Trust Router Overview

IETF 86, Orlando, FL

Routing Area Meeting

Margaret Wasserman

mrw@painless-security.com

Problem Statement

- https://datatracker.ietf.org/doc/draft-howlett-abfab-trust-router-ps/
- Describes the problems that motivated the Trust Router work

Trust Router Draft

- https://datatracker.ietf.org/doc/draft-mrw-abfab-trust-router/
- Describes the role and purpose of a Trust Router
- Defines the concept of communities
  - COIs and APCs
- Defines two protocols
  - Temporary Identity (TID) Protocol
  - Trust Router Protocol

Trust Router Overview

- Trust Router Motivations
- Trust Router Operation
- Communities
- Temporary Identity Protocol
  - Message contents
  - Role of Trust Router as gateway
- Trust Router Protocol
  - Message contents
  - Trust link types
- Implementation Status

Trust Router Motivations

- Scalability of ABFAB Federations
  - Eliminate need to configure credentials for every pair of RPs and IdPs
  - Eliminate need to configure manual “routing” information in intermediate AAA Proxies
  - Reduce costs of adding new members, removing members, changes in peer relationships
- Flexibility to create new Communities
  - Groups that want to share access to a set of services, m apped to registrar Communities for authentication
  - Eliminate need to set up new Registrar Community for every group

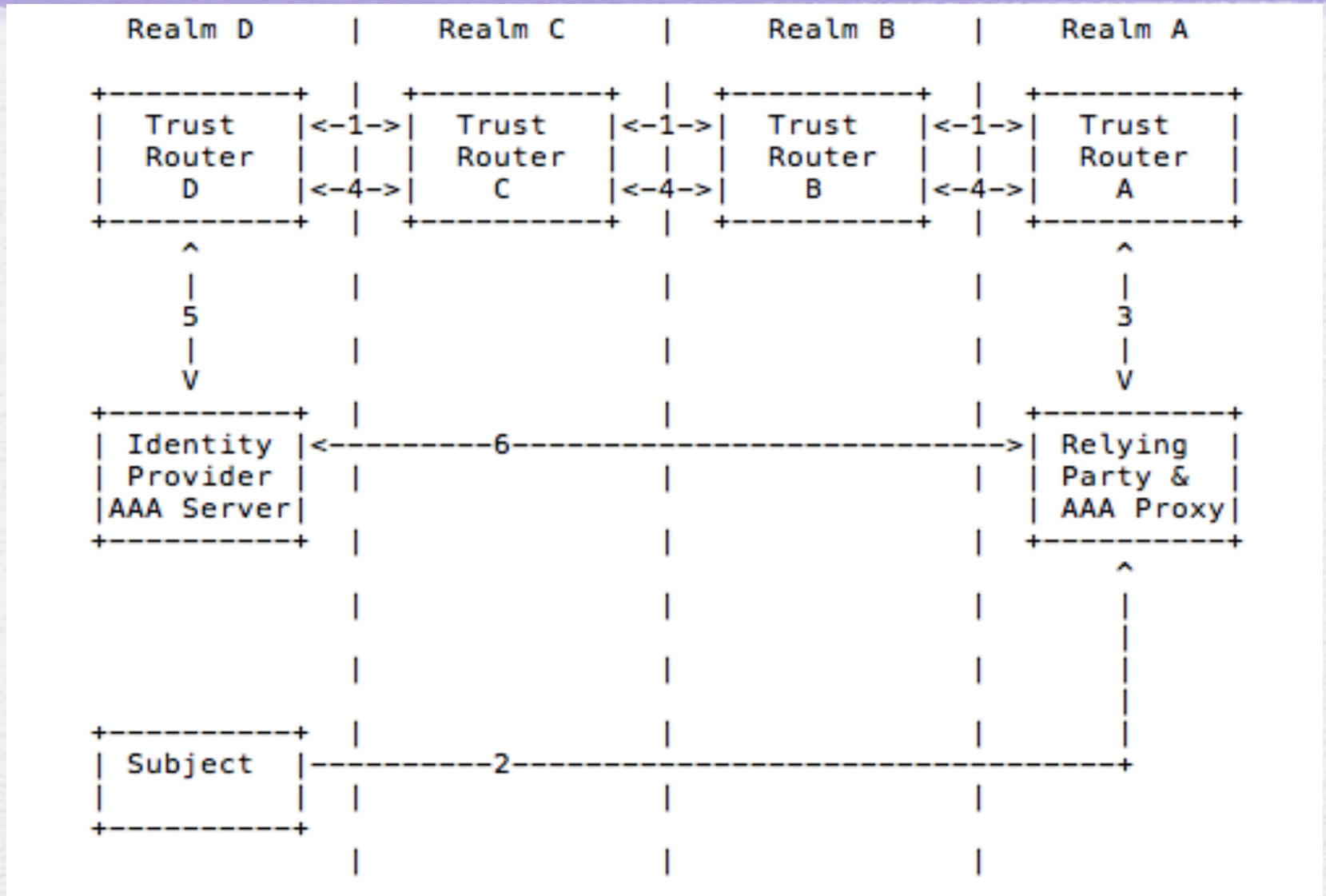
Looks Familiar?

