What's different in the new WebSocket protocol
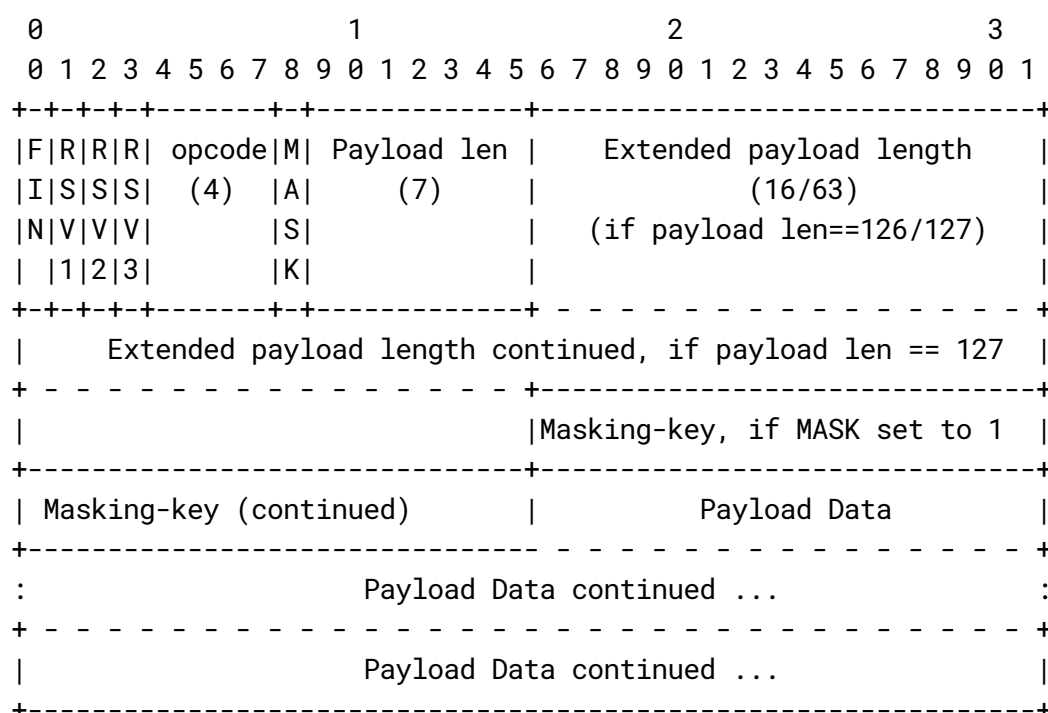
By [Eiji Kitamura](#)

Developer Advocate in Tokyo

The WebSocket protocol specification has recently been updated to solve previous security concerns and is largely stable. Below is a summary of the changes involved, along with some notes on current implementations.

What has been changed since WebSocket HyBi 00?

- The protocol frame format has been changed. HyBi 00 used to use `"0x00"` for head and `"0xff"` for tail for each frame. HyBi 10 now uses new format like following:

```
 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
+-+-+-+-+-------+-+-------------+-------------------------------+
|F|R|R|R| opcode|M| Payload len |    Extended payload length    |
|I|S|S|S|  (4)  |A|     (7)     |             (16/63)           |
|N|V|V|V|       |S|             |   (if payload len==126/127)   |
| |1|2|3|       |K|             |                               |
+-+-+-+-+-------+-+-------------+ - - - - - - - - - - - - - - - +
|     Extended payload length continued, if payload len == 127  |
+ - - - - - - - - - - - - - - - +-------------------------------+
|                               |Masking-key, if MASK set to 1  |
+-------------------------------+-------------------------------+
| Masking-key (continued)       |          Payload Data         |
+-------------------------------- - - - - - - - - - - - - - - - +
:                     Payload Data continued ...                :
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
|                     Payload Data continued ...                |
+---------------------------------------------------------------+
```

Security issues have been addressed.

- `Sec-WebSocket-Key` and `Sec-WebSocket-Accept` are added in place of HyBi 00's three keys. The browser gives randomly generated number to `Sec-WebSocket-Key`. Then, the

server uses it with WebSocket protocol's specific GUID (`258EAFA5-E914-47DA-95CA-C5AB0DC85B11`) and SHA1 / BASE64, etc to return `Sec-WebSocket-Accept` so that browser can confirm that it understands WebSocket. This prevents a cross-protocol attack.

- On each frame, *frame masking* is now required. This prevents cache poisoning on proxy. `Sec-WebSocket-Origin` is added to prevent access from scripts that the service provider isn't aware of.

- `Sec-WebSocket-Origin` is added in place of HyBi 00's Origin key to prevent access from scripts that the service provider doesn't aware of. Note that this will be just "`Origin`" on HyBi 11.

JS API changes

- `subprotocol` can now be array, allowing a method signature of `new WebSocket(String url, Array subprotocol)`

- `.protocol` attribute [String]

- `.binaryType` attribute [Blob|ArrayBuffer]

- `.extension` [String]

- Status code and reason (why the connection is closed) have been added to `CloseEvent`. The `close()` function has also been changed to accept these two arguments accordingly.

Extensions

- `Sec-WebSocket-Extensions` is added. Proposed extensions are:

- `deflate-frame` makes frames compressed at source and extracted at destination.

- `x-google-mux` to support multiplexing but is in early stage.

Is there compatibility between HyBi 00 and HyBi 10 on both server and browser implementation?

- Server implementations can support both HyBi 00 and HyBi 10 by looking at the handshake HTTP header. However, it is not recommended to support HyBi 00 since it's known to be vulnerable.

- The WebSocket JavaScript API is largely similar between old and new versions. But as noted above, we don't recommend supporting HyBi 00 since it's known to be vulnerable.

Which browser support HyBi 10?

- Chrome 14 supports HyBi 10 protocol although the WebSocket JavaScript API changes mentioned above are still on the way. Firefox 7 is also planned to support HyBi 10.

Last updated July 2, 2018.