Autentizace a identifikace uživatelů

Jan Krhovják, Václav Matyáš, FI MU

Asi každý kdo se pohybuje v prostředí Internetu již někdy slyšel pojmy jako *autentizace* či *identifikace uživatelů*. My se v tomto příspěvku zaměříme na základní metody autentizace/identifikace uživatelů a jejich vlastnosti. Částečně budeme vycházet z [1]) a volně navážeme na článek „Na pohádky s vtipem, na bezpečnost s čipem!" publikovaný v červnovém čísle Zpravodaje.

1 Základní přístupy a jejich vlastnosti

Připomeňme si na úvod, že autentizační metody mohou být založené buď na něčem co *daný uživatel zná*, něčem co *daný uživatel má*, nebo něčem čím *daný uživatel je*. Typickým příkladem metod spadajících do první z těchto kategorií je nějaké tajemství, jako například PIN, heslo či přístupová fráze. Do kategorie druhé lze zařadit různé fyzické objekty, mezi něž patří například platební karta. A konečně, do kategorie třetí pak spadají různé charakteristiky daného jedince, jejichž typickým příkladem je otisk prstu. Všechny tyto metody ale mají svá pro a proti.

Výhodou „něčeho co daný uživatel zná" je, že se nejedná o fyzický objekt, ale o abstraktní znalost, kterou lze snadno přenášet, zadávat do počítače. Systém pro tuto metodu autentizace lze snadno ovládat a nevyžaduje složitou údržbu. Nevýhodou pak je, že tajná informace může být snadno zjištěna, a to dokonce bez vědomí uživatele. Navíc lidská paměť je s ohledem na zapamatování „náhodných" informací poměrně omezená (složitá hesla si lze jen velmi obtížně zapamatovat), což negativně ovlivňuje celkovou bezpečnost této autentizační metody.

Oproti tomu „něco co daný uživatel má" je fyzický objekt – v tomto kontextu často označován jako *token*. Výhodou tokenu je, že ho lze jen velmi obtížně zkopírovat, jeho ztráta je snadno zjistitelná, a je schopen uchovávat a především pak i často zpracovávat náhodné informace s velkou entropií (míra informace). Nevýhodou pak je, že různé typy tokenů nejsou vzájemně kompatibilní a mohou být z hlediska fyzického provedení značně složité (aby je nebylo možné snadno zkopírovat). K jeho použití musí také existovat příslušná čtecí zařízení, což zvyšuje náklady při zavádění systému do praxe. Dalším negativem je, že uživatel nemůže být bez tokenu rozpoznán a vytvoření náhradního předmětu (např. po ztrátě) je časově i procedurálně náročné (což z hlediska uživatele není příliš pohodlné). Token se navíc může porouchat, a to je samo o sobě před vlastním pokusem o autentizaci jen velmi obtížně zjistitelné.

Zcela odlišným přístupem je využití „něčeho čím daný uživatel je", tj. nějaké automatizovaně hodnotitelné biologické informace – tzv. *biometriky*. Typicky se jedná o část těla, či určitou charakteristiku osoby. Výhodou těchto autentizačních metod je, že biometriky nelze zapomenout či ztratit. Nevýhodou pak je, že biometrické informace jsou jen velmi obtížně měřitelné (značně ale závisí na tom, co je měřeno) a právě přesnost měření výrazně ovlivňuje celkovou bezpečnost mnoha biometrických systémů.

Aby se při současném zachování výhod těchto metod co možná nejvíce eliminovaly jejich nevýhody, je častým řešením jejich vhodná vzájemná kombinace. Použití metod ze dvou výše uvedených skupin se pak označuje jako *dvoufaktorová autentizace* a použití metod ze všech tří skupin jako *třífaktorová autentizace*. V současné době se nejčastěji používá dvoufaktorová autentizace a jejím nejběžnějším příkladem je personalizace mobilního telefonu pomocí SIM karty (token), jejíž obsah, resp. přístup k němu, je chráněn přístupovým PINem (tajemství).

Procesem následujícím obvykle po autentizaci uživatele je *autorizace uživatele* – tj. přiřazení oprávnění (na základě identity a bezpečnostní politiky) pro práci v systému a specifikace co daný uživatel může, příp. nemůže.

