traffic observation in a stateless data networking environment

CRISP/CISAC's IC3T
7 dec 99

kc, UCSD/SDSC/CAIDA
kc@caida.org
www.caida.org

outline

- define stateless

- what to protect, how to parameterize
- what is the threat model

- what can we realistically measure
- what technical facilities do we have

- need to protect user privacy
- need for community buyin on an international scale
- need for secrecy

stateless

- cannot assume any end–to–end state
  (unlike telephony systems)

- little (no) facility for realistic tracking
- high probability (assured) attribution distortion

- IP
  - self–contained
  - "fire and forget"
  - no acknowledgments required -- source forgeable

.... all By Design

what to protect?

how to parameterize the problem

- end systems
- routing infrastructure
- non–networking/non–hosts objectives
  (funky political stuff i don't get)

what is the threat model?

who are we protecting against

- bored (albeit brighter/quicker than we) kids and high school hackers
- criminals with Teleological Objectives
- good guys, probably overworked
  (have you tried to configure a router lately?)

relative threat of malice vs incompetence
(damage * intention) product way higher for latter

--> **system just plain fragile**

what can we realistically measure?

1) active tagging

2) passive observation

both require

- vendor & community buyin (+laws)
- phenomenally complex
  data collection infrastructure

what technical facilities have we?

- routing/switching equipment
  - can be modified if needed (at cost)
- performance measurement infrastructures
  - active monitoring
  - many specialized ones
  - much weak, inconsistent methodology
- workload characterization infrastructures
  - NLANR (NSF-sponsored HPC sites)
  - passive monitoring

... none exist enuf for global traffic tracking

CoralReef

most appropriate available platform

- high flexibility wrt dynamic requirements
- public
- US tax dollars help fund

hard part remains

- define (realistic) requirements
- deploy infrastructure
- synchronize collections
  (through multiple measurement points)

need to protect user privacy

- IP header fields (esp. IP addresses)
- IP data content

- intertwined w encryption
- tremendous opportunities for abuse, if/as implemented
- govts must defend need for capability to screw over every citizen, provide assurance that "terrorism capes" won't be used against them

...or they'll just 'route around the damage'

need for secrecy?

communicating attack profiles

- attack by outlaws on others
- attack by law enforcement on non–outlaw citizens

should terrorism counter–measure architecture/implementation be public?

- secrecy complicates agenda

need for ISP community support

- o/w just non-starter at best
- insulting at worst
- ISPs work way harder than we do
- most are (after capitalist) libertarian
- many disagree with us
- or just think you're reality-detached
- seriously, talk to some of them

"...insanity in the face of a bunch of war nuts and cops trying to build a regime that can regulate what it's taken us 30 yrs to deregulate (end-to-end free expression independent of media or borders)"

".... governments have killed far more people than 'terrorists' or citizens ... public acceptance of the Internet may perhaps mean that we who built it have somewhat of a clue as to how the world should be governed (or not governed, as the case may be)"

"danger of govt by the clueless, over a place they've never been, using means they don't possess"

www.caida.org/Presentations/

k claffy
UCSD/SDSC/CAIDA
kc@caida.org
www.caida.org