

# Mise en accord de clé de session authentifiée par mot de passe

Laboratoire d'informatique – École normale supérieure  
Groupe de Recherche en Complexité et Cryptographie

- Directeur de stage : David Pointcheval (DI-ENS)  
`http://www.di.ens.fr/users/pointche` – `David.Pointcheval@ens.fr`
- Directeur du laboratoire : Jacques Stern (DI-ENS)  
`http://www.di.ens.fr/users/stern` – `Jacques.Stern@ens.fr`

- Exposé général de la situation du sujet :

La cryptographie en pratique est essentiellement connue par ses applications phares SSL/TLS et SSH, qui permettent d'établir un canal sécurisé entre deux machines. Le plus souvent, nous l'utilisons en tant que client auprès d'un serveur en possession d'un certificat sur une clé publique, permettant de vérifier l'identité de ce serveur. Le client pourrait être authentifié de la même manière, à l'aide de mécanismes asymétriques, mais cela nécessiterait la possession d'un certificat. Or notre seul moyen d'authentification est souvent un simple mot de passe. Nous vérifions rarement le certificat du serveur (parfois d'ailleurs auto-certifié, et lors de la mise en garde de la part du navigateur, nous acceptons la connexion), et alors notre authentification par mot de passe peut être transmise à un serveur erroné. Une confusion entre les multiples mots de passe à retenir peut également nous conduire à transmettre au serveur  $A$  le mot de passe utilisé pour s'authentifier auprès du serveur  $B$ .

Le but des protocoles de mise en accord de clés de session avec authentification par mot de passe que nous considérons ici permettent à deux machines (ou individus) qui partagent un mot de passe (quelques caractères, et donc dont la recherche exhaustive est aisée) d'établir un canal sécurisé sans faire appel à un quelconque certificat, de telle sorte qu'aucune attaque passive ou active ne permettra de découvrir le mot de passe. La seule attaque inévitable est l'attaque active qui permet d'éliminer **au plus un** mot de passe par tentative de connexion. Une attaque passive (simple espionnage de la communication) ne doit en revanche rien révéler sur le mot de passe. Ainsi, un serveur malhonnête ne pourra extraire le mot de passe d'un client, et un client malhonnête ne pourra se faire passer pour quelqu'un d'autre auprès d'un serveur.

- Résumé du travail souhaité :

Notre équipe a étudié et prouvé la sécurité de plusieurs protocoles de ce type [1, 2, 3, 4], et le but de ce stage serait tout d'abord de se familiariser avec les outils cryptographiques utilisés, puis d'implémenter l'un de ces protocoles afin d'évaluer son efficacité. L'utilisation des courbes elliptiques pourra être envisagée, et peut-être souhaitable.

- Connaissances préalables : un peu de théorie des nombres, programmation en C ou java.

## Références<sup>1</sup>

- [1] M. Abdalla and D. Pointcheval. Simple Password-Based Encrypted Key Exchange Protocols. In *CT-RSA '05*, LNCS, Springer-Verlag, 2005.
- [2] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated Key Exchange Secure Against Dictionary Attacks. In *EUROCRYPT '00*, LNCS 1807, Springer-Verlag, 2000.
- [3] E. Bresson, O. Chevassut, and D. Pointcheval. Security Proofs for Efficient Password-Based Key Exchange. In *ACM CCCS '03*, ACM Press, 2003.
- [4] E. Bresson, O. Chevassut, and D. Pointcheval. New Security Results on Encrypted Key Exchange. In *PKC '04*, LNCS 2947, Springer-Verlag, 2004.

---

<sup>1</sup>toutes disponibles sur `http://www.di.ens.fr/users/pointche`.