ÚVT MU

zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • říjen 2007 • roč. XVIII • č. 1

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 charak-

teristiku 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 buď to 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. □

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 bankovnictví 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.

[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.

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.

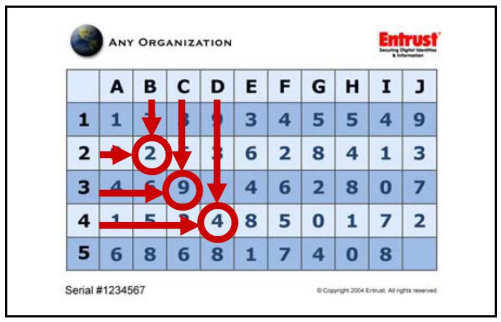
Uživatelské jméno a heslo lze považovat za základní způsob ověření identity uživatele, který je však vhodný kombinovat s některým dalším. Bohužel u některých bank je toto jediný možný způsob. Důležitými bezpečnostními aspekty u hesel jsou požadavky kladené na nově volená hesla (minimální délka; zda musí 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 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



Obrázek 1: Uživatelská karta.

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. □

Útoky na platební systémy

Jan Krhovják, Marek Kumpošt, Václav Matyáš, FI MU

V předchozích příspěvcích jsme se seznámili se základními mechanizmy autentizace/autorizace a s jejich bezpečným nasazením v reálných (zejména bankovních) systémech. Mnohdy jsme se však zmiňovali, že korektní implementace či začlenění těchto mechanizmů do systému není až tak jednoduchá a přímočará, a že jakákoliv (byť jen nepatrná) chyba může vést k různým útokům a zneužití systému. V tomto příspěvku se tedy zaměříme právě na existující nedostatky současně používaných metod.

1 Analýza a identifikace nedostatků současných metod

Jak již bylo naznačeno v předchozích článcích, existuje celá řada bezpečnostních problémů, které se týkají jak používaného hardwaru a jeho softwarového vybavení, tak i používaných komunikačních protokolů. Je proto snaha celou situaci s bezpečností takovýchto zařízení držet na vysoké úrovni, což mají za úkol některé existující normy a standardy (FIPS 140-1, 140-2, právě vyvíjená 140-3, případně pak také např. Common Criteria). Tím se však ani zdaleka neřeší všechna rizika.

Při běžném používání čipové karty nebo kryptografického tokenu je totiž v cestě celá řada autorit a institucí, kterým je třeba bezvýhradně

věřit. Od počátečního výrobce, jemuž je nutné důvěřovat, že se nedopustil žádných chyb (ať už záměrných nebo náhodných) v návrhu, přes autora aplikace, která na takových kartách poběží a bude zpracovávat důvěrné informace, dále pak přes inicializaci dat na tokenu až konečně k fázi předpersonalizace a personalizace. Teprve v tento okamžik se karta s jejím obsahem dostává ke koncovému uživateli a další bezpečnost závisí na tom, jakým způsobem s ní bude on zacházet.

Většina bezpečnostních procesů a metod se v současné době zabývá zejména zajištěním co nejmenšího rizika při průchodu kryptografického zařízení výše uvedeným řetězcem autorit a samotnému používání karty pak není věnována pozornost na potřebné úrovni. Přitom z pohledu uživatele je právě fáze vlastního provozu karty tím nejdůležitějším bodem, kdy většinou ručí za veškeré operace s jeho tokenem provedené.

Při práci s počítačem a v něm uloženým kryptografickým materiálem si uživatelé zvykají na ukládání privátních klíčů v bezpečných úložištích, ať už jde o (speciální) USB tokeny, čipové karty nebo o využívání nově nastupující technologie *trusted computing* [4] a souvisejících služeb.

V bankovním sektoru je situace jiná. Z historického hlediska je možné rozlišovat dvě různé možnosti autorizace finančních transakcí pomocí platebních karet. Jedna, založená na klasických ručně psaných podpisech, bývala výhradně určena při platbách u obchodníků; druhá, za použití PINu, zase při výběrech hotovosti z bankomatů. Během tohoto období si uživatelé zvykli používat různá bezpečnostní měřítka při autorizaci – bankomat byl a stále bývá považován za bezpečné prostředí, zatímco u obchodníka se při autorizaci podpisem očekávalo, že případné zfalšování podpisu půjde vždy dodatečně prokázat.

Postupem času, zejména s nástupem EMV čipových karet [5], se však začala situace měnit. A to nejen v České republice, ale i po celé Evropě. Autorizace plateb se i u obchodníků začíná provádět čím dál častěji pouze za pomoci platební karty a odpovídajícího uživatelova PINu, což s sebou přináší další problematický bod, kterým je prokazování neoprávněných transakcí a zodpovědnosti bank za sporné platby. U podpisů totiž bylo možné nechat znalecky ověřit zfalšovaný podpis a často pak prokázat, že uživatel platební karty neprovedl autorizaci vlastnoručně. Vyzrazení nebo ukradení PINu a jeho následné zneužití někým jiným než právoplatným vlastníkem karty je však zpětně jen velmi obtížně prokazatelné.

V tomto bodě se liší i přístup amerických a evropských bank k odpovědnosti za sporné platby. Zatímco banky v USA se v případě elektronického bankovnictví musí řídit tzv. „Regulation E", kdy za všechny platby ručí banky a v případě pochybností je jejich povinností prokázat, že se uživatel dopustil podvodu, v evropském bankovnictví je tomu přesně naopak. Veškeré platby, u kterých je pochybnost, jsou připsány na vrub vlastníkovi a ten pak musí prokazovat, že je neprovedl on. Odpovědnost je pak na straně uživatele (typicky, neprokáže-li jinak), nebo obchodníka (byla-li platba autorizována prokazatelně falešným podpisem).

Je tedy v nejvyšším zájmu uživatele kryptografického tokenu ochránit se před jeho zneužitím, identifikovat možné zdroje potenciálních rizik při prováděných operacích a efektivně jim předejít. To samozřejmě vyžaduje alespoň základní povědomí uživatele o existujících rizicích a útocích, které jsou pro daný systém relevantní. V následujících částech se proto také změříme na některé typy útoků, které do značné míry závisí i na samotných uživatelích (jejich chování, obezřetnosti či manipulaci se systémem).

2 Útoky z pohledu uživatelů

Podívejme se tedy nejprve na nejběžnější útoky se kterými se může uživatel (resp. zákazník banky) v dnešní době při realizaci (bezhotovostních) plateb či transakcí setkat.

