Processing Encrypted Streams for Traffic Oversight

Traitement des flux chiffrés pour la gestion du trafic

PRESTO

Appel : AAPG 2019

Année : 2019

Instrument : PRCE

COORDINATEUR : David Pointcheval

PARTENAIRES : ENS, IMT, LORIA, Orange Labs, 6cure

Le RGPD (Règlement Général sur la Protection des Données) apporte de nombreuses garanties quant au respect de la vie privée, avec de fortes contraintes sur la collecte des données, tandis que les menaces croissantes de la cybercriminalité nécessitent une surveillance accrue du trafic pour prévenir les activités dangereuses ou malveillantes. PRESTO a pour objectif de concilier ces deux objectifs *a priori* contradictoires.

CONTEXTE ET OBJECTIFS

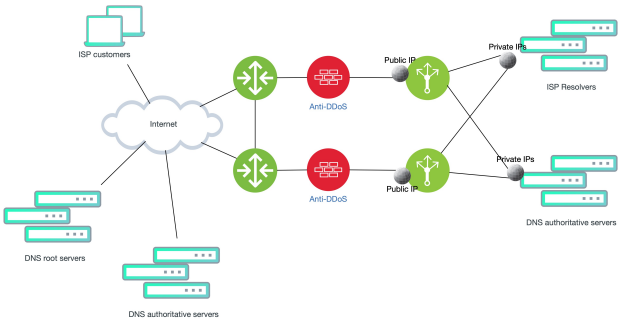
PRESTO exploite les récentes avancées en cryptographie pour concilier respect de la vie privée et garanties de sécurité dans plusieurs cas d'usage :

- Filtrage de contenu (contrôle parental)
- Détection d'attaques (DDoS)
- Analyses légales d'attaques *a posteriori*

afin que le RGPD ne pénalise pas les niveaux de sécurité mis en place sur le trafic en clair.

MÉTHODOLOGIE ET RÉSULTATS

Méthodologie : en enrichissant les protocoles de communication (couche TLS) avec des algorithmes de chiffrement avancé, certaines informations nécessaires au filtrage des contenus ou à l'analyse de requêtes restent accessibles au matériel de sécurité, sans pour autant exposer les données sensibles ; en parallèle, la recherche dans des archives chiffrées reste possible en utilisant des techniques de chiffrement cherchable.



[1] Elie Bouscatié, Guilhem Castagnos, Olivier Sanders - *Public Key Encryption with Flexible Pattern Matching*. ASIACRYPT (4) 2021: 342-370

[2] Cécile Delerablée, Lénaïck Gouriou, David Pointcheval - *Key-Policy ABE with Delegation of Rights*. IACR Cryptol. ePrint Arch. 2021: 867 (2021)

Cas d'usage et résultats :

- **Filtrage de contenu** au niveau de la box internet du domicile ou d'un équipement de réseau d'entreprise, en fonction des droits associés aux utilisateurs et selon des catégories prédéfinies partagées avec les fournisseurs de contenus, sans nécessiter d'accéder à tout le contenu chiffré dans le canal TLS. Nous concevons pour cela un schéma d'**ABE** (*Attribute-Based Encryption*) [2] et l'extension TLS le supportant.

- **Protection** des *DNS Resolvers* contre les attaques par **DDoS**, sans pour autant déchiffrer les requêtes et les réponses, mais en permettant un accès limité, par construction, à certaines données par le matériel Anti-DDoS : recherche de séquences malveillantes dans les requêtes chiffrées [1].

- **Archivage sécurisé** des journaux de requêtes/réponses pour identifications ultérieures d'**IoC** (*Indicators of Compromise*) : chiffrement cherchable.

Deux solutions ont été implémentées sur les journaux DNS : une asymétrique à base d'**IBE** (*Identity-Based Encryption*), l'autre symétrique reposant sur des **Constrained PRF** (*Pseudo-Random Functions*).