Internet Engineering Task Force

Standards & ideas for the Internet

Scott Bradner
Harvard University

The IETF

- Internet Engineering Task Force
- formed 1986 - less than 50 people
- original purposes
    - coordinate operations of ARPANET
    - discussion group for new applications
- now mainly a standards development group
    - “standards” in the sense that lots of people use them
    - no IETF protocol police
    - no submitting to other standards bodies
        - but some joint work

Scale

- 2400 attendees in Washington DC
- 1400 attendees in Adelaide, Australia
- unknown number on mailing lists
- individuals not companies
- but from 100s of companies
  - biggest industry sector in the last few meetings: telephony
  - i.e. convergence is a big issue
- no defined membership thus no voting
  - consensus determination by show of hands, discussion on mailing list (or humm)

IETF Relevance

- not the only Internet-related standards organization
  - ITU, ETSI, W3C, ISO etc
- but main body dealing with basic Internet protocols
  - all significant Internet infrastructure protocols
  - Internet protocols - IPv4 & IPv6
  - Transport protocols - TCP, UDP, HTTP 1.1, SCTP
  - Routing protocols - OSPF, BGP, MPLS, updates to IS-IS
  - Management protocols - SNMP, SNMPv3
  - Security protocols - IPSec, TLS
  - Quality of Service protocols - RSVP, diffserv
  - Applications protocols -SMTP, MIME, LDAP, iCalendar

Security

- IETF has required security focus for IETF protocols for years
- all protocol documents must discuss security of protocol
  - including privacy risks
- weak security is no longer acceptable
- security must be built in from the start
  - e.g. IPv6 & IPSec
  - SCTP & DoS attacks

IETF Policy Discussions

- IETF not all that good at policy issues
- techies tend to be libertarian
- a complication is that the IETF is international
- some examples of IETF policy discussions
  - IPv6
  - RFC 1984
  - raven

IPv6

- from the IPng recommendation

  "We feel that an improvement in the basic level of security in the Internet is vital to its continues success. Users must be able to assume that their exchanges are safe from tampering, diversion and exposure. Organizations that wish to use the Internet to conduct business must be able to have a high level of confidence in the identity of their correspondents and communications. **The goal is to provide strong protection as a matter of course throughout the Internet.**"

IPv6 Mandatory to Implement

- IPv6 recommendation was to mandate security
- to be able to state standards adherence
  - must implement authentication & algorithm
  - must implement privacy (encryption) & algorithm
- significant pushback because of U.S. export laws
  - since changed
- major (heated) plenary discussion
- rough consensus was to mandate encryption support (but not use)
  - but some strong opposition

RFC 1984

- IAB & IESG statement on encryption
- worried about the security of the Internet
- some points
  - support structure of Internet must be able to be protected
    - encryption is key to this
  - encryption technology is not secret
  - export & use controls counterproductive to security
  - key escrow weakens security
  - identification keys should never be escrowed
    - can impersonate user - could void prosecution

Raven

- an IETF telephony working group brought up wiretapping issue
- IESG created new mailing list to discuss issue
  - "raven"
  - two month period
  - over 500 subscribers, 10% sent at least one message
- also discussion in IETF plenary
- conclusions to be published as RFC 2804

Raven, Conclusions

- show of hands in DC plenary
  - consensus to not mandate wiretapping features
  - no consensus to block discussion
  - no consensus to design un-tappable protocols
- thus
  - IETF will not develop standards track protocols with wiretapping features
  - but will not block publication of informational documents that describe such technologies
- a number of reasons