Asi nejrozšířenějším druhem podvodu, při kterém je od uživatele získána důvěrná informace, je *phishing*. Útok probíhá tak, že uživateli je doručena zpráva, která ho jménem důvěryhodné instituce žádá o osobní informace. Toto je obvykle provedeno e-mailovou zprávou, ale v poslední době jsou stále častěji využívány systémy

umožňující přenos digitalizovaného hlasu (VoIP – Voice over Internet Protocol). V prvním případě je uživatel vyzván k navštívení stránek např. své banky, aby změnil přihlašovací informace ke svému účtu – daná stránka je ovšem stránka vytvořená útočníkem, která je obvykle obtížně rozeznatelná od originálních stránek. Ve druhém případě je využíváno sociální inženýrství přes telefon, ve kterém je uživatel vyzván k návštěvě stránek, které mohou nápadně připomínat stránky organizace, jejíchž služeb využívá. Uživatel v domnění, že komunikuje s důvěryhodnou institucí, předává např. autentizačnímu formuláři své identifikační údaje. Útočník tak získá citlivé údaje, které později velmi pravděpodobně zneužije pro neoprávněný přístup.

Novějším a mnohem důmyslnějším útokem je pak *pharming*. Ten staví – namísto na sociálním inženýrství – na manipulaci DNS záznamů a je tak v principu vlastně obdobou DNS spoofingu. Cílem útočníka je automatické přesměrování uživatele na vlastní stránky, které mohou být replikou stránek bankovních institucí a sloužit tak např. k získávání přihlašovacích údajů zákazníka. V horším případě pak mohou sloužit také jako jakýsi prostředník mezi uživatelem a skutečným systémem internetového bankovnictví – ten pak například korektně přeposílá pouze autorizační údaje, zatímco informace vztahující se k samotné transakci (číslo účtu, velikost převáděné částky) již mohou být zmanipulovány útočníkem.

Spyware je druh programu, který je spuštěn takovým způsobem, že o něm uživatel nemá tušení. Úkolem spywaru je sbírat informace o činnosti uživatelů. Do počítače se dostává např. v podobě trojského koně – škodlivého kódu přibaleného k jinému programu. Díky rozšířenosti operačního systémů Windows s webovým prohlížečem Internet Explorere je snazší psát i šířit spyware, stačí se zaměřit na chyby v těchto programech. Příkladem budiž „útok hackerů na Komerční banku" v roce 2006, kdy trojský kůň pravděpodobně posloužil ke krádeži desítky přístupových certifikátů a hesel k elektronickému bankovnictví a následně ke krádeži peněz z postižených účtů. Novějším příkladem jsou trojské koně typu „Sinowal" zobrazující podvržené stránky internetbankingu SERVIS 24 (Česká spořitelna). Problémem spywaru je, že je velice obtížné předcházet jeho „získání" a je třeba pravidelně kontrolovat stav počítače; pozitivní zprávou je relativně snadné odstranění spywaru z počítače.

Útok pomocí tzv. *libanonské smyčky* (viz obrázek 1) spočívá ve vhodném umístění části nařízнuté pásky videokazety do štěrbiny pro vkládání platební karty v bankomatu. Pokud je karta vložena, zadrží ji páska tak, že ji bankomat není schopen dále zasunout ani vysunout. K oběti se přiblíží útočník a poradí jí opětovné vložení PINu, který odpozoruje. Jakmile oběť odejde problém reklamovat, vytáhne útočník kartu z bankomatu a s pomocí zjištěného PINu z karty odcizí požadované peníze ještě před zablokováním karty.

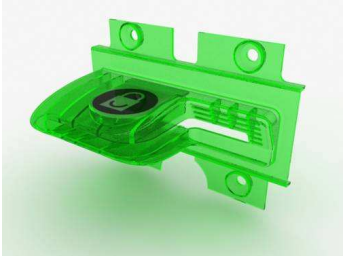
Obrázek 1: Libanonská smyčka.

Skimming je útok, jehož cílem je zkopírovat magnetický proužek platební karty. Ke zkopírování magnetického proužku může dojít buď ve čtečce umístěné u vstupu do prostoru bankomatu nebo ve čtečce umístěné přímo na bankomatu samotném (viz obrázek 2). Útočník např. umístí na bankomat repliku klávesnice (resp. PINpadu), která v sobě zaznamená zadané PINy. Replika klávesnice je na bankomatech doplněna speciálním „nástavcem" na štěrbinu, do které se vkládají platební karty a která je nerozeznatelná od součástí bankomatu. Útočník po získání informací velmi jednoduše vyrobí kopie platebních karet, které může použít k výběru hotovosti v bankomatech. K odpozorování PINu pak lze kromě výše zmíněné falešné klávesnice využít například i poblíž nainstalované kamery.

V současné době právě kvůli tomuto typu útoků mnohé české banky instalují ochranná zařízení (FDI – Fraudulent Device Inhibitor) pro štěrbinu

Obrázek 2: Kryt s falešnou čtečkou.

na vkládání karty do bankomatu (viz obr. 3). Pro neinformované zákazníky však takto vyvstává problém rozhodnout, zdali se jedná o zařízení banky či zařízení útočníka.



Obrázek 3: Ochranný nádstavec.

Alternativně také může útočník PIN odpozorovat přímo při jeho zadávání v libovolném místě prodeje a poté platební kartu zcizit (obtížností odpozorování se zabýval experiment popsaný v další části).

3 Experiment zabývající se autorizacemi bezhotovostních plateb

V letech 2005–2006 proběhl na Fakultě informatiky MU (FI MU) experiment zaměřený na bezpečnost plateb kartami v „kamenných" obchodech za fyzické přítomnosti karty a jejího držitele. Cílem experimentu bylo zjistit:

1. Jak obtížné je odpozorovat PIN, který zadává zákazník v obchodě při platbě platební kartou.
2. Jak snadno lze napodobit cizí podpis při autorizaci platby podpisem.

Celý experiment byl rozdělen do dvou fází, kdy první z nich proběhla na jaře 2005 v knihkupectví P. Marečka na FI MU a druhá část ve skutečném supermarketu v Brně v březnu 2006. Detailní popis průběhu experimentu lze nalézt v [1].

3.1 Výsledky experimentu

Co se týče autorizace pomocí PINu, tak zde je zřejmé, že solidní kryt klávesnice velmi přispívá k bezpečnosti při zadávání PINu s ohledem na možného pozorovatele, který není přímo vedle zákazníka, který PIN zadává. Nicméně zatím je stále poměrně velké procento terminálů vybaveno PINpadem bez ochranného krytu nebo neúčinným krytem (viz obr 4).

Obrázek 4: Srovnání krytů PINpadů.

