IRTF
Authentication Authorisation and Accounting ARCHitecture Research Group
chairs:
C. de Laat and J. Vollbrecht

Content of this talk has contributions from many persons including:
• This space is intentionally left blank
• Networking
  – Focus on applications for Physics
  – QoS networks for computing, collaboratories and telelearning
  – Distributed systems topics:
    » Modeling
    » Optimization
    » Simulation
    » Emulation
• EU project REMOT / DYNACORE
  – Collaboratories, virtual control rooms
  – Support science at the home institutes
  – Groupware, Videoconference tools point to point and point to multipoint
  – Corba services, distributed object db
  – www.phys.uu.nl/~dynacore
Physics-UU to IPP-FZJ => 7 kingdoms

- Netherlands
  - Physics dept
  - Campus net
  - SURFnet

- Europe
  - TEN 155

- Germany
  - WINS/DFN
  - Juelich, Campus
  - Plasma Physics dept

Multi Kingdom Problems

USA line

3 ms

2.5 ms

17 ms
The need for AAA

See IRTF AAA-ARCH Research group
Policy based networking example

Experiment - Pc - Policy based networking switch with > layer 4 AAA functionality - Macintosh - Camera - AAA

BBI
Applications

- Network Access
- Bandwidth Broker
- Authorization of resources living in many administrative domains
- Grids of any kind
- Budget system
- Library system
- Computer based education system
- E-Commerce
- Micro-payments
- Car Rental
- Daily life
Example application: bandwidth brokerage at Enterprise/Service Provider boundary
Roaming “Pull” Authorization Model

Example applications: Mobile IP, PPP dial-in to NAS
Example application: Internet printing, where file and print servers are in different admin domains
AAA Server building block

Rule example: Auth\_A = (B>9) \text{.or.} C \text{.and.} D

Types of communication:
1: “The” AAA protocol
2: interface (API) to app specific module (addressing!)
3: interface (API or connection) to repositories (e.g. LDAP)
Generic AAA server
Rule based engine

Application Specific Module

Policy
Events

Service

Types of communication:
5: Towards service (f.e. COPS, CLI, SNMPv3)
Generic AAA server
Rule based engine

Application specific Module

Policy

Events

Types of communication:
4: Legacy protocols (Radius, Diameter, …)
Generic AAA server
Rule based engine

GW
Application specific Module

Policy
Events
AAA Server with Accounting as Separate Service

1. Generic AAA server
   Rule based engine

2. Application Specific Module

3. Accounting Module

4. Service

5. Metering

6. Acct Data

Policy

Events
AAA Server with Accounting as Part of the Service

1. Generic AAA server
   Rule based engine

2. Application specific Module

3. Policy
4. Events

5. Service
6. Accounting/
   Metering
7. Acct Data
Example: Interaction with Authorization

User

AAA Server

Service Equipment

Collectors

Meters

Visited ISP

Bill

Home ISP

Charging & Billing

ARs

Accounting Records (ARs)

Service parameters including Accounting Policy

Charging Policies

(optional online charging)
Specific goals of the RG are:

- develop a generic AAA model by specifically including Authentication and Accounting
- develop an audibility framework specification that allows the AAA system functions to be checked in a multi-organization environment
- develop a model that supports management of a "mesh" of interconnected AAA Servers
- define a distributed policy framework, coordinate with policy framework WG and others
- develop an accounting model that allows authorization to define the type of accounting processing required for each session
Specific goals of the RG are:

- implement a simulation model that allows experimentation with the proposed architectural models (also work on an emulation)
- describe interdomain issues using generic model
- work with AAA WG to align short term AAA protocol requirements with long term requirements as much as possible
- complete the work in Q4 - 2000 (ambitious)
The three scenario's

• **Bureaucracy**
  – Do the advanced applications by hand
  – Long turnaround \(\text{rtt} \approx \text{days}\)

• **Complexity**
  – Automatic application setup
  – Need advanced middleware and probably also bureaucracy

• **Throw Bandwidth at the problem**
  – Might go wrong at bottlenecks
  – Easiest solution
  – Do it yourself services
Stretching the OSI model

- Services
- Applications
- Middleware
- Network

Graphs showing relationships between complexity and bandwidth over time.
Current topics in the RG (Dublin 26-27 June)

- accounting model development in relation to generic architecture
- authentication: what is identity, model of authentication
- security, is that only a transport layer problem, encryption
- PKI infrastructure
- simulation, progress, what do we want to learn
- in light of the AAA-WG discussion, do we think of backward compatibility
- session identification (the need for layered modeling?)
- SIP (session initialisation protocol)
- Policy Definition Language
- inter kingdom relations and consequences for generic model
- management and auditing
- RG reaction to AAA-WG protocol discussions
- organizational stuff: IETF meeting, other meetings, drafts to produce ...
Questions

- Resource discovery <-> AAA discovery
- Is AAA high or low in middleware?
- All A's together or not?
- Should AAA be visible in the app or only stay in middleware and this way solve its user interface problem
• Research Group Name: AAAARCH - RG
• Chair(s)
  – John Vollbrecht -- jrv@merit.edu
  – Cees de Laat -- delaat@phys.uu.nl
• Web page
  – www.irtf.org
  – www.phys.uu.nl/~wwwfi/aaaarch
• Mailing list(s)
  – aaaarch@fokus.gmd.de
  – For subscription to the mailing list, send e-mail to
    majordomo@fokus.gmd.de with content of message
    subscribe aaaarch
    end
  – will be archived, retrieval with frames and in plain ascii:
    » http://www.fokus.gmd.de/glone/research/aaaarch/
    » http://www.fokus.gmd.de/glone/research/mail-archive/aaaarch-current
    » ftp://ftp.fokus.gmd.de/pub/glone/mail-archive/aaaarch-current