Ověřovat však můžeme nejen identitu uživatelů, ale i původ dat – pak mluvíme o tzv. *autentizaci dat*. V tomto případě ověřujeme, že data jsou autentická, tj. že známe autora či odesílatele daných dat. Autentizace dat do značné míry souvisí s ověřováním integrity. Obvykle je ověření integrity zprávy jedním z kroků, který je třeba udělat, abychom dokázali autentičnost dat či zprávy a tím určili autora nebo odesílatele.

1.1 Hesla a PINy

Autentizace pomocí hesla je nejjednodušším způsobem autentizace v současné době. Přesto, nebo právě proto, je používána ve velkém množství aplikací. Jako příklad můžeme uvést SMTP, POP3 a IMAP protokoly pro připojování k e-mailovým serverům, ICQ pro komunikaci přes Internet, apod. Protokol spočívá v tom, že Alice prostě pošle Bobovi heslo. Bob má někde v databázi uložena hesla všech svých komunikačních partnerů a po příjmu hesla si najde příslušný záznam patřící Alici a porovná zaslané heslo s kopií ve svém záznamu.

Heslo typicky bývá řetězec dlouhý 6–10 znaků, v ideálním případě netriviální (odolný proti možnému slovníkovému útoku, či útoku hrubou silou), ale uživatelem snadno zapamatovatelný. Uživatel předkládá systému heslo (sdílené tajemství) společně se svou identifikací – *uživatelským jménem (loginem)*. Systém tyto autentizační údaje kontroluje s daty uloženými k danému uživateli. Prokázání znalosti tajemství je vyhodnoceno systémem jako korektní prokázání identity.

Běžní uživatelé si většinou nejsou vědomi (ne)bezpečnosti, kterou jejich hesla reprezentují. Dnešní systémy spravující hesla proto umožňují kontrolu bezpečnosti vkládaných hesel (včetně populárních indikátorů vhodnosti), příp. uživateli vygenerují heslo s požadovanými parametry. Požadavky kladené na tato hesla jsou pak součástí bezpečnostních politik systému. Stinnou stránkou tohoto přístupu ale je, že uživatel si heslo bude obtížněji pamatovat a často zapomínat.

Jako bezpečné heslo (jakkoliv je pojem relativní) lze považovat to, jehož prolomení obvyklými technikami je časově náročné. Typicky se jedná o řetězec s délkou 8–12 znaků, který obsahuje znaky z více různých skupin – malá i velká písmena, číslice, další tisknutelné znaky – a zároveň není v dostupných slovnících. Doporučovaným způsobem pro zvyšování bezpečnosti hesla je zvětšování základní množiny znaků před prodlužováním.

PINy poskytují jinou možnost posílení bezpečnosti. V tomto případě omezujeme počet pokusů, které máme k dispozici pro uhádnutí hodnoty PINu. Pokud se v daném počtu pokusů netrefíme, tak systém PIN zablokuje a je nutné použít nějaký složitější mechanizmus na odblokování PINu a tím vynulování počtu chybných pokusů. Tímto druhým mechanizmem může být mnohem delší PIN (někdy označován jako PUK), nebo např. osobní kontakt se zákaznickým centrem, které bude vyžadovat předložení např. identifikačních dokladů před tím, než bude PIN odblokován.

Díky tomuto omezení je možné značně zjednodušit formu a délku PINu v porovnání s heslem. Obvyklý PIN je složen pouze z číslic a jeho délka bývá 4–8 znaků. V mnoha případech si uživatelé mohou PIN sami měnit podle potřeby. U nás je to obvyklé např. u mobilních telefonů, v jiných zemích je možné měnit PIN i pro platební karty.

Bohužel, mechanizmus omezení počtu pokusů není vhodné obecně použít pro hesla (zejména pak, je-li login veřejně známý či snadno odvoditelný), protože by reálně hrozil útok odmítnutí služby. Jestliže by vám chtěl někdo znemožnit přístup do systému, prostě by několikrát zadal správné stejné jméno a chybné heslo.

Nutným předpokladem pro fungování tohoto mechanizmu je však nutnost fyzického vlastnictví autentizačního předmětu (tokenu), jedná se vlastně tedy o tzv. dvoufaktorovou autentizaci. Bez vlastnictví autentizačního předmětu pak není možné PIN vůbec zadat. Tímto předmětem může být mobilní telefon, SIM karta, nebo kreditní karta.

1.2 Autentizační tokeny

Tokeny jsou, zjednodušeně řečeno, zařízení, která mohou uživatelé nosit neustále s sebou a jejichž vlastnictví je nutné pro to, aby se mohli autentizovat do systému. Mají buď specifické fyzické vlastnosti (tvar, elektrický odpor, elektrickou kapacitu, ...), nebo obsahují specifické tajné informace (např. kvalitní heslo nebo kryptografický klíč), nebo jsou dokonce schopny provádět specifické (obvykle kryptografické) výpočty.

Asi nejčastějším autentizačním tokenem současnosti jsou karty. Můžeme je dělit na několik typů – typicky podle jejich obsahu a schopností. Úplně

nejjednodušší jsou karty s magnetickým proužkem (obsahují obvykle neměnnou informaci, kterou lze ale kdykoliv přepsat), složitějšími a dražšími jsou čipové karty (dokáží provádět nad uloženými/zaslanými daty různé operace). Téměř každý, kdo má bankovní účet, tak vlastní alespoň jednu platební kartu. Každý kdo má mobilní telefon, pak vlastní čipovou kartu ve formě SIM karty.

Dalším obvyklým typem tokenu je tzv. *autentizační kalkulátor*. Samotné kalkulátory mohou být založeny buď na tajemství, které je uloženo v kalkulátoru a v autentizačním serveru, nebo na synchronizovaných hodinách. Důležitou vlastností kalkulátorů je způsob komunikace s uživatelem – klasické komunikační rozhraní typicky zahrnuje pouze klávesnici a displej, speciální optická rozhraní či infračervený port umožňují navíc kalkulátoru komunikovat přímo s počítačem.

V posledních letech se poměrně rozšířily také tzv. *USB tokeny*. Pojem „token" zde však byl použit pro zařízení, která v drtivé většině případů neposkytují bezpečné úložiště dat, a jsou tedy pro účely autentizace zcela nevhodná. I zde samozřejmě existují výjimky (specializované USB tokeny), které typicky využívají stejnou technologii jako čipové karty. Cena takového tokenu je ale výrazně vyšší, a množství dat, které dokáží bezpečně uchovat, se už nepohybuje v řádech megabajtů či gigabajtů, ale pouze v řádech kilobajtů.

1.3 Biometriky

Biometrické techniky můžeme použít na dvě rozdílné aplikace: na autentizaci neboli verifikaci identity a na identifikaci. *Autentizace/verifikace* je proces, při kterém subjekt předkládá tvrzení o své identitě (např. vložením karty nebo zadáním identifikátoru) a na základě takto udané identity se srovnávají aktuální biometrické charakteristiky s uloženými charakteristikami, které této identitě odpovídají podle záznamů autentizační databáze. Odpovídáme na otázku: „Je to opravdu ta osoba, za kterou se sama vydává?" Při *identifikaci* (nebo také *vyhledání*) naopak člověk identitu sám nepředkládá, systém prochází všechny (relevantní) záznamy v databázi, aby našel patřičnou shodu a identitu člověka sám rozpoznal. Systém odpovídá na otázku: „Kdo to je?" Je zřejmé, že identifikace je podstatně náročnější proces než verifikace. Se zvyšujícím se rozsahem databáze se přesnost identifikace snižuje a rychlost klesá.

Biometrických technologií existuje mnoho a jsou založeny na *měření fyziologických vlastností* lidského těla (např. otisk prstu nebo geometrie ruky) nebo *chování člověka* (např. dynamika podpisu nebo vzorek hlasu), přičemž se jedná o měření automatizovaným způsobem. Některé technologie jsou teprve ve stádiu vývoje (např. analýza pachů), avšak mnohé technologie jsou již relativně vyzrálé a komerčně dostupné (např. otisky prstů nebo systémy porovnávající vzorek oční duhovky). Systémy založené na fyziologických vlastnostech jsou obvykle spolehlivější a přesnější než systémy založené na chování člověka, protože měření fyziologických vlastností jsou lépe opakovatelná a nejsou ve velké míře ovlivněna daným (psychickým, fyziologickým) stavem jako např. stres nebo nemoc.

