draft-handte-httpbis-dict-sec

“Security Considerations Regarding Compression Dictionaries”

Felix Handte

w@felixhandte.com

Facebook

IETF 106, HTTPbis Session II, Singapore

Thursday, November 21st, 2019
Motivation

Size Matters!
HTTP Compression @ Facebook

<table>
<thead>
<tr>
<th>Algo</th>
<th>Ratio</th>
<th>gz</th>
<th>br</th>
<th>zstd</th>
</tr>
</thead>
<tbody>
<tr>
<td>gzip</td>
<td>4.45x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>brotli*</td>
<td>4.95x</td>
<td>+11%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zstd</td>
<td>4.99x</td>
<td>+12%</td>
<td>+ 1%</td>
<td></td>
</tr>
<tr>
<td>zstd+dict</td>
<td>5.84x</td>
<td>+31%</td>
<td>+18%</td>
<td>+17%</td>
</tr>
</tbody>
</table>

*results simulated
Dictionary-Based Compression

- Dictionary
- Message
- Match
- External dependency
- Compressed message
Challenges

- Statefulness
- Complexity
- Security
Path Forward

**Eventually:** ship dict-based compression.

**But first:** understand its security properties.
• Surveys integration choices
• Enumerates security risks
• Discusses mitigations
CRIMEs

secret

message

guess

compressed message

partial match
CRIMEs

- Dictionary
  - Secret
  - Implicit

- Message
  - Guess
  - Compressed
Dictionary Lifecycle

- Generation
- Identification
- Distribution
- Selection
- Compression
- Decompression
- Deletion
Risks Currently Discussed

- Revealing Message Content
- Revealing Dictionary Content
- Manipulating Message Content
- Obfuscating Message Content
- Tracking Users
- Denial of Service
- Resource Exhaustion
- Generating Dictionaries
- Complexity
Adopt this document?
Thanks!

draft-handte-httpbis-dict-sec

w@felixhandte.com