Raven, Reasons

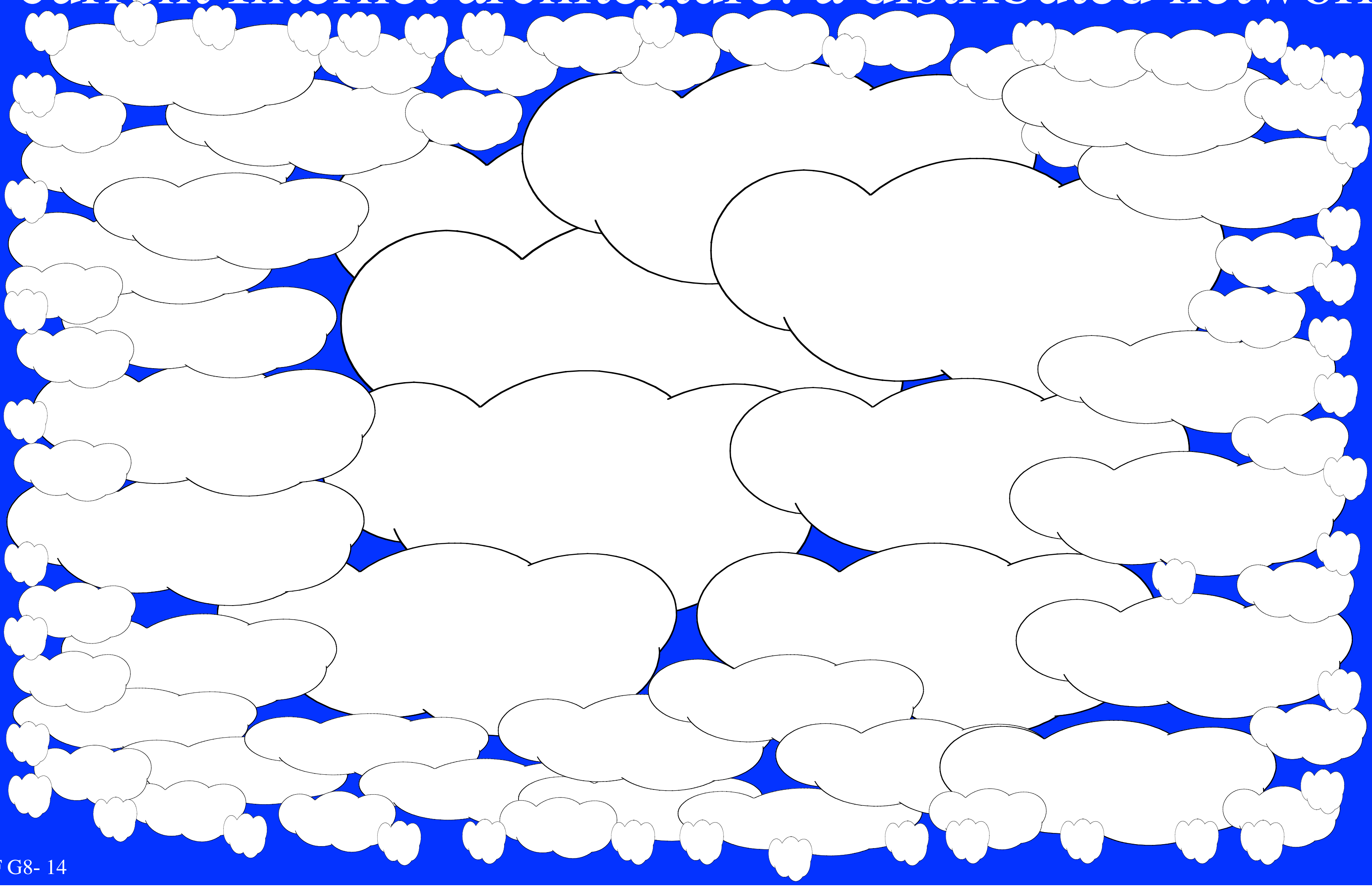
- IETF is an international body making international standards
  - conflicting intercept requirements in different jurisdictions
  - conflicting privacy requirements
- adding wiretap features will weaken security of protocols
- current IP tools can deal with general problem
  - which is monitoring data traffic
  - but hard to identify individuals rather than hosts
- note: not a position based on moral judgement

Internet Architecture

- end-to-end model
  - important Internet fundamental
  - most Internet development is between end hosts
    - no per application support in network
  - no support or permissions are required from ISPs
    - world wide web an example
  - e.g. Internet telephony can be end-to-end with little
    - or no support in network other than packet transport
  - Internet "stupid network" vs. telephone "smart network"
  - applications in network for telephone net
  - applications in hosts for Internet

