IRATI
INVESTIGATING RINA

The Pouzin Society

Security in RINA

IRATI Workshop

Barcelona, Spain

John Day

Lou Chitkushev

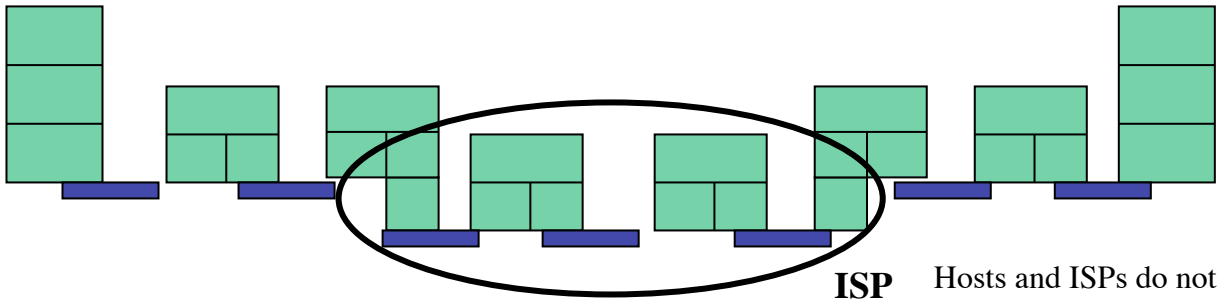
IRATI
INVESTIGATING RINA

The Pouzin Society

First a Word on Method

- When trying to work out the IPC Model absolutely no thought was given to security. All of the focus was just understanding the structure.
- People kept asking, What about Security? Is there a security layer?
- Didn't Know. Hadn't thought about it.
- There was the obvious:
  - The recursion of the layer provided Isolation.
  - That only the Application Name and local port-id were exposed to the correspondents.
- Interesting, but hardly an answer
- But it wasn't the time for those questions . . .
- At least not yet . . .

The Recursion Provided Isolation



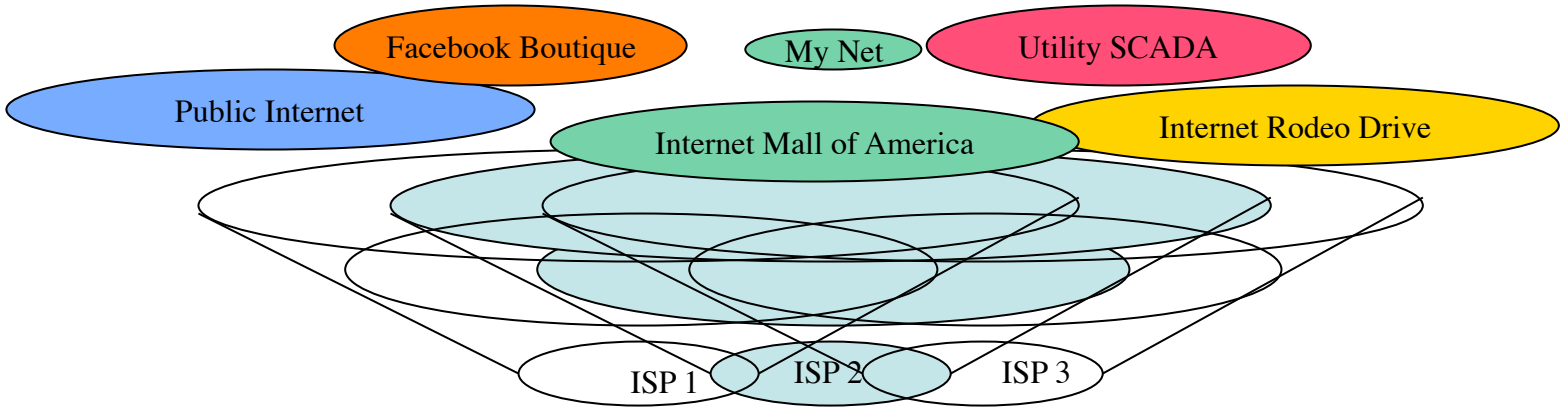
Hosts and ISPs do not share DIFS.
(ISP may have more layers

- Security by isolation, (not obscurity)
- Hosts can not address any element of the ISP.
- No user hacker can compromise ISP assets.
  - Unless ISP is physically compromised.

