TDR authentication requirements

Dr. Ian Brown

University College London

Key Requirements for full TDR service

- Verify TDR authorisation at originating, terminating and intermediate network nodes
- Minimise impact of Denial of Service attacks

Three stage authorisation

1. Verify user’s TDR credentials
2. Verify signalling is from authorised user
3. Verify data flows are part of an authorised session

Credential verification mechanisms

- GETS: PIN entered by user
- GSM/TIPHON: challenge-response registration protocol between user device, local and home networks. User enters PIN to device
- SIP: HTTPS with client authentication used to fetch token?

Verifying user credentials

- Ideally done by local domain
  - e.g. GSM, TIPHON retrieve user profile
  - allows local transport priority – edge networks important, as most likely to suffer congestion
- Otherwise done remotely
  - e.g. GETS, SIP proxy

Verifying signalling

- In trusted federation of domains, may rely on ingress policing
- But this has problems with transitive trust, DoS and complex network topologies which are difficult to map to international TDR agreements
- Possibility of independent verification better

Authorisation token

- IP client obtains token from server like tdr.ncs.gov
- Token included in SIP call setup message and can be verified by SIP nodes along whole path to IP endpoint
- Endpoint can interrupt lower priority sessions or take other TDR-specific action
- International Emergency Priority Parameter proposed for ISUP, B-ISUP and BICC CS-2

Flow verification

- Session setup most important in Circuit Switched Networks
- But Packet Switched Networks need mechanism to differentiate specific packet flows

QoS mechanisms

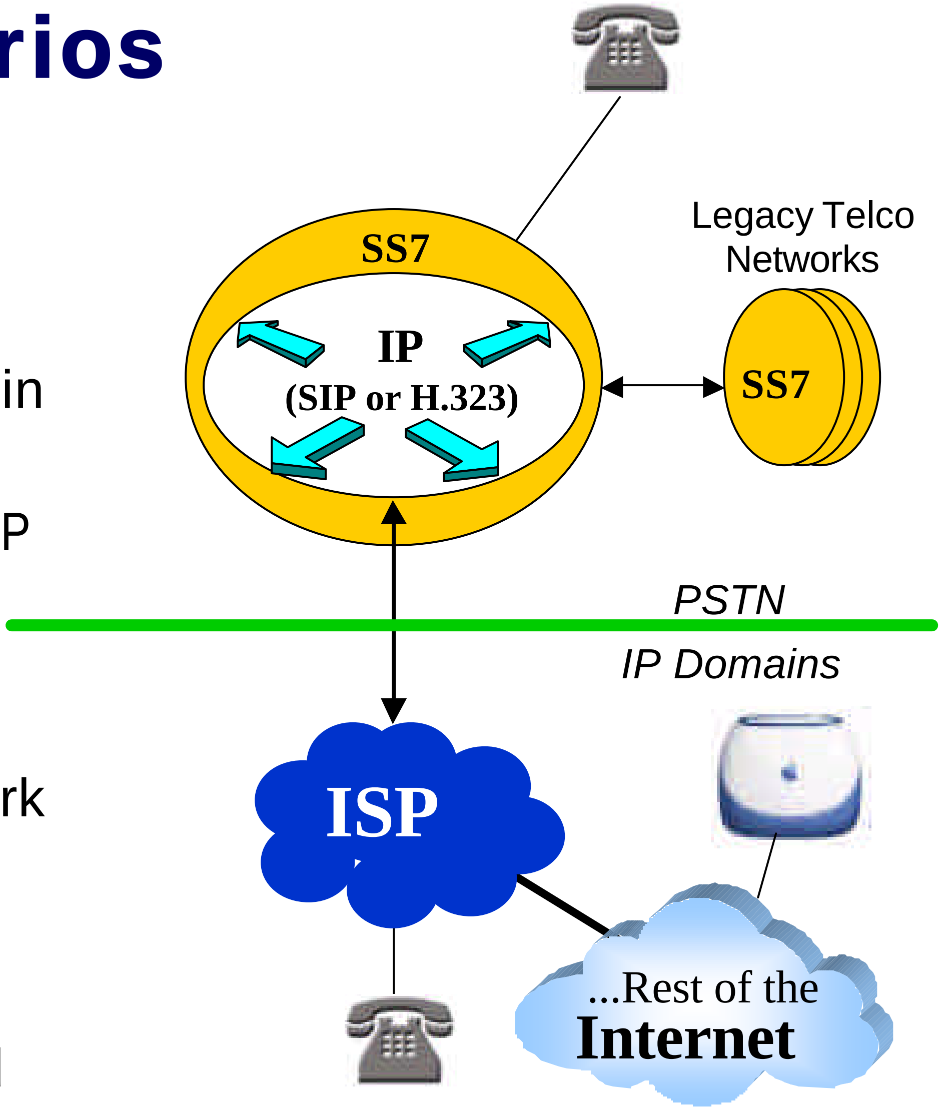
- DiffServ, RSVP, MPLS all possibilities
- All unpopular inter-domain with ISPs due to potential security problems between untrusted networks
- Hardest remaining problem for multi-domain networks!

Gateway support

- Gateways must translate TDR markings appropriately, and carry authorisation through if possible
- Cryptographic link between IP source and PSTN gateway allows PSTN priority even without IP-side support. But gateway should check authorisation on destination network first

VoIP scenarios

- Single IP backbone network connecting SS7 switches
  - Authorisation done in PSTN
  - ISUP tunnelled in SIP



- **Internetwork**
  - Home+access network authorise transport priority
  - Proxy/gateway authorises session and PSTN priority