DCCP Spec as of Last Call

Eddie Kohler
UCLA

IETF 60 DCCP Meeting
August 5, 2004

Overview

- Removed mobility and multihoming
- Extended sequence numbers
- Feature negotiation
- Other changes

Mobility and multihoming

Extended sequence numbers

- Problem 1: Blind attacks
  - Sequence number security main defense against blind attacks
  - Corresponds to recently publicized “tcpsecure” issues
  - Our charter disallows cryptographic mechanisms
  - High success probability of blind reset attacks with 24-bit seqnos
- Problem 2: Sequence number transition
  - Was overly complex

Solution: Make them required

- The single canonical form for sequence numbers is 48 bits long

  Removes sequence number transition issues

- DCCP-{Request, Response, CloseReq, Close, Reset, Sync, SyncAck} packets MUST contain 48-bit sequence numbers

  Blind attacks instantly much harder

  "For N = 10,000, W = 2000, and L = 48, a DCCP-Sync attack will succeed with probability $7 * 10^{-8}$. Attacks involving DCCP-CloseReq, DCCP-Close, and DCCP-Reset packets are more difficult still, since 48-bit Sequence and Acknowledgement Numbers must both be guessed."

- DCCP-{Data, DataAck, Ack} packets MAY use short sequence numbers

  Unless Allow Short Seqnos feature is false

Extending a 24-bit seqno to 48 bits

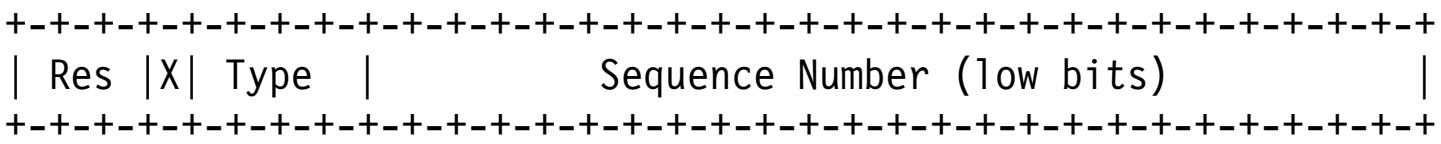
```
procedure Extend_Sequence_Number(S, REF)
   /* S is a 24-bit sequence number from the packet header.
      REF is the relevant 48-bit reference sequence number:
      GSS if S is an Acknowledgement Number, and GSR if S is a
      Sequence Number. */
   set REF_low := low 24 bits of REF
   set REF_hi := high 24 bits of REF
   if REF_low (<) S           /* CIRCULAR comparison mod 2^24 */
         && S |<| REF_low:    /* NON-CIRCULAR comparison */
      return (((REF_hi + 1) mod 2^24) << 24) | S
   otherwise:
      return (REF_hi << 24) | S
```

Feature negotiation

- Update reordering protection
  - Endpoints can change preference lists in the middle of a negotiation
  - A new UNSTABLE state guarantees agreement anyway
  - Expect this to be simpler to implement
  - Note: Document currently contradicts itself, my apologies; see mailing list
- Remove empty Change options
  - Was used to verify the current value of a feature
  - Interfered with negotiation & reordering protection

Other changes (1)

- Rearrange header



- The Ack# on a DCCP-Sync does not indicate acknowledgement

  Since the DCCP-Sync might have been sent in response to a sequence-invalid packet

- Describe DCCP-Reset codes in more detail
- Options on DCCP-Reset packets are processed

  May lead to resetting a Reset

Other changes (2)

- Add Minimum Checksum Coverage feature
  - Check whether your peer is willing to accept packets with reduced Checksum Coverage
- Added section on Congestion State and Reset Congestion State option
  - If the path changed, send Reset Congestion State and slow start
  - Suggested by mobility issues
  - Worth keeping?
- CCID-specific feature and option processing defined, simplified
- Describe Ack Ratio in more detail
  - Allow ack piggybacking, rate-pacing, delayed acks, etc.
- Update boilerplate, writing improvements