Co se týče korektně odpozorovaných číslic PINu, tak porovnání úspěšnosti v obou fázích je 60 % a 42 %, což není veliký rozdíl. Co se týče celých PINů, v první fázi se podařilo korektně odpozorovat celkem 18 ze 32 PINů (56,25 %) a ve druhé fázi pouze 4 z 20ti zadaných PINů (20 %).

Velký rozdíl jsme pozorovali v podpisové části, kde v druhé fázi experimentu nebyl odhalen jediný (!) zákazník falšující podpis někoho jiného, zatímco v první fázi experimentu bylo odhaleno 70 % falešných podpisů. Částečně si to vysvětlujeme tím, že obchodník v první fázi experimentu měl zkušenosti s prací v klenotnictví, kde se platí obecně řádově vyšší částky než v běžném supermarketu a podpisům se proto věnuje vyšší pozornost. Naše domněnka, že možná v supermarketu provádějí důkladnější kontrolu až v okamžiku, kdy částka za nákup přesáhne určitou hodnotu, se bohužel nepotvrdila. Celkově lze tedy říci, že při ztrátě karty stačí tomu, kdo ji nalezne, cca 20 minut na nacvičení podpisu a má téměř stoprocentní šanci, že v běžném supermarketu nebude odhalen. Jedinou ochranou jsou

v tomto případě kamerové systémy v supermarketech

3.2 Shrnutí

Z výsledků experimentu je zřejmé, že autorizace podpisem, která v současné době převládá ve většině obchodů, není příliš bezpečná a v případě ztráty karty může velmi rychle dojít k jejímu zneužití. Ovšem zlepšení úrovně důslednosti ověření podpisu alespoň při platbě vyšších částek může nejen zabránit přímým ztrátám obchodníků, ale také částečně ochránit majitele inkriminovaných účtů.

Co se týče autorizace PINem, tak zde je situace v případě ztráty výrazně lepší, ovšem v případě cílené krádeže jen minimálně. V případě falšování podpisu stačí útočníkovi pouze karta – v případě autorizace PINem musí útočník nejprve úspěšně odpozorovat PIN a pak získat platební kartu. To je jen o něco málo složitější – ovšem se zpochybněním transakce to bude právě naopak! Při zvážení obtížnosti reklamace transakce se správně zadaným PINem je tedy na místě otázka, zda z pohledu nezapomětlivého držitele karty (tzn. zohledňujícího především otázku krádeže) není karta pro platby s autorizací PINem méně výhodná.

V každém případě lze jen doporučit volbu takové platební karty, u které lze okamžitě provést zablokování při zjištění její ztráty. Případně pak karty takové, kterou je možno dočasně blokovat nezávislým způsobem, např. kanálem GSM bankovnictví.

4 Bezpečnost PIN-mailerů

Položme si však nyní otázku, zdali je odpozorování PINu jediná možnost jak může útočník k PINu přijít. Mnohé banky své zákazníky nabádají, aby si svůj PIN po přečtení zapamatovali, obálku s PINem zničili a hlavně PIN nikdy a nikde nezapisovali. Útočníkovi tak již nezbývá mnoho možností, kde jinde PIN získat; a protože PIN je po vygenerování vytištěn tzv. *PIN-mailerem* přímo do zapečetěné obálky, tak by k němu neměli mít přístup ani bankovní pracovníci ani nikdo na cestě mezi bankou a zákazníkem. Zdali je však PIN v obálkách skutečně bezpečně ukryt před potenciálním útočníkem, to bylo předmětem našeho dalšího experimentu.

Jedním z kroků při zakládání účtů a vydávání platebních karet (nezbytných pro druhou fázi předcházejícího experimentu) bylo i získání obálek s odpovídajícími PINy. Protože část platebních karet vyžadovala při bezhotovostních transakcích autorizaci PINem, byli jsme také nuceni část těchto obálek otevřít. Inspirováni článkem [2] z roku 2005, který popisuje nedostatečnou bezpečnost PIN-mailerů využívajících laserového tisku, rozhodli jsme se ověřit situaci u České spořitelny, u níž jsme si v rámci výše zmiňovaného experimentu nechali založit účty a vydat karty. Přečtení PINů z prvních šesti uzavřených obálek však bylo (i s běžně dostupnými zdroji světla) natolik snadné, že jsme se po dalších úvahách rozhodli zhodnotit situaci i v dalších třech českých bankách.

Před vlastním popisem provádění a výsledků našich testů ještě připomeňme, že koncem roku 2006 došlo k napadení několika účtů v internetovém bankovnictví Komerční banky. To vedlo u většiny ostatních bank k revizím stávajících bezpečnostních opatření, které mnohdy zahrnovaly např. zákaz zasílání platebních karet poštou. Z několika vhodných kandidátů jsme proto záměrně zvolili banky, které ještě umožňovaly zaslání karty nebo obálky s PINem (ideálně však obojího) poštou. Pokud byla u těchto bank v ceně standardního účtu nabízena také aktivace Telebankingu či Internet-bankingu, provedli jsme ji rovněž, čímž jsme obvykle získali další obálky s PINy či hesly.

Naším cílem nebylo poukázat na slabiny konkrétních PIN-mailerů – jejich typy jsme neznali a ani jsme po nich nepátrali. Tímto se již zabývali autoři [2], a jejich závěry byly výrobcům PIN-mailerů a postiženým britským bankám známy ještě půl roku před zveřejněním (v listopadu 2004). Naším záměrem bylo spíše ukázat, jakou mají útočníci (mezi které řadíme i pracovníky na pobočkách bank) šanci s běžně dostupnými prostředky nepozorovaně zcizit citlivé údaje – a zda se tedy téměř po třech letech od zveřejnění problému s PIN-mailery a po půl roce od napadení několika účtů přes internetové bankovnictví (a

následné revizi bezpečnostních opatření mnoha bank) situace nějak zlepšila.

4.1 Provedení a výsledky

Celkem jsme testovali PIN-mailery používané čtyřmi českými bankami: Česká spořitelna, eBanka, GE Money Bank, HVB Bank. Z první banky jsme měli k dispozici pět obálek s PINy k platebním kartám a z ostatních tří bank jsme měli vždy po dvou obálkách. U druhé a třetí banky jsme měli také po dvou obálkách s přihlašovacími údaji pro Internet-banking a u čtvrté banky po dvou obálkách s přihlašovacími údaji pro Tele-banking. K prosvěcování obálek jsme použili běžně dostupných zdrojů světla – největší úspěchy jsme zaznamenali s klasickou kapesní svítilnou a s LED diodami. K prvnímu úspěšnému prosvícení obálky (a následnému úspěšnému přečtení PINu) dokonce posloužila běžná optická počítačová myš (!).

