Autentizace podle Lamporta

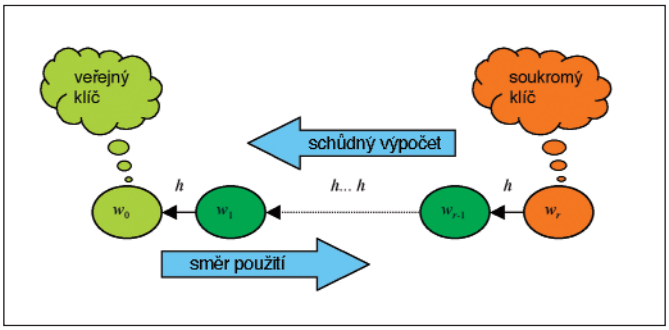
Autentizační procedury v poslední době procházejí důkladnými revizemi. Důvodem jsou měnící se podmínky jejich provozu. Až do nedávné doby se například běžně předpokládalo, že klient internetového bankovnictví dokáže svůj počítač udržet prostý všech škodlivých kódů. Praxe však ukazuje jasně, že pro běžného uživatele je toto sotva dosažitelná meta. Na tahu jsou tedy architekti použitých aplikací, kteří musí používat metody, jež nejsou pro útočníky píšící škodlivé programy tak „na ráně“ jako například klasická hesla.

Pragmatický přehled autentizačních metod počínaje právě (kvazi)statickými hesly a konče schématy z oblasti asymetrické kryptografie je možné najít v [3]. Asymetrické metody jsou z čistě bezpečnostního hlediska ideální, neboť počítají i s takovými útoky, které zatím příliš běžné nejsou, avšak které na sebe nejspíš nedají dlouho čekat. Za všechny jmenujme nepopiratelnost samotného přihlášení. Představme si, že klient se přihlásí do internetového bankovnictví, kde zadá platební příkaz. Po čase však přijde do banky s reklamací, že žádný takový příkaz nedal a že to celé je útokem ze strany neznámého pachatele na straně banky. Při použití asymetrických technik je v takové situaci argumentace banky podstatně usnadněna tím, že z detailního záznamu přihlášení je zřejmá spolupráce někoho, kdo znal příslušný soukromý klíč, což přinejmenším odvrací podezření jinam. Matematicky jde o to, že v pořízeném záznamu jsou zaznamenány jisté číselné hodnoty splňující určité algebraické vztahy, u kterých se předpokládá, že bez znalosti hodnoty soukromého klíče je nalezení jejich řešení nezvládnutelná úloha.

Nevýhodou asymetrických technik je výpočetní náročnost použitých operací, která může být ještě dnes pro řadu jednoúčelových zařízení, čipových karet (zejména bezkontaktních) a programových platforem omezující. Ne vždy je ovšem nutné zcela kapitulovat a vzdát se všech užitečných vlastností asymetrických schémat. Jistý kompromis mezi výpočetní náročností a bezpečností nabízí Lamportovo schéma [2] založené na jednosměrných funkcích. Na těch jsou ostatně založeny i asymetrické protokoly, takže intuitivně není překvapující, že Lamportovo schéma je jim v řadě věcí podobné (zejména pokud jde o nepopiratelnost). Přitom je zde pro nás důležitá toliko samotná jednosměrnost, o vlastnosti operace skládání se už například zajímat nemusíme. Vystačíme si tak s podstatně jednodušší podobou těchto funkcí.

Popis protokolu

Systematicky vzato je Lamportovo schéma protokolem jednorázových hesel. Na rozdíl od běžných metod tohoto druhu zde ovšem ověřující strana není schopna dopočítat následující jednorázové heslo, dokud jí ho přihlašující se uživatel sám nesdělí. Přitom ho ale dokáže bezpečně ověřit. Označme h nějakou jednosměrnou funkci. Pro jednoduchost výkladu předpokládejme, že h: $\{0,1\}^n \rightarrow \{0,1\}^n$, kde $n \geq 128$. V praxi můžeme ke konstrukci h použít například kryptografickou hašovací funkci, u které nebyla vlastnost jednosměrnosti dosud oslabena. Můžeme použít i jiné vhodné schéma založené třeba na blokových šifrách. Za všechny předveďme například základ Davies-Meyerovy metody [3]: Buď E_K(x) šifrovací transformace blokové šifry (například AES se 128b klíčem K). Potom můžeme položit $h(w) = E_w$(IV), kde IV je nějaký konstantní, veřejný inicializační vektor (například identifikátor uživatele).



