Flow (DDOS) Security in Emerging Internets

How to create Peaceful Domains (unbaked arbitrary musings)

Jerry Sobieski
NORDUnet

DDOS

- Why is this a problem? What allows these types of malflows to exist?
- Much effort to staunch the bleeding and deflect the bullets... But little effort to stop the shooting... To change the fundamental security flaw in IP networks that allow DDOS processes to exist:
  - Sender initiated flows
  - Anonymous (unAuthenticated) flows

- Will authenticated and authorized network flows undermine an imporatnt feature of IP?
- Do all IP applications need/want anonymity?
- Can we domains that are auth*'ed
- How do we scale the auth* services to allow flow based permissions?

A Big Picture approach…

- How can we “undefine” [d]DOS attacks in a future internet?
  - Prob: Unwanted flows are able to saturate an interface
- FI strategy: Authorized data plane flows only
  - Protected domains within which only auth flows exist
    - “Hope” is not a strategy. ☺
  - TCP session intercept/extensions, and/or TLS enhancements, ...
  - UDP flows will need a session Auth*
  - Automated network integrated flow queuing...(until the flow is authorized and released.)
    - Is this practical?
- What prevents the control plane from being DOS’ed?

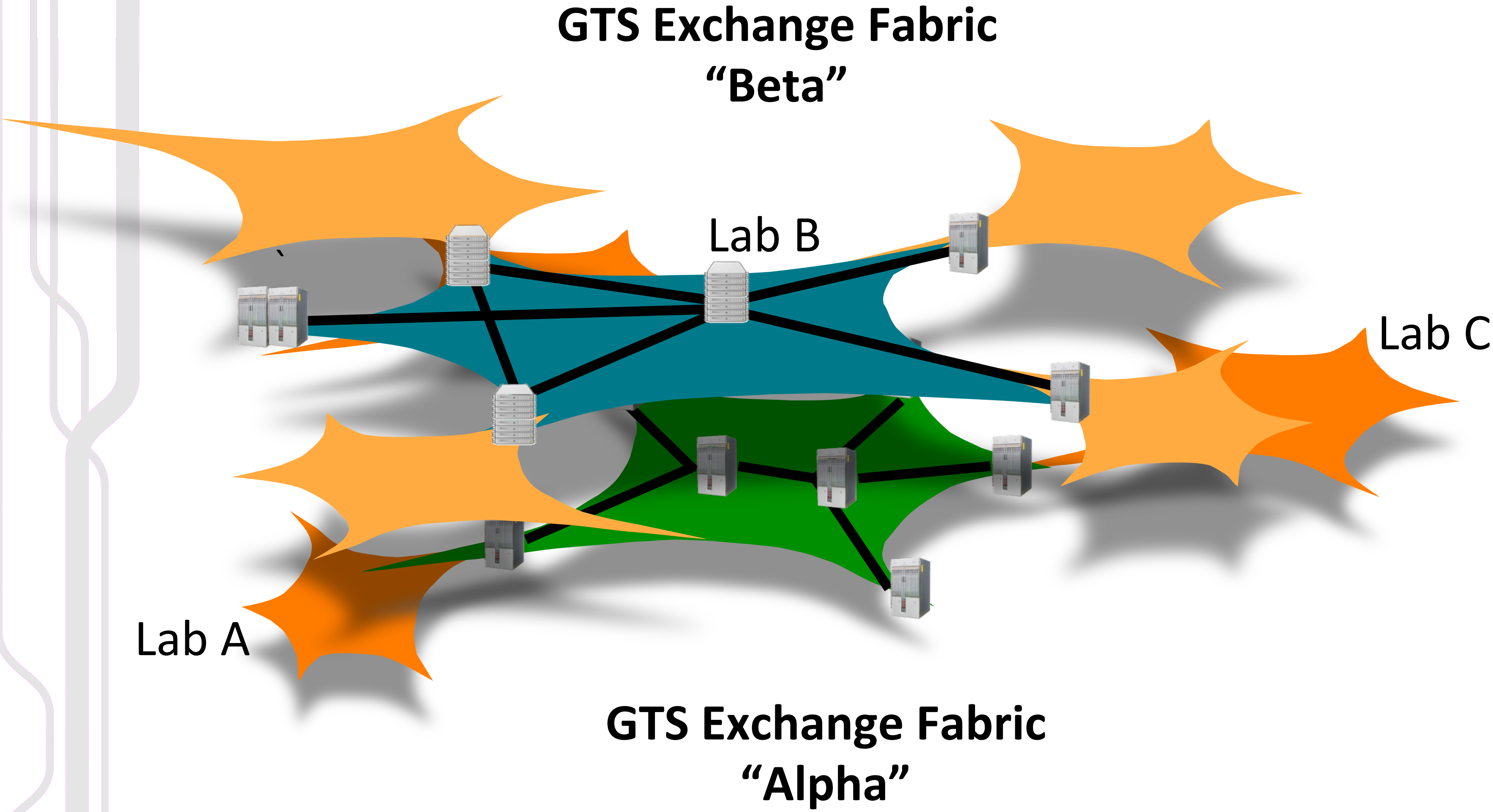
Anonymity and Authorization

- DDOS is successful/possible due to anonymity in the internet
  - Existing flows are delivered to end system/interface ->based on the sender's desire
  - The receiver is not consulted! The sender is not known...
- Future network protocols should be based on flows that have been explicitly authorized (not just the service itself) –
- Can we construct service domains that allow only known flows in or out??
  - This is a service paradigm that is not a traditional IP mindset
- We need a means of the receiver to be consulted before a flow is enabled to a end system...
  - So all inbound flows will be authorized? But authorization requires authentication....
  - i.e. loss of anonymity?
  - Can we separate services that expect AA from "open" unauthenticated "wild west" services...??

“Software Defined eXchange”

- Software Defined eXchange “SDX”
  - SDX: A service infused open exchange facility that can provide a wide range of multi-species resources and services – e.g. computational facilities, data transport circuits, switching/forwarding elements, storage, etc – and supports SDN control principles. (credit: Zink & Mambretti @ FIDC 2014)
- SDXs could be the basis for secure “peaceful” domains...
  - An example: GEANT Testbeds Service
  - used to incrementally construct regions of known flows...

[GEANT] SDX Fabrics



Peace and Love, man!

- Peaceful networks require a “citizenship” or community that no longer exists in the internet
- How do we re-create peaceful secure domains?