Étude et implantation des méthodes d'authentification à base de mots de passe jetables.

proposé par Magali Bardet

22 octobre 2013

L'authentification a pour objectif de vérifier l'identité dont une entité (personne ou machine) se réclame, pour lui autoriser l'accès à des ressources ou à certains privilèges. On appelle demandeur celui qui tente de prouver son identité, et receveur celui qui doit vérifier l'identité avant d'autoriser certaines actions.

Le mécanisme le plus connu est celui du login + mot de passe. Or, ce mécanisme ne réalise pas ce que l'on peut attendre d'un protocole d'authentification cryptographique : en particulier, il est vulnérable à des attaques par *rejeu* (tout adversaire écoutant les communications entre le demandeur et le receveur peut intercepter le mot de passe et le réutiliser pour se faire passer pour le demandeur) ou par *usurpation d'identité* (si le receveur n'est pas honnête, il peut lui aussi réutiliser le mot de passe pour se faire passer pour le demandeur).

L'objectif du projet est d'étudier les mécanismes d'authentification par mots de passes jetables, qui renforcent la sécurité des mécanismes par mots de passe, sans toutefois atteindre la sécurité des protocoles d'authentification cryptographiques.

Dans une première partie, il est demandé de faire un état de l'art des protocoles d'authentification par mots de passe jetables, en précisant leur fonctionnement, leurs faiblesses, leurs avantages et les cas concrets d'utilisation. Voir par exemple [ANS10], le document RGS_B_3, [MvOV97] [1] chapitre 10, le module OTPW d'authentification pour PAM (Pluggable Authentication Modules) [], le système d'OTP proposé dans SSH [RFC06], la RFC 2289 [RFC98], un OTP basé sur HMAC [RFC05] et son extension TOTP [RFC11], l'OTP pour EAP [RFC07], le Google Authenticator [goo]

Dans une seconde partie, il est demandé de sélectionner certains de ces protocoles pour les mettre en oeuvre concrètement. Il est demandé en particulier de proposer une implantation de protocoles sur cartes à puces et son utilisation concrète, mettant ainsi en oeuvre des procédés d'authentification dits « forts » (les cartes à puces et les lecteurs de cartes, ainsi qu'une documentation d'utilisation seront fournis), et/ou une implémentation sur mobile.

1. `http://cacr.uwaterloo.ca/hac/`

Références

[ANS10] ANSSI. Référentiel général de sécurité. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite, 2010.

[goo] Google Authenticator. https://code.google.com/p/google-authenticator/.

[MvOV97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[RFC98] A One-Time Password System. http://tools.ietf.org/html/rfc2289, 1998.

[RFC05] HOTP : An HMAC-Based One-Time Password Algorithm. http://tools.ietf.org/html/rfc4226, 2005.

[RFC06] Generic Message Exchange Authentication for the Securer Shell Protocol (SSH). http://tools.ietf.org/html/rfc4256, 2006.

[RFC07] The EAP Protected One-Time Password Protocol (EAP-POTP). http://tools.ietf.org/html/rfc4793, 2007.

[RFC11] TOTP : Time-Based One-Time Password Algorithm. http://tools.ietf.org/html/rfc6238, 2011.