

Community oriented measurement infrastructure: how do we get there?

Gianluca Iannaccone
Intel Research @ Cambridge

MOME Panel (at TNC 2005)
Poznan, June 7, 2005



First, know the trade-off!

- value vs. anxieties
- network operators
 - every day activities driven by “process”.
 - anxiety for anything “disruptive” (outside the process)
 - however, they are in need of value-added services.
- network equipment manufacturers
 - want demonstrated value in the infrastructure.
 - but, cannot “miss the train”!
- network users
 - privacy is a concern but not always.
 - corporate networks have a lot of freedom in this area.

Finding Value

- support for **arbitrary traffic queries**
 - perform any computation on traffic streams
 - coordinate responses from multiple monitors
 - applications to security, TE, planning, accounting, ...
- work in **multiple, diverse environments**
 - high speed links, wireless links, NetFlow feeds, etc.
 - require no changes to queries
- infrastructure for **fast prototyping**
 - minimal effort for new users to access the infrastructure and prototype new methods

Finding Valium

- anonymization is the wrong solution
 - never enough for data owners
 - always too much for data users
- **data ownership** is what really matters!
- **move queries to the data**
 - operator sees the query coming and allows it
 - no packet ever leaves the monitoring system
 - source code for queries is available to data owner.
- challenge: how to automate all this!

Next Steps (my sales pitch!)

- The CoMo project @ Intel Research
 - open platform for network monitoring
 - early stages of development (v0.3 release)
 - open source software, BSD license
 - *como.sourceforge.net* for more details