Revenge of DCCP Spec

Eddie Kohler
UCLA

IETF 61 DCCP Meeting
November 10, 2004

Thanks to

- Allman, Perkins, Westerlund
- Fairhurst, Falk, Gharai, Vos . . .

Header rearrangement

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |            Dest Port          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data Offset  | CCVal | CsCov |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     |       |X|               |                               .
| Res | Type  |=|   Reserved    |  Sequence Number (high bits)  .
|     |       |1|               |                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                  Sequence Number (low bits)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- No change:

  Allman/Perkins: Get rid of 24-bit sequence numbers?

  Allman/Perkins: Too much reserved space? (27 bits with ackno!)

Header analysis

		--- Header lengths -----		
	Frequency	Current	Restricted	45-bit seqnos
CCID2 Data	X	3/4	4	3/4
CCID2 Ack	X/2	4/6 + AV	5 + AV	4/5 + AV
CCID3 Data	X	3/4	4	3/4
CCID3 Ack	1/RTT	4/6 + ~5	5 + ~5	4/5 + ~5
DataAck	?	4/6 + ??	5 + ??	4/5 + ??

Possible alternate header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |           Dest Port           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data Offset  | CCVal | CsCov |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Res | Type  |1|   Reserved    |  Sequence Number (high bits)  .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                  Sequence Number (low bits)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.               Acknowledgement Number (high bits)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Ack Number (low bits)     |             Options           .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Feature negotiation

- Remove out-of-band negotiation
- Allow preference changes during negotiation (consistency)

Congestion control

- Remove CCID 1
- Define acknowledgeability (Step 8 of pseudocode)
- Perkins: ECN mandatory? (Floyd: Oy)

  ECN Capable $\longrightarrow$ ECN Incapable, encourage use of ECN
- Add CCID Profile Requirements
- Remove Reset Congestion State option
- Falk: Explicitly mention Data Dropped is reliable
- Ack CC required

Packet exchange

- SHOULD report zero-length Data and DataAck packets to the app

  Perkins asked for MUST, Minshall asked for nothing

- DCCP-Reset options are processed
- Timers, exponential backoffs, rate limits more explicitly defined
- Clarify pseudocode with comments

Ignoring options on DCCP-Data

- Problem: DCCP-Data(Mandatory, unknown-option)
  - Previously, receiver MUST reset connection
  - But if receiver allowed short seqnos, the attacker could easily generate this packet!
  - Problem most significant on DCCP-Data because of single seqno
- Solution: Ignore "state-changing" options on DCCP-Data packets
  - Mandatory, feature negotation, Init Cookie, . . .
  - Protocol should NEVER reset connection b/c of something weird in DCCP-Data
  - (One exception: DCCP-Data arrives in REQUEST state)
  - Also reduce other resets (e.g., server receives CloseReq)
- Potential issue: DCCP-Reset(Aggression Penalty)?

Security

- List number of packets required to achieve 50% attack success

  24-bit DCCP-Data: 83,000; DCCP-Sync: 10^{11}

Miscellaneous

- Default RTT to 0.2s; more conservative for timer setting
- Fairhurst/Welzl: Tweak checksum coverage discussion
- Timestamp option: Defined granularity (10 μs)

  Also, explicitly allow multiple Timestamp Echoes
- PMTU

  Restructure, describe which packets may be sent unfragmentable, IPv6
- Perkins: All-new IANA Considerations
- Westerlund: Maximum Sequence Window length

Open questions

- Rosen: Shouldn't claim to be suitable for interactive voice

  Point taken, see later

- Allman: Specify other ICMP interactions?

  Probably by reference to TCP?

- I'm inclined to leave these undone

  Falk/Westerlund: List Service Codes

  Allman: Provide sample Init Cookie implementation

  Perkins: Multiple Service Codes per port considered harmful

  Glossary?

- Aggression Penalty reset considered harmful