Nejvýznamnější rozdíl mezi biometrickými a tradičními technologiemi je odpověď systému na autentizační požadavek. Biometrické systémy nedávají jednoduché odpovědi typu ano/ne. Heslo buďto je „abcd" nebo ne, magnetická karta s číslem účtu „1234" jednoduše je nebo není platná. Podpis člověka však není vždycky naprosto stejný, stejně tak pozice prstu při snímání otisku se může trochu lišit. Biometrický systém proto nemůže určit identitu člověka absolutně, ale místo toho řekne, že s určitou pravděpodobností (vyhovující autentizačním/identifikačním účelům) se jedná o daného jedince.

Mohli bychom samozřejmě vytvořit systém, který by vyžadoval pokaždé téměř 100% shodu biometrických charakteristik. Takový systém by však nebyl prakticky použitelný, neboť naprostá většina uživatelů by byla téměř vždy odmítnuta, protože výsledky měření by byly vždy alespoň trochu rozdílné. Abychom tedy udělali systém prakticky použitelný, musíme povolit určitou variabilitu biometrických charakteristik. Současné biometrické systémy však nejsou bezchybné, a proto čím větší variabilitu povolíme, tím větší

šanci dáváme podvodníkům s podobnými biometrickými charakteristikami.

2 Složitější autentizační schémata

Probíhá-li autentizace uživatele v zabezpečeném výpočetním prostředí, jsou i přenášená *autentizační data* (tajné informace nezbytné pro korektní autentizaci – např. PINy, hesla, šifrovací klíče) v bezpečí. To však neplatí pokud se uživatel autentizuje ke vzdálenému systému. Autentizační data jsou pak totiž přenášena nezabezpečeným prostředím (např. počítačovou sítí, která není pod naší kontrolou) a mohou být snadno odposlechnuta a zneužita pro neoprávněný přístup ke vzdálenému systému. Pouhé hašování (tj. zpracování vhodnou jednosměrnou funkcí) či šifrování autentizačních dat není samo o sobě vhodným řešením – autentizační data sice zůstanou utajena, ale pro neoprávněný přístup k systému stačí příslušný haš (tj. výsledek hašování) či zašifrovaná autentizační data.

Proto se používají složitější autentizační schémata – tzv. *autentizační protokoly* – která umožňují demonstrovat znalost sdíleného tajemství, aniž by během autentizace poskytla případnému útočníkovi (ať již pasivnímu či aktivnímu) jakoukoliv užitečnou informaci využitelnou pro další (neoprávněnou) korektní autentizaci a následný (neoprávněný) přístup k systému. Tyto protokoly jsou většinou budovány s využitím základních kryptografických primitiv (symetrické či asymetrické kryptosystémy, kryptografické hašovací funkce apod.) a pracují na principu výzva-odpověď. Základní myšlenkou tohoto přístupu je ověřování správnosti a čerstvosti (nebyl dříve odposlechnut) autentizačního požadavku. Ten je typicky zaslán jako odpověď na unikátní výzvu, a demonstruje tak znalost nějakého sdíleného tajemství, které je kryptografickými prostředky aplikováno na onu autentizační výzvu. Na tomto principu fungují například mnohé autentizační kalkulátory.

Většina běžně používaných autentizačních protokolů však vyžaduje předem ustavené sdílené tajemství – např. šifrovací klíče. Ty jsou dlouhé řádově stovky bitů a proto bývají na straně uživatelů typicky uloženy na nějakém tokenu. Poměrně efektivním řešením tohoto problému jsou speciálně navržené autentizační protokoly umožňující namísto klíčů použít data s menší entropií – jako například PINy či hesla – která je schopen si uživatel zapamatovat. Tyto protokoly, někdy označované jako *eskalační*, jsou založeny na kombinaci symetrické a asymetrické kryptografie. Oproti běžným autentizačním protokolům umožňují použití hesel aniž by je vystavovaly off-line útokům hrubou silou (tj. také slovníkovým útokům). Tyto eskalační protokoly však zatím pronikají do praxe jen pozvolna. Jsou již ale součástí některých nově vytvářených norem a standardů.

