A polytheistic approach to securing interdomain routing

Ratul Mahajan
Microsoft Research

Much work on interdomain routing security but little deployment

Myriads of security protocols

- S-BGP
- soBGP
- SPV
- Listen and Whisper
- IRV
- psBGP
- Pretty Good BGP
- …

How can we explain that?

Is the problem not important?

Are all those approaches broken?

Maybe, its futile to look for “the one” perfect solution

- One size does not fit all
- Coordination
- Incentives

A polytheistic approach

Instead of designing one solution for everyone, design a broad range

- ISPs pick zero or more, as per their needs

How is this chaos secure?

Lessons from the road network

- Different cars, drivers, skill-levels
- But the network is reasonably secure
- Two key underlying factors
  - visibility and financial disincentives

Hypothesis: routing can be secured by engineering these factors

Simple changes are enough

Engineering visibility

- Pinpoint who is sourcing and propagating bad routing updates

Engineering financial disincentives

- Build on bilateral contracts
  - Penalties for sending bad updates to neighbors
- No need for regulation

The end result

Appropriate aligning of incentives

- Each ISP does what it takes to run a secure network

Security properties similar to the road network

- accident prevention is not guaranteed