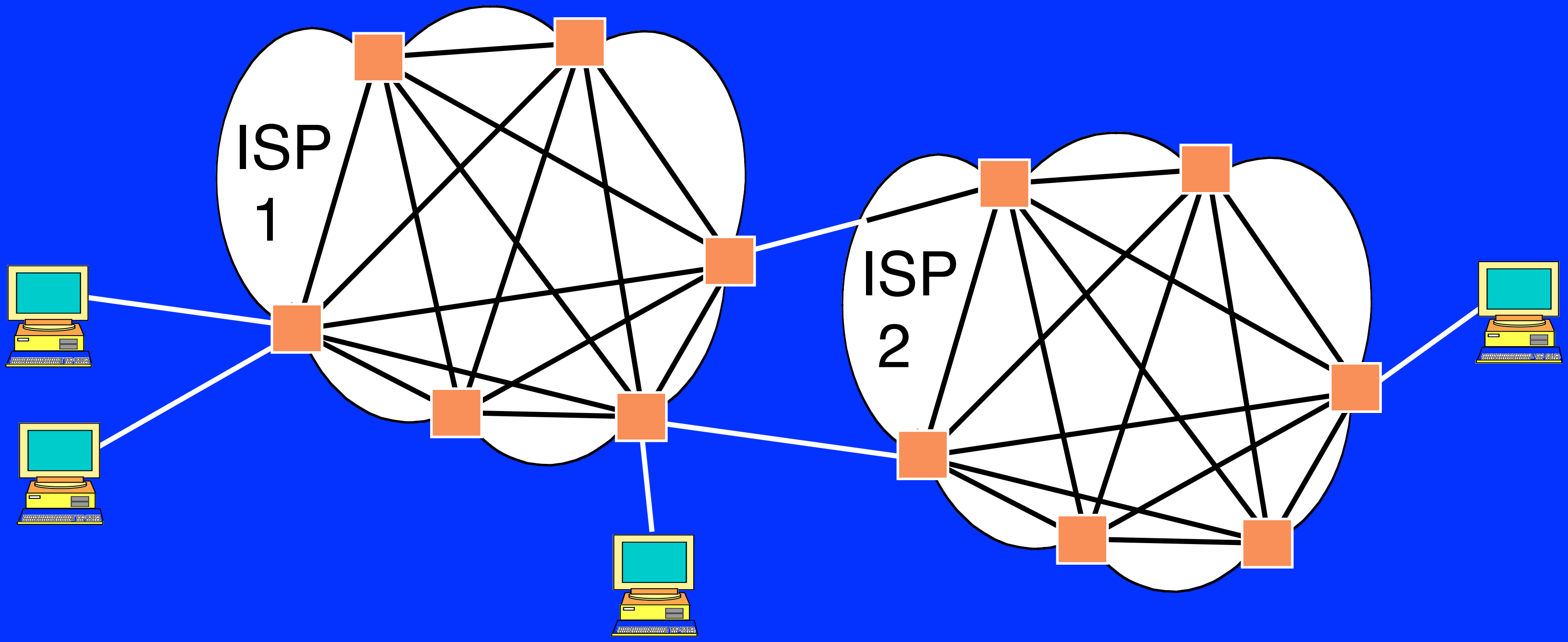
Internet Architecture, contd.

- current Internet architecture: a distributed network



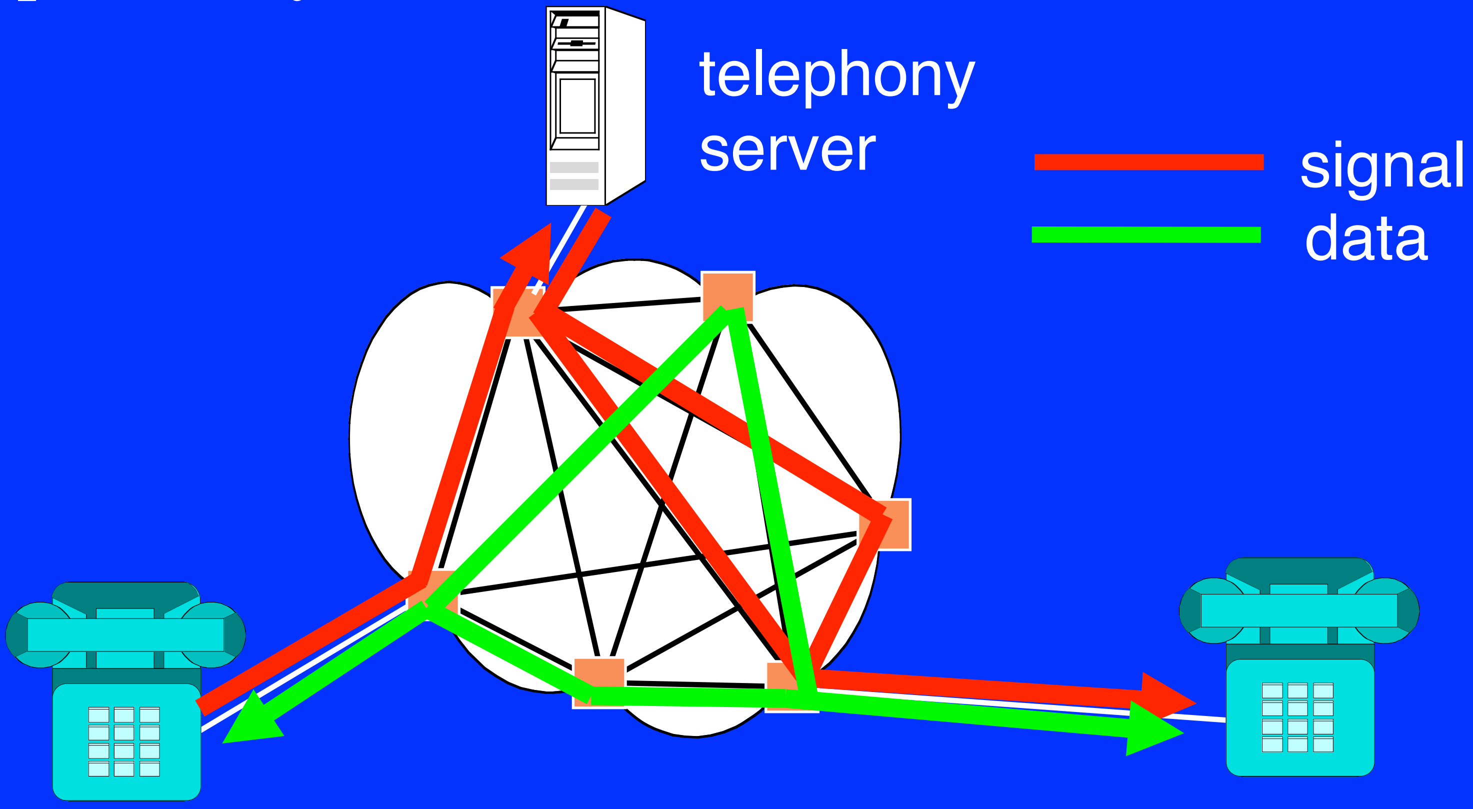
Internet Architecture, contd.

