Thinking about handling PM in OPS

stephen.farrell@cs.tcd.ie

Background

- draft-farrell-perpass-attack will be a BCP that sets out the principle that pervasive monitoring (PM) is an attack we need to consider
- There's text in there about managing networks
- The idea here is to continue the discussion of that

My Questions

- How can we make security protocols (TLS, Ipsec) more attractive so that they're used more broadly e.g. beneath RADIUS/Diameter?
  - E.g. on-by-default and what'd you need to change for that?
- Are there ways in which you could minimise the data you want to collect and still get the job done?
  - E.g. sampling instead of recording everything
- Encryption will be used more and more. How can you keep doing your work in a world like that?
  - No need to assume more-than-MTI btw, it'll just happen