Projet CASSIOPEE® :
« Database Firewall »
Compte rendu d'avancement n°02

Liste de diffusion : Grégory Blanc, Grégoire Menguy, Baptiste Polvé

Ordre du jour

- **Fonctionnement du protocole MySQL (achevé)**
- **Développement client/serveur intégrant échange MySQL (bien commencé)**
- **Développement du parser (commencé)**

Fonctionnement du protocole MySQL

Nous avons souhaité nous intéresser ensemble au fonctionnement du protocole.
Baptiste a étudié la documentation officielle de MySQL et a fait la synthèse des éléments qui nous intéressent.
Grégoire quant à lui à illustrer cette documentation en récupérant les trames réelles via wireshark pour expliquer plus concrètement le protocole.

Pour plus d'information, le document est dans la partie Documentation.

Développement client/serveur intégrant échange MySQL

Les recherches sur le fonctionnement du protocole MySQL ont permis d'accélérer grandement le développement du client/serveur avec principalement l'intégration du fonctionnement du protocole MySQL.
Baptiste a réussi à mettre en place le proxy, l'application est maintenant capable de tourner mais le trafic passe totalement par le DBF.

Développement du parser

Grégoire a commencé la prise en main de LEX & YACC. Il a ainsi produit un premier parser MySQL pour des requêtes simples créées sur un alphabet réduit (SELECT, FROM, WHERE, AS). La difficulté majeure est de gérer les productions pour les sous requêtes. Il est en effet nécessaire de parser toutes les possibilitées, tout en restant strict pour ne pas accepter des requêtes illégitimes.

Une question émerge alors : Serait-il possible de limiter le parser pour qu'il n'accepte pas les requêtes trop compliquées (terme à définir) même si elles respectent la grammaire MySQL ?

Idée : Nous avons remarqué que pendant une attaque, les éléments en commentaires sont également envoyés. On pourrait donc parser également les commentaires. Si les commentaires ressemble à du SQL cela pourrait signifier que l'on a affaire à une attaque.

Ce CR sera considéré comme validé lundi 20/03/2017 en l'absence de remarque.