Na pohádky s vtipem, na bezpečnost s čipem!

Václav Lorenc, ÚVT MU

Laskavý čtenář promine, ale dnešní příspěvek o bezpečnější autentizaci začneme poněkud netradičně, pohádkovým vstupem.

Bylo, nebylo...

V učebnicích a skriptech o počítačové bezpečnosti je možné najít tři základní způsoby prokázání identity jedince. Zkusme se tedy společně podívat na konkrétní případy a zmínit si jejich výhody, nevýhody a případná možná vylepšení.

Popořadě tedy – prokázat svoji identitu mohu něčím (a) co znám, (b) co mám, (c) čím jsem. Zabrouzdejme tedy do zmiňovaného pohádkového světa a pokusme se podpořit stručný výčet vhodnými ilustracemi.

Velice pěkný příklad něčeho, *co známe*, jsou hesla, v pohádkách známá již přinejmenším tisíc a jednu noc. Vzpomeňme na Alibabu a jeho pohádkovou jeskyni plnou pokladů. Přístup k ní nebyl chráněn ničím jiným, než právě heslem. A to ne zrovna slabým – „Sezame, otevři se". Heslo to není triviální, nedostatečně dlouhé, ba dokonce i vůči slovníkovému útoku tehdejší doby by jistě obstálo.

Příběh sám nám však dává odpověď na otázku, má-li tento způsob přihlašování slabiny. Bohatě totiž postačí, když si dotyčné heslo někdo poslechne, a jeho prostým zopakováním se dostane do zabezpečené jeskyně. Samotná hesla tedy moc bezpečí nepřinesou, nezdaří-li se je vhodně ochránit.

Prokazování se něčím, *co mám*, je trochu větší oříšek. Často k tomuto účelu slouží tzv. tokeny, tedy klíče nebo královské pečeti, rozličné šátky, prsteny, královští koně a nebo dostatečně vznosné oblečení. Ostatně rozlišit lháře od pravého zachránce se na královské hostině zadaří právě pomocí prstenu, který statečný kovář Mikeš dostal od princezny při jejím zachraňování (tábor příznivců Bajaji si vzpomene na podobnou situaci, kde však hrál hlavní roli šátek).

I tato metoda má však svoje nedostatky. Jak například postupovat v případě krádeže? Jak zabezpečit, aby dotyčná věc byla natolik jedinečná, aby nešla zfalšovat? Vždyť nejedna pohádka dokonce začíná touto premisou, kdy důkaz původu získá nesprávná osoba. Je tedy často nutné obezřetně volit, co použijeme v roli tokenu.

Nu a třetím případem, moderně zvaným biometriky, je autentizace něčím, *co jsme*, nějakou vlastností, kterou si neseme stále s sebou. I tento způsob není v pohádkách nikterak neobvyklý. „Šaty s vlečkou, stříbrem vyšívané, ale princezna to není, jasný pane." Vzpomínáte? Vměstnat se do miniaturního střevíčku dokázala z celého království pouze jediná slečna, byť měla tváře od popela umazané. A právě neobvykle malá velikost Popelčiny nohy je v tomto případě onou biometrikou.

Najít však dostatečně charakteristický znak pro každou pohádkovou bytost by bylo více než obtížné. A to ani nezvažujeme nutnost nejen získat, ale i uchovat střevíc každé osoby v království, pokud bychom tuto metodu chtěli použít plošně.

Současně vyvstává i poměrně přirozená otázka – je možné jednotlivé metody kombinovat? Ale dozajista! Takový přístup je velice důležitý pro zvýšení bezpečnosti celého řešení. Ostatně i tady máme velice pěkný příklad. Tři kůzlátka, zavřená v domečku, se snaží odhalit, je-li osoba za dveřmi jejich maminka, nebo zlý a hladový vlk. Vlk, pamětliv Alibaby, odposlechne heslo a okamžitě zkouší, bude-li fráze „Kůzlátka, kůzlátka, otevřete vrátka..." dostatečným oprávněním ke vstupu. Ale ouha, je třeba navíc prokázat, že i hlásek má vlk natolik tenounký, aby zněl stejně jak maminka koza.

V království plném bitů...

V tuto chvíli však opustíme pohádkový svět a vrhneme se do vod kruté digitální reality, v němž je magie v mnohém nahrazena matematikou a fyzikou.

Na výše uvedených příkladech je vidno, že ačkoliv se jednotlivé metody dají samy o sobě poněkud vylepšit, jejich kombinace se prokazují jako

mnohem odolnější vůči útokům. Zkusme si ukázat i příklady bezpečnější autentizace v běžném životě.

Typickým případem je přihlašování se k počítači. Je již zažitým zvykem používat pro takovou situaci kombinaci jména a hesla, v lepším případě s nějakou politikou změny hesla, jeho minimální délky či odhadované odolnosti vůči slovníkovému útoku.

