BEZPEČNOSTNÍ RIZIKA HTTP COOKIES

František Zeman

katedra informatiky a počítačů, Přírodovědecká fakulta Ostravské univerzity,
30. dubna 22, 701 03 Ostrava, email: Frantisek.Zeman.cz@gmail.com

Abstrakt

Úvod

Tento příspěvek popisuje co jsou to http cookies, k čemu jsou určeny, jak bývají v praxi používány, jakým způsobem s nimi pracují prohlížeče a jaká rizika jejich užívání představuje. Cílem práce bylo zjistit, jaká nebezpečí představuje pro uživatele případné odcizení cookie souborů uložených prohlížečem v počítači a znázornit jak jednoduše může dojít k jejich zneužití.

Metody

Http cookie je textový řetězec, který je www serverem uložen na počítači uživatele. Tato data jsou při každé další návštěvě téhož serveru prostřednictvím prohlížeče odeslána zpět na server a tím je identifikován konkrétní webový prohlížeč.

Zacházení s cookies bylo zkoumáno ve třech běžně používaných webových prohlížečích, konkrétně se jednalo o Microsoft Internet Explorer, Mozilla Firefox a Google Chrome. Ke čtení uložených cookies byl využíván program SQLite Database Browser s výjimkou cookies uložených Internet Explorerem, k jejichž čtení stačí běžný textový editor. Vytváření nových cookies přímo v prohlížeči se zdařilo pouze v Google Chrome pomocí dopňku Edit This Cookie.

Výsledky

Bylo provedeno několik testů, ve kterých byla prověřována domněnka, že pouze se znalostí obsahu některé z cookies, zaslané dříve serverem danému uživateli, bude možno získat přístup k uživatelskému účtu tohoto uživatele na různých webových službách a tak i k citlivým datům tohoto uživatele. Do defaultně nastaveného prohlížeče Google Chrome byla úspěšně vložena nová cookie, obsahující data zaslaná dříve ze serveru jinému prohlížeči. Při navštívení těchto stránek pomocí prohlížeče Google Chrome s vloženou cookie byl prohlížeč na základě cookie rozpoznán a došlo k automatickému přihlášení do uživatelova účtu, bez nutnosti znát uživatelovo jméno či heslo. Tento výsledek byl úspěšně zopakován v několika dalších případech s několika dalšími servery používajícími různé systémy přihlašování. Zmíněný postup ovšem nebyl účinný ve všech případech. Některé servery (např. Facebook) používají vícestupňovou ochranu při přihlašování a mohou být kromě cookies navázány kupříkladu na lokaci IP adresy.

Závěr

Ačkoliv používání http cookies často zvyšuje pohodlí při běžném používání Internetu, uživatel se vystavuje riziku v případě, že by tyto soubory byly odcizeny a zneužity. Uživatel by tedy měl být obezřetný a nepoužívat cookies na serverech, kde by v případě získání kontroly nad účtem cizí osobou hrozilo odcizení citlivých dat či způsobení jiné závažné škody. Pro znemožnění odposlechu cookies při komunikaci se serverem je možno používat zabezpečené spojení https, které ovšem není vždy k dispozici. Taktéž by uživatel měl, pro minimalizaci rizika odcizení cookies, zamezit přístupu cizích osob ke svému počítači a využívat možnosti zaheslovaného uzamčení operačního systému.

Klíčová slova: *http cookie; webový prohlížeč; bezpečnost*

Poděkování

Tímto bych chtěl poděkovat RNDr. Tomáši Sochorovi, CSc. za metodické připomínky a poskytování odborných konzultací.