Autentizace a autorizace finančních transakcí

Jan Krhovják, Václav Lorenc, Václav Matyáš, FI a ÚVT MU

Bezhotovostní platby v kamenných obchodech či přes Internet, stejně jako správa osobních účtů a realizace finančních transakcí prostřednictvím různých systémů elektronického bankovnictví, již v dnešní době patří ke každodenním činnostem mnoha z nás. Jakákoliv manipulace s finančními prostředky (a zejména, jedná-li se o vyšší obnosy) je už po staletí považována za velmi citlivou operaci – přitahuje totiž pozornost mnoha jednotlivců či organizovaných skupin hledajících stále nové a nové možnosti, jak se snadno a rychle obohatit na úkor ostatních. Tato individua či skupiny se ještě před několika desítkami let musely spokojit s přepadáváním bank, prováděním loupeží, či různými obchodními podvody. Doba však pokročila, mnohé transakce se už provádějí bezhotovostně elektronicky a mnohé bezpečnostní (zejména kamerové) systémy vystavují kriminálníky poměrně velkému riziku odhalení a následného dopadení.

Na druhou stranu se však ukazuje, že správná a korektní implementace systémů realizujících finanční transakce je poměrně obtížná a přináší s sebou mnohá úskalí. Asi největší pozornost v tomto případě přitahuje právě způsob autentizace a autorizace finančních transakcí. V tomto příspěvku si proto popíšeme základní techniky autentizace a autorizace finančních transakcí používané mnohými bankami, a seznámíme se také s bezpečnostními prvky různých systémů elektronického bankovnictví.

1 Autentizační mechanizmy v praxi

K autorizaci finančních transakcí se v současnosti nejčastěji používá nějaká forma dvoufaktorové autentizace. Výběr konkrétních metod, které jsou k autentizaci používány, však závisí na mnoha okolnostech. Jedna skupina metod se používá v případě výběru peněz z bankomatu, jiné při bezhotovostních platbách u různých obchodníků, či na Internetu, a jiné zase k přístupu do systémů elektronického bankovnictví.

První metodou autentizace je typicky použití tokenu. Tím jsou nejčastěji platební karty s magnetickým proužkem; nebo nověji také čipové (EMV) platební karty. Obojí se používají v případě výběru hotovosti z bankomatu a v případě jednorázových plateb, ať již prováděných v kamenných obchodech nebo přes Internet.

Druhá metoda je pak typicky použití nějaké biometriky či znalosti. Při výběru hotovosti z bankomatu je kromě zákazníkovy platební karty vyžadována i znalost příslušného PINu. Při provádění bezhotovostních plateb na Internetu je kromě čísla virtuální či klasické platební karty (nejčastěji však karty embosované[1]) vyžadováno také ochranné číslo karty – trojčíslí, označováno jako CSC (Card Security Code), CVV (Card Verification Value), CVC (Card Verification Code) apod., které je v podstatě analogií PINu[2].

Při provádění bezhotovostní platby v kamenném obchodě, kdy je karta fyzicky předložena obchodníkovi, je pak kromě platební karty vyžadován vlastnoruční podpis držitele karty nebo PIN. Podle typu autorizační metody může být vyžadován jak PIN, tak i podpis. Která z těchto dvou autentizačních metod je v místě prodeje požadována závisí také na typu (magnetický proužek vs. čip) a druhu (např. MasterCard, VISA, American Express, Discover, ...) platební karty, platebním terminálu a smlouvě, kterou má obchodník uzavřenu s bankou/institucí, která pro něj zprostředkovává platby.

Je-li autentizace úspěšná, následuje ověření velikosti disponibilního zůstatku, a pokud je dostatečný, platba proběhne. Je-li naopak autentizace neúspěšná, lze ji (v závislosti na bezpečnostní politice banky) ještě několikrát zopakovat. Po vyčerpání předem stanoveného počtu pokusů (u bankomatů typicky 3–5) však může dojít k zablokování karty (a u bankomatu navíc též k zadržení karty).

Situace je poněkud odlišná v případě zabezpečení přístupu do systémů elektronického ban-

[1] Karta na níž jsou identifikační údaje vyznačeny reliéfním písmem (tj. vystupují z její plochy).

[2] Mechanismus je navržen tak, že CSC/CVV/CVC slouží pro on-line autorizaci platby a nesmí být (na rozdíl od čísla platební karty) uložen v žádné databázi obchodníka. Tento požadavek však v praxi mnohdy nebývá splněn.

kovnictví a správy bankovních účtů. Zde se k samotnému přístupu do sytému využívá většinou přístupových hesel či frází. Bezpečnější způsob pak zahrnuje použití asymetrické kryptografie (a certifikátů) nebo použití autentizačních kalkulátorů a jim podobných zařízení.

Pokud je již uživatel do systému jednou přihlášen, může s účtem libovolně manipulovat a provádět libovolné pasivní operace. Pro aktivní finanční transakce je v některých případech vyžadována opětovná autentizace/autorizace. Někdy je toto opětovné potvrzení vyžadováno jen tehdy, pokud transakce přesáhne určitou (předem stanovenou) hodnotu či denní limit. V tomto případě může být autorizace jednodušší, např. jednorázovým heslem zaslaným pomocí SMS.

2 Systémy elektronického bankovnictví

Zvykem (zejména českých) bank je nabízet v základní nabídce svého elektronického bankovnictví pouze omezené bezpečnostní mechanizmy. Za vyšší bezpečnost uživatel typicky připlácí. Dalším bezpečnostním omezením elektronického přístupu je cílové zařízení, pro které je připraveno. Nelze očekávat stejné možnosti zabezpečení např. u telefonického a internetového bankovnictví. Podívejme se proto nyní na přístupy, se kterými je možné se u reálných systémů setkat.

2.1 Telefonické bankovnictví (telebanking)

Telebanking je služba využívající klasické telefonní linky či mobilního telefonu. Uživatel provádí své operace po zavolání na speciální telefonní číslo banky a komunikuje přímo s telefonním bankéřem – reálnou osobu nebo automatem, tzv. IVR (Interactive Voice Response). Forma telefonního bankéře může záviset na operaci, kterou má uživatel v úmyslu provést – aktivní (zadání příkazu k úhradě či investice do podílových fondů) nebo pasivní (zjištění zůstatku na účtu či historie).

Vlastní vstup do systému předchází ověření autenticity uživatele. Ve většině případů se ověřuje uživatelské jméno a heslo či PIN přidělené uživateli při zřízení služby. Některé banky přidělují svým klientům sadu jednorázových hesel pro jedno použití. K autentizaci lze také využít mobilního či elektronického klíče. Pokud komunikace probíhá s telefonním bankéřem, může být součástí autentizace i ověření znalosti identifikačních údajů vlastníka účtu, čísel smluv atp. Dialog může být veden selektivně, tj. ověření jen náhodně vybraných údajů nebo jejich částí.

2.2 GSM bankovnictví (GSM banking)

Jedná se o pokročilejší formu bankovnictví, která ke svému fungování vyžaduje GSM telefon, nejlépe s podporou přídavných funkcí SIM karty – tzv. *SIM toolkit*. Základním prvkem je pak bankovní aplikace uložená na kartě, která zprostředkovává přes intuitivní rozhraní komunikaci mezi bankou a klientem.

Přístup ke zprávám banky či nakládání s účtem je zabezpečen přístupovým bankovním PINem. Komunikace mezi bankou a telefonem (resp. aplikací na SIM kartě) je šifrovaná. Bankovní aplikace může navíc obsahovat i funkce pro generování dalších přístupových kódů atp. Přínosem pro bezpečnost může být i fakt, že GSM bankovnictví k jednomu účtu lze provozovat pouze z jedné SIM karty.

2.3 Internetové a domácí bankovnictví (Internet and home banking)

Internetové bankovnictví jsou služby pro manipulaci s účtem prostřednictvím počítače a sítě Internet. Z hlediska nároků na vybavení službu dělíme na tzv. internet banking, pro jehož provoz uživateli postačuje webový prohlížeč, a home banking, využívající speciální program dodaný bankou. Zatímco s první variantou uživatel spravuje svůj účet (takřka) z kteréhokoliv počítače připojeného k Internetu, druhá varianta jej omezuje na konkrétní stroj a instalaci softwaru. Výhodou naopak může být lepší integrace softwaru do programů třetích stran (např. účetní či ekonomický software).

