

R3 Security: Self-defense and Policing

Jonathan M. Smith
Jms@cis.upenn.edu



Router Self-defense

- Modern routers are complex hardware/software artifacts
- As with any system with $>10\text{MLOC}$, bugs
 - Some fraction are exploitable
- Routers are harder to exploit than hosts
 - Not immune, and we're not prepared
- Consequences of a router exploit
 - Possibly local, possibly (very) global...
 - Black Holes, BGP, route around FWs, ...

A few observations about software

- Verification useful, but...
 - Axioms may be violated in the field
- Big software: no single designer
 - Interface/assumption mismatches
- Security is a software engineering story
 - All in “The Mythical Man Month”!
- A good software architecture gains a lot

Architectural desiderata

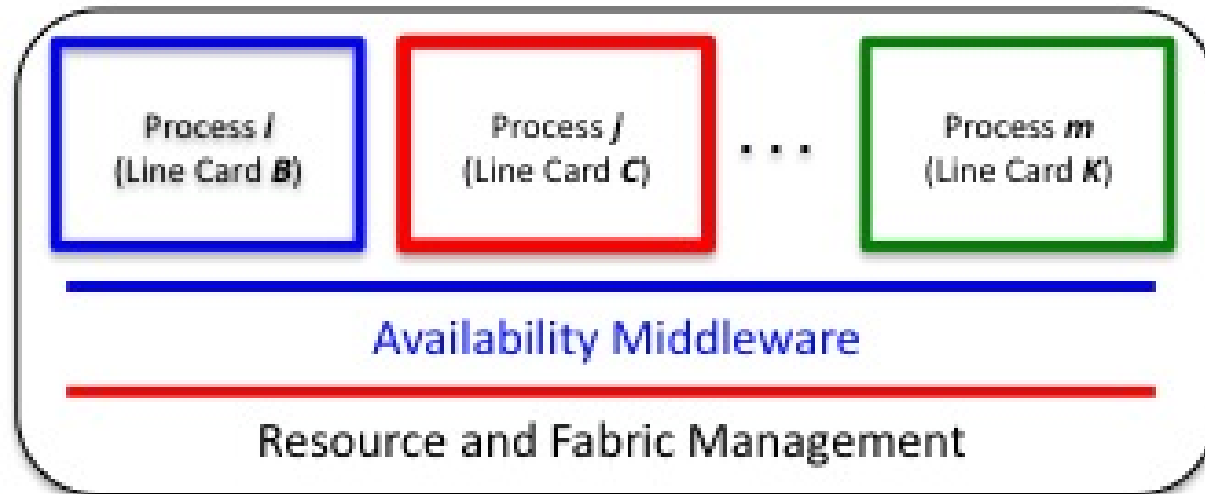
These are built on R. Broberg requirements

- Isolation
 - The effect of an exploit is limited
- Recoverability
 - Can recover from faults (and exploits)
- Availability
 - Fault recovery concurrent with operation
- Virtualization
 - Multiple networks running at once

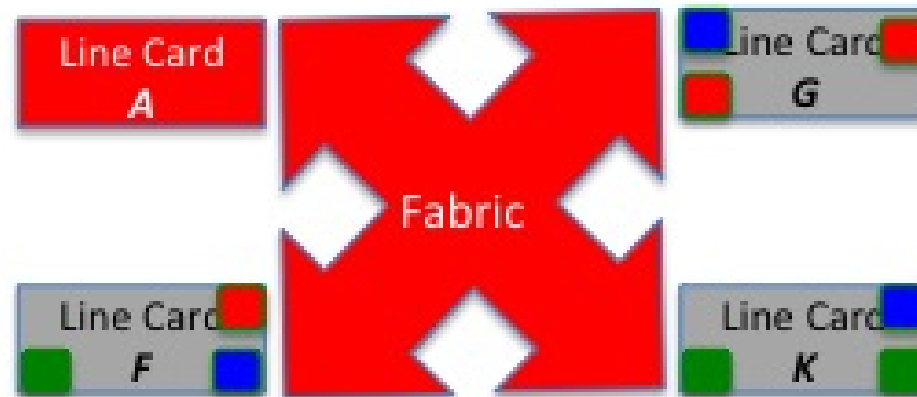
Router Reliability Research (R3)