Obr. 1 Posloupnost jednorázových hesel v Lamportově protokolu

Při inicializaci Lamportova schématu si uživatel zvolí tajnou náhodnou hodnotu, kterou označíme jako w_r, kde r je celé kladné číslo udávající počet jednorázových hesel v jedné instanci protokolu. Prakticky to znamená, že po nejvýše r přihlášeních bude muset dojít k nové inicializaci protokolu. Čím vyšší r zvolíme, tím složitější bude inicializační a přihlašovací procedura (viz dále). Proti tomu stojí požadavek, aby inicializace nemusela probíhat příliš často. Na základě konkrétního účelu použití pak zvolíme prakticky přijatelný kompromis. Podotkněme, že při opakovaných inicializacích již není nutná speciální spolupráce ze strany uživatele, zejména tedy osobní návštěva u ověřující protistrany. Dokud nejsou vyčerpána hesla pro bezpečné přihlášení, je možné plynule navázat automatickou registrací nové instance (sady hesel) přes internet, atp. Nyní uživatel podle rekurzivního vzorce $w_i = h(w_{i+1})$ postupně pro $i = r–1, r–2,.., 0$ odvodí z w_r hodnotu w_0. Provede tedy r enumerací funkce h. Hodnotu w_0 si nechá registrovat u ověřující protistrany. Je to v podstatě obdoba jeho veřejného klíče v asymetrických metodách. Obdobou klíče soukromého je pak hodnota w_r, kterou si uživatel musí chránit, respektive chrání ji technická opatření na jeho straně. Označme i index naposled použitého přihlašovacího hesla z posloupnosti $(w_0, w_1, \ldots, w_r)$. Iniciálně nastavíme $i = 0$. Při přihlášení uživatel podle výše uvedeného vzorce ze svého soukromého klíče w_r vypočte w_j pro nějaké $j > i$. Provede tedy $r – j$ výpočtů hodnoty h. Dvojici (j, w_j) odešle protistraně k ověření. Ta zkontroluje, zda skutečně platí $j > i$ a zároveň $w_i = h^{j-i}(w_j)$, kde jsme použili jen jiné označení pro již zavedenou rekurzi: $h^a(w) = h(h^{a-1}(w))$, $h^0(w) = w$. Při ověřování je tedy provedeno $j – i$ výpočtů hodnoty funkce h. Pokud kontroly souhlasí, je autentizace považována za úspěšnou a obě strany si nastaví $i = j$. Vidíme, že pokusům o výpočet následujících hesel v posloupnosti ať už ověřující stranou nebo někým, kdo spojení odposlouchává, brání právě vlastnost jednosměrnosti použité funkce h. Ilustraci podává *obr. 1*. Vynechali jsme některé implementační detaily jako solení hesel, provedení výzvy protistrany, časově omezená hesla, atp. Ty však už není složité na kostru představeného protokolu přisadit (viz např. [1]).

Závěr

Lamportův protokol představuje z teoretického i praktického hlediska zajímavou alternativu k běžným přihlašovacím metodám. Nároky se podobá spíše symetrickým schématům, avšak nabízí přitom hlavní výhody schémat asymetrických.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Haller, N., Metz, C.: A One-Time Password System (RFC 1938), 1996

[2] Lamport, L.: Password Authentication with Insecure Communication, Comm. of the ACM 24, 770–772, 1981

[3] Menezes, A. J., van Oorschot, P. C., Vanstone, S. A.: Handbook of Applied Cryptography, CRC Press, 1996