SwitchWare

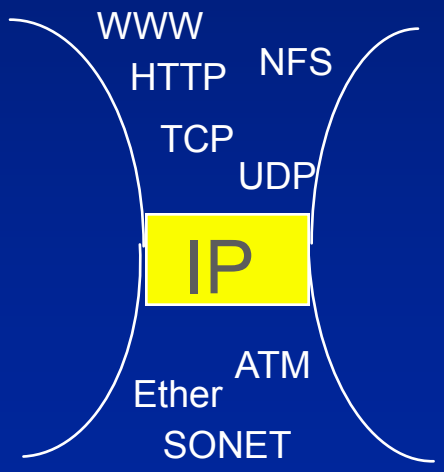
Accelerating Network Evolution

Jonathan M. Smith, jms@cis.upenn.edu

University of Pennsylvania

Virtual Infrastructures, e.g., IP

- IP is a network interoperability layer
- Interoperable through minimality:



Overlays (running at hosts)

Virtual Network Infrastructure (runs globally)

Subnetworks (run IP locally)

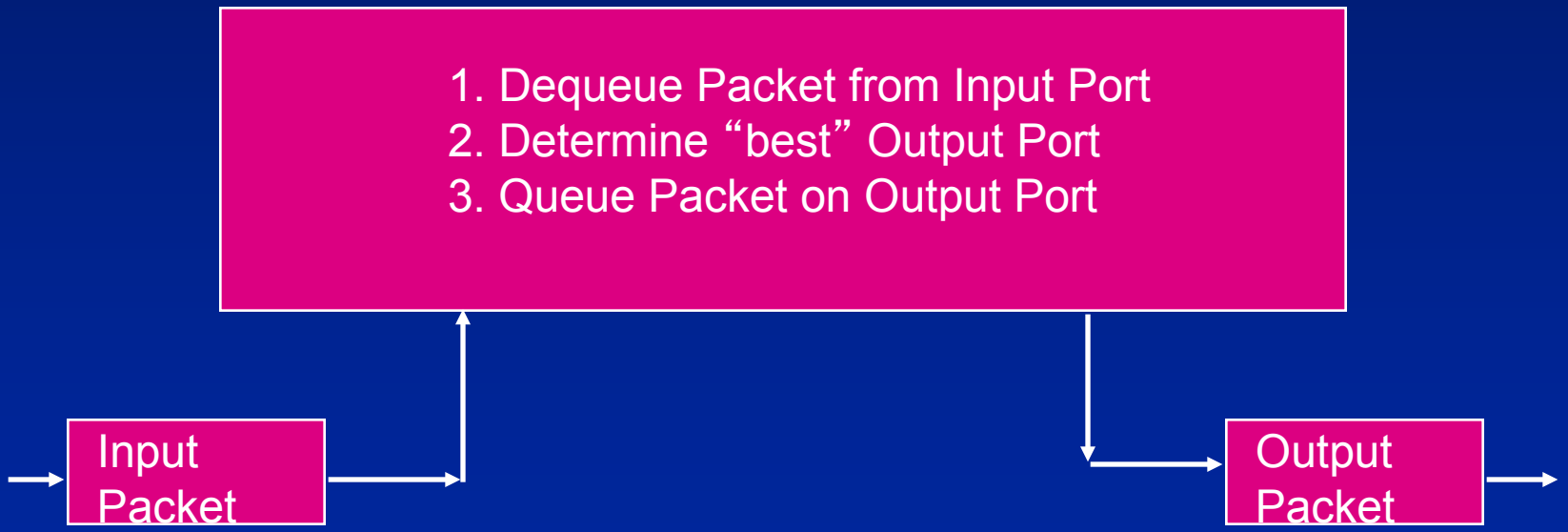
But, TNSTAAFL*....

- Interoperability layer: IP packet format
- IP must run everywhere
  - » all enhancements are at hosts
  - » Problems for MBONE, RSVP
- Worse: IETF and standardization
- Tempo is political, not technical!!!

*There's No Such Thing as a Free Lunch!

