klimarossa_M 18.8.2006 9:17 Stránka 15

S hesly nově!

Pravidla se mění

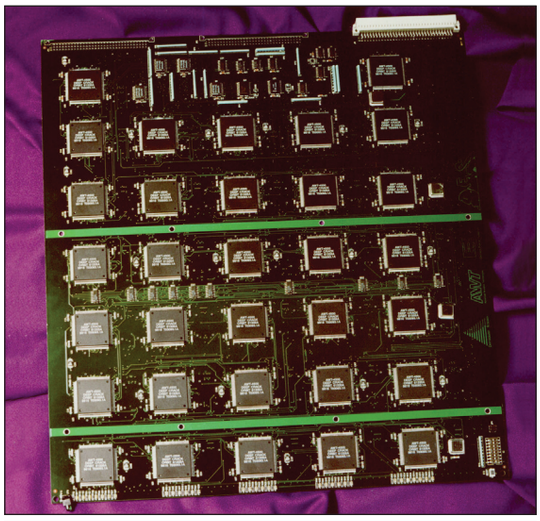
V posledních dvou letech dochází v odborné komunitě ke změně postoje vůči heslům. Na jedné straně přibývá aplikací, které chtějí po uživatelích hesla, na druhé straně se pedantsky kontroluje kvalita a délka hesel a nepřipustí se staré ani nekvalitní (krátké, strukturované, atp.) heslo. Umění volby a používání hesel se stává součástí počítačové gramotnosti. Nedávno vyšla dokonce v pořadí už několikátá kniha o heslech [1] pojednávající o jejich kvalitě, délce, tvorbě, pamatování a podobně. Také bylo provedeno několik nových průzkumů toho, jak lidé volí hesla a jak si jich považují. Při jednom průzkumu bylo možné za prozrazení hesla získat tabulku čokolády, při jiném propisovačku. Rozdalo se hodně čokolády a propisovaček a díky tomu se získalo hodně statistických údajů. Jedním z výsledků bylo, že hesla jsou stále slabá! V tomto a následujících dílech se proto na hesla zaměříme trochu víc. Nebudeme se pouštět do teoreticky zaměřených studií, ale budeme se věnovat odlehčenému, esejovému pojednání vybraného tématu.

Jak žít s množinou hesel

Zajímavé je, že všechny rady i celá kniha o heslech směřují k tomu, jak zvolit jedno heslo, resp. několik hesel. Zatím jsme se však nesetkali s radami a návody jak tvořit a pamatovat si systém hesel, například systém cca deseti hesel, z nichž některá se čas od času mění. Tahle úloha většinou řešena není, a přesto je to přesně ta úloha, kterou v životě potřebujeme řešit.

Vtip je v tom, že každý, kdo vymyslí nějaký systém tvorby hesel, většinou ví, že kdyby ho prozradil, budou všechna jeho hesla oslabena. To je ostatně dáno už principem takového systému, který informační složitost uhodnutí hesla do určité míry kompenzuje složitostí vyznat se v onom cizím systému, nebo chcete-li v cizím způsobu uvažování. Například jeden šéf nám přidělil pro šifrovanou komunikaci s ním heslo JLvk205101. Když jsme potřebovali rozšifrovat soubory pro jiné kolegy, stačilo jen vědět, jak se jmenují a jaké mají číslo dveří. Šéf měl prostě na nástěnce před sebou seznam podřízených a čísla jejich kanceláří. Z iniciál jmen a čísel dveří pak sestavoval hesla. To je pochopitelně krátkozraké a vzniklý systém trpí z analytického hlediska závažnou slabinou, neboť ze znalosti svého hesla mohl každý snadno odvodit použitý systém a potažmo s ním hesla svých kolegů.