Banka 1 – Česká spořitelna

K dispozici jsme měli pět obálek (všechny zaslány poštou) s PINy k platebním kartám, k jejichž vytvoření byl použit PIN-mailer využívající laserového tisku. Prosvěcovaní a zjišťování PINů zde patřilo k nejsnazším, obálky obsahovaly pouze jeden list papíru s vytištěným PINem. Celkově (včetně obálky) bylo tedy nutno prosvítit tři listy papíru (s černým krytím vždy pouze z jedné strany) a správně přečíst PIN. Celý úkol nám výrazně usnadnilo, že jsme již z předchozí analýzy (otvírání prvních šest obálek) věděli, kde je PIN umístěn – tj. že se nachází v oblasti obdélníkového červeného razítka. Úspěšnost útoku byla 100%, všech pět PINů bylo přečteno bez jediné chyby. K prosvěcování se nejvíce osvědčily LED diody – byla použita klasická optická počítačová myš (červené světlo) nebo čelovka (bílé světlo) obsahující tři takové diody. Se znalostí umístění PINu bylo jeho přečtení v tomto případě natolik snadné, že to do dvou minut (a opět se 100% úspěšností) zvládli i dva naprostí začátečníci. S trochou tréninku k jeho přečtení dokonce nebyla nutná ani absolutní tma – stačilo pouze dostatečné přítmí, např. v pootevřené zásuvce stolu.

Banka 2 – eBanka

Zde jsme testovali čtyři obálky – dvě s PINem ke kartám a dvě s přihlašovacími údaji pro Internet-banking. První dvě obálky byly zaslány poštou, druhé dvě obálky bylo nutno převzít na pobočce a otevřít je. Ve všech čtyřech případech byl použit průklepový tisk na samostatný prostřední list. U prvního typu obálek byly dokonce čtyři vrstvy černého krytí, u druhého typu pak opět pouze tři vrstvy.

V tomto případě nevedlo prosvěcování obálek s PINy k platebním kartám k žádným výsledkům, avšak u přihlašovacích údajů pro Internet-banking jsme již zaznamenali částečný úspěch. Ze čtyř vytištěných PINů (každá obálka obsahovala dva) se nám podařilo jeden PIN přečíst úplně a další s jedinou chybou. U zbylých dvou PINů jsme si byli vědomi, že jsme vždy jednu číslici nepřečetli, ale ze zbylých šesti jsme tři přečetli správně.

Důvodem úspěšného přečtení těchto PINů bylo použití modrého podkladu, na němž byly PINy vytištěny. Je však třeba poznamenat, že prosvěcování a úspěšné přečtení PINu již vyžadovalo značné soustředění a také poměrně velkou tmu.

Banka 3 – GE Money Bank

K analýze jsme opět měli čtyři obálky – dvě s PINem ke kartám (zaslány nedoporučeně poštou) a dvě s přihlašovacími údaji pro Internet-banking (vyzvednuty na pobočce). V prvních dvou případech byl použit opět průklepový tisk na samostatný prostřední list a na obálce byly čtyři vrstvy černého krytí. Námi prováděnými technikami nebylo možno PIN zjistit.

U druhého typu obálek byl použit laserový tisk a pouze dvě ochranné vrstvy černého krytí. Přístupové heslo k Internet-bankingu bylo vytištěno přímo na vnitřní straně obálky a navíc ještě výrazně větším písmem. Jeho přečtení proto při prosvícení obálky nečinilo žádné problémy. Díky výše popsaným technikám (technologie tisku, umístění PINu, velikost fontu) bylo jeho přečtení ještě snazší než přečtení PINu z obálek České spořitelny.

Banka 4 – HVB Bank

I v tomto případě jsme k testování měli čtyři obálky – dvě s PINem ke platebním kartám (za-

slány poštou) a dvě s přihlašovacími údaji pro Tele-banking (vyzvednuty na pobočce). V prvních dvou případech byl použit laserový tisk. Kromě standardních dvou vrstev černého krytí byla na prostředním listu použita speciální černá odnímatelná krycí vrstva nalepená na průhledné fólii. PIN byl vytištěn z druhé strany průhledné fólie a pravděpodobně měl být čitelný pouze po odstranění odnímatelné krycí vrstvy. To se však po otevření obálky nepotvrdilo – PIN šel přečíst i bez odstranění černé fólie. Zjišťování hodnoty PINu prosvěcováním uzavřené obálky bylo v tomto případě poměrně obtížné, ale i přesto se nám podařilo jeden PIN určit přesně a u druhého jsme nedokázali přečíst jen první číslici.

U druhého typu obálek byl použit průklepový tisk s dvěma vrstvami černého krytí. Kromě zjištění, že bylo vytištěno sedm řádků textu a určení pozice a délky PINu se však bez znalosti obsahu obálky nedalo nic s jistotou přečíst. Po otevření obálky se ukázalo, že prvním řádkem textu byl skutečně šestimístný PIN a zbylých šest řádků překvapivě odpovídalo jeho číslicím zapsaným slovy. To však umožňuje útočníkovi ke zjištění/upřesnění hodnot číslic PINu využít také znalost délky jejich slovního zápisu (jak jsme již uvedli výše, tu lze při použití průklepového tisku snadno určit). Navíc celý PIN lze, s výjimkou číslic dvě a devět (které je možné snadno odlišit na základě jejich délky), jednoznačně určit pouze na základě prvního písmene slovního zápisu. Toto počáteční písmeno je navíc vždy velké a dá se proto částečně rozpoznat. S pomocí znalosti délky slovního popisu je možné proces rozpoznání prvního písmene značně ulehčit.

I přes všechna výše uvedená tvrzení se při experimentu ukázalo, že přesné určení všech číslic PINu zůstává poměrně obtížné. Redundance v podobě slovního zápisu číslic PINu však rozhodně není z bezpečnostního hlediska příliš žádoucí.

Dále zmiňme, že HVB banka umožňuje stále zaslání PINu i karty poštou – platební kartu je však nutno před prvním použitím aktivovat. Bohužel tato banka poštou zasílá i embosované karty a dává tak útočníkovi šanci získat (přežehlit) údaje vyryté na kartě. Stačí použít jen kousek papíru a obyčejnou tužku. Útok lze při použití klasické tuhy provést řádově během desítek sekund (a nezáleží ani, která strana karty je kopírována) a při použití hrany dřevěné tužky obarvené červenou barvou během jednotek sekund (zde již je třeba mít kartu správně otočenou embosovanou stranou nahoru). Zkopírované údaje pak mohou lehce posloužit k vytvoření padělku embosované karty. Zasílání platební karty poštou umožňuje také eBanka – nikoli však embosovaných. Nepovedlo se nám ji k tomu přinutit ani tím, že jsme zažádali o zaslání elektronické karty a později pak o změnu typu karty na embosovanou.

