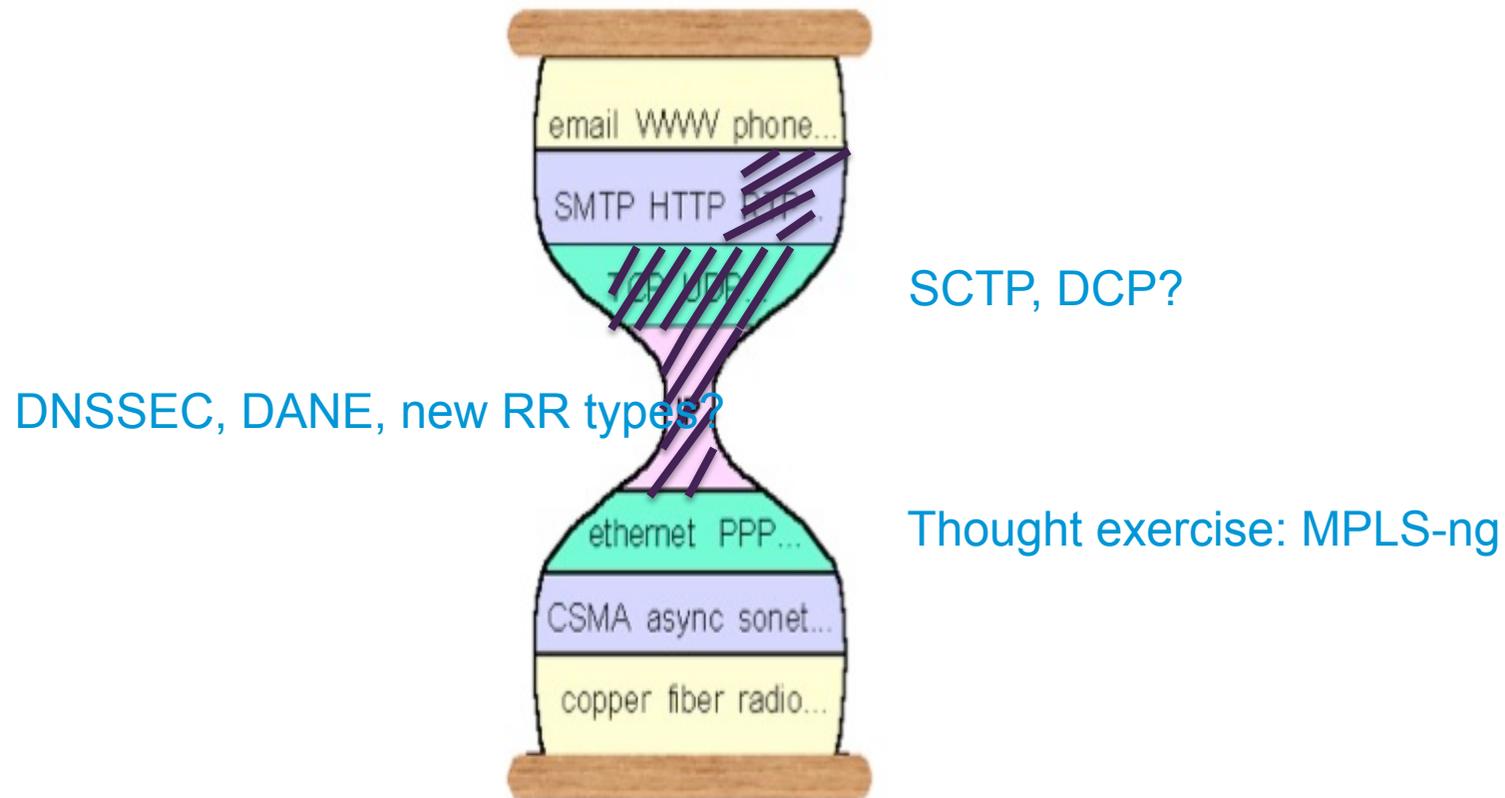


# IAB Internet Technology Adoption and Transition (ITAT) Workshop

Eliot Lear

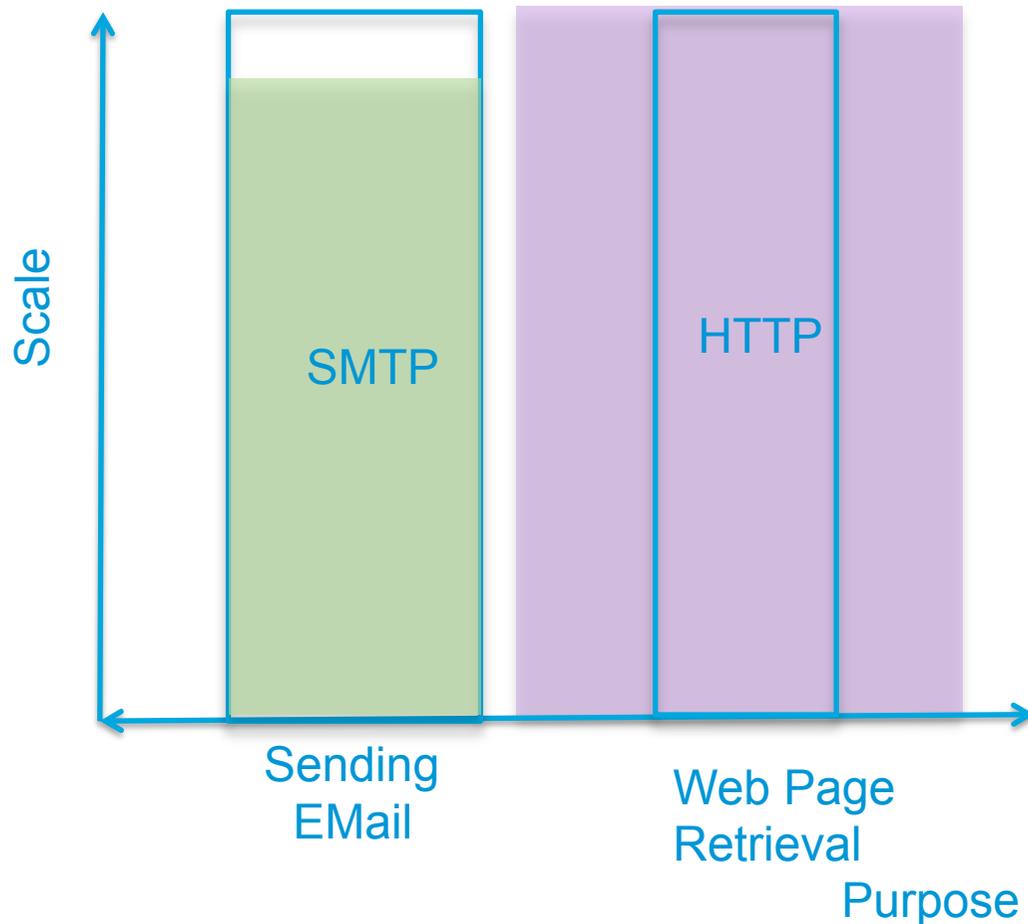
# Is the “neck” closed for business?



# Motivations for ITAT

- What will it take to get DNSSEC deployed? Anything we can do?
- What can make new transport protocols more palatable? Can WebRTC really be a game changer for SCTP?
- Can the next generation HTTP succeed with only TLS as an option?
- Will we ever see everyone implementing ROAs and do we need to to declare success?
- What is the impact of a “mandatory to implement” feature on the market place?
- Papers available at <http://www.iab.org/activities/workshops/itat/>
- Draft report available: draft-lear-iab-itat-report-00.txt

# Where did we start? RFC 5218 & Success Factors



- Initial Success Factors
  - Positive Net Value
  - Incremental Deployability
  - Open Code Availability
  - Freedom from Usage Restrictions
  - Open Specifications Availability
  - Good Technical Design
- Wild Success Factors
  - Extensible
  - No Hard Scalability Bound
  - Threats **Sufficiently** Mitigated

# Andrei Robachevsky on Averting the Tragedy of the Commons

- Problem:

The global inter-domain routing system is a commons, and many of the costs and benefits are external

Analogy: polluters often don't pay their full production/destruction cost

Analogy: Fisherman overfish without some form of regulation, which many of them support

- Solutions:

Turn the commons into private property that can be in some way accounted and charged for;

Tax and regulate; **or**

Find a “bottom up” cooperative model

# Prerequisites for “bottom up” approach

1. Common understanding of the problem
2. Common understanding of the solutions
3. Understanding of common and individual benefits
4. An ability to assess risks



Build critical mass through strengthening of collaboration and communication

# Weber, et al: Bundling: When Are Two Services Better Than One?

- Given two independent services, examine independent utility, costs, and externalities
- Combine them together, and examine the circumstances where such a combination would increase (or decrease) adoption for both
- Can lead us to answer questions about Mandatory to Implement (MtI)

Examples:

WebRTC & SCTP or WebRTC and an MTI CODEC

DNSSEC & DANE

DNSSEC & Application discovery?