Všimněme si, že se zde setkáváme s pojmy dobře známými z teoretické kryptografie (paradigma výpočetní složitosti, útok se znalostí šifrového textu, atp.), jen je nyní aplikujeme na něco, co je dál od počítačů a blíž k lidem. Podobně při příchodu do nového zaměstnání jsme dostali vstupní heslo do lokální sítě, které znělo jouda123. S „joudou" se šlo přihlásit za mnoho zaměstnanců po dobu několika let. Známe mnoho lidí, kteří mají podob-



Pro luštění hesel existují už specializovaná zařízení

né systémy tvorby hesel. Dobrých systémů je jak šafránu a špatné se nevyplatí prozrazovat. To je důvod, proč nenajdeme mnoho popisů takových systémů. Dále se v poslední době setkáváme se změnou přístupu k tvorbě a ukládání hesel. Uznává se, že hesla je nutno tvořit kvalitně, nejlépe náhodně, ale že pro běžného smrtelníka není možné si takových hesel pamatovat deset a více a ještě je čas od času měnit. Proto se již připouští, že hesla je možné si psát na papírek, ukládat do mobilního telefonu, do kapesního počítače nebo do šifrovaných souborů na PC pomocí různých programů na ochranu hesel. My se k myšlence – donedávna totálně kacířské – **psaní hesel na papírek** stavíme tak, že to **je přípustné**. Zásadou je, že každý by si měl vybrat tu metodu, která je pro něj nejvhodnější a u které může zajistit maximální ochranu seznamu hesel. U někoho je to diář, u jiného mobilní telefon, někdo nedá z ruky PDA. Další zásadou je být připraven na situaci, kdy dojde buď ke ztrátě, zničení nebo ke krádeži tohoto seznamu. Jednou k tomu dojde, taková je realita. Proto je nutné mít seznam zálohován, abychom v takovém případě mohli hesla ještě pomocí starých hodnot změnit na nová. Rozhodně s tím počítejte.

Neprozradit systém

V případě, že přece jen máte svůj systém tvorby hesel, nesmíte ho prozradit, viz úvahy uvedené výše. Dále by měl být systém tvořen tak, aby nebyl prozrazen, i kdyby z něho někdo získal skupinu několika hesel. V různých aplikacích jsou totiž hesla chráněna různě kvalitně a jen poměrně malá část reálných výpočetních prostředí přístup k vašemu heslu neumožní. Proto další zásadou je odlišovat tvorbu hesel pro případy, kdy příliš nevěříme poskytovateli příslušných služeb nebo kdy chráněný zájem není tak důležitý, od případů, kdy jde o bankovní a jiné důležité zájmy. Prozrazení hesel z méně důležitého systému nesmí vést k prozrazení nebo oslabení hesel v systému důležitějším. Ideální situace je ta, kdy všechna hesla volíme náhodná. Taková hesla si pak zapíšeme do svého seznamu a uložíme. Seznam těchto náhodných hesel pak chráníme pomocí kvalitního superhesla.

Co to je kvalitní heslo

Několikrát jsme použili pojem kvalitní heslo. Kvalitní heslo je co nejvíce nepredikovatelné. To odráží všechny jeho potřebné vlastnosti. Případný útočník, nemaje možnost predikce, musí zkoušet velmi mnoho jeho možností. A kvalitní heslo musí mít takové množství možností, které nelze vyzkoušet žádnými dostupnými prostředky. O nepredikovatelnosti a kvalitě hesel ještě pojednáme podrobněji.

Závěr

Nárůst počtu hesel mění i pohled na jejich ochranu. Bez jejich zaznamenání bychom už mnohdy nebyli schopni si je pamatovat. Jakmile si vytvoříme půdu pro chráněný seznam hesel, můžeme hesla tvořit zcela náhodně, a tudíž velmi kvalitně. Naše starost se pak přesouvá na zapamatování si jednoho kvalitního hesla (superhesla), které chrání tento seznam, a na zálohování a ochranu tohoto seznamu. Kromě toho můžeme mít jedno nebo dvě další superhesla pro nejdůležitější aplikace. V příštím dílu budeme pokračovat zásadami pro tvorbu superhesel.

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

LITERATURA

[1] Burnett, M., Kleiman, D.: Perfect Passwords – Selection, Protection, Authentication, Syngress Publishing, USA, 2006.

[2] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz