ANR SafeTLS (2017-2021)

SSL/TLS est aujourd'hui une brique de base de la sécurité des échanges sur Internet. Le projet ANR SafeTLS, qui a débuté en Octobre 2017, a pour objectif d'oeuvrer à la sécurisation de l'Internet du futur avec TLS 1.3. Pour cela, plusieurs aspects seront abordés. Tout d'abord, avec la spécification en cours de TLS 1.3, des efforts de modélisation et de preuves de sécurité calculatoires permettront d'assurer que le protocole apporte bien les propriétés de sécurité attendues. Ensuite, il est important d'évaluer le déploiement actuel du protocole TLS à l'aide de mesures, afin de mieux comprendre l'état actuel des connexions sécurisées. L'usager étant principalement affecté par le design de la connexion, ce projet a pour objectif de meilleur informer celui-ci sur la sécurité de chaque connexion TLS, afin que l'usager puisse mieux gérer l'information envoyé sur https:// .Enfin, le projet apportera des éléments sur les aspects touchant à l'implémentation du protocole, afin de s'assurer que les propriétés de sécurité prouvées sont bien garanties jusque dans le code exécuté.