How Does It Work?

Security

- A Hacker in the Public Internet cannot connect to an Application in another DIF without either joining the DIF, or creating a new DIF spanning both. Either requires authentication and access control.
  - Non-IPC applications that can access two DIFs are a potential security problem.
- Certainly promising



IRATI
INVESTIGATING RINA

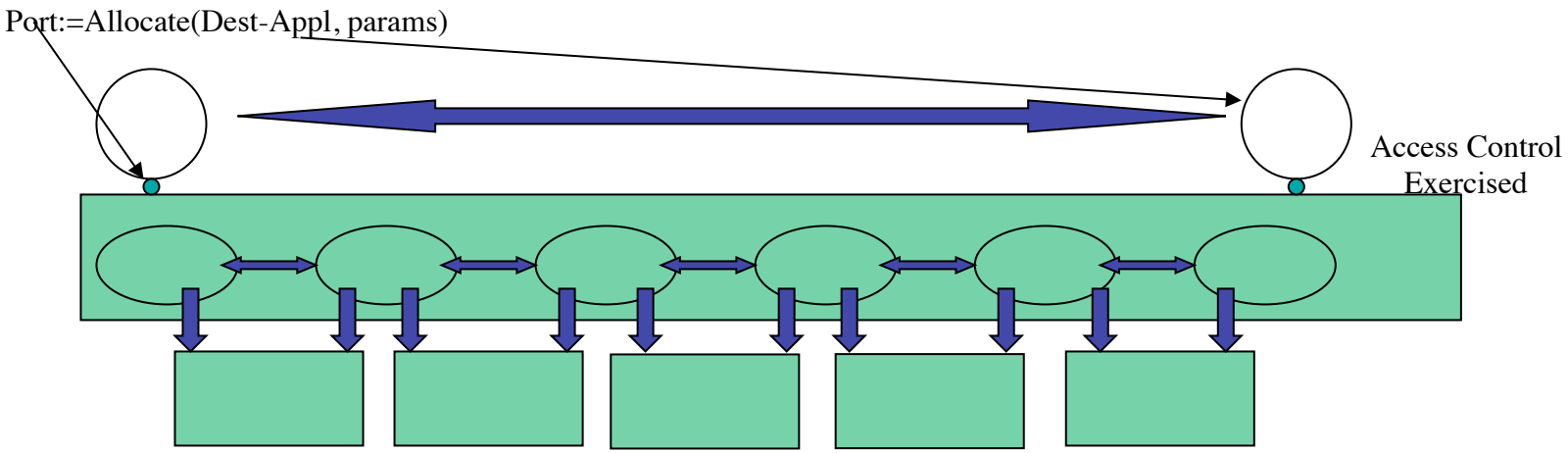
The Pouzin Society

But When It Was Time

- The question was not, how to put in security?
- The question was,
- What does the IPC Model tell us about security?
  - Remember, our first task is always *understanding*.

- Let the Problem Answer the Question!
  - Let the Problem Tell Us What to Do.

The Problem Had a Lot to Say



- We Already Mentioned How Little is Exposed the Layer Above.
- The Original OS Model indicated where Access Control went.
- Creating the Application Connection for Enrollment indicated where Authentication belonged, and that
  - Authentication of Applications must be done by the Applications themselves.
  - All members of the layer are authenticated within policy.
- SDU Protection clearly provided Confidentiality and Integrity.
- That implied that only Minimal trust was necessary:
  - Only that the lower layer will deliver something to someone.

