

# The Challenges and Opportunities of Security and Virtualization for Distribution of Functions in an IP Network

Paul Gleichauf  
PRESTO Conference  
Princeton, NJ  
May 30, 2007



# Can next generation networking research be done without corporate collaborations?



# Can next generation networking research be done without corporate collaborations?

- No



Can next generation networking research be  
done without academic researcher  
collaborations?



# Can next generation networking research be done without academic researcher collaborations?



- No



# Where are governments?

- Grand challenges
- More or less silent
- Small funding allocations
- High overhead



# Academic's (Dis-?)incentives

- Enable publication and platform access to international communities of academic researchers including students.
  - New companies often spin out from research institutions
- Funding is hard to find
  - Governments usually limit to crisis solutions or
  - Rare visionary jump-starting a critical technology
  - Funding amounts are too small
    - Overhead addiction
    - Academic research not easily incorporated into products
- Open source is to enable widest possible collaboration



# Corporate (Dis-?)incentives

- Economics is important to companies. What's in it for them?
  - Cautious about creating their next generation of competitors
  - Short-term is more important than long-term
  - Proprietary components are prized
- Highly expert technical staff members are decreasingly rewarded for following their own muse.
- Governments dislike research funding given to corporations
- Standards for interoperability to increase market size at risk of sharing
- Open source for off-loading well known solutions as cost savings

# Companies and academic researchers are becoming codependent

- Funds from corporations to researchers need to increase as long as government does not step-in
- Mixtures of proprietary and open-source solutions can account for range of incentives in both communities
- Flexibility to accelerate development is needed
- Common agreed upon pre-standards architecture



# Virtualization properties list

- Platform independence
  - Efficient use of SW and HW by logical partition and unification of processing nodes, links, storage
  - Dynamic movement of SW across HW
  - VM's bind application to OS
- Isolation
  - Security of VM's (HW and SW support)
  - Hypervisor OS below OS's

# Mechanisms to bridge the divide

- Security
- Virtualization
- Good-enough components evolution
- Economic models and constraints (e.g. \$ and power)
- Assume a layered model (for now)



# Security

- Transparency (layer independent service)
- Authenticated sources (device, user, code/data)
- Data and code treated essentially identically
- Authorized traffic (DPI, layer violation)
- Tunneling creates overlays
- Virtualization complicates security

# Virtualization

- Mix proprietary and open source implementations on a common shared substrate (learn from IP)
- Mix of SW evolving to HW
- Security complications
  - Replay
  - VM identity
  - VMM is just another OS “layer”

# Good enough components evolution

- Start cheap, simple, secure, cool
- Commodity platforms evolve fastest, 2x cores/10 mo.
- HW support for virtualization security exists
- Software flexibility first, lock in HW as needed
- Even on multicores, HW cores will eventually mix
- Edge of network already moving onto virtualized machines, network devices already being virtualized

# Economic models and constraints

- Let companies hold on to but incorporate modules they consider high value
- Let academic researchers open up their own modular implementations
- Provide high-level shared architecture that is legally minimally encumbered (learn from IP)