Zabezpečení komunikace v rámci internetového bankovnictví obvykle bývá řešeno standardním protokolem SSL (HTTPS). Většina českých bank pro svou identifikaci používá certifikáty vydané obecně uznávanými autoritami (např. VeriSign), jejichž certifikáty jsou standardní součástí webových prohlížečů, nebo národními certifikačními

autoritami (v České republice např. I.CA). V prvním případě není problém s automatickým ověřením platnosti certifikátu banky.

Možnosti autentizace uživatele pracujícího prostřednictvím počítače jsou ovšem mnohem bohatší. Můžeme se setkat s autentizačními systémy, které využívají: uživatelského jména a hesla; certifikátu; čipové karty; SMS kódu; či autentizačního (PIN) kalkulátoru.

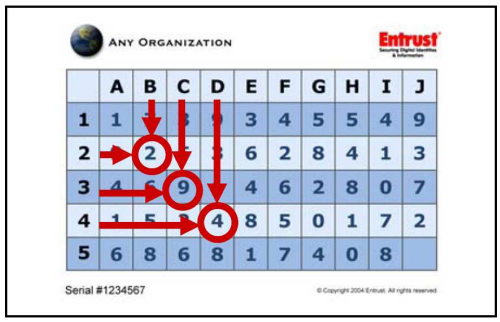
Uživatelské jméno a heslo lze považovat za základní způsob ověření identity uživatele, který je však vhodný kombinovat s některým dalším. Bohužel u některých bank je toto jediný možný způsob. Důležitými bezpečnostními aspekty u hesel jsou požadavky kladené na nově volená hesla (minimální délka; zda musí obsahovat číslice, velká písmena, speciální znaky) či počet chybných ověření, po kterých dojde k dočasnému zablokování účtu. Pro odblokování je typicky vyžadována návštěva pobočky, u některých bank je možné účet odblokovat i telefonicky.

Obvykle za poplatek vydávají některé banky svým klientům časově omezený certifikát, který je použit pro ověření žádostí o autentizaci (podepsané příslušným soukromým klíčem). Tento certifikát, ale hlavně příslušný soukromý klíč, by měly být uloženy na externím paměťovém médiu (disketa, flash disk) a nahráván pouze v okamžiku, kdy je potřeba. Opět většinou za příplatek lze zvolit umístění těchto citlivých dat na kryptografickou čipovou kartu, kterou tato data neopustí, protože čipová karta provádí požadované kryptografické operace s citlivými klíči sama.

Dále je možné pro autentizaci využít jednorázová hesla generovaná uživatelovým PIN kalkulátorem nebo jednorázová hesla bankou odesílaná přes jiný komunikační kanál, např. formou SMS zprávy.

Méně nákladným je pak řešení firmy Entrust [1] zvané Identity Guard. To umožňuje oboustrannou tzv. *souřadnicovou autentizaci*. Každý uživatel je vybaven kartou (která se čas od času mění). Karta je potištěna tabulkou (viz obrázek 1 – převzato z oficiálních materiálů firmy Entrust [1]).

Při autentizaci je pak uživatel kromě jména a hesla dotázán na několik znaků vytištěných na



Obrázek 1: Uživatelská karta.

konkrétních políčkách v tabulce (např. B2, C3 a D4). Tento dodatečný autentizační mechanizmus poskytuje dobrou ochranu také proti podvrženým stránkám či různým druhům malwaru – několik útoků, které by odhalily login a heslo, dokáže totiž odhalit jen poměrně malou část znaků na autentizační kartě. Jednodušší formou tohoto mechanismu je volba sekundárního hesla, ze kterého musí uživatel při autentizaci zadat několik znaků z náhodně vybraných pozic.

Jako částečnou ochranu proti různým druhům podvržených přihlašovacích webových formulářů lze také využít tzv. *personalizovaný login*, kdy si uživatel zvolí nějaký obrázek či oslovení, a pokud se během procesu přihlašování na stránce nevyskytnou, rozpozná, že jde o podvrženou stránku a ukončí komunikaci ještě před zasláním citlivých informací. Tento mechanizmus je však účinný pouze pokud je aktivní HTTPS spojení, které chrání proti aktivním tzv. *man-in-the-middle* útokům, což samotný personalizovaný login nedokáže (po vyřazení HTTPS můžou v případě důmyslně provedeného útoku být totiž obrázek i oslovení automaticky stahovány z autentického bankovního systému).