IRATI
INVESTIGATING RINA

The Pouzin Society

A Very Unexpected Result

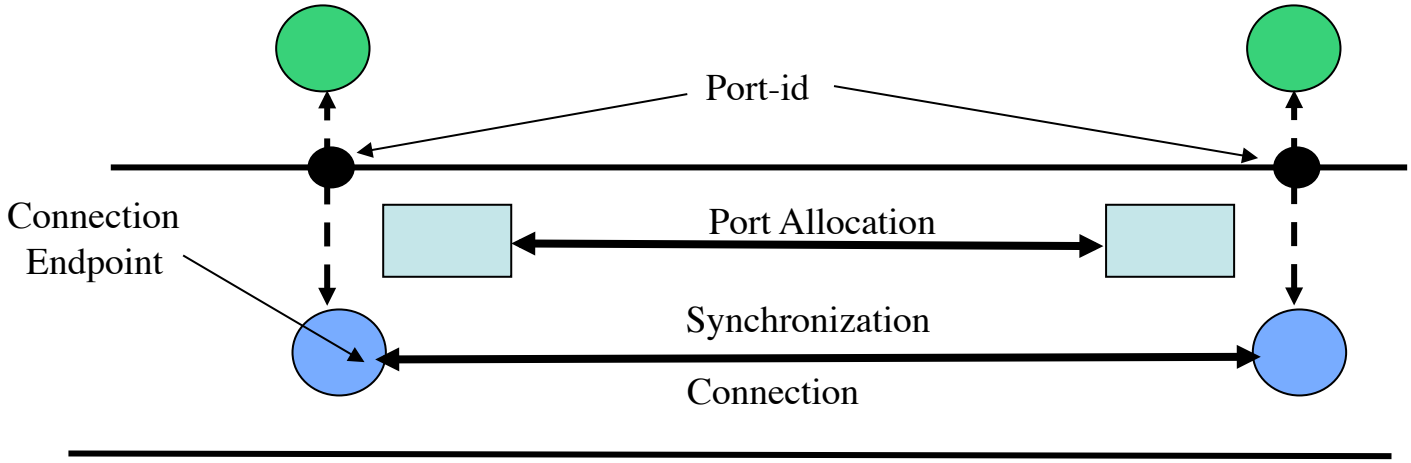
- A DIF with no explicit security mechanisms is inherently more secure than the current Internet under the same conditions!
- It would appear that
  - A DIF is a Securable Container.

IRATI
INVESTIGATING RINA

Other Things Fall Into Place

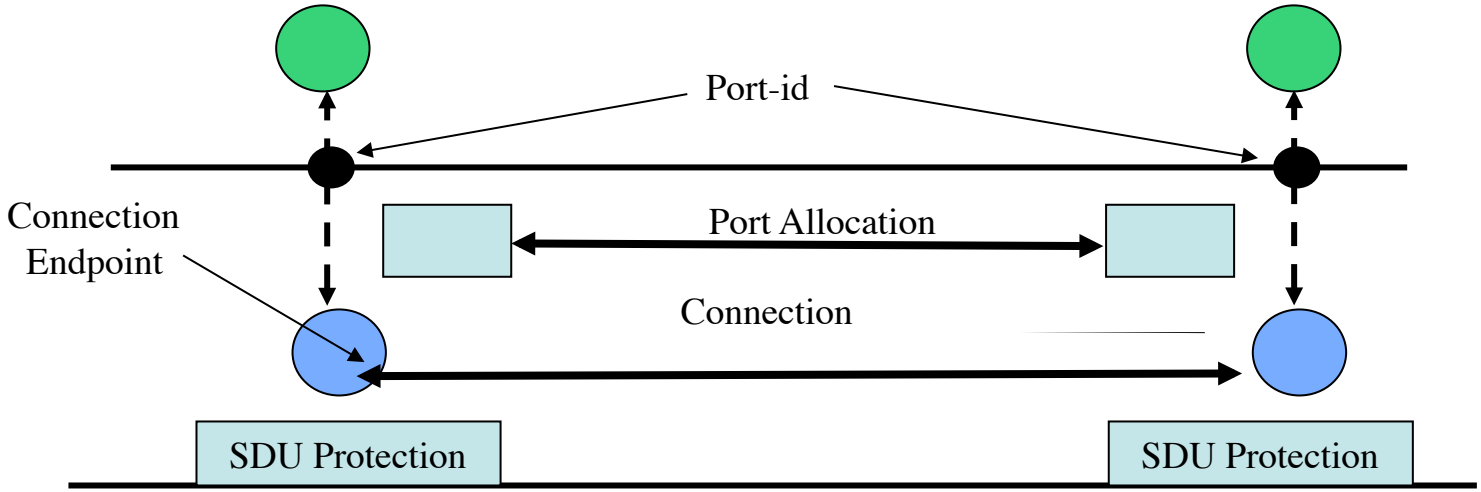
- Data Transfer in RINA is based on Delta-t (Watson, 1980)
- Lot has happened in 30 years, many attacks on TCP have been found:
  - Port scanning
  - SYN attacks
  - Reset Attacks
  - Reassembly Attacks
- Long after delta-t was designed, what about delta-t?
- Short answer:
  - None of them work (Boddapati, et al., 2012)
    - Amazing, totally unexpected
  - Why not?
- Multiple fundamental reasons, but all inherent in the structure:
  - First, have to join the DIF (all members are authenticated)
  - Second, No Well-Known Ports
    - Would have to scan all possible application names!
  - Third and more importantly, . . .

