Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2013/14

Lezione XV: Single sign-on sul web

Il single sign-on (SSO)

L'idea di avere credenziali che permettono l'accesso a sistemi diversi è appetibile per una serie di ragioni

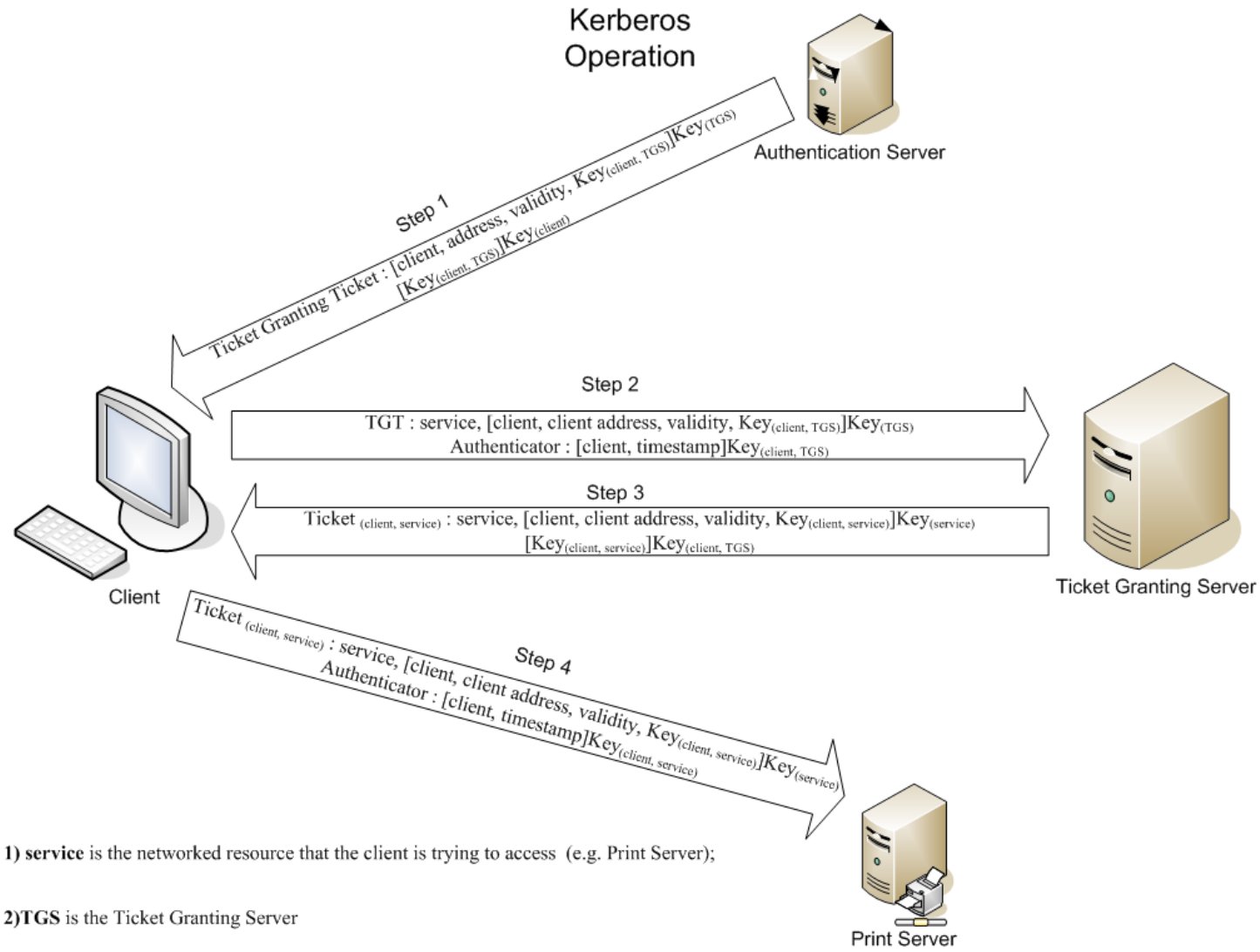
- Riduce il problema di trovare un buon segreto (sufficientemente casuale, ecc.)
- Riduce l'overhead totale di gestione degli accessi
- Permette la gestione centralizzata degli accessi, piú semplice da manutenere

(Aumenta la criticità delle credenziali, però)

Architettura di base

La maggior parte dei protocolli sono disegnati sull'impronta di Kerberos, che è una variazione con timestamp del protocollo Needham-Schroeder.
Un Ticket-Granting Server (TGS) fornisce ticket d'accesso a scadenza.

Kerberos



[Figura: wikipedia.org]

Il SSO sul web

Il SSO sembra particolarmente attraente in situazioni come i servizi web a bassa criticità:

- Decine di password da ricordare
- Utenti poco sensibili al problema

Ma soluzioni tipo Kerberos sono difficili da adottare, perché occorre che servizi indipendenti concordino sulla KDC.

OpenID

L'idea è che esistano siti che facciano da OpenID provider (OP) e gli OpenID Consumer (OC) accettano come credenziali quelle che gli utenti ottengono dagli OP (cui sostanzialmente gli OC delegano l'autenticazione)

Lo schema

1. Alice si connette al sito `meraviglie.org`
2. Per accedere comunica che ha un account su `faccialibro.com/openid/alice`
3. Alice accede (con credenziali tradizionali) a `faccialibro.com` e produce un certificato d'accesso
4. `meraviglie.org` accetta il certificato d'accesso come credenziale d'autenticazione

Problemi di OpenID

Lettura obbligatoria:
http://www.untrusted.ca/cache/openid.html
I principali rischi

- Facilità di allestire inganni di tipo **phishing**
- Privacy

Alternative migliori

In realtà sembra meglio avere credenziali multiple e gestirle con modalità come:

- PasswordSafe (`http://passwordsafe.sf.net`): un db criptato
- SuperGenPass (`http://supergenpass.com/`): un'unica password viene giustapposta ad un identificatore del sito e la vera password è ottenuta con una funzione hash. L'idea è ottima, la realizzazione ha diverse vulnerabilità: meglio usare alternative piú *crypto-savvy*, p. e.s. (`http://hpass.chmd.fr/`).

Riassumendo

Il SSO

- tipo kerberos è inadatto alla gestione di servizi web indipendenti
- le soluzioni del tipo OpenID presentano diversi problemi