TLS protocole pour la sécurité des échanges : réalité et illusion

Ahmed Serhrouchni
GET / ENST Paris, CNRS LTCI – UMR 5141
46 rue Barrault 75013 Paris
Email: ahmed@enst.fr

Nous proposons dans cet article d'exposer et d'analyser une solution de sécurité des échanges des plus déployées. Le protocole TLS (Transport Layer Secure). Le protocole TLS ou SSL (Secure Socket Layer) a été initialement conçu par la compagnie Netscape et intégré au browser navigator. Il a par la suite été normalisé au sein de l'IETF sous le nom de TLS. Ce même protocole a été adopté dans la pile WAP (Wireless Application Protocol) sous le nom de WTLS (Wireless Transport Layer Secure). Ce protocole est une solution de sécurité transparente aux applications qui sont basées en natif sur le protocole de transport TCP. Les services de sécurité ainsi fourni aux applications sont les mêmes. Il est dans ce contexte un protocole générique. Il ne couvre pas des besoins spécifiques à certaines classes d'application. Tels que les applications de paiement sur Internet. Encore une fois, il faut souligner que ce protocole à l'origine n'avait pas pour ambition de couvrir tous les besoins mais uniquement de sécuriser avec les services standard de sécurité le protocole http (HyperText Transfert Protocol). Le déploiement de ce protocole TLS est devenu tellement déployé que plusieurs propositions ont été faites pour l'étendre à de nouveaux services. Nous même avons proposé plusieurs extensions, notamment pour le support des services d'autorisation, de la signature électronique et du contrôle d'accès par un secret pré partagé. On peut notamment souligner son intégration au niveau du WIFI pour assurer l'authentification des accès. Nous exposerons l'ensemble de cette évolution et proposition d'extensions de TLS. Le corps de ce papier se focalisera sur le protocole TLS et ses extensions futurs. Nous ferons ainsi une analyse sur la situation actuelle de ce protocole, et on le situera par rapport à d'autres solutions telles que le protocole IPsec par exemple. Ceci nous conduira également à donner l'essence du protocole IPsec.

On se doit avant d'exposer cette solution de commencer par poser la problématique et les enjeux de la sécurité. Cet exposé nous conduira à donner un point de vue sur la situation actuelle de la sécurité. Nous donnerons par la suite une typologie des attaques. Il est nécessaire de faire cette typologie des attaques pour connaître leurs origines et mieux situer les solutions. Plusieurs typologies existent. Celles qui classifient selon les effets. Celles qui classifient selon les protocoles. Celles qui classifient selon les systèmes d'exploitation. Nous proposons nous même une nouvelle classification qui d'abord permet de cerner mieux les parades et ensuite de connaître les origines. Et surtout pour ce qui concerne ce papier pour mieux situer l'action du protocole TLS.
Dans un autre ordre nous conclurons par une synthèse sur la sécurité et les enjeux politiques, économiques et techniques.

TLS protocol for secure data exchange: reality and illusion

Ahmed Serhrouchni
GET / ENST Paris, CNRS LTCI – UMR 5141
46 rue Barrault 75013 Paris
Email: ahmed@enst.fr

In this paper, we propose to expose and analyze the TLS (Transport Layer Secure) protocol, the most deployed security data exchange protocol. TLS or SSL (Socket Secure Layer) protocol was initially conceived by Netscape Company and integrated into Web navigator. Thereafter, it was standardized within the IETF under the name of TLS. This same protocol was adopted in WAP (Wireless Application Protocol) under the name of WTLS (Wireless Transport Layer Secure).
This protocol is a transparent security solution to applications which are natively based on the TCP transport protocol. Thus, security services provided to the applications are the same. In this context, TLS is a generic protocol. It does not meet specific needs to some classes of application such as internet payment applications.
Once again, it should be noted that, in the beginning, this protocol did not have as objectives to meet all the security needs but only to secure services like HTTP (Hyper Text Transfer Protocol) protocol.
This protocol TLS became so deployed that several proposals were made to extend it with new services. Even us, we proposed several extensions, in particular for authorisation, electronic signature and authentication with pre shared keys. One can underline his integration on the WIFI level to ensure authentication. We will expose the whole of this evolution and extensions for TLS.
The body of this paper will focus on TLS protocol and its futures extensions. Thus, we will give a complete analyse of the current situation of this protocol and we will situate it in comparison to other solutions such as the IPSec protocol. This will also result in giving the essence of the IPSec protocol.

We must before exposing this solution to start by raising the problems and the security stakes. This will lead us to give a point of view on the current situation of security. Thereafter, we will give a typology of attacks. It is necessary to make this typology of attacks to know their origins and to better locate the solution. Several typologies exist. Those which classify according to effects. Those which classify according to protocols. Those which classify according to operating systems. We propose a new classification which makes it possible to better encircle the parades and then to know the origins and especially for those concerning this paper for better locating the actions of TLS protocol. Finally, we will conclude by a synthesis on security and politic, economic and technical stakes.