Decoupling Port Allocation and Synchronization



- No Way to Know What CEP-ids are Being Used, Since There is No Relation Between Port-id and CEP-id.
  - Syn Attack: must guess which of 2^16 CEP-id.
  - Data Transfer: must guess CEP-id and seq num within window!
  - Reassembly attack: Reassembly only done once.

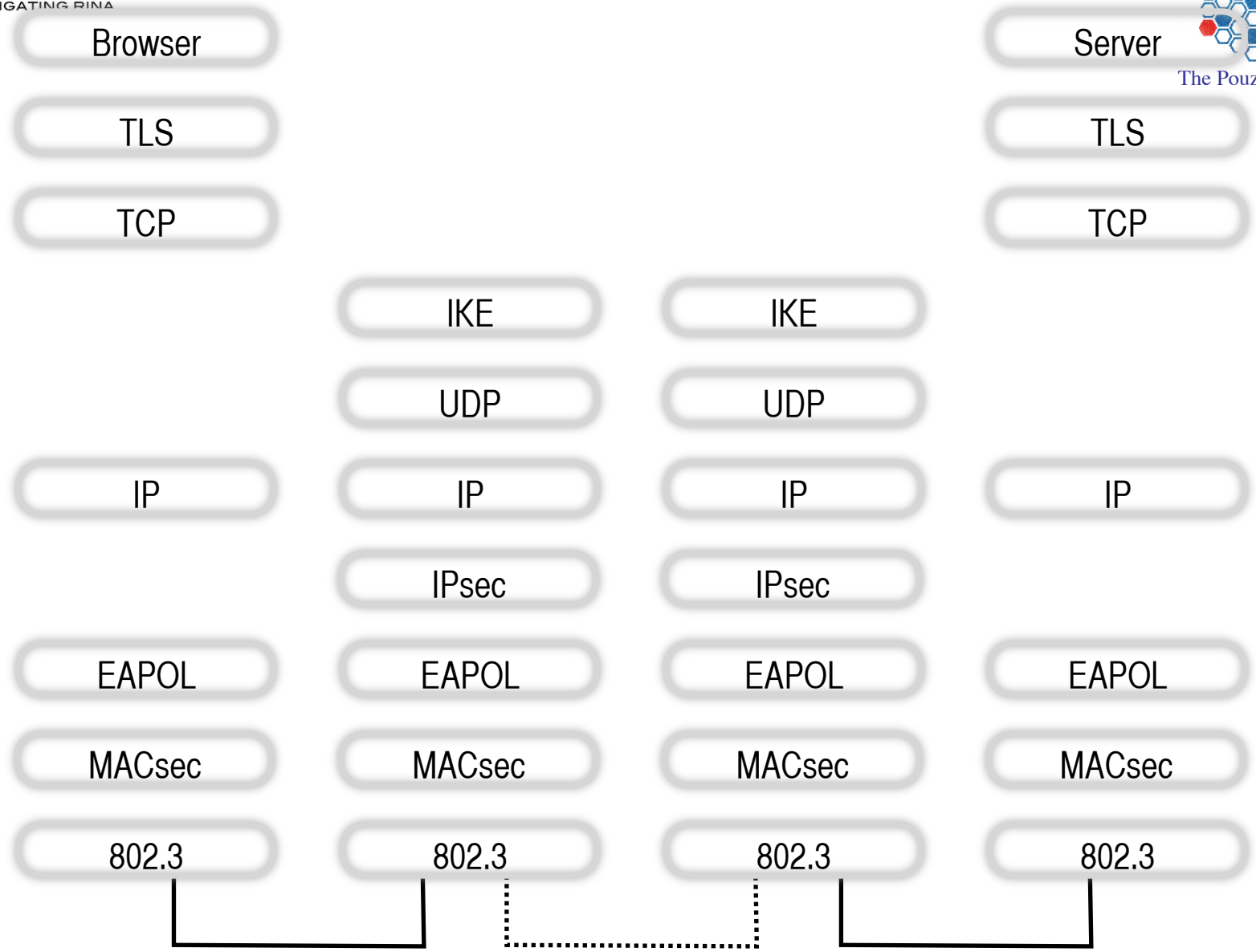
Decoupling Port Allocation and Synchronization: No IPSec