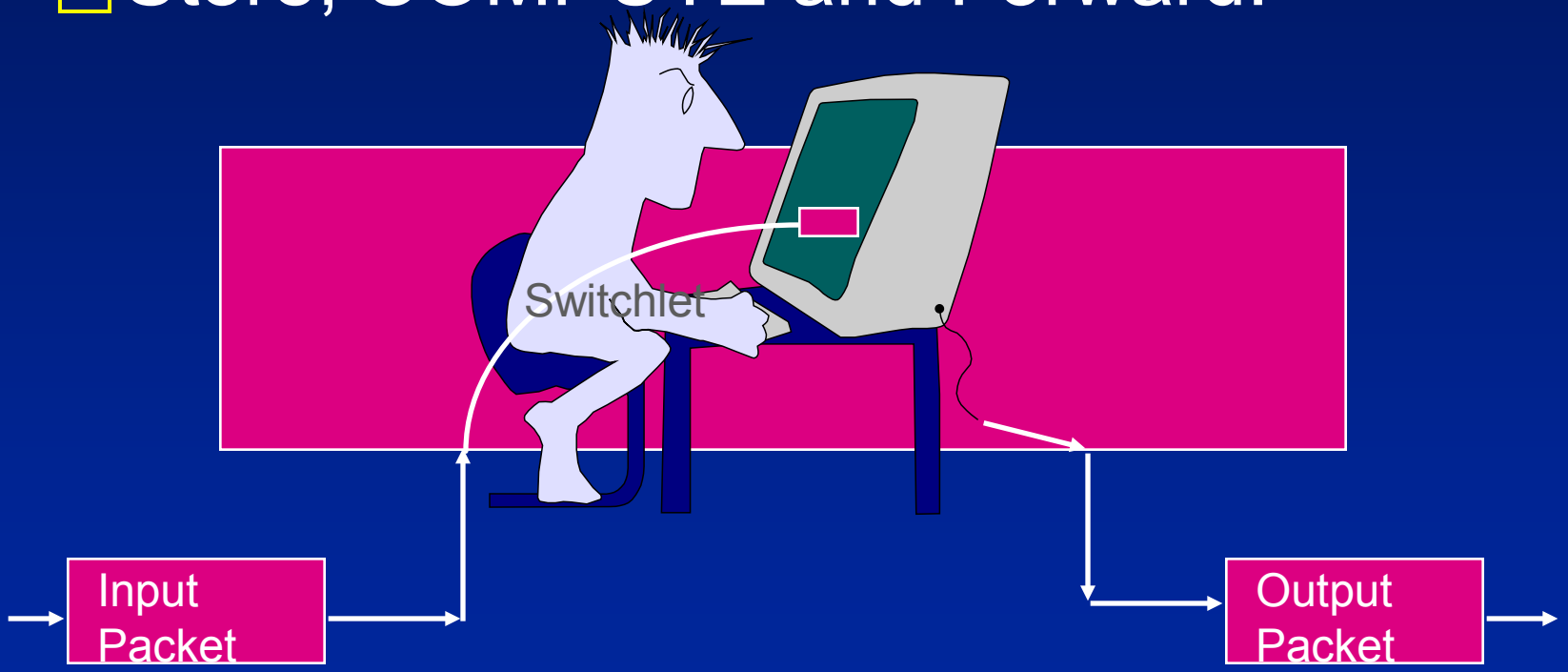
IP Routing Infrastructure

- Model: Store and Forward



SwitchWare switching

- Store, COMPUTE and Forward!



Result: ‘‘Active’’ Networks

- Accelerate service creation with programmable network infrastructure
- Programmable on per-user or per-packet basis
- Is this just another O.S. problem?
- See Tennenhouse, Smith, et al. survey in IEEE Network Magazine, Jan. 1997

Hard Problems & Approaches

- Performance: Well, yes but *Correctness* FIRST!
- Safety: Good guys can make mistakes...
- Security: Bad guys can program too...
- Network Infrastructure is *shared*
  - » it MUST work (telephony as example)
- Can we get **FLEXIBILITY** *and* **SECURITY**?

Security is not Cryptography!

