Use of DIAMETER for Inter-Gatekeeper Communication

Pat R. Calhoun
Technology Development/ Sun Microsystems, Inc.
Roaming Operations Co-Chair/Internet Engineering Task Force
PCalhoun@Eng.Sun.Com
DIAMETER History

- RADIUS has been successfully used for many years as a protocol to authenticate, authorize and generate accounting information for dial-in users.

- At the April 1995 IETF meeting a working group called RADIUS was created. The charter of the WG was to document the protocol as it was already deployed in the field.

- At the December 1995 IETF meeting I held an informal BOF meeting to talk about a RADIUS replacement (RADIUSv2) that could satisfy current and future requirements.
DIAMETER History

- At the June 1996 IETF meeting a working group called Roaming Operations (ROAMOPS) whose charter is to define how roaming users can get Internet access while they are out of their ISPs service area.

- At the December 1997 IETF meeting, I submitted a proposal to the WG based on DIAMETER that could support Roaming Consortioms (a.k.a clearing houses) while maintaining end-to-end integrity/non-repudiation.

- At the December 1997 IETF meeting the ROAMOPS WG stated that RADIUS was unable to satisfy their requirements.
DIAMETER History

- In March 1998, the IESG decided to shut down the RADIUS WG to open the way for a new protocol.

- Today DIAMETER is much more than just another RADIUS. It is being also being investigated for other services such as Quality of Service for both Int-Serv (or RSVP) and Diff-Serv (or Type of Service byte in IP header).
Roaming Operations - Today

- The ROAMOPS charter is to define a way (and possibly a protocol) to allow roaming users to gain Internet access from a provider other than their “home” provider.

- This requires providers to establish business relationships with other providers.

- Recently there has been a demand by smaller ISPs for roaming consortiums. These entities allow ISPs to provide roaming capability throughout the world by dealing with a single entity.

- The roaming consortiums provide settlement services (see www.ipass.com and www.gric.com for more info).
Roaming Operations - Today

Roaming Consortium
“Clearing House”

Home provider

-OR-

Visiting Provider

Authentication, Authorization and Accounting

Authentication, Authorization and Accounting

Authentication, Authorization and Accounting
IP Telephony Clearing Houses

- Companies such as Internet Telephony eXchange Carrier now provide clearing house services to service providers for IP Telephony (see www.itxc.com for more info).

- The support of Clearing Houses simplifies initial deployment since it does not require service providers to setup business relationships with all other providers (full mesh problem).

- Over time larger providers will begin to setup direct relationships in order to cut costs.
Inter-Gatekeeper Requirements

- It is therefore imperative that any Inter-Gatekeeper Communication Protocol support both models:
  - Service providers (GK) communicate directly.
  - Service providers (GK) communicate through a third party GK.

- Document [1] defines an inter-gatekeeper protocol based on SSL/TLS and SMIME. This is problematic since it allows the third party GK (clearinghouse) to modify information in transit.

- What is really needed is a protocol that allows the clearinghouse to be involved, but still maintain end-to-end integrity/non-repudiation (if required).

Clearing House Support

- DIAMETER can support such clearing houses by allowing both end GK to exchange certificates through a bootstrap DIAMETER message.

- GK performs a digital signature of the DIAMETER message, which provides end-to-end integrity, encryption and non-repudiation with replay protection.

- All DIAMETER nodes that the message traverses can also add their own digital signature if the packet is modified in transit. Otherwise intermediate nodes add an Integrity Check Vector that provides hop-by-hop integrity and replay protection.
Clearing House Support

Roaming Consortium

Hop-by-Hop Integrity (Shared Secret)

End-to-End Integrity, Encryption, non-repudiation

Home provider

Visiting Provider

Hop-by-Hop Integrity (Shared Secret)
Why not use Directory Services?

- Today there is a tendency to use Directory Services for everything.

- The problem with the use of DS as the Inter-Gatekeeper communication is that many customers are not willing to open their directory for read access to the outside world.

- What is needed is a protocol that can transmit a portion of a policy, without compromising the DS.