2.4 Bankovnictví přes PDA (PDA banking)

Jedná se o internetové (webové) bankovnictví, jehož prostředí je zjednodušeno do té míry, aby bylo zobrazitelné i z kapesních počítačů. Tento způsob elektronického bankovnictví však není zatím příliš rozšířen, např. v Čechách jej jako jediná nabízí eBanka.

2.5 Dodatečné metody autorizace transakcí

Pro autorizaci transakcí prováděných v rámci elektronického bankovnictví se používají stejné mechanizmy jako při autentizaci uživatele.

Může být použit soukromý klíč a příslušný podpisový certifikát opět umístěný na počítači, nebo čipové kartě. Banka může také generovat jednorázové autorizační kódy s časově omezenou platností a zasílat je klientovi jiným komunikačním kanálem, např. SMS zprávou. Klient také může od banky jednorázově dostat sadu (např. 100) jednorázových autorizačních kódů, které postupně zadává při požadavku na autorizaci / autentizaci. Tyto jednorázové kódy bývají označovány jako TAN (Transaction Authentication Number) a lze je získat několika způsoby: přímo na pobočce, poštou, nebo formou (šifrované) SMS.

Pro šifrování dat v GSM sítích se používá symetrický algoritmus A5 (existuje v několika variantách). Tímto algoritmem jsou šifrována pouze data mezi telefonem a základnovou stanicí (BTS). Z toho vyplývá, že organizace spravující infrastrukturu GSM má přístup k dešifrovaným datům (samotný operátor u SMS uchovává minimálně informace o odesílateli a příjemci zprávy a datum). Šifrování přenášených dat však není povinná vlastnost sítě a není obtížné ji také obejít. Proto jsou zprávy odesílané v rámci GSM bankingu navíc šifrované SIM toolkitem se sdíleným symetrickým klíčem uloženým v bance a na SIM kartě.

Některé banky nabízejí klientům formu autorizace operací s platební kartou v podobě jejího uzamčení. Dokud je karta „uzamčena", nelze s ní provádět žádné finanční transakce. Jakmile dá klient pokyn (např. SMS zprávou), karta se pro finanční operace odemkne. Toto odemknutí může být permanentní, ale i časově omezené.

Kromě již popsaných způsobů autorizace je pro elektronické transakce nastaven časový limit, během kterého lze provést transakce v určité maximální výši. Časový limit obvykle bývá denní a výše transakce se v různých bankách liší, v českých maximálně až 300 tisíc Kč. Pro rychlé zjištění neoprávněné operace je také dobré povolit notifikaci klienta o transakci formou SMS zprávy.

Stručný přehled používaných autentizačních/autorizačních mechanizmů mnohých českých bank lze nalézt například v [2]. V současné době však již tyto zdroje nejsou příliš aktuální a například Citibank nově ke vstupu do systému zavedla použití autentizačního kalkulátoru, zatímco Česká spořitelna již naopak nové autentizační kalkulátory už neposkytuje (podpora stávajícím je však stále zachována).

3 Bezpečnost platebních systémů

Vývoj platebních systémů se v mnoha zemích ubíral (a stále ubírá) poměrně odlišnými cestami. Ačkoliv jsou v dnešní době jednotlivé bankovní sítě vzájemně propojeny, existuje mezi nimi stále značná nehomogenita. Příkladem mohou být např. mechanizmy propojení banky s vlastními bankomaty. Společné rysy technického, bohužel však ne legislativního, pokroku jsou sice patrné ve všech zemích – např. přechod od offline k online bankomatům, umožnění provádění plateb v místě prodeje, možnost vzdálené správy účtu – jejich primárním cílem ale není zvýšení pohodlí či bezpečnosti prováděných transakcí zákazníka.