- What happens when there are dependencies between technologies?
- Possible research group activity here

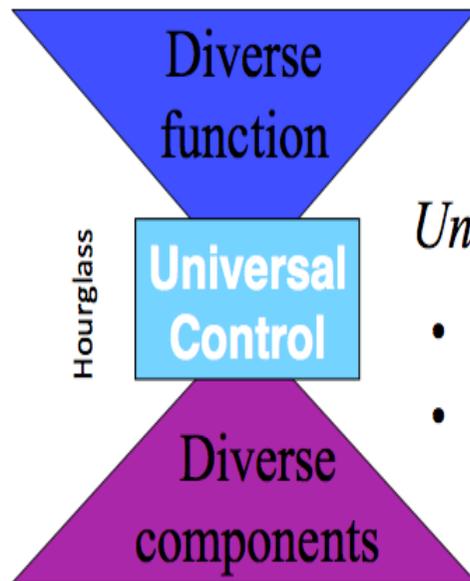
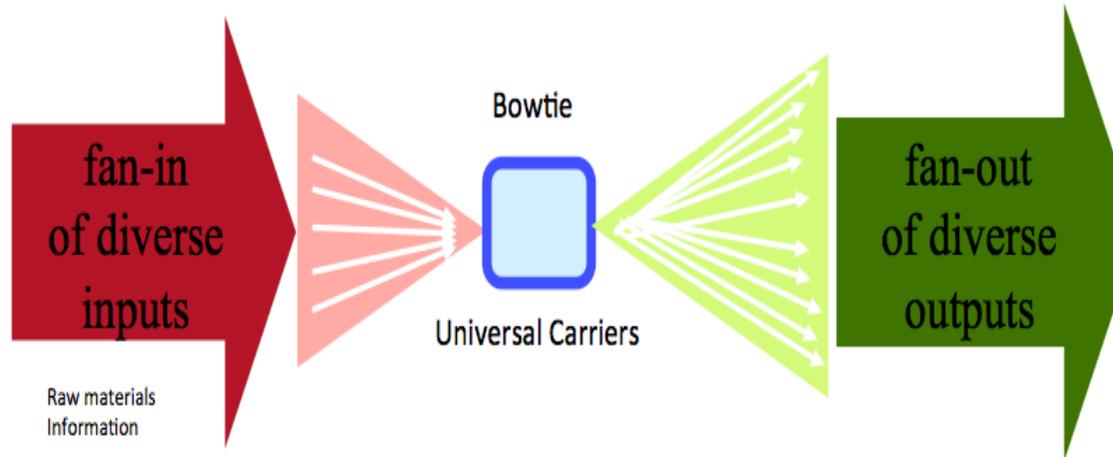
# Getting .SE signed by Anne-Marie Eklund and Patrik Wallström, .SE

- Innovative Approach: provide people incentives to sign their domains
- Learned the hard way (by charging people first for DNSSEC)
- Issues for signing domains
  - A pain to sign once, maintaining signatures is even harder
  - not enough software available to do the job
- .SE team engaged not only signing domains but their registrars, educating and prodding to get registrar functionality enabled
- Funded tooling to ease deployment (e.g., opendnssec)
- Provided a price reduction for those domains that continue to validate
  - Mechanism may not be easily applied to lower margin and larger TLDs like .COM or .NET
- **Results: 300 000 / 1 300 000 domains are signed**

# Rainer Böhme: Bitcoin success factors

- Built-in reward system for early adopters
  - Both a unique benefit and a network effect
- Adaptors in the ecosystem (exchange rates)
  - In other words- ways to gateway
- Interpretation as money
  - If not money, then data
- Key lesson:
  - Individual participants need to capture value to others (in this case through cash)
- Applicability:
  - SMTP/Anti-spam? Communication that is not pre-arranged