4.2 Shrnutí

Provedené útoky prosvěcováním patřily k těm zcela nejjednodušším – ostré světlo LED diod (např. použitá počítačová myš) se ukázalo vhodně k prosvěcování obálek tištěných laserovým tiskem, klasická kapesní svítilna se ukázala vhodnější k prosvěcování obálek tištěných průklepovým tiskem. Každý čtenář špionážní literatury jistě zná i účinnější postupy. Počet vrstev černého krytí u laserového tisku také nehrál nijak zásadní roli a útoky příliš neztížil. Použití speciálních technik, jakými je např. odnímatelná krycí vrstva, také nemělo žádný výrazný efekt. Přidání redundantních informací či barevného podkladu naopak některé útoky spíše usnadnilo. Stejně tak je pro útočníka příznivý i fakt, že všechny banky tisknou PIN vždy na stejné místo (což je dle našeho soudu pouze softwarový problém).

Během návštěvy bank jsme také zpozorovali další zdánlivě nenápadné a nevýznamné bezpečnostní problémy. Mnohé z nich – zmiňme například dodatečně neautorizovanou změnu seznamu příjemců plateb a vzorů platebních příkazů v systémech České spořitelny či eBanky – lze odhalit i s minimálním vhledem do problematiky; jejich popis lze nalézt v [3].

5 Závěr

Je známý fakt, že žádný systém není absolutně bezpečný, ale rozumné úrovně bezpečnosti lze vždycky nějakým (mnohdy ne příliš levným) způsobem dosáhnout. Bohužel banky často volí cestu kompromisů, tváří se, že právě ony absolutní bezpečnosti ve svých systémech dosáhly a

skutečné bezpečnostní problémy a incidenty důsledně tají. Pokud se na veřejnost nedostane nějaká informace o bezpečnostních rizicích či útocích na jejich systémy, tak se banky předhánějí v informování klientů, že právě jejich banka již problém vyřešila (či právě řeší).

Nelze samozřejmě předpovědět, zda se přístup bank k bezpečnosti změní k lepšímu, ale dobrým signálem je, že mnozí klienti bank již bezpečnosti začínají přikládat vyšší váhu, a může u nich hrát dokonce roli při volbě banky.

Literatura

[1] Matyáš Václav, Kumpošt Marek, Krhovják Jan. *Platby kartou s použitím PINu.* Data Security Management (DSM), roč. 2006, č. 5, ISSN 1211–8737.

[2] Bond Mike, Murdoch Steven, Clulow Jolyon. *Laser-printed PIN Mailer Vulnerability Report.* 2005. Dostupné na: `http://www.cl.cam.ac.uk/~mkb23/research/PIN-Mailer.pdf`.

[3] Krhovják Jan, Kumpošt Marek, Matyáš Václav. *Jsou PINy zasílány bankami bezpečně?* Data Security Management (DSM), roč. 2007, č. 3, ISSN 1211–8737 *(přijato k otištění)*.

[4] *Trusted Computing Group*. Dostupné na: `http://www.trustedcomputinggroup.org/`.

[5] *EMVCo website.*. Dostupné na: `http://www.emvco.com/`. □

Autentizační HW a možná vylepšení

Václav Lorenc, Václav Matyáš, ÚVT a FI MU

Zamýšleli jste se někdy nad tím, co vše se děje uvnitř počítače, když právě zadáváte platební příkazy do své banky přes Internet? Jsou všechna elektronicky podepsaná data v souladu s tím, co jste opravdu chtěli podepsat? Jak přežít ve světě, který je plný záškodnických programů – malwaru, spywaru, virů?

1 Bezpečnost hardwarových tokenů

Aby mohl nějaký hardwarový token bezpečně poskytnout autentizaci uživatele a autorizaci jeho operací, je nutné, aby především on sám byl navržen s ohledem na požadovanou míru bezpečnosti. Ačkoliv se může zdát, že zařízení dostupná v současné době na trhu mají v tomto smyslu obdobné vlastnosti, ani zdaleka tomu tak není. V této části nastíníme některé otázky a problémy, které se týkají oblasti zabezpečení právě HW tokenů.

Základní rozdělení kryptografických zařízení je dle jejich ceny a schopnosti odolávat určitým útokům. Z tohoto pohledu rozlišujeme *jednočipová zařízení*, *čipové karty* (paměťové, procesorové či kryptografické) a *hardwarové bezpečnostní moduly (HSM)*.

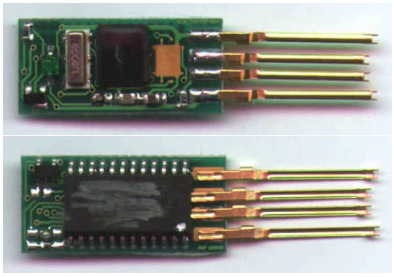
I útoky na zařízení se dají přesněji rozdělit – například dle toho, je-li třeba mít zařízení fyzicky k dispozici, nebo jde-li o útoky spíše softwarové (*logické*). Druhý z oněch případů je velmi podobný klasickým útokům, tak jak je známe z počítačového světa – jde o objevení softwarové chyby, kvůli které jsou pak data dostupná i bez znalosti hesla, případně PINu.

Podívejme se teď v rychlosti na první zmiňovaný způsob útoků, *fyzický*. U nich je možné rozpoznat případy, které se liší obtížností a náročností na vybavení útočníka. *Neinvazivní* metody jsou nejméně náročné, spočívají často zejména ve změně provozních podmínek zařízení tak, aby se chovalo jiným způsobem, než je obvyklé. Nejznámějším případem jsou změny teploty, ať už podchlazení, nebo přehřátí.

Na opačném konci stojí *invazivní* metody, kdy se zařízení nejprve rozebere až na samotný čip, odstraní se krycí vrstvy i z něj a útočník se následně pomocí speciálního hardwaru, mikroskopů a mikrosond napojí na sběrnici, případně vyčítá data přímo z paměti. Tyto metody patří mezi nejnáročnější na vybavení, už kvůli nutné míře potřebných znalostí i miniaturním rozměrům současných čipů. Proto jsou nejčastěji používány zejména pro čipové karty.

Středně obtížné, přesto však velice účinné, jsou poměrně moderní *semiinvazivní* postupy. V nich

Obrázek 1: Čip obalů zbavený.



