# draft-ietf-crisp-iris-lwz-06
# draft-ietf-crisp-iris-xpc-04
# draft-ietf-crisp-iris-common-transport-03

(the drafts I should have updated but didn't because I'm lazy)

CRISP Working Group, IETF 67
7 November 2006
San Diego, CA, US

Andrew Newton

# LWZ Security

- Usual bloviation from security wonks
  - Need to state the consequences if this public data is modified.
    - Point specifically to the BCP 38 on UDP reflection attacks
      - (though they didn't know what it was)
- Point to XPC if you want ANY security.

# LWZ Congestion Control

- Congestion Control is completely absent.
- No particular consistency among UDP apps.
- My suggestion: follow DTLS in emulating TCP timeout/backoff.
  - Initial timeout of 1 second.
  - Double value at each retransmission
  - Up to the maximum of 60 seconds

# LWZ Gen-Art Review

- UDP header should be removed
- Many small, but fair nits
- Suggestion to point out that XPC should be used for many, many thousands of transactions instead of spending a lot of time on non-random transaction IDs.

# XPC Gen-Art Review

- Need ASCII diagrams in Section 5 & 6 of block header and chunk descriptor
- Section 6: chunk ordering and combination restrictions need to be separated out for clarity.
- Section 9: explain when/why TLS is to be used.
- 500 other nits from Marcos

# XPC Security Review

- Need to comply with Section 4 of RFC 4422.
- Changes needed:
  - mostly text pointing out compliance
  - XML in common-transport may need to contain arbitrary data in authentication notices.
  - Restrict XPC to one SASL mechanism at a time.

# Common Transport

- Modification to meet SASL requirements.
  - (mentioned before)
  - Text stating that protocols using security measures should offer the authenticationIds (i.e. <version>) in initial responses to avoid downgrade attacks.