Traffic Analysis of HTTPS

László Zömbik

Secure web access became remarkable need for nowadays users. Surfers of the Internet are not only able to reach web pages advertising information, but they even interactively use the services of web server. The essentiality of the interactivity based upon that the user sends information in order to the server can select, create and provide user specific answer. When the users give extra information, this is in most cases not sensitive, (e.g. when a user specifies the date and the destination to query timetables of railway company) but in certain cases user generated traffic must be protected (e.g. when client checks his account using services of an online bank).

Without protecting the sensitive web traffic an eavesdropper may deduce parameters or behavior of the user or even an attacker can identify and impersonate the victim. Therefore several security solutions has evolved, the two most notable security protocol are the SSL [1] and the TLS [2]. The two protocols are very similar, before sending user information the client and the server initially negotiate about the security association, including cryptographic algorithms and keys. After the handshake phase protected traffic is transmitted. If a web server uses SSL or TLS then the HTTP [3] communication is secured. In this case the communication is HTTPS.

It is beneficial to have a model for HTTPS for bandwidth or for cost estimation. This is extremely important for communications that contains expensive links or the link capacity is limited and secure web access is required. Example can be that the subscribers use satellite terminals or GPRS, UMTS equipment for browsing on the web.

In this presentation we introduce a traffic model for HTTPS. This model is verified by traffic measurements. Suggestions for achieving effective HTTPS conversation for web server developers and for users are presented. A correlation between HTTP and HTTPS traffic is shown, and traffic flow confidentiality of HTTPS is evaluated.

References

[1] Frier, Karlton, Kocher, “The SSL 3.0 Protocol”, Netscape Corp., 1996.

[2] Dierks, T. and C. Allen, “The TLS Protocol”, RFC 2246, 1999.

[3] Fielding et Al, “Hypertext Transfer Protocol - HTTP/1.1”, RFC 2616, 1999.