Authentication, Authorisation and Accounting (AAA) Framework
(RFC 2904)

Vedavyas Duggirala
(vyas@vt.edu)
Background

- Not a standard. Establishes requirements for Authentication, Authorization & Accounting (AAA)

- Related RFC’s
  - 2906 – Authorization Requirements
  - 2905 – Authorization Application Examples

- Authentication method and Accounting requirements are outside the scope of this document, except to the extent they influence the authorization process

- Sample applications referenced in RFC 2905
  - PPP with dialin with roaming
  - Mobile IP
  - Bandwidth broker for QoS
  - Internet Printing
  - E-commerce
  - Computer based education and Distance Learning
Authorization Entities and Relationships

♦ Entities
  - User - one who accesses the service or resource
  - UHO - User Home Organisation. Verifies that user is allowed to access the requested service. May carry information required to authorize the user and this information may not be known to the service provider
  - Service Provider’s (SP) AAA server - Authorizes a service based on an agreement with UHO & without specific knowledge of individual user. SP and UHO can be either in same or different administrative domain.
  - Service Equipment (SE) - belongs to Service Provider and provides the actual service e.g. router in QoS, Printer or NAS in dial service

♦ Relationships
  - Authorization is based on “static” trust agreements between UHO and SP
  - Trust agreements may be chained between various organisations
  - Static trust relationships between different entities are used to establish dynamic trust between User and Service Equipment
Message Sequences

♦ Single domain - Agent Sequence
♦ AAA server acts as agent between User and Service Equipment

1. User sends request to Service Provider’s AAA server
2. AAA server forwards request to Service Equipment
3. Service Equipment responds to AAA server informing if the service is set up or not
4. AAA server replies to User based on SE’s response
Message Sequences

- Single domain - Pull Sequence
- Service Equipment Pulls authorization information from AAA Server

1. User sends request to Service Equipment
2. Service Equipment forwards request to AAA server
3. AAA server responds to Service Equipment if the request can be honored
4. Service Equipment informs User that service is ready (if not, denies the service)
Message Sequences

- Single domain - Push Sequence
- User Pushes authorization obtained from AAA server to Service Equipment

1. User sends request to Service Provider’s AAA server
2. AAA server authorizes the user and gives him a ticket
3. User presents the ticket to Service Equipment
4. Service Equipment verifies the ticket and grants User access to Service
Roaming

- Roaming - UHO and SP can be different organizations
- Agent sequence with roaming
- UHO authenticates the user but service is provided by different organization
Roaming

♦ Pull sequence with roaming

Diagram:

1. Service Provider
2. AAA Server
3. User Home Organization (UHO)
4. User
Roaming

- **Push sequence with roaming**

![Diagram showing the push sequence with roaming](Image)

1. User requests service from the Service Provider.
2. User's request is authenticated by the AAA Server.
3. AAA Server communicates with the User Home Organization (UHO).
4. User receives service from the Service Provider.

---

CS 6204, Spring 2005
Distributed Services

- Many organizations may be cooperating to offer the service e.g. QoS
- Message Sequences between organizations might be different. e.g. User and Org1 use Pull sequence. Org1 and Org2 use Agent sequence
- Other message semantics are also possible. Org1 can send a response before verification by Org2. In such case protocol must support revocation.
- Roaming and distributed services can be combined leading to SuperOrg and Broker
Authorization Policy

Policy Framework Working Group specifies a way to represent, manage and share policies and policy information in a vendor-independent, interoperable and scalable manner (RFC 3060)
- Defines a hierarchical Object based structure (CIM)
- LDAP based implementation of CIM

Each organization has policies defined independent of other administrations

Authorization is the result of retrieving, evaluating and enforcement of each independent policy

Policy definitions are stored in a Policy Repository, accessible to the organization that requires them. The Organization requiring the policy is responsible for determining which policy is to be applied
Distributed Policy

- Policy Retrieval Point (PRP) retrieves policy from Policy Repository
- Policy Decision Point (PDP) evaluates the Policy
- Policy Enforcement Point (PEP) or Policy Target enforces policy
- AAA servers can be PRP and PDP. SE acts like a PEP
- Policy Repository can be stored in directories or at AAA server
- Policy Information Points contain information against which policy conditions are evaluated (resource status, session state or time of day)
Policy Evaluation and Enforcement

♦ Policy Decision Point must either
  – have a way to query remote administration for information necessary to evaluate policy
  – or forward the local policy to remote administration for evaluation

♦ Policy Enforcement is performed by Service Provider on Service Equipment. SE is same as Policy Target described in PFWG. SP’s AAA server and SE might communicate via a own protocol or use the same protocol used between different AAA servers
Attribute Certificates

- Attribute Certificate (AC) is like a Public Key Certificate (PKC) except that it contains group membership, role, clearance and other access control information.
- PEP and PDP has to ensure that AC owner is the one who requested the service. AC can contain a pointer to owner’s PKC.
- PKC can be considered like a Passport and AC like entry visa.
- Client can push the AC to server or Server can retrieve AC from a repository.
- Standards are being defined by PKIX working group.
Resource Management

- Authorization may involve a chain of servers
- In many applications authorization results in establishing an “ongoing service” (session)
- AAA servers have to keep track of session state and make changes as necessary
- AAA server MAY have a Resource Managers. RM tracking a session need to be able to initiate changes and communicate with other peer RMs
- Each session is identified by a session identifier (SID) unique to a AAA server. It is desirable that SID is same across all AAA servers
Service Equipment should be able to notify RM of change in session state.

RM will need to keep state of each session fresh via periodic keep alive messages or querying.

Any RM in the chain must have the ability to terminate a Session. Each RM must know at least its adjacent AAA servers.

RM must conceal identity and location of its private internal AAA components from other administrative domains.

RM must cooperate with PDP and PEP. It acts like a PIP.
Message Forwarding and Delivery

- AAA server forwards message to a “logical destination address”
- Every Application defines the mapping from logical address to network address. e.g. NAI for roaming dialin
- When forwarding messages for an established session, messages must be prefixed by Session Identifier
- Underlying message delivery system must support
  - Unicast
  - Data Integrity and error detection
  - Reliable data transport
  - Sequenced data delivery
  - Responsive to network congestion
End to End security

- AAA protocols are used to provide security, so they themselves must be free from security holes
- End to End message integrity
- Confidentiality
- Replay protection
- Non-repudiation
- Ability to secure portion of payload
- Intermediate AAA Servers must be able to securely attach local policy information to messages before forwarding
- Some applications can provide direct end to end authorization by having the Broker act as certification authority
Possible attacks

- Authorization protocols must be impervious to replay attacks
- If proxying is used, man-in-the-middle attacks must be avoided
- If Push model is used, the ticket must not be hijackable by third party
- In multi-party authorization, sensitive information should be protected from unauthorized parties involved in making decision
- Should guard against Denial of Service attacks