Abstract

HTTP/2 is the newest version of the HTTP1.1 protocol that was finalized in May 2015 and introduced as the IETF standard for web communication. HTTP/2 provides significant performance improvements by addressing well-known problems with HTTP/1.1 (e.g., head of line blocking and redundant headers) some of this features may have indirect impact in security. Also, HTTP/2 introduces new features like the default encryption which causes traffic hiding consequently affects a number of services (e.g., web Caching, Traffic classification). HTTP/2 may have some problems (vulnerabilities) like any new develop protocol lead to Denial of Service (DoS) attacks. The research try to figure out the pros and cons of the this new protocol version from different aspect specially security issues.

References

3. Peter Megyesi, Zsolt Kramer and Sandor Molnar, “Comparison of web transfer protocols”,
Keywords

DoS, IETF, Vulnerabilities, Caching