Navíc není neobvyklé, že mnoho lidí mívá přístup do různých systémů. Jedno heslo pak používá pro přihlášení se ke svému osobnímu počítači, jiné pro přístup k e-mailu, další pak pro přístup k elektronickému bankovnictví či k účetnímu programu. V lepším případě jsou tato hesla různá a nadprůměrně kvalitní, v horším to končívá jedním jednoduchým a snadno zapamatovatelným heslem, které je ke všemu napsané na papírku u monitoru.

Celá situace se ještě trochu zamotá, přidáme-li digitální identitu člověka a s ní související elektronický podpis. Pamatovat si odpovídající podepisovací klíče, reprezentované několika tisíci jedniček a nul, již opravdu není v silách běžného uživatele, proto bývají uloženy někde na disku. A právě obrana elektronické identity by měla být prioritou - nikdo by nebyl rád, kdyby se jeho jménem páchaly digitální zločiny.

Zatímco u klasických klíčů je jejich krádež a kopírování přinejmenším zjistitelné, neb je bude jejich majitel po nějakou dobu pohřešovat, u digitálních je situace mnohem horší. Pořídit digitální kopii dat je možné nepozorovaně a s téměř nulovými náklady, v případě klíčů pak i velice rychle.

Ideální úložiště důvěrných dat (klíčů) by tedy mělo být takové, které by umělo chránit libovolná data do něj vložená, a v případě nutnosti provádět nad těmito daty požadované kryptografické operace tak, aby uchovávané tajemství žádným způsobem toto úložiště neopustilo. Ačkoliv to zní jako úkol pro chytrou horákyni, taková zařízení existují.

Jsou jimi kryptografické čipy. Běžněji se s nimi potkáte v nově vydávaných platebních kartách, kde nahrazují funkci nepříliš důvěryhodného magnetického proužku, v dobách předmobilních se s nimi mnoho lidí potkávalo v předplacených telefonních kartách, dnes v podobě SIM karet, v bezkontaktní podobě i v nedávno zavedených elektronických kartách Českých drah.

Pro potřeby bezpečného přihlašování a podepisování dat na počítači existují speciální USB zařízení, která právě takovou funkci poskytují. Obsahují kryptografický čip s bezpečným úložištěm dat, jejich podpora v operačních systémech se různí, ale zlepšuje se, a zejména jsou to zařízení natolik přenosná, že jejich nošení u klasických klíčů od bytu či auta nečiní problémy. A ač se taková zařízení často neliší vzhledem, liší se právě svým obsahem, tedy klíči na nich uloženými. Jedná se tedy o variantu tokenu.

Pozorní čtenáři si jistě uvědomili, že spousta z výše jmenovaných zařízení, neposkytuje své funkce každému na potkání. Stejně jako byl Golem spouštěn svým šémem, kryptografické čipy často požadují autentizaci uživatele předtím, než začnou pracovat. Ta se děje nejčastěji za pomoci tzv. PINu, tedy nějakého číselného kódu rozumné délky.

Tím jsme se v pohádkovém i reálném světě dostali ke stejnému poznatku – kombinaci více faktorů při prokazování identity uživatele. Nikoliv však hláskem a heslem, ale v tomto případě PINem a odpovídajícím USB tokenem. Potenciální zákeřný lupič tak musí nejen ukořistit přístupový PIN, ale i token samotný, což mu rozhodně lup neusnadní.

Bylo by příjemné říci, že jsme se tímto dostali k nejvyspělejší technologii bez jakýchkoliv chyb, nebyla by to však pravda. Právě masivnější rozšíření kryptografických USB tokenů ukazuje, že ač je míra jimi poskytované bezpečnosti obvykle opravdu vyšší, je stále řada nedořešených otázek. V prostředí úkolů řešených ve spolupráci s Masarykovou univerzitou jsou to např. projekty Medimed a provázané gridové aplikace. Objevuje se potřeba důvěryhodných vstupů a výstupů tak, aby bylo zařízení schopno pracovat i v nedůvěryhodném prostředí, tedy obchodech, internetových kavárnách nebo učebnách. Tedy i v takových situacích, kdy je samotný počítač napadený virem nebo pod kontrolou útočníka, a přesto by bylo vhodné nějakým způsobem zabránit úniku důvěrných informací.

To jsou témata, nad kterými v současnosti probíhá výzkumná práce a objevují se prototypy nových zařízení. Doba prostých hesel však již pomalu končí a je třeba se dívat do budoucnosti, se všemi jejími klady i zápory.

Zazvonil zvonec…

Pohádkou jsme začali, pohádkou skončíme. Vždyť i bájné království, které se snažilo předejít strašlivé sudbě, nakonec neuspělo pro jednu jedinou růži či kolovrátek. A že jim odstranění problému trvalo sto let? Budiž to pro nás poučením – každý řetěz je jen tak silný, jak silný je jeho nejslabší článek… □