Why I’m Excited About DELEG

Ben Schwartz, DELEG @ IETF 119
Meta Platforms, Inc.

RFC 9539* Is Not Enough

- Opportunistic security == Incentive to deploy downgrade attacks
  - …and downgrade attacks on DoT/DoQ are trivial.
- Downgrade resistance for a few weird resolvers is not sufficient.
  - The downgrade attacks will just become an outage for those few resolvers.
- Widely deployed downgrade resistance will only happen if normal resolution isn't slowed down.
  - This means resolvers need to know whether to encrypt *during delegation*.
- **Dream scenario for DELEG:**
  - Widely deployed resolver implementations do downgrade-resistant DoT out of the box.
  - Some major TLDs add support for downgrade-resistant DoT.
  - Most connections to www.example.org are guaranteed never to put "example" on the wire.

*Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS

Dream Scenario Sketch