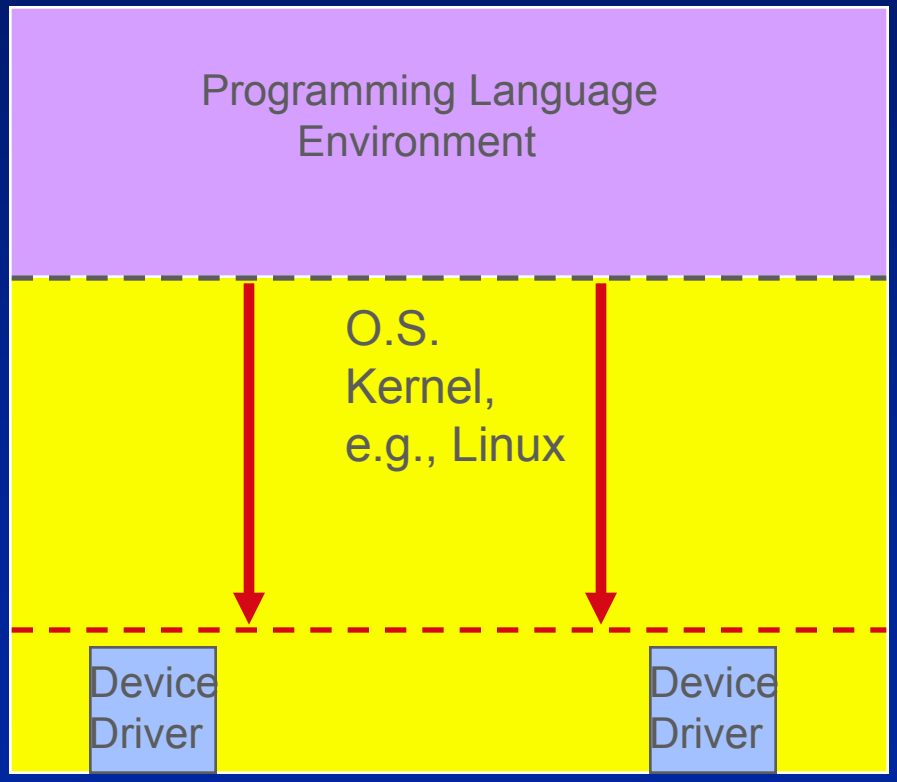
- Is your message "secure" if it doesn't get there? (e.g., denial of service)
- Security is adherence to a security policy
- Unfortunately, in many systems policy is informal, defined in *ad hoc* manner, and focused only on *selected* attacks
- NB: Attacker may not agree on selection

Network Infrastructures

- Shared, so virtualization matters
- Need timing, privacy and authentication
- Focus must be on protection of the network elements (what will be programmed), in spite of improved flexibility
- Node security, then network security

How do we control programs?

- Safety & Security: P.L., O.S. or hybrid?

