Ukázka z kapitoly *4. Klíče a hesla*

Hesla

S výše uvedenou zásadou Augusta Kerckhoffa, věnovanou vytváření klíčů, jsme se neztotožnili, protože jsme popisovali vytváření klíčů pro moderní šifrové systémy, které musí odolat těm nejsložitějším kryptoanalytickým útokům a využití nejmodernější výpočetní techniky a její obrovské síle. V době Augusta Kerckhoffa byla situace přece jen výrazně odlišná. Kerckhoff se zabýval především polními vojenskými šiframi, které byly ruční a byly masově nasazeny a klíčové hospodářství z tohoto důvodu muselo být velmi jednoduché. Výpočetní technika dnešního typu samozřejmě ještě neexistovala takže možnosti kryptologa, byly z hlediska využití útoku založeném na testování klíčů omezené. Důležité tehdy bylo především to, aby vojáci vytvářeli klíče k šifrám kvalitní, dostatečně dlouhé, ale současně si je zapamatovali a nemuseli si je někde zaznamenávat, což by mohlo vést k jejich vyzrazení. Podmínky při práci s těmito klíči připomínaly dnešní situaci, kdy zadáváte přístupová hesla k různým systémům a aplikacím. Na jedné straně by to měla být hesla odolná útoku hrubou silou (dostatečně dlouhá a dostatečně „náhodná“), na druhou stranu si je musíte zapamatovat, abyste si je nemuseli zaznamenávat, což může jednak vést k jejich kompromitaci a jednak k tomu, že když je potřebujete, nejste schopni se k záznamu dostat a heslo použít.

Správci systémů a aplikací vám často předepisují určitou politiku, kterou musíte při zadání hesla splnit. Např. se předepisuje délka hesla, hlídá se současné použití malých a velkých písmen a případně využití číslic či dalších speciálních znaků. Jste upozorněni, že v hesle by nemělo být obsaženo vaše jméno, jména vašich známých, jste nuceni hesla pravidelně obměňovat apod. I přes tato doporučení a kontrolu je běžné, že hesla nejsou kvalitní a jsou nejslabším článkem daného systému. Připočteme-li k tomu neprofesionální chování uživatelů jako např. prozrazení hesla sekretářce, heslo napsané na papírku nad monitorem, použití stejného hesla ke všem systémům, ponechání defaultního (předdefinovaného) hesla, při vynucené změně jen nepatrné a odvoditelné pozměnění (např. doplnění číslice za heslem), neopatrné zadávání hesla před svědky apod., je pak právě „heslo“ tou vstupní branou, kterou hacker projde do jinak bezpečného systému či aplikace.

Jak tedy správně postupovat při vytváření vhodného hesla? Jedna z nejstarších rad, která se k tomuto tématu vztahuje, je v knize Řeka Aineia Taktika *Obrana opevněných míst* ze 4. st.

př. n. l., kde autor radí římským vojákům vydávat hesla do stráže snadná pro zapamatování a svým významem co možná nejbližší zamýšlené akci. Je vidět, že bylo v tomto případě preferováno hledisko „pamatovatelnosti“ oproti hledisku kvality hesla. Důležité také je, že v případě hádání hesla před strážní hlídkou se útok hrubou silou (zkoušení různých hesel) použít nedá. To bychom asi dopadli velmi špatně. Kvalita hesla je tedy přímo závislá i na okolnostech použití. Obdobně se dá proto v případě bankovní čipové karty použít PIN (heslo) pouze v délce 4 číslic – služba je totiž po stanoveném počtu pokusů odmítnuta a karta zablokována.

Existuje řada různých systémů a situací, které vyžadují zadání hesla, a podle konkrétní situace je nutné klást důraz na různé aspekty hesla. V současné době se při stanovení požadavků na profesionální heslové systémy vychází nejčastěji z dokumentu *Příručka pro řízení správy hesel* (Password Management Guidelines), který byl vydán před dvaceti lety v USA (Department of Defense, April 1985).

Obecně stačí, když si zapamatujeme následující zásady pro běžné užívání hesel:

- délka hesla nejméně 8 znaků (znaky, pokud je to možné, vybírat z celé typové nabídky, tj. využívat velká a malá písmena, číslice, specifické znaky)
- heslo má být uživatelem snadno zapamatovatelné, má se dát snadno a rychle napsat, ale nelze je nepovolanou osobou uhádnout
- heslo nikdy nikomu neprozraďte
- heslo nikdy nikam nezapisujte a neukládejte
- pro různé systémy používejte různá hesla
- heslo měňte (přibližně za čtvrt až půl roku).