- See <http://r3.cis.upenn.edu>
- Open project with many participants
 - Cisco, Cornell, Delaware, MIT, Penn, Purdue, VU and potentially more...
- Goal: rethink control plane software
- Track or exceed capacity scaling
- Best of breed ideas at multiple levels
- Target: architectural desiderata

Abstract R3 Architecture



- External (e.g., OpenFlow)
- Internal Open Source
- Internal Proprietary



Ludd Security

Observations

- Reliability and security have overlap
 - Malice versus nature
 - But very similar mechanisms
- Isolation naturally contains many faults
- R3 middleware compact enough to verify?
- R3 research: router self-defense

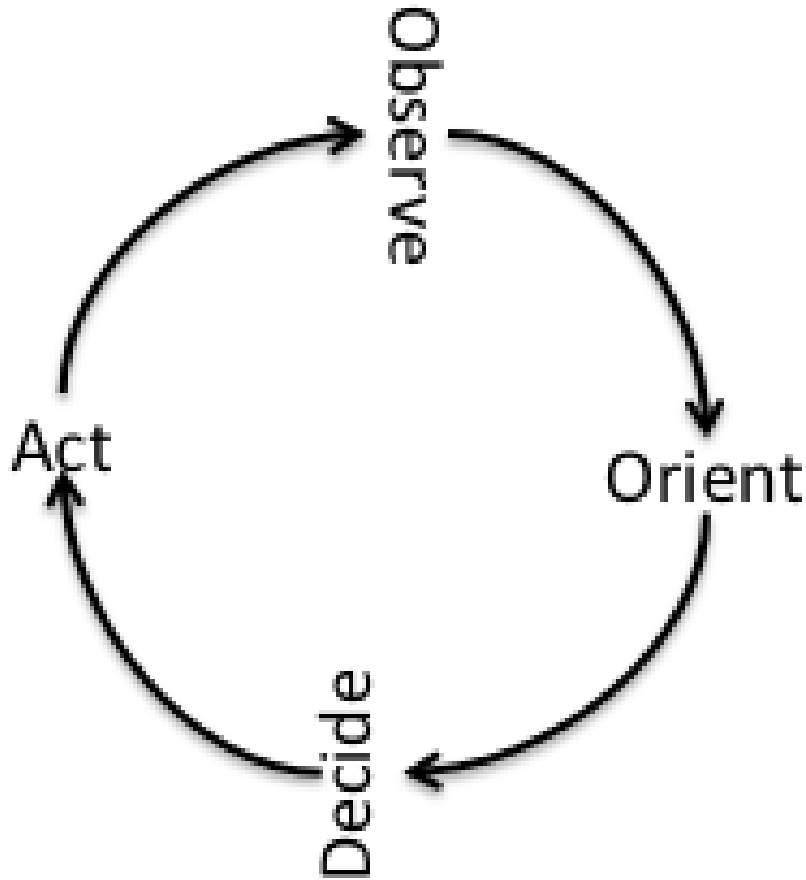
New forms of Trust-based isolation

- IPC middleware can use packet filters / FWs
- Signed downloads of new / maintenance SW
- Use of Trusted Platform Modules
 - Minimal Trusted Computing Base (TCB)
- Trust decisions based on use of protocols
 - IPsec
 - BGPsec