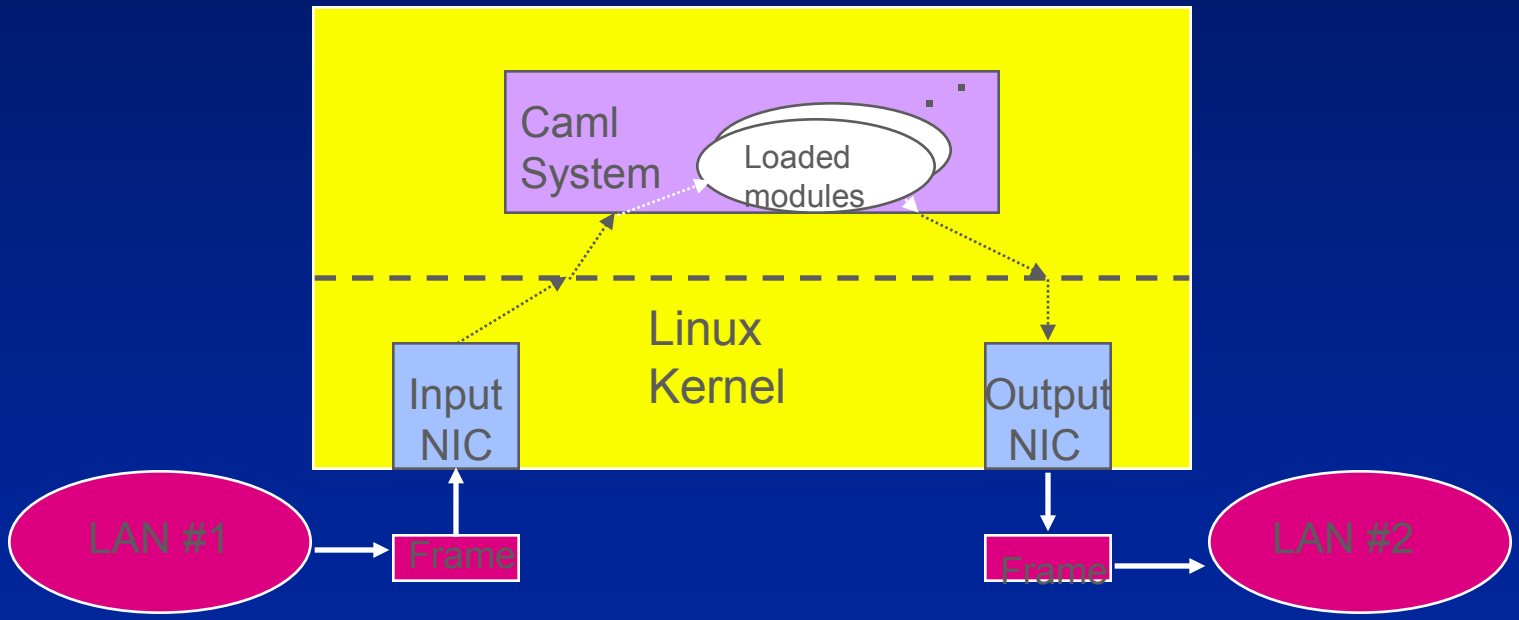


A Language-Oriented Model

- Switchlet Language for users (SL)
  - » formal semantics restrict programs
  - » (e.g., packet filters use regexps)
- Wire Language for communicating (WL)
  - » formal semantics across boundaries
- Infrastructure Language for Virtual Machine (IL)
  - » formal semantics supported on metal: run-time

Current Software

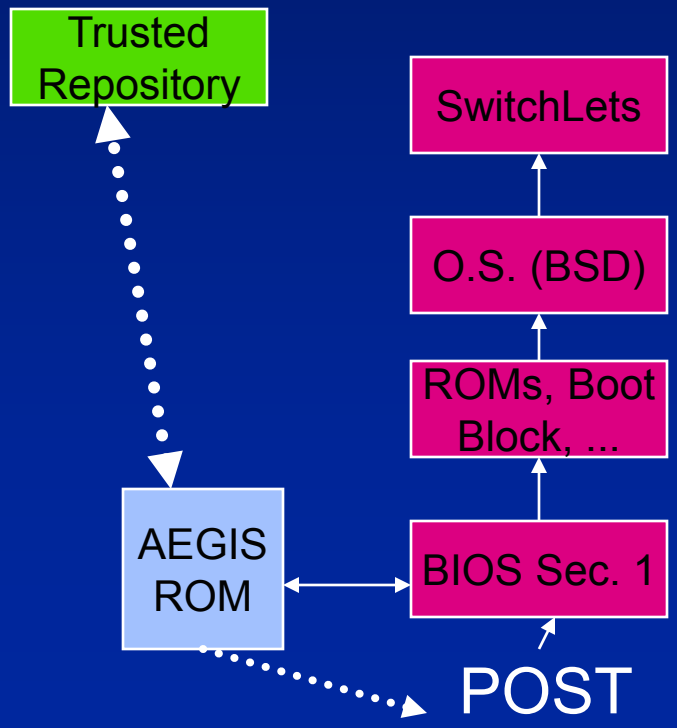
- Active Bridging (Scott Alexander)