- IPsec is necessary with TCP/IP because no authentication and Sequence numbers turn over too quickly: don't repeat sequence number with same CEP-id.
- With RINA and delta-t, IPC Processes all authenticated, SDU Protection does the encryption, and packet sequence numbers slows rollover, but if it does, then simply allocate a new connection
- And bind it to the same port-ids, old one disappears after 2MPL.

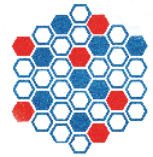
RINA is Inherently More Secure and Less Work

- A DIF is a Securable Container. (Small, 2011)
  - What info required to mount an attack, How to get the info
  - Small does a threat analysis at the architecture level
- Implies that Firewalls are Unnecessary,
  - The DIF *is* the Firewall!
- RINA Security is considerably Less Complex than the Current Internet Security (Small, 2012)
  - Only do a rough estimate counting protocols and mechanisms.
    - See paper for details.



Protocols: 15 Non-Security: 89 Security: 28

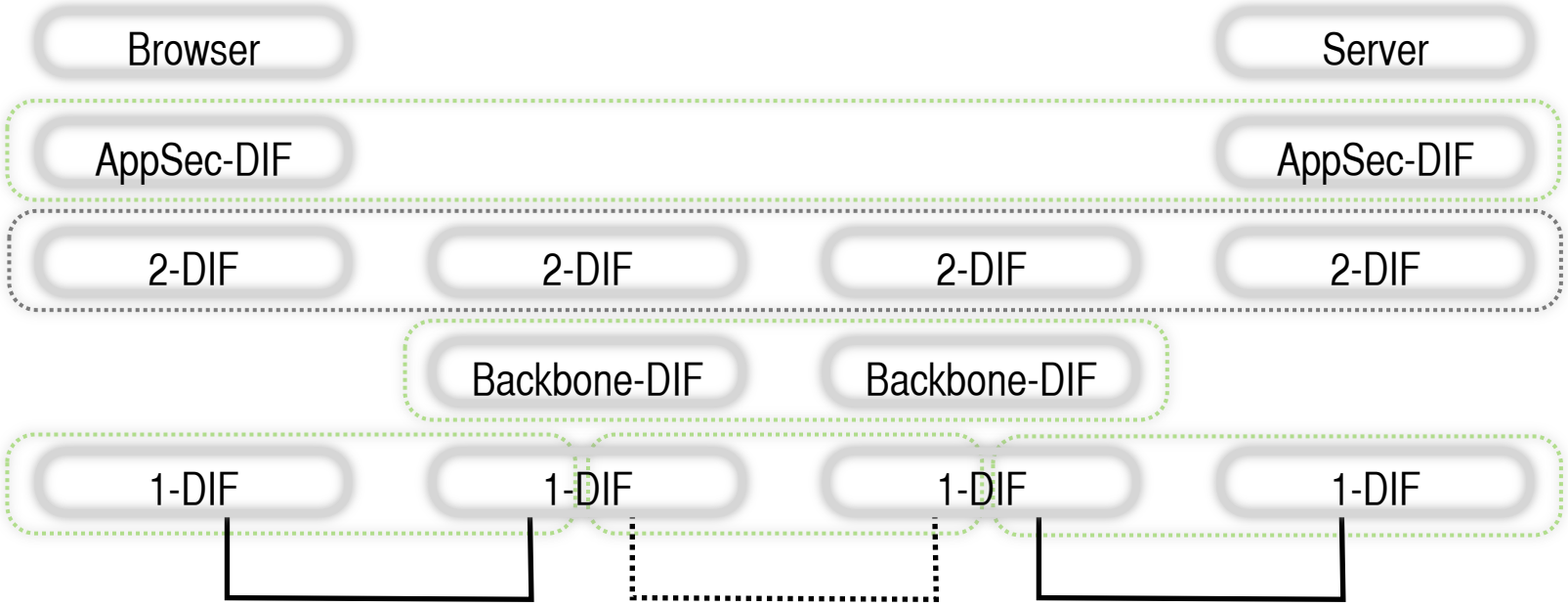
IRATI
INVESTIGATING RINA



The Pouzin Society

What Does This Mean?

- Protocols – We Know What That Refers To
- Security Mechanisms – Authentication, Access Control, Integrity, Confidentiality, Non-Repudiation.
- Non-Security Mechanisms – All the others listed in the book: delimiting, relaying, ordering, multiplexing, fragmentation/reassembly, Lost and Duplicate Detection, Flow Control, Retransmission Control, Compession, Addressing, Initial State Synchronization.