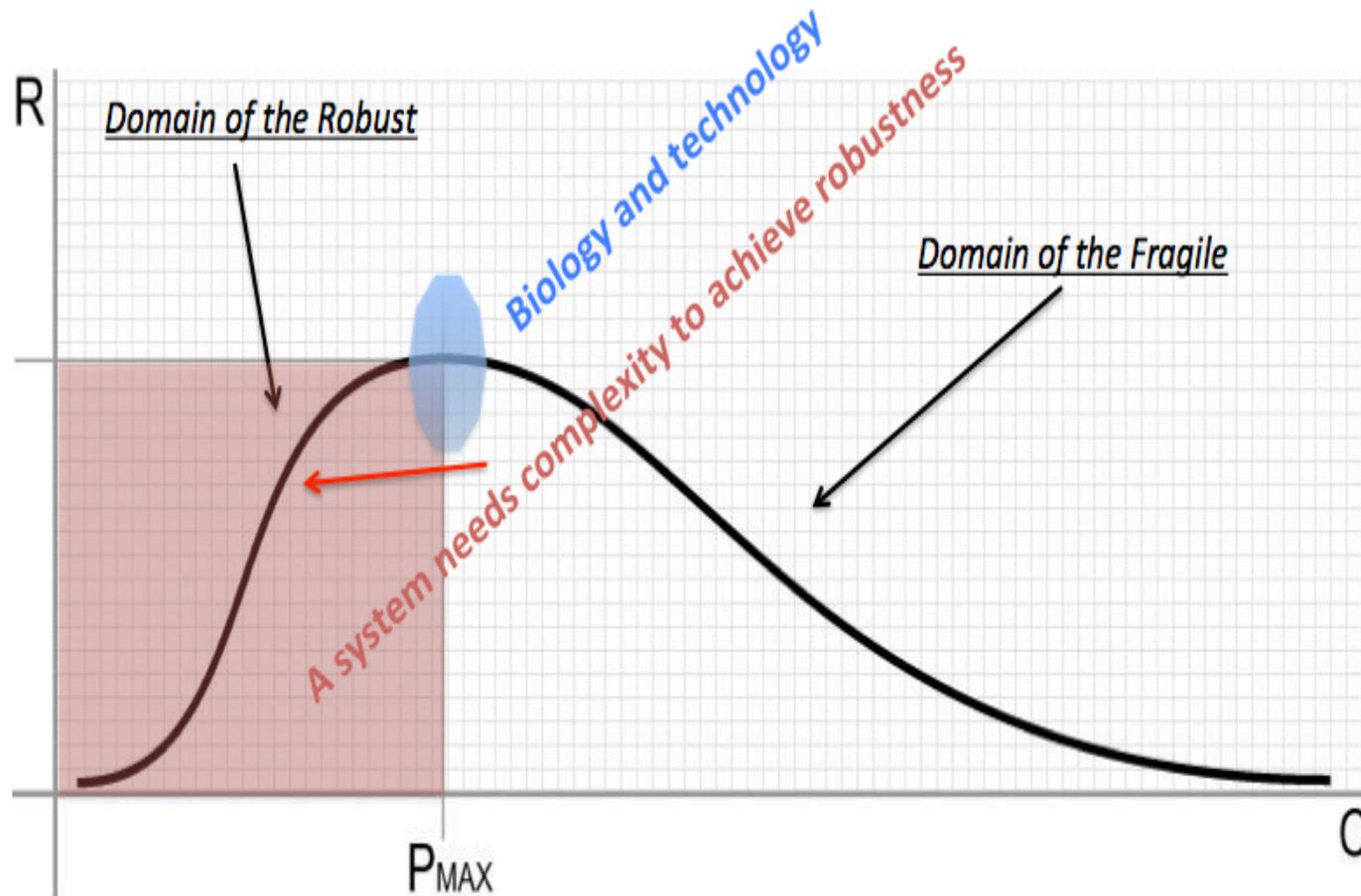
# Leaving the realm of economics, Dave Meyer, John Doyle & Systems Biology



## *Universal Architectural Principles*

- *Hourglasses* for layering of control
- *Bowties* for flows within layers

# Leaving the realm of economics, Dave Meyer, John Doyle & Systems Biology



Increasing number of policies, protocols, configurations and interactions (well, and code)  
→

# Hannes Tschofenig: Getting to TLS 1.3 - a roundtable discussion

- According to at least one survey, TLS 1.0 is still widely prevalent
- What is needed to encourage adoption of an improved TLS 1.3?
- Some ideas
  - Don't call it "TLS 1.3" but use a major number
  - There must be sufficient additional benefit to displace existing capabilities in 2.0
  - Many protocols and crypto linger. 3DES is still used
  - An easily accessible test harness could move the ball, since TLS is pretty complicated

# Potential Next Steps

- Possible formation of GAIA working group on issues facing environments with limited capabilities
  - Alternative stack models
- Facilitating of bundling research (Weber, et. al) through possible new RG. Need WG chairs and authors to engage
- The IAB & IESG should keep in mind the parameters of RFC 5218 when considering BOFs
- Possible discussion about how we can facilitate interoperability (test harnesses, others)
- Track success, wild success, failure, and what we think happened in each case