Banky se ubírají směrem zvyšování počtů transakcí a vlastních zisků, a pokud jim to zákon umožňuje, přesouvají maximální míru odpovědnosti za všechny transakce na zákazníka (to neplatí např. pro USA, kde byla přijata „Regulace E" [3] přisuzující veškerou zodpovědnost za transakce bankám). Nově zaváděné bezpečnostní prvky (např. modernizace bankovních sítí či přechod na čipové karty a autorizaci PINem) pak většinou chrání zájmy bank a obchodníků – nikoliv však jejich zákazníků – tím, že zjednodušují „dokazování viny" zákazníka v případě zneužití platební karty.

Ať je současný model v jakémkoliv směru dokonalý, postavíme-li do role útočníka samotného obchodníka, zjistíme, že téměř žádný z používaných bezpečnostních prvků mu samostatně nemůže zabránit zneužít svého postavení a podvést zákazníka. Jeho postavení je výjimečné tím, že pro platby poskytuje tzv. „důvěryhodný terminál". Stačí mu tedy jen podstrčit falešný displej zobrazující sumu rozdílnou od té, která je právě odečítána ze zákazníkova účtu. Zákazník

na místě nemá žádnou šanci takovou transakci před provedením potvrdit či zastavit, obrana je možná až v případě, kdy se vyskytne větší množství stížností na jednoho obchodníka.

Obecně platí, že terminál je pod výhradní kontrolou obchodníka, platební karta pod kontrolou banky, avšak zákazník nemá k dispozici žádnou technologii, které by mu umožnila ověřit, že obchodník zadal skutečně správnou sumu (tj. tu, která se zobrazuje na displeji terminálu).

Podobně je na tom i uživatel přistupující ke svému účtu přes systémy elektronického bankovnictví. Zde je jako bezpečná autorizační metoda mnohdy používána čipová karta s uloženými soukromými klíči a certifikáty veřejných klíčů. Pokud však útočník získá kontrolu nad celým počítačem a odposlechne PIN, který „odemyká" čipovou kartu, může této čipové kartě neomezeně zasílat příkazy k autorizaci nejrůznějších transakcí. Útok je sice komplikovanější než pouhé odposlechnutí hesla (např. pomocí Trojského koně) a jeho následné zneužití, ale se současnými automatizovanými nástroji pro provádění útoků je stále poměrně snadno realizovatelný. Obzvláště když některé banky umožňují využití čipové karty a certifikátu zároveň i pro přihlášení do operačního systému a tím kromě neustále vložené karty vynucují i mnohem častější zadávání PINu.

Toto neuspokojivé postavení klienta je hlavním důvodem pro reálnou potřebu levného a jednoduchého zařízení komunikujícího s platební kartou (či jiným tokenem), které by bylo výhradně pod kontrolou zákazníka, a umožňovalo by mu plnou kontrolu nad zpracováváním transakcí – ideálně zobrazením dat, např. částky a čísla cílového účtu, které jsou posílány čipové kartě k podpisu.

4 Závěr

Viděli jsme, že různé systémy a jimi prováděné operace využívají různé autentizační a autorizační metody. Zdaleka ne vždy se však jedná o metody pro danou situaci ideální či dokonce vhodně a správně implementované. Mezi zřejmé nevýhody celého systému patří, že platební terminály jsou pod výhradní kontrolou obchodníků; použití karet s magnetickým proužkem může vézt k jejich snadnému kopírování a padělání; použití dodatečných autentizačních-autorizačních mechanizmů bývá aplikováno pouze selektivně (na vybrané operace) apod. Tyto a jim podobné nedostatky pak dávají útočníkům možnost systém nějakým způsobem zneužít. Různé typy (mnohdy relativně jednoduchých) útoků na bankovní systémy realizující hotovostní či bezhotovostní platby si popíšeme v následujícím článku.

Literatura

[1] Entrust IdentityGuard. *Securing What's at Risk: A Common Sense Approach to Strong Authentication.* Dostupné na: `http://entrust.com/resources/download.cfm/22313/`.

[2] P. Krčmář. *Autorizace v internetovém bankovnictví.* 2006. Dostupné na: `http://www.root.cz/clanky/autorizace-v-internetovem-bankovnictvi/`.

[3] *Board of Governors of the Federal Reserve System: Part 205 – Electronic Fund Transfers (Regulation E),* 61 FR 19669, May 2, 1996. □