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

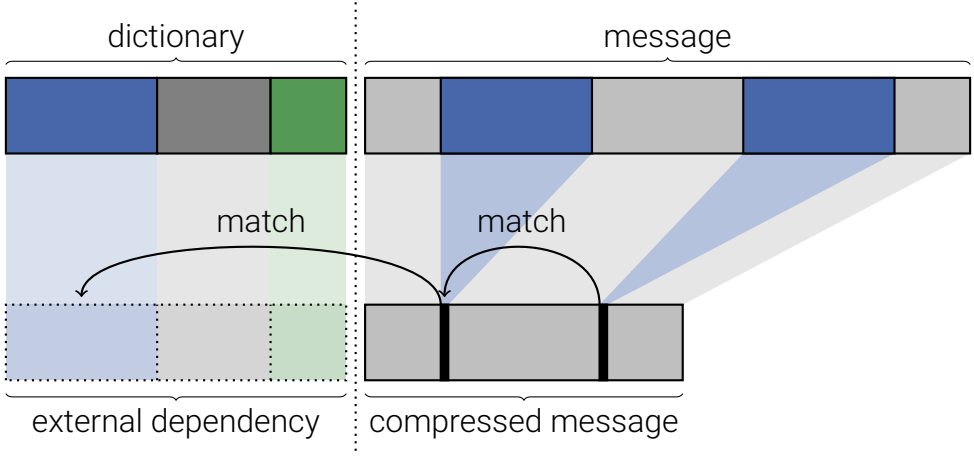
Size Matters!

HTTP Compression @ Facebook

Algo	Ratio	Versus gz	Versus br	Versus zstd
`gzip`	4.45x			
`brotli`*	4.95x	+11%		
`zstd`	4.99x	+12%	+ 1%	
`zstd+dict`	5.84x	+31%	+18%	+17%

*results simulated

Dictionary-Based Compression



Challenges

Statefulness

Complexity

Security

Path Forward

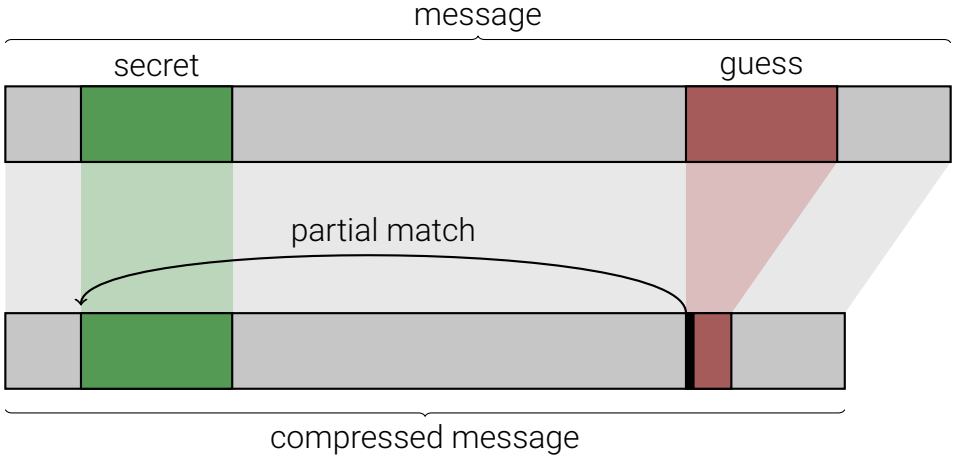
Eventually: ship dict-based compression.

But first: understand its security properties.

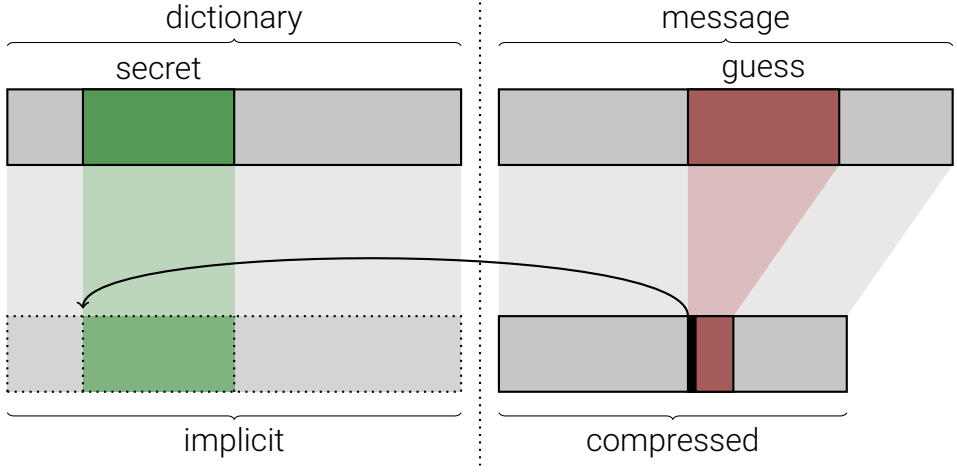
`draft-handte-httpbis-dict-sec`

- Surveys integration choices
- Enumerates security risks
- Discusses mitigations

CRIMEs



CRIMEs



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