- no Internet backbone that data flows through
- local interconnections between ISPs
- local routing of data within ISPs



Internet Architecture, contd.

- signaling and data paths in Internet do not coincide and paths vary



Internet Architecture, contd.

- service provided by 3rd parties - not only by ISPs
- different from phone world
- a quote from Sun, 16 Apr 2000 11:10:57 +0200

> Hi Roy,
>
> I still don’t understand why it is a "users" choice where the "services" are executed - I would have thought that this would be networks choice - and the means for doing that is what we are now discussing. Can you please clarify why a user "MAY" which to decieded this.

Some Example Issues

- some other issues and IETF responses
  - DoS
  - Kerberos
  - IP address as identity

Denial of Service

- denial of service (DoS) attacks are a major issue
  - SYN attack, smerf attack, etc
  - in addition to crashing computers etc
- advantage if perpetrator can spoof source address
  - harder to track down
- RFC 2267 upgraded from informational to BCP
  - urges that ISPs filter traffic from customers
  - only accept packets with that customer's addresses
- RFC 2644 published as BCP
  - change default broadcast behavior - limit smerf attack

Kerberos

- Kerberos is an MIT-developed security system
  - keeps passwords off of networks
- further development in IETF: RFC 1510
- fields in authentication data for extension
- Microsoft used fields to store MS-specific info
  - legit to do so based on standard
- refused to document for quite a while
  - said would compromise security - reverse of fact
- now document but with restrictions on use of info
- IETF has learned - no more such flexibility

IP Address as Identity

- IP address can not be used as an identity token
  - identifies computer not user
  - also dynamic assignment (dial-up & LAN-based)
- network address translator
  - translate private internal to public external addresses
  - can translate multiple machines to same IP address
- privacy issue with IPv6 addresses
  - fixed MAC address in lower part
  - now random number supported
- application-level authentication more definite
  - but might be encrypted

Some Opinions

- anonymity
  - uses: political (note US Supreme Court ruling)
    - AIDS hot line, anonymous tips etc
  - easy to do in many areas
- circumvention technologies
  - desire to prevent finding out if protections work
  - e.g. - banning work on circumvention technologies
  - protection is a balance of power
  - blocking legitimate testing surrenders the field to the attackers and they will win

Some More Opinions

- security in applications
  - seems to be very hard to get vendors to pay attention to security
  - little excuse for MS Exchange still having the same flaw that was exploited on 1987 with IBM xmas virus and Melissa or MS Word having the macro virus weaknesses it has
- protecting IPR is a major issue but little noted here
  - napster / gnutella

Part of the Landscape

- script kiddies:

  Internet Attacking for Dummies

  no longer have to be an expert to attack sites

  experts create scripts then distribute them

- backbone speeds

  multi Gbps link speeds

  vast amount of data

  hard to sort through

Some Positive Notes

- security is no longer an add-on for new protocols
  - from IETF but less so from other standards groups
- SSL, TLS quite good
  - secure browsers very secure (assuming good keys)
  - e-commerce with secure browsers safe transport
    - but servers can be the weak point
- IPSec effective
- intrusion detection technology getting better
- governments can help by requiring good security in products they buy

Role of International Standards Groups

- ensure that Internet technologies are:
  - secure - can conflict with monitoring
  - simple to configure - to reduce chance of misconfiguration
  - timely - deal with issue while it is still the issue
  - open - to ensure there are no back doors
- but they can not resolve conflicting jurisdiction-specific requirements

In Chaos is Innovation

- remember planning?

  telco planning cycle ~10 years

- Internet planning? (what is that?)
- but telco planning did not yield innovation

  *69 is the highlight

- looks like chaos - everyone trying everything

  but that leads to understanding

  will also mean many (most) efforts fail

  “*the power of the Internet is chaos*”