AAA developments

www.science.uva.nl/~delaat

Cees de Laat

SURFnet

EU

University of Amsterdam
Generic AAA server
Rule based engine

Application Specific Module

Service

Accounting Metering

Policy Data

Acct Data

API

PDP

PEP

rfc 2903-2906
Token Based Networking
Access Control, Resource Management and Path Selection in Optical Networks using Tokens


Virtual Machine Traffic Controller
- Token PEP
- Token PDP
- HDPEL DRAC

Amsterdam - Netherlight

Chicago - Starlight

Tokens performing Path Selection and Access Control at Optical Inter-Connection Points

Link Owner
- Link Owner PEP
- Token PDP

UvA Token Switch

Token marked IP packets will allow:
- Economic Link Owners to assign usage rights without routing changes.
- Recognition at Inter-Connection Points (Optical Exchanges). When authentic and valid, token marked traffic will use the Link Owners path.
- Implementations that support different business models
- Hardware (NPU based) recognition rate expected to be a 10 Gbit/s.

UvA RFC 2953 Generic AAA server

Rule Based Engine

Application Specific Module

Policy Enforcement

Anonymous usage
- Resource Management

Tokens will allow:
- Separation of (slow) authorization process and real time usage.
- Binding to many different types of attributes: user, time, resource, etc.
- Policy Decision to be abstracted from Policy Enforcement Point.
Features:

- The IXP 2850 is able to perform packet functions at 10 gb/s
- 16 programmable Micro Engines to allow parallel dataplane processing.
- Two crypto units support bulk security algorithms (AES, DES, 3DES, SHA1)
- Designed for IPSec, however is general enough to do other things.
- Supports Cypher Block Chaining in combination with MAC.
Resource Brokering: Your Ticket Into NetherLight

Application architecture:

Lambda networking allows the creation of application specific light paths.

Lambda networking facilities empower users to request services and provision end-to-end light paths if and when they need it.

NetherLight, located in Amsterdam, The Netherlands, is one of such facilities.

The Amsterdam LightHouse is a joint research laboratory of the UvA and SARA.

Resources in the LightHouse can be used by collaborators to prove the concepts of hybrid networks.

Lightpath setup components:

We make use of semantic web techniques. The description of the network is contained in RDF files.

We provide web services interfaces to the client for: reservation handling.

We provision the paths on the LightHouse equipment.

Semantic web
The Network Description Language, an RDF Schema, describes networks in a standard, interoperable way.

Web Services
A WSDL file describes the interfaces to the service available to clients. Clients can interact with the service directly or via a portal.

Our SC105 demonstration
We show the setup of dynamic connections between two computing nodes through the LightHouse/NetherLight Optical Exchange.
Web Services and Grid Security Vulnerabilities and Threats Analysis and Model

Vulnerability-Incident-life cycle

Service/Resource Security zones

Related SGAMA CC activities and technical objectives

Future development

ASK YURI DEMCHENKO
Example experiment agent model

Network Domain A (Amsterdam)

Cluster A

AAA

Cluster C

AAA

Network Domain C (Chicago)

O

X

C

BEN

Cluster A

Cluster C

Border Router

Border Router

Token Switch

Token Switch

PEP

PEP
• finesse the control of bandwidth across multiple domains
• while exploiting scalability and intra-, inter-domain fault recovery
• thru layering of a novel SOA upon legacy control planes and NEs
The VMs that are live-migrated run an iterative search-refine-search workflow against data stored in different databases at the various locations. A user in San Diego gets hitless rendering of search progress as VMs spin around.
Software Status

• The AAA toolkit CVS repository is downloadable. It requires JAVA programming skills to use at this point.  
  – http://www.science.uva.nl/research/air/projects/aaa/demokit

• Also available demo-scenario's (magic 8 ball by Fred Wan)

• Low- and highlevel components in Lighthouse and Netherlight AAA manageable (Glimmerglass / Calient OXC's) en DRAC. It requires a scenario to use or show something.
Software To-Do

• If we can agree on an application-scenario in OptIPuter, we can work out how to fill in the AAA components. That is why scenario's, as shown by Paola at SC2005, are important to push our work.

• We currently try to bring in workflow tools like BPEL to make AAA easier applicable. This is currently the focus of our brainstorm sessions.

• Flexible complex multi domain policy management and execution is key! [ref dr. Carl]
Business as usual :-}
Questions?

Credits:
– Leon Gommans, Paola Grosso, Bas Oudenaarde, Arie Taal, Freek Dijkstra, Bert Andree, Jeroen van der Ham, Hans Blom, Yuri Demchenko, Fred Wan, Karst Koymans, Martijn Steenbakkers Jaap van Ginkel
– SURFnet / GigaPort, Kees Neggers, Erik-Jan Bos, et al!
– NORTEL: Franco Travostino, Kim Roberts, Rod Wilson
– SARA: Anwar Osseryan, Paul Wielinga, Pieter de Boer, Ronald van der Pol, teams
– Joe Mambretti, Bill stArnaud, GLIF community
– Tom & Maxine & Larry, Laurin, OptIPuter, OnVector team !!!!