R3 enables new defenses

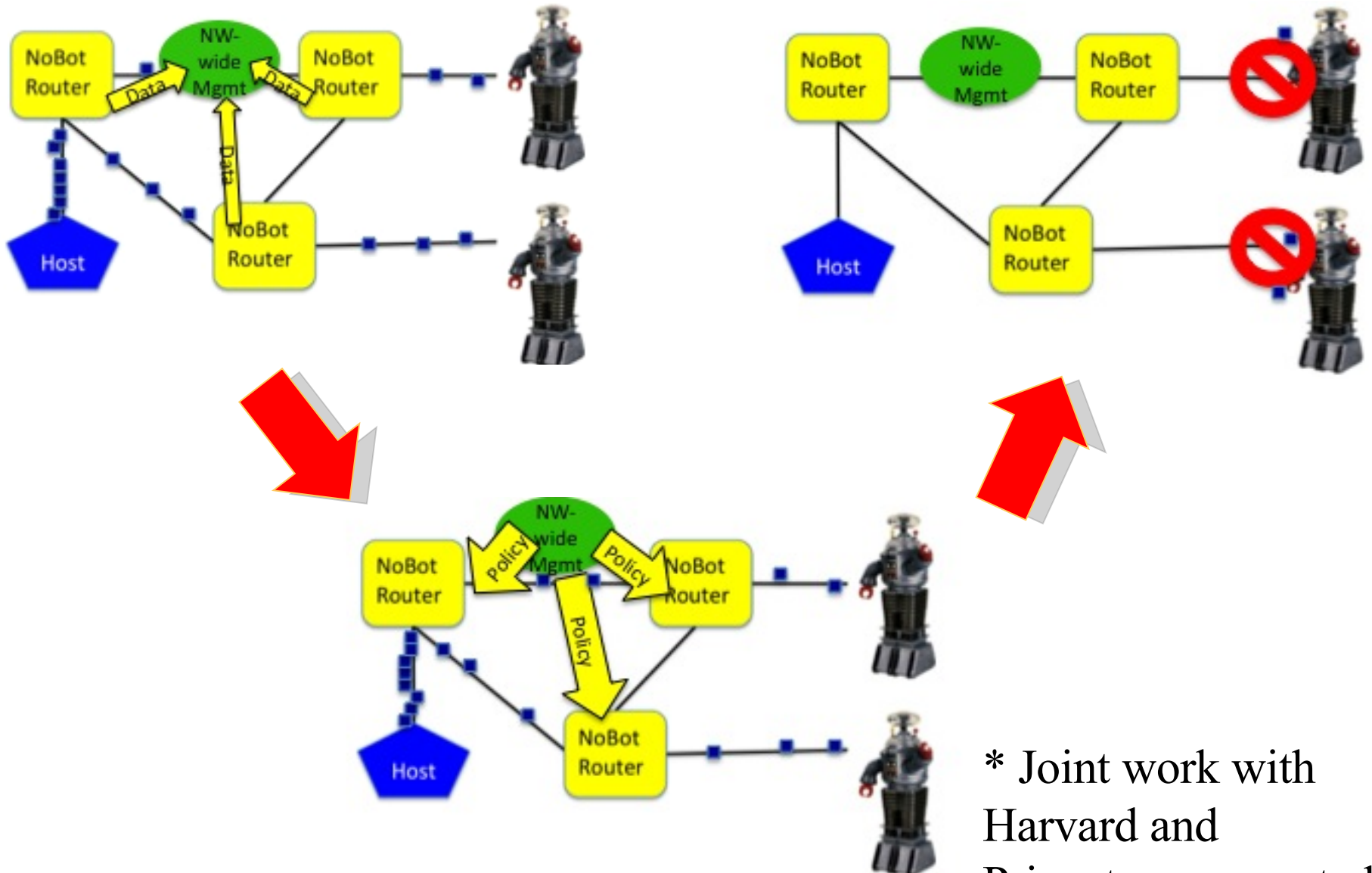
- Consider the botnet threat:
 - Large # of managed infected hosts
 - Toxic cloud computing?
 - Effects: spam, DDoS
 - Command and control channel (arms race)
- Possible solutions
 - Fix host software / train users?
 - Reform black hats?
 - Use the network?

