclosed to server
- All direct connections Mutual TLS authed

NAT Traversal

- CONNECT method used to establish transport layer connections for
  - ASP itself
  - SIP
  - Other things
- CONNECT and its response implement ICE
  - ICE usage defined in some detail
- Peers can act as STUN and TURN servers
  - Central STUN server used during bootstap
  - Users use central stun to guess at whether they are natted or not
  - If they can act as STUN or TURN, write into one of N different seeds, defined by size of DHT and density of STUN/TURN servers

Extensibility

- New attributes and commands
  - BGP-style treatment fields (mustUnderstand, mustReflect) for attributes
- Upgrading DHT entirely
  - Run parallel rings
  - Synchronize complete switchover through enrollment server over period of months

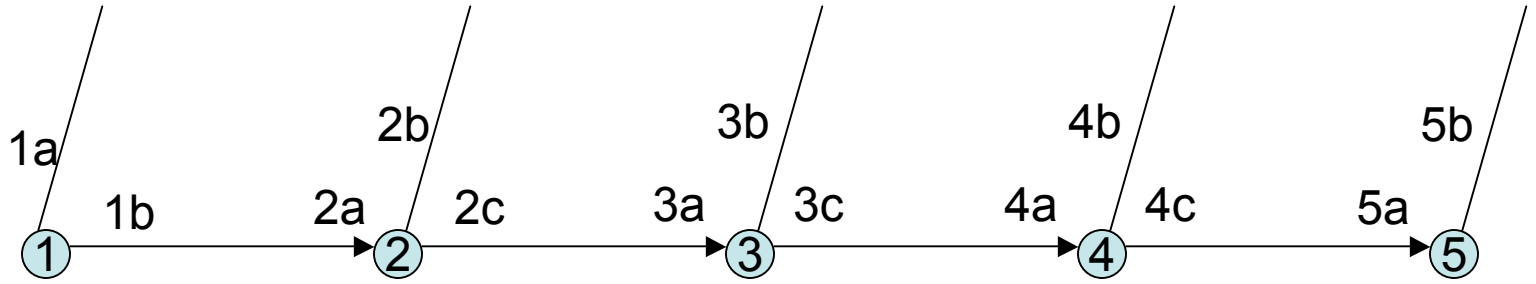
Usage Model

- Each usage defines a set of types
  - Each type defines
    - Data structure (single value, set, dictionary, etc.)
    - Access controls
    - Size limits
    - How to form seed
    - Merging rules
- SIP Usage (AOR to contact mappin)
- Certificate Usage
- STUN Usage
- TURN Usage

Forwarding Layer

- Binary protocol
- Requests can be forward based on routing header only
- Label stacks
  - For responses: Via stack containing list of locally meaningful connection identifiers
  - For requests: Anonymity

Label Stacks: Responses



Dst:	PeerID: 5	PeerID: 5	PeerID: 5	PeerID: 5	
Src:	PeerID: 1	Cxn: 2a PeerID: 1	Cxn: 3a Cxn: 2a PeerID: 1	Cxn: 4a Cxn: 3a Cxn: 2a PeerID: 1	Request

---

	PeerID: 1	Cxn: 2a PeerID: 1	Cxn: 3a Cxn: 2a PeerID: 1	Cxn: 4a Cxn: 3a Cxn: 2a PeerID: 1	
Dst:					Response
Src:					