- In addition, reading the directory would provide user’s clear text passwords to the outside world.
Why not use Directory Services?

- There is also a discussion to use the Directory Server to send zone information (pseudo-routing protocol).

- Directory Servers are not intended to work in the push model.

- The use of a DS seems inappropriate in this case and it appears that a protocol would be the correct approach.

- Bernard Aboba (MS) has a good presentation entitled “Appropriate use of Directory Services” (see http://murchiso.com/den/).
Authentication Requirements

■ In the case of a roaming user, authentication of a user MUST occur between the user and its Home Gatekeeper.

■ It is imperative that the user’s password is never exposed to a visiting Gatekeeper.

■ In authentication schemes such as hashing, it would be necessary for the Home Gatekeeper to generate the challenge. This will eliminate replay attacks.

■ It would be desirable to support authentication schemes such as One Time Passwords (i.e. token cards), smart cards, biometrics, etc.
Authentication in ROAMOPS

In ROAMOPS, the use of EAP (Extensible Authentication Protocol) ensures that authentication is end-to-end, minimizing exposure of sensitive information to the visiting authentication server.
Authentication in ROAMOPS

- In the previous diagram, the user is authenticated (and authenticates) the Home Gatekeeper.

- Each intermediate node simply “shuttles” the EAP packets back and forth until an EAP-Success or EAP-Failure message is received by the Home GK.

- This mechanism ensures that the user’s password is never compromised, and allows for inexpensive authentication mechanisms (i.e. static password and MD5).
Why Bother?

■ Why should the inter-gatekeeper authentication model be similar to the ROAMOPS one?

■ I envision being able to use a Public IP Telephone at the airport and being able to use the SAME credentials that I always do. This way I receive a single bill at the end of the month.

■ Ideally all that would be needed in a token/smart card and a PIN (or retina scan) to get authenticated.

■ User Names should conform to the ROAMOPS NAI when possible.

■ I think this functionality is crucial in order to get mass deployment.
Address Resolution

- There are really two different types of users whose addresses need to be resolved: static and nomadic.

- In the case of static address resolution DIAMETER can easily be extended to support a new message set: ResolveAddressRequest and ResolveAddressResponse.

- In the case of nomadic users with dynamic addresses, the server that is aware of the user’s current address is the authentication and authorization server (or DIAMETER).
Accounting Requirements

- One missing element from all Inter-Gatekeeper proposal thus far is the ability to transfer accounting information about a specific session.

- A group of people are currently in the process of defining the DIAMETER Accounting Extension. This accounting protocol MUST scale to the order to millions of users and thousands of nodes.

- End-to-end integrity is essential to remove the possibility of a fraudulent clearing house.

- Real-time as well as batch transfer of accounting records is required.
Quality of Service

- Document [2] states that an Inter-GK protocol must provide Bandwidth Control (QOS Support).

- Bandwidth Control adds an additional problem since it is possible that both providers do not do peering, meaning their IP networks may not be directly connected.

- In this case a third party must also allow the bandwidth to be allocated.

- DIAMETER supports both Int-Serv (for the small network or at the edges of large networks) as well as Diff-Serv (for the large/backbone networks).

Quality of Service is accomplished by either using RSVP (small or edge networks) and by using the Type Of Service (TOS) field within the IP Header.

QOS Support

- APC-1385 states that Bandwidth Control is required. This means that QOS policy is not static. Decision is made by observing both the static policy as well as current network bandwidth allocation.

- DIAMETER QOS Extension provides this functionality (see draft-calhoun-diameter-qos-00.txt).
Support of other VoIP Networks

- Support of a Inter-Gatekeeper protocol that can support protocols other than H.323 is a MUST. Some provider will offer different flavors of Voice/IP products (i.e. SIP Gateways).

- The Inter-Gatekeeper communication protocol is the logical entity to act as a bridge between both types of networks.

- DIAMETER already fulfills this role in the QOS arena by bridging Integrated and Differentiated Services networks. It would be a great candidate to bridge VoIP networks as well.