3 Řetězce důvěryhodných autorit

Mnohé v současné době nasazované metody a autentizační protokoly pro ověření autentičnosti dat uložených na tokenu nějakým způsobem využívají prostředků asymetrické kryptografie (kryptosystémy založené na problémech teorie čísel a složitosti). Mezi ně patří např. i systémy pro ověřování nových elektronických (biometrických) pasů, či nových čipových platebních (kreditních i debetních) karet v tzv. *EMV platebních systémech*.

Aby takovéto řešení mohlo v praxi fungovat, je nutné vytvořit *infrastrukturu veřejných klíčů* (PKI – Public Key Infrastructure). Ta je budována pomocí řetězce důvěryhodných autorit, kde každá autorita v řetězci ověří a certifikuje veřejný klíč následující autority . Jelikož je veřejný klíč jednoznačně matematicky svázán s příslušným soukromým klíčem, je takto vytvořen efektivní mechanismus pro ověření totožnosti vlastníků soukromých klíčů pomocí „automatické kontroly" certifikátu v řetězci. Tyto důvěryhodné autority se nazývají *certifikační autority (CA)*. CA jsou uspořádány do hierarchické struktury s jasně definovanými vztahy podřízenosti / nadřazenosti. Průchod takovou strukturou vytváří výše zmíněný řetězec autorit s počátkem v kořeni hierarchické struktury.

V praxi je ale často používán pouze jedno- až tří-úrovňový hierarchický stromový model. *Certifikát* je digitálně podepsaná zpráva sestávající ze dvou hlavních informací: jména vlastníka veřejného klíče a samotného veřejného klíče. Hlavním účelem certifikátu je kryptografické spojení

veřejného klíče a identitou daného subjektu (za korektnost této vazby ručí CA, která certifikát vydala). Více informací lze nalézt v [2].

Certifikační autoritu může zřídit libovolná organizace a výstupy používat pro svou interní potřebu (toho využívají některé velké instituce jako banky či univerzity [3]) nebo v rámci účelového sdružení více institucí, které deklarují vzájemnou důvěru k vydaným klíčům a certifikátům. Subjekt stojící mimo sdružení může ale i nemusí takovéto CA důvěřovat.

Akreditované CA jsou certifikačními autoritami, které prošly akreditačním procesem ze strany státních orgánů (u nás např. První certifikační autorita I.CZ, Česká pošta, eIdentity). Mají proto postavení kvalifikované instituce s obecně uznávanou důvěryhodností a využitím zejména pro orgány státní správy, a také bez omezení pro libovolné nestátní subjekty. Toto postavení akreditované CA můžeme přirovnat k funkci notáře – kdy notářem podepsaná písemnost nebo ověřený podpis občana jsou obecně důvěryhodné pro ostatní instituce a není potřebné dále zpětně zkoumat pravost. Těmto CA se také někdy říká *kvalifikovaná certifikační autorita*.

4 Závěr

Seznámili jsme se se základními pojmy a metodami vztahujícími se k autentizaci a identifikaci uživatelů. Pozorného čtenáře však jistě napadlo, že problematika volby vhodné a bezpečné autentizační (případně identifikační) metody není zdaleka tak snadná, jak by se na první pohled mohlo zdát. Existuje poměrně mnoho různých metod či schémat, a také mnoho možností, jakým způsobem je do systému správně implementovat. V následujícím příspěvku se proto podíváme, jakým způsobem se s tímto problémem vypořádaly různé banky.

Literatura

[1] Matyáš Václav. *Principy a technické aspekty autentizace.* Data Security Management (DSM), roč. 2007, č. 1, ISSN 1211–8737.

[2] D. Kouřil. *Certifikáty veřejných klíčů.* Zpravodaj ÚVT MU. ISSN 1212–0901, 2000, roč. X, č. 4, s. 5–9.

[3] D. Rohleder. *Certifikační autorita Masarykovy univerzity.* Zpravodaj ÚVT MU. ISSN 1212–0901, 2000, roč. X, č. 5, s. 14–18. □