Protocols: 3 Non-Security: 15 Security: 5

IRATI
INVESTIGATING RINA

The Pouzin Society

Totals	Internet	RINA
Protocols	15	3
Non-Security Mechanisms	89	15
Security Mechanisms	28	7

IRATI
INVESTIGATING RINA

The Pouzin Society

To Add Security	Internet	RINA
Protocols	8	0
Non-Security Mechanisms	59	0
Security Mechanisms	28	7

IRATI
INVESTIGATING RINA

The Pouzin Society

Why Is Internet Security So Bad?

- The Standard Rationale One Sees is that They Didn't Think About It at the Beginning.
  - Neither did We.
  - Nor did Watson.
  - But RINA and delta-t are more secure.

- That Seems to Imply that
  - Good Design May be More Important to Security than Security Is.

IRATI
INVESTIGATING RINA

Conclusion

The Pouzin Society

- This is a MAJOR Improvement in Internet Security.
  - Not only more secure, but for less cost, with less overhead.
- So is Internet Security solved?
  - Hardly.
  - Still need: to develop the plug-in policy modules
  - to consider DDoS (we have some ideas)
  - As well as protecting against Rogue IPC Processes
  - and much more to explore.
- Most attacks are in the Applications, this does nothing about that.
  - But Much of this applies equally well to DAFs
    - Model implies that OS security reduces to Bounds Checking on Memory and IPC Security.
  - May also make it harder, might be able to deflect more DDoS attacks

The Pouzin Society

Questions?