- http://oilhead.cis.upenn.edu/~salex

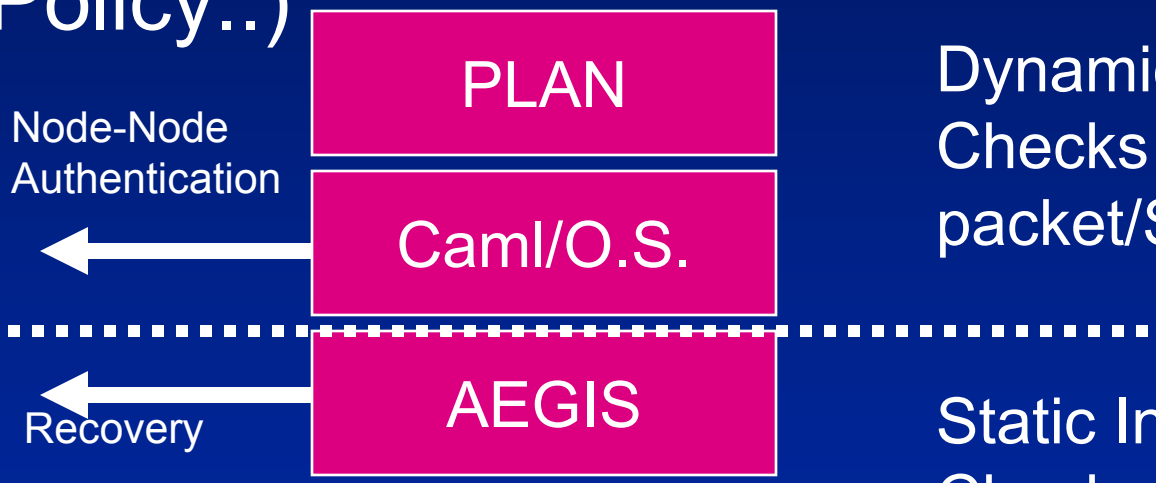
AEGIS Secure Bootstrap

- Integrity Guarantees for Dynamic Integrity Checking (http://www.cis.upenn.edu/~waa)



Secure Active Network Element (SANE)

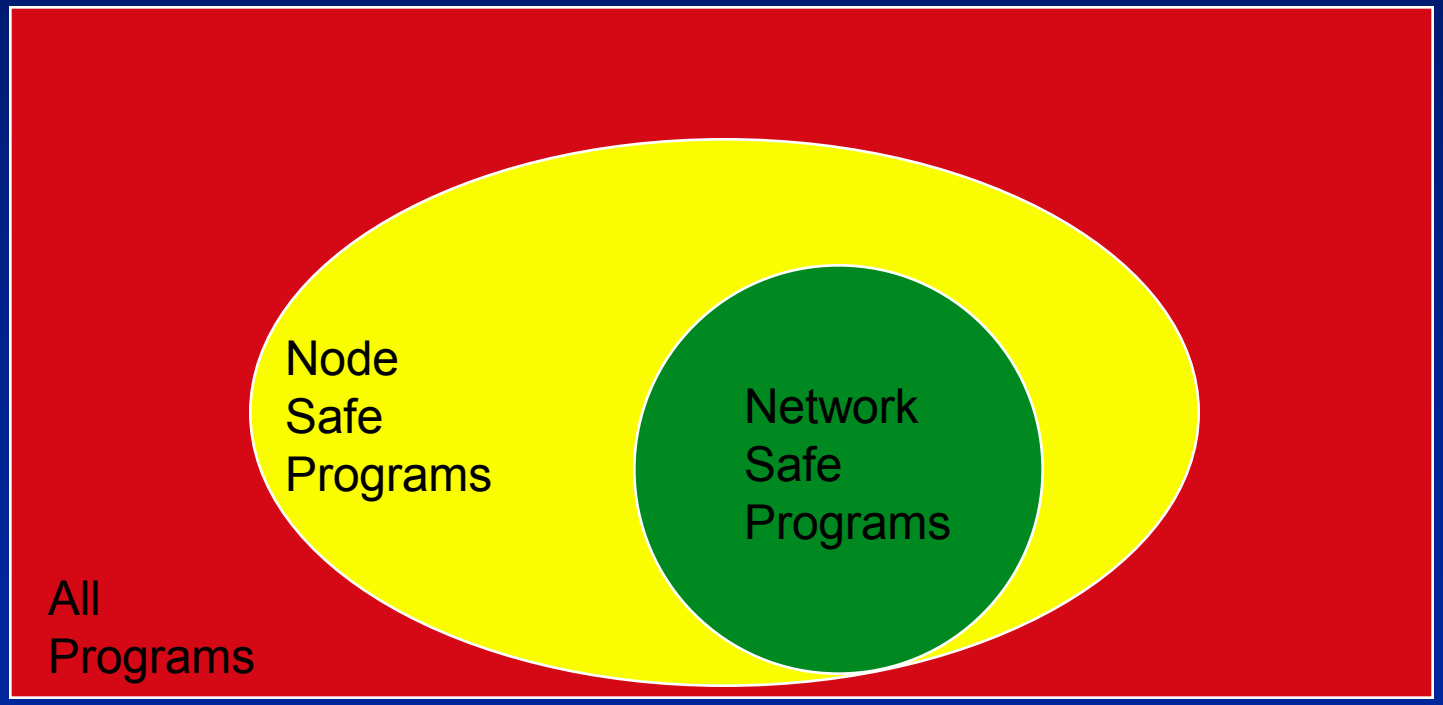
- "Trust, but Verify" (U.S. Nuclear Policy..)



