Two Open and Shut Case Studies

Jon Crowcroft

The Computer Laboratory
University of Cambridge
http://www.cl.cam.ac.uk/~jac22

The
Cambridge-MIT
Institute

1. Open Systems Interconnection 21st century style

- I have 1Mbps DSL and a 802.11a WiFi router (45$)
- My neighbours (within 500 yards) have:
  - 20Mbps DSL and WiFi
  - 2Mbps DSL + WiFI
  - Approx 1Mbps Cable Modem and WiFi
  - We all have open WiFi (no WEP key etc)
  - We all know about security (use SSH or other VPN)
  - We prioritise each others traffic in the router (easy as most routers are linux/open source - see ipchains etc)
    - (so we get best performance for ourself first, then neghbours, then others)
- We are a *virtual* wireless ISP -
  - to talk to each other involves **no** ISP at all

2. . Open Source Security

- Open Source is available for scrutiny
  - When bad things happen, many people can fix
  - On the other hand, many people can make bad things happen
- Closed Source Software is opaque
  - Bad things have to be fixed by proprieter
  - Maybe harder to find exploit/vulnerability
- Nice example of arms race
  - If occurrence of exploit/fix events independent,
  - Then nicely balanced
  - But they are not independent!
- So open source maybe safer, but also instills trust
  - (like child rearing, punishment and reward are equally effective, but which would you rather ? :-)

Questions?

- What about new models of ISPs then
  - new Internet perhaps should include providerless networks
    - a component model without “levels”
    - Abandon *Vertical* versus *Horizontal* bundling models
    - More flexible (google seem to have half the idea!)
- New security models of security might be thermodynamic
  - See paper by Ross Anderson et al, in Computer lab.

- Any other examples?