The case for R3-like elements: John Boyd's OODA Loop



- Faster cycles than adversary: win
- Technologies should therefore focus on accelerating OODA loop cycles
- Example: F15

Networks opposing Botnets (NoBot)*



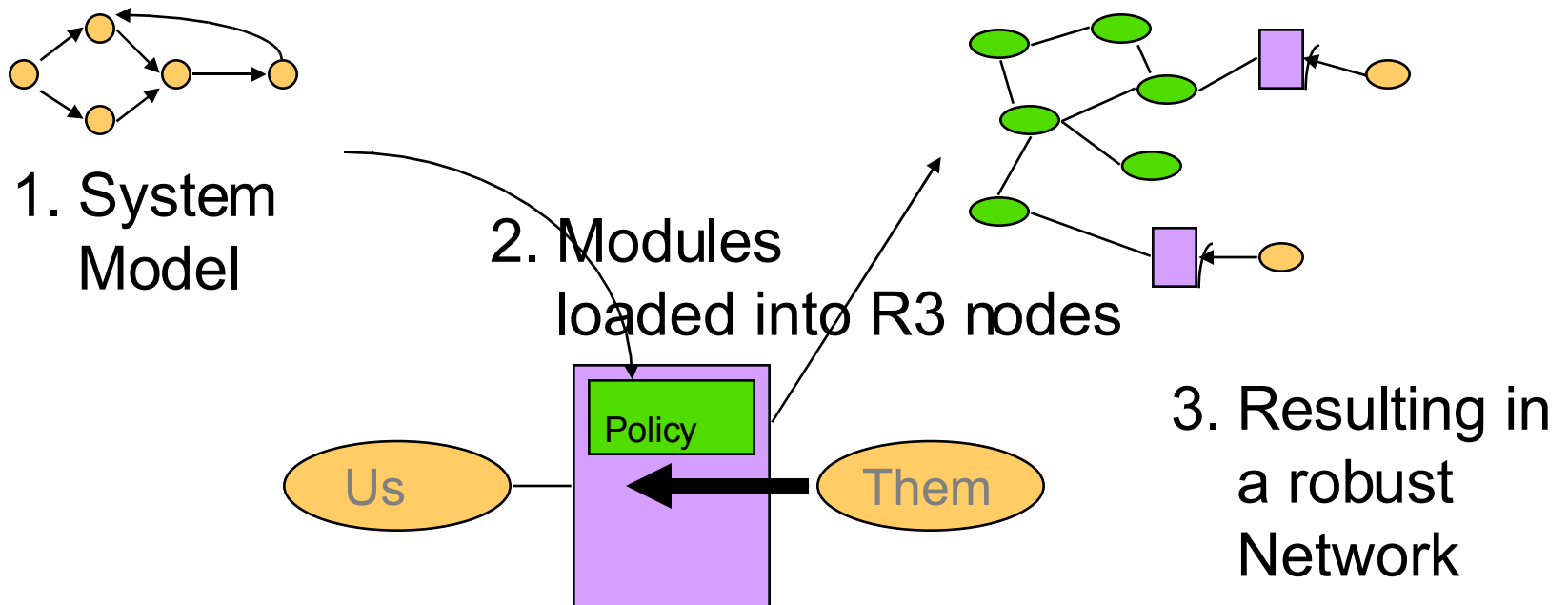
* Joint work with Harvard and Princeton, supported by ONR

How does R3 help with NoBot?

- Can support safe dynamic updates
- Can isolate virtual networks
- Can gather statistics as required
 - E.g., new processing of line card data, for example with machine learning in R3 App.
- Can introduce new protocols
 - E.g., data sharing for cooperative defense
 - E.g., policy sharing: circle the wagons
 - E.g., Bellovin, Ioannidis “DDoS pushback”

Model->Modules->Actions

- R3 moves the Network towards a distributed systems model
- Example: Securing a Network



Conclusion

- Routers are as much SW artifacts as HW
 - Therefore they have vulnerabilities
 - Some subset will be exploitable
 - Network positioning / power law: bad news
- Routers as elements in network defense
 - Apply Boyd's OODA loop
 - Exploit R3 for rapid updates
- The network is an important part of the solution