SARNET: Security Autonomous Response with programmable NETworks

Cees de Laat
System and Network Engineering
Why me?

Was here on sabbatical in March 😊

CdL Sabbaticals in spring 2015

1 - Berkeley - San Diego
All Photos sabb-1

2 - Washington - Chicago - Ottawa
All Photos sabb-2

Activity

work  leisure

Purpose

This personal website contains logs of my sabbatical activities in the spring of 2015. I went on these sabbaticals to be able to engage the community based on content, the more and more managerial stuff I was sucked into at UVA. Also my participation in the SURF scientific advisory board made it necessary to study future directions in infrastructure. Apart from those I always keep on my toes if the research questions we as a group at UVA are studying, are still novel and valid. Directions change very rapidly in particular field of study in System and Network Engineering.

Goals

- Discuss with peers the 5 and 10 year outlook for Cyber Infrastructure. Budgets are shrinking, networks become mature, Supercomputing and High Throughput computing is now also done with huge commercial cloud centers, so what is the position of specific mission resources in this wild ocean of public capabilities.  
- Science community need to do ourselves and what can we just buy in the future from the (cloud) market. What do and what do we not need to do on leadership supercomputing. How do we relate to public cloud. We also do not have scientific water. What do we need to do on data at the central level? Do we need a national service including data stewardship, etc.
- Next year we are chairing the eIRG with 4 speakers
- Reflection on our own research questions

Personal

- Take some holiday
- Have Emelia joining me for a couple of days
- Drive the HWY1
- Visit the desert
- Go to Chicago theatre, music bars, parks
I want to show Big Bug Bunny in 4K on my Tiled Display using green Infrastructure.

- Big Bugs Bunny can be on multiple servers on the Internet.
- Movie may need processing / recoding to get to 4K for Tiled Display.
- Needs deterministic Green infrastructure for Quality of Experience.
- Consumer / Scientist does not want to know the underlying details.

His refrigerator also just works!
Yesterday’s Media Transport Method!

8 TByte
The GLIF – LightPaths around the World

The GLIF – LightPaths around the World

Layers

Doing Science

Wisdom

Knowledge to act

Information

Data

ICT to enable Science

Tada

Schedulers to act

OWL

XML, RDF, rSpec, text, Java based, etc.
The Big Data Challenge

Doing Science

Wisdom

Knowledge

Information

Data

ICT to enable Science

Schedulers

Ta da

MAGIC DATA CARPET

curation – description – security – policy – integrity - storage

XML, RDF, rSpec, text, Java based, etc.
Why is more resolution better?

1. More Resolution Allows Closer Viewing of Larger Image
2. Closer Viewing of Larger Image Increases Viewing Angle
3. Increased Viewing Angle Produces Stronger Emotional Response
Moving Big Data Objects Globally

- **Digital Motion Picture for Audio Post-Production**
  - 1 TV Episode Dubbing Reference ~ 1 GB
  - 1 Theatrical 5.1 Final Mix ~ 8 GB
  - 1 Theatrical Feature Dubbing reference ~ 30 GB

- **Digital Motion Picture Acquisition**
  - 4K RGB x 24 FPS x 10bit/color: ~ 48MB/Frame uncompressed *ideal*
  - 6:1 ~ 20:1 shooting ratios => 48TB ~ 160TB digital camera originals

- **Digital Dailies**
  - HD compressed MPEG-2 @ 25 ~ 50 Mb/s

- **Digital Post-production and Visual Effects**
  - Gigabytes - Terabytes to Select Sites Depending on Project

- **Digital Motion Picture Distribution**
  - Film Printing in Regions
    - Features ~ 8TB
    - Trailers ~ 200GB
  - Digital Cinema Package to Theatres
    - Features ~ 100 - 300GB per DCP
    - Trailers ~ 2 - 4GB per DCP
John Graham’s Network Results
Moving the CineGrid Exchange 30TB
UCSD< --> UvA

Iperf3 mem to mem : 32 Gbps

Animations Folder Transfer

Limited by many 25 Mbyte 4k frame files, file system, ZFS, sata interfaces, etc.
Network virtualizations and SDN

Reasoning

Risk evaluation

Trust groups

Execute response & adaptation
Line of research

• 1997: Need for authorization framework for combination of resources across domains
• 1998: AAA-ARCHitecture research in IRTF
• 2000: RFC 2903-2906, 3334
• 2005: open versus not so open exchanges
• 2006: start of trust research (also in rfc 2904)
• 2012: I2-spring session presenting line of research
• 2014: PhD defense of research plus publication
• 2015: Here we are.
Cyber security program

• Research goal is to obtain the knowledge to create ICT systems that:
  – model their state (situation)
  – discover by observations and reasoning if and how an attack is developing and calculate the associated risks
  – have the knowledge to calculate the effect of counter measures on states and their risks
  – choose and execute one.

In short, a we research the concept of networked computer infrastructures exhibiting SAR: Security Autonomous Response.
Timeline

• 1\textsuperscript{st} year
  – Make infrastructure programmable (SD)
  – Observe and measure
  – Model organisations & relationships

• 2\textsuperscript{nd} year
  – Multi domain
  – Countermeasure patterns
  – Assign value, cost assessment

• 3\textsuperscript{rd} year
  – Autonomous response across domains
  – Reasoning
  – Visualisation
  – Performance
Ciena’s CENI topology

- Ottawa - Chicago Infrastructure
- Canarie MANLAN link
- ESnet alt route segment
- Link to Ciena Station Ridge HQ
National Science Foundations ExoGENI racks, installed at UvA (Amsterdam), Northwestern University (Chicago) and Ciena’s labs (Ottawa), are connected via a high performance 100G research network and trans-Atlantic network facilities using the Ciena 8700 Packetwave platform. This equipment configuration is used to create a computational and storage test bed used in collaborative demonstrations.
Service Provider Group framework

A Service Provider Group (SPG) is an organisation structure providing a defined service only available if its members collaborate.

Examples:

- Internet2
- NET+
- SKYTEAM
- geni
- glif
- eduroam
- MasterCard
- Multi-Domain Authorization for e-Infrastructures
Service Provider Group Characteristics

- **Autonomous members** acting together on a decision to provide a service none could provide on its own
- Appears as a single provider to a customer
- Appears as a collaborative group to members with standards, rules and policies that are defined, administered, enforced and judged by the group.
- Autonomy in the group: every member signs an agreement declaring compliance with common rules, unless local law determines otherwise.
- Membership rules organizes trust amongst members and manage group reputation and viability.
Envisioned role of the SPG: define slice archetypes?

SPG - A

Privacy
Big Science
DRP

Service Provider Group level

Slice Creation level

Aggregate Manager

Service Provider Infrastructure Level
More Info

• [http://delaat.net/sarnet](http://delaat.net/sarnet)
• Rudolf Strijkers, "Internet Factories", UvA, Nov 2014.
• Contact us:
  – [delaat@uva.nl](mailto:delaat@uva.nl)
  – [l.gommans@uva.nl](mailto:l.gommans@uva.nl)
  – [rwilson@ciena.com](mailto:rwilson@ciena.com)
  – [Robert.meijer@tno.nl](mailto:Robert.meijer@tno.nl)
  – [T.M.vanEngers@uva.nl](mailto:T.M.vanEngers@uva.nl)