- Current SAML Federations are reminiscent of early Internet
  - SAML metadata (like host tables) is distributed manually and configured by every IdP or RP
  - Need for every end-site to know about every other end-site, or they can't connect
- Solution: Routing!
  - Although we won't be forwarding IP packets, the distribution of trust information looks a lot like the distribution of routing information

Communities

- Authentication Policy Communities (APCs)
  - Used to authenticate access to RP Services
- Communities of Interest (COIs)
  - Group of RP Clients, IdPs and Trust Routers that share access to a set of services
  - COI must be resolved to an APC (for a given IdP Realm), before authentication can be achieved

Trust Router Operation



Temporary Identity Protocol

- Used by an RP to negotiate a Temporary Identity on a (set of) AAA Server(s) in a target realm
- TID Request is sent to the RP's local Trust Router and forwarded across a Trust Path to the target AAA Server(s)
- Response is returned by reversing the Trust Path

Temporary Identity Protocol

- Simple request/response protocol
  - Messages are encoded in JSON
  - Uses GSS-API for authentication
- Request include ½ of a DH exchange
- Server replies with a list of AAA Server IP Addresses
  - Response includes the other ½ of a DH exchange for each AAA Server
- Both ends can compute a shared key that is used for the subsequent AAA authentication
  - Key cannot be computed by intermediate Trust Routers

Example TID Request


```
{"msg_type": "TIDRequest",
 "msg_body":
     {"rp_realm": ”mit.edu",
      "target_realm": ”oxford.uk.ac",
      "community": ”abfab-hackers.communities.ja.net",
      "dh_info":
        {"dh_p”:
            "FFFFFFFF…",
         "dh_g": "02",
         "dh_pub_key":
            "FBF98ABB…”}
     }
}
```

Trust Router as TID Gateway

- Trust Router receives a TID Request from an RP Client (e.g. AAA Proxy)
- Determines appropriate APC for the community included in the original request
  - If different, moves original COI into orig-coi field
- Finds matching rp_client entry (from gss_name), applies filters, and adds constraints to the message
- Determines "Trust Path" and adds it to the message.
- Forwards message to AAA Server (or next hop Trust Router)

Trust Router Protocol

- Runs between pairs of Trust Routers
  - Configured as "peers" with GSS credentials to reach each other
- "Routing" protocol used to dynamically distribute information about
  - Available Trust Links
  - Used to route TID requests and responses across the federation
  - RP Client membership in COIs
  - APC to use for each IdP Realm/COI pair

Trust Link Types

- Trust Link Types (named by target type)
  - Routing Links
    - Trust Router Link
      - Indicates that the originating trust router can provide temporary IDs to reach the target trust router
    - IdP Realm Link
      - Indicates that the originating trust router can provide temporary IDs to reach the AAA servers in the target realm
  - Information Flooding Links
    - COI RP Membership Link
      - Indicates that the the target RP Client is a member of the indicated COI
    - APC Link
      - Indicates that authentication for a target realm and COI should use the target APC

Trust Path

- A Trust Path is a set of Trust Links that forms a path across a federation between an RP and the AAA Server(s) in a Target IdP Realm
- A Trust Path is valid for a given Community
- Trust Routers forward TID Requests/ Responses along Trust Paths, ultimately resulting in a TID that the RP can use to reach AAA Servers in the Target IdP Realm.

Next Steps

- [We held a Bar BOF at lunch today]
- We hope to hold a Pre-WG BoF at IETF 87
  - Need active discussion on the list
- Join our mailing list!
  - trust-router@ietf.org

Questions?
Feedback?