http://www.cis.upenn.edu/~waa
http://www.cis.upenn.edu/~angelos

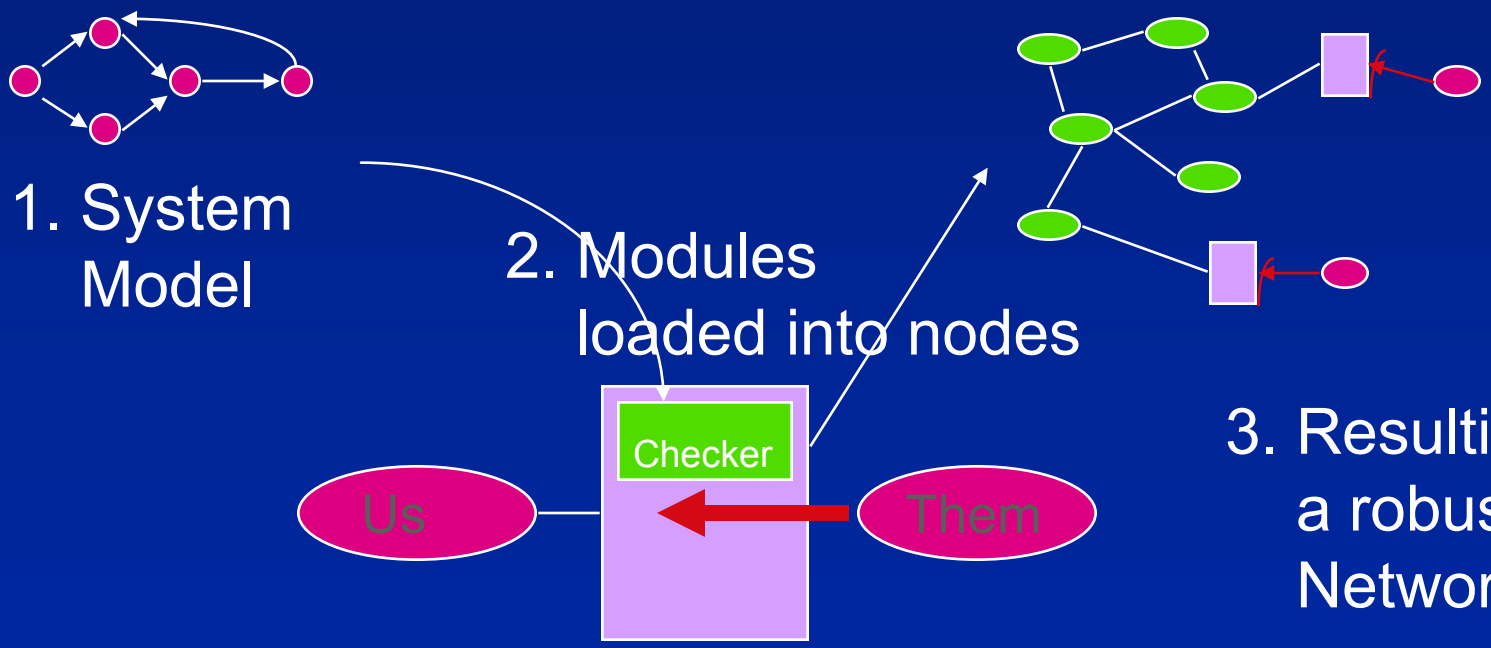
Restricting Programs

- Node safe versus network safe



Model->Modules->Actions

- Syntax, Semantics, Node vs. Network
- Example: Securing a Network



Credits:

- DARPA Contract #DABT63-95-C-0073
- Collaborators @ Penn, Bellcore and MUSIC Semiconductors (Farber, Feldmeier, Gunter,Marcus, McAuley, Nettles, Segal and Sincoskie)
- Hewlett-Packard and Intel Corporations
- U. Cambridge and EPSRC (sabbatical)

Accelerating Network Evolution

- *Trying to change the "tempo" of network evolution from political to technological by design/architecture*
- *Programmability / Extensibility*
- *Security by design, not afterthought*

http://www.cis.upenn.edu/~switchware