Obrázek 2: I takto může vypadat USB token uvnitř.

je čip rozebrán jen částečně, obvykle pouze zbaven vrchní vrstvy nebo plastového krycího pouzdra (obr. 1, 2), a dále je na něj působeno některým druhem záření, obvykle elektromagnetickým či silným světelným zdrojem. Tento druh útoků je finančně dostupný a potřebné znalosti jsou nižší, než u invazivních útoků. Výsledky jsou jim však často velice blízko.

Semiinvazivní útoky jsou často používány pro útoky na USB zařízení – jejich velikost je dostatečná na to, aby nebylo nutné používat mikroskopy a často si při jejich výrobě sami výrobci pomáhají různými testovacími obvody, které pak nedostatečně odstraňují. To vede ke zjednodušení situace při získávání klíčů a jiných citlivých dat uložených na takovýchto zařízeních.

Aniž bychom zabíhali do dalších detailů (pro zájemce doporučujeme nahlédnout do [1] a [2]), lze zjednodušeně tvrdit, že hardwarové bezpečnostní moduly jsou zdaleka nejbezpečnější, ovšem za cenu vysokých pořizovacích nákladů. Obvykle nebývají navrhovány s ohledem na přenosnost, často je váha jedním z pasivních prostředků zajištění fyzické bezpečnosti – jen málokomu se chce odnášet pod kabátem půl tuny vážící zařízení, aby z něj následně získával data. Obsahují také řadu aktivních bezpečnostních mechanizmů, které v případě narušení, tedy například při pokusu o otevření, dokážou bezpečně zničit důvěrný materiál. Využívány bývají zejména ve větších centrech vydávajících certifikáty a čipové karty.

Zařízení vystavěná na jednočipových řešeních jsou obecně levná, rychlá, často však náchylná na celou řadu útoků, které vedou k úniku jim svěřených důvěrných dat. Nejlepší variantou kombinující vysokou mobilitu, rozumnou cenu a kvalitní bezpečnost, jsou kryptografické čipové karty.

Proti zmíněným útokům se postupem času objevilo množství obranných mechanizmů a postupů, díky kterým se bezpečnost jednotlivých tokenů zvyšuje. Bohužel to však neznamená, že současně vyráběná zařízení jsou mnohem bezpečnější, než tomu bylo v minulosti.

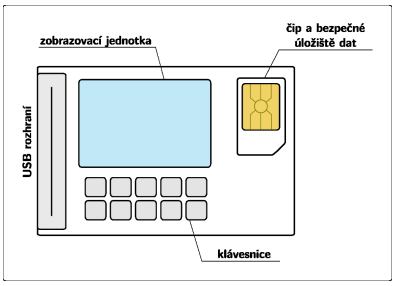
Takovým případem z poslední doby jsou výrobky BioStick či SecuStick, které jsou inzerovány jako bezpečné úložiště dat, ve skutečnosti však neodolají ani jednoduché modifikaci ovladačů v počítači[3]). Jedná se tak o názornou ilustraci toho, že technika *„security through obscurity"* nefunguje, tedy snaha vytvořit zdání bezpečnosti za pomoci pochybných postupů je chybná již v myšlence, natož pak v realizaci. Nebezpečnost tohoto útoku je i v tom, že ačkoliv nalezení slabého místa a sestavení programu, který toho využije, je náročné, samotné opakované spouštění je již možné i deitalů neznalými uživateli.

2 Kdo ochrání uživatele?

Bezpečnost však není jednosložková, pojďme se tedy společně podívat na další aspekty, které jsou pro praktický život stejně důležité.

Používáte-li platební kartu, je v řetězci operací několik různých druhů zařízení, která se na úspěšné transakci podílejí. Platební karta je ve správě banky, která dbá na její řádné vydání a náležitosti, platební terminál je pod opatrovnictvím obchodníka.

Z předcházejících článků je zřejmé, že celá řada zařízení během platebních operací důvěryhodná být nemusí – ať už jde o zmiňované problémy s bankomaty, nebo s platebními termínály.



Obrázek 3: Návrh nového tokenu.

Situace se dále komplikuje v případě, že se jedná o používání HW tokenů v počítači pro potřeby nesouvisející s elektronickým bankovnictvím – např. pro autentizaci vůči firemní síti, ustanovení bezpečného připojení či pro podepisování a šifrování e-mailů. Tyto útoky, často automatizované, nevyžadují ani zásah další osoby, aby mohly provádět neautorizované operace za pomoci hardwarového tokenu – to vše bez vědomí vlastníka!

Také nastává problém s počítači, kterým není možno buď plně nebo jakkoliv důvěřovat – typicky v internetových kavárnách a knihovnách. Ačkoliv kryptografické algoritmy fungují bezpečně, je třeba zabezpečit také svá hesla, případně i manipulaci s nimi.

Jak na to? Nejlepší se v tomto směru jeví myšlenka *elektronického zástupce (electronic attorney)*, tedy zařízení, které by se svojí funkcí blížilo zástupcům z reálného světa. Znalo by informace, které by navenek nebyly zjistitelné, a bezpečným způsobem by je za určitých podmínek mohlo předat právě čipové kartě či jinému tokenu.

3 Autentizační token nové generace

Konstrukce současných tokenů předpokládá, že jsou používány v důvěryhodném prostředí, což ale nelze vždy zaručit. V předcházejících částech jsme naznačili možné problémy, které mohou být způsobeny použitím tokenů v prostředí, jehož bezpečnost nemá uživatel pod kontrolou. Použití současných tokenů v takovém prostředí může vést až ke zneužití uložených dat, často bez vědomí majitele.

Co vlastně přesně je tou chybějící komponentou? Vyřešil by tyto problémy projekt bezpečného PINpadu? Právě jeden z možných způsobů řešení navrhoval, aby byli všichni obchodníci vybaveni zařízením, které je odolné vůči modifikacím a je schopno viditelně signalizovat i pouhé pokusy o narušení. Zákazník by tak měl představu o tom, může-li obchodníkovi při transakci kartou důvěřovat. Dle diskusí odborné veřejnosti se však ukazuje, že sebelepší zařízení je možné nahradit jeho replikou, kterou by uživatel nepostřehl.

Důležitým prvkem je tedy interakce s uživatelem nezávislá na vnějším prostředí – tedy nějaká možnost, jak by přímo token (čipová karta, USB klíčenka) mohl zobrazit svému majiteli informace o právě probíhajících transakcích. A současně od něj vyžadoval jejich autorizaci, potvrzení, že s prováděné akce jsou v souladu se záměry vlastníka tokenu. Ilustrační schéma navrhovaného tokenu ve variantě USB je možné vidět na obr. 3 a rozsáhlejší diskuzi této problematiky lze nalézt v [4].

U platebních transakcí by tak samotný token (v takovém případě čipová karta) zobrazil placenou částku a nechal na sobě zadat PIN tak, aby jej žádné jiné zařízení nemohlo po cestě odchytit. V případě elektronického podpisu by tak bylo například možné zkontrolovat celý dokument předtím, než jej karta celý podepíše – ať už jde o elektronickou poštu, nebo třeba platební příkaz odesílaný bance.

Z hlediska používání by tak byl největší změnou požadavek na autorizaci všech operací s citlivými daty, což není v současné době obvyklé. Tento požadavek na další interakci je však plně vyvážen výrazně vyšší úrovní ochrany dat, kterou tato nová architektura nabízí.

Kombinace kvalitní kryptografické čipové karty by zaručilo fyzickou bezpečnost dat, přitom by však uživatel měl stále přehled a možnost ovlivnit funkci této čipové karty a v případě podezření operaci zakázat. Právě tato nezávislost na okolním pracovním prostředí, v němž se může objevovat mnoho nedůvěryhodných komponent, je důležitým prvkem pro zvýšení bezpečnosti práce s citlivými daty.

Současně tato nová architektura vyžaduje jen minimální změny na straně současných aplikací, mělo by být tedy možné ji snadno integrovat do stávajících systémů, kde se již čipové technologie používají, a přímočaře tak navýšit jejich bezpečnost.

4 Závěr

Ačkoliv by se z předchozích řádků mohlo zdát, že používání jakýchkoliv zařízení v prostředí, které nemáme plně pod kontrolou, je neodpustitelným riskem, jedná se spíš o ukázku, že bezpečnost jako taková není stavem, ale neustálým procesem. Vyvíjejí se jak techniky útoků, tak naštěstí i způsoby obrany.

Zařízení postavená na kryptografických čipových kartách v současné době poskytují dostatečnou míru bezpečnosti pro mnoho aplikací. Budou-li v budoucnu obohacena o možnost zobrazovat informace o prováděných operacích, přidají-li se prvky pro jejich potvrzení či odmítnutí a bezpečné zadávání PINu, bude zase o něco náročnější zneužívat jejich slabiny.

Literatura

[1] Joe Grand, Grand Ideas Studio. *Attacks on and Countermeasures for USB Hardware Token Devices*. 2001. http://www.grandideastudio.com/files/security/tokens/usb_hardware_token.pdf.

[2] Ross Anderson, Mike Bond, Jolyon Clulow, Sergei Skorobogatov. *Cryptographic Processors – A Survey*. 2005. http://www.cl.cam.ac.uk/~mkb23/research/Survey.pdf.

[3] Secustick review. 2007. http://spritesmods.com/?art=secustick

[4] Matyáš Václav, Kouřil Daniel, Cvrček Daniel, Lorenc Václav. *Autentizační hardwarový token nové generace*. Datakon 2006. ISBN 80-210-4102-1, s. 229-238. 2006, Brno. □

Z historie výpočetní techniky na MU. Úvod

Miroslav Bartošek, ÚVT MU

V rámci letošního ročníkového seriálu chceme přiblížit čtenářům Zpravodaje ÚVT historii počítačů a výpočetní techniky na univerzitě. V každém čísle přineseme osobní vzpomínku některého z přímých účastníků – systémových programátorů – na počítače, které představovaly ve své době milníky v zavádění a využívání výpočetní techniky na naší škole.

Zatímco v tištěné verzi zpravodaje budou prezentovány většinou jen texty, v on-line verzi (http://www.ics.muni.cz/zpravodaj/) najdou zájemci i bohatší obrazovou dokumentaci k popisovaným počítačům.

První počítače na univerzitě byly v provozu od roku 1968 ve *Vědecko-metodickém středisku pro výpočetní techniku* při Katedře matematických strojů, na oboru matematika Přírodovědecké fakulty. Od roku 1979 převzal starost o zajišťování a provoz centrální výpočetní a komunikační technologie univerzity *Ústav výpočetní techniky*. Články seriálu pokryjí časově období let 1968 – 1994; tedy dobu od instalace prvního počítače na univerzitě až po okamžik, kdy končí éra velkých sálových počítačů a vlády se definitivně ujímají stroje vycházející z technologií osobních počítačů. Jde o čtvrtstoletí, v němž počítače představovaly fascinující zařízení dostupná jen hrstkám „zasvěcených"; čtvrtstoletí kdy počítače ještě zdaleka nebyly oním všedním a běžným nástrojem dostupným každému z nás.

Přehled důležitých milníků v historii výpočetní techniky na univerzitě je uveden v tabulce na následující straně.

V dnešním čísle zavzpomínáme na vůbec první skutečný počítač na univerzitě – počítač MSP 2A. V příštím čísle se pak budeme věnovat „vlajkovým lodím" výpočetní techniky minulého století – sálovým počítačům. Poté dojde na minipočítače, mikropočítače a nakonec i na první superpočítač na MU. □

1967	AP-4	analogový počítač (ČSSR);
1968	MSP 2A	malý samočinný počítač (ČSSR), první číslicový počítač na MU;
1979	EC-1033	sálový počítač (SSSR, kompatibilní s IBM 360), dávkové zpracování - ekonomické agendy, výuka;
1980	PDP-11/34	16-bitový minipočítač (USA), interaktivní přístup - výuka, výzkum;
1981	Consul	disketová pracoviště (Zbrojovka Brno), pořizování dat na floppy-disky;
1981	SAPI-1	8-bitový mikropočítač (ČSSR), řízení laboratorních zařízení a experimentů;
1986	PC10	první počítač třídy PC na UJEP (Commodore);
1987	PC TNS	slušovické počítače třídy PC;
1989	EC-1027	sálový počítač (ČSSR, kompatibilní s IBM 370), nahradil počítač EC-1033, ekonomické agendy;
1990	HDS 6660	sálový počítač (Hitachi, Japonsko, IBM 370), uzel počítačové sítě EARN/Bitnet;
1992	Internet	MU připojena do Internetu;
1994	SGI Power Challenge L	první superpočítač na MU;
1995	Sun SPARC Server 1000	na univerzitě ukončen provoz sálových počítačů, začíná éra malých výkonných Unixových serverů.

Tabulka 1: Důležité milníky v historii výpočetní techniky na MU

Z historie výpočetní techniky na MU. 1. Počítač MSP 2A

Jiří Franek, ÚVT MU

1 Prehistorie

Vědecko-metodické výpočetní středisko při Katedře matematických strojů Přírodovědecké fakulty UJEP (dále jen VS) – to byl celý honosný název výpočetního střediska, které bylo prvním specializovaným pracovištěm starajícím se na univerzitě o výpočetní techniku, a tedy i přímým zárodkem dnešního Ústavu výpočetní techniky MU[1] . VS vzniklo na jaře roku 1968 a zpočátku nemělo k dispozici vůbec žádnou výpočetní techniku; ta měla být dodána až v průběhu roku. Studenti oboru matematika, specializace numerická matematika, museli před rokem 1968 zpracovávat své úlohy buď na počítačích VUT (LGP 30, později SAAB) nebo Vojenské akademie (počítač Minsk 22). Programovalo se v jednoduchém procedurálním jazyce MAT 2, později ve Fortranu, Cobolu nebo Algolu 60.

Na univerzitě byl nejprve pořízen a nainstalován *analogový počítač AP-4*. Byl to zřejmě úplně první počítač, který kdy brněnská univerzita vlastnila (kromě oboru matematika měli s výpočetní technikou co dělat ještě lidé z oboru fyzika). Pro rozsáhlejší výpočty se však nehodil. Prvním skutečně univerzálním počítačem univerzity se stal teprve počítač MSP 2A.

V srpnu 1968 přibyl k počítači AP-4, umístěnému v suterénu budovy oboru matematika na Janáčkově náměstí, dlouho očekávaný přírůstek: první „sériově“ vyráběný počítač československé výroby – *počítač MSP 2A*. Poznámka k sériovosti: nejprve byly vyrobeny dva kusy počítače MSP 2, a po jistých úpravách pak 10 nebo 11 kusů s označením MSP 2A; z nichž hned druhý nebo třetí kus dostala naše univerzita. Tím také celá série skončila. Ostatní kusy z této „obrovské” série dostaly vesměs vysoké školy (VUT Brno, UK Bratislava, VŠP Nitra, Západočeská univerzita v Plzni, VŠE Praha aj.), takže se mezi nimi okamžitě rozběhla čilá spolupráce a výměna zkušeností. Jeden ze

[1] Ústav výpočetní techniky MU vznikl v roce 1979. O jeho historii se lze dočíst v článku M.Bartoška: *25 let ÚVT*, Zpravodaj ÚVT MU, roč. XIV, č. 5, s. 1-6, 2004. Online dostupný na `http://www.ics.muni.cz/zpravodaj/articles/304.html`

Obrázek 1: Studenti u operátorske konzoly počítače MSP 2A

strojů byl dodán brněnskému VUT a zpočátku byl umístěn v budově na Antonínské, tedy „za rohem". Tehdejší vedoucí Katedry matematických strojů, docent Jiří Hořejš[2] , okamžitě zorganizoval program společných seminářů, a mezi technikou a univerzitou byla navázána úzká spolupráce na vývoji programového vybavení.

2 Počítač MSP 2A

Počítač MSP 2A byl z dnešního hlediska velmi primitivní. Měl ferritovou paměť a registry založené na tzv. zpožďovacích linkách – což byly, laicky řečeno, stočené měděné dráty. Ty byly velmi citlivé na každou změnu teploty nebo napájecího napětí. Takže při každé exkurzi k počítači, kdy se na sále objevilo více osob najednou, docházelo pravidelně k tzv. generálskému efektu, kdy z důvodu zvýšení teploty na sále (o jeden až dva stupně) si počítač „postavil hlavu" a bylo potřeba vyčkat, až se zpožďovací linky „protáhnou".

Paměť počítače měla 10 000 míst, každé s dvanácti 5bitovými dekadickými znaky. Paměťové místo mohlo obsahovat buď číslo v pevné řádové čárce nebo dvě strojové instrukce obsahující dvoumístný operační kód a čtyřmístnou adresu. Soubor instrukcí byl dosti obskurní, svou filozofií však umožňoval některé zajímavé programátorské triky. Například indexování vícerozměrných polí se programovalo velmi pohodlně. Rychlost počítače MSP byla u běžných příkazů

[2]Osobnost Jiřího Hořejše přibližuje článek R. Ochranové a M. Bartoška: *K nedožitým sedmdesátinám docenta Jiřího Hořejše*, Zpravodaj ÚVT MU, roč. XIV, č. 1, s. 1-3, 2003. On-line dostupný na `http://www.ics.muni.cz/zpravodaj/articles/283.html`

asi 8 000 operací za sekundu, operace s čísly s pevnou řádovou čárkou byly o něco pomalejší. Protože počítač neměl procesor pro výpočty s pohyblivou řádovou čárkou, bylo nutno tyto operace emulovat a rychlost výpočtu v pohyblivé čárce byla až o dva řády nižší.

Co se týče periferních zařízení, byl počítač vybaven dvěma snímači a dvěma děrovači pětistopé děrné pásky, úzkou 16sloupcovou tiskárnou (pouze číslicovou), a mohutnou tzv. „rychlotiskárnou" o 128 sloupcích alfanumerických znaků. Pro bezprostřední ovládání počítače sloužil připojený elektrický psací stroj a malý panel s tlačítky pro vlastní start (viz obrázek). Psací stroj se také používal jako standardní vstup a výstup malého objemu dat.

Počítač neměl žádný operační systém nebo jiný programový prostředek, který by se dal takto nazvat. První akcí bylo vždy zavedení tzv. *zavaděče* – asi metrového kusu děrné pásky, který obsahoval jednoduchý program umožňující zavedení větších programů. Počítač také neměl žádnou vnější elektronickou paměť, kam by se daly ukládat programy a data (ty se děrovaly do děrných pásek); diskové paměti ještě neexistovaly, jen tu a tam se objevovaly bubnové magnetické paměti, a jediným použitelným typem vnější paměti byly magnetopáskové jednotky. Náš technik začal okamžitě vymýšlet způsob připojení magnetopáskových jednotek, dodávaných pro jiné počítače, k našemu MSP. Připojení dvou takových jednotek se nakonec podařilo. A protože tato vnější paměť' okamžitě pozvedla počítač MSP na podstatně vyšší úroveň, byly podobné úpravy – za našeho přispění – provedeny i na dalších strojích (UK Bratislava, VŠP Nitra, VUT, Plzeň).

Programy pro počítač byly psány buď' přímo ve strojovém kódu nebo v *Autokódu*, což byl jednoduchý jazyk dosti podobný jazyku MAT 2 u Minsku 22. Stejný jazyk byl tehdy používán také u počítače Elliot 503, který k nám byl dovážen z Francie. Aby se ušetřila práce, byl překladač Autokódu pro Elliot převeden nejprve do jakéhosi mezikódu a poté do strojového kódu MSP – počítalo se přitom s tím, že mezikód bude využit pro generování překladače i pro jiné typy počítačů (k čemuž ale nakonec nedošlo). Tento postup měl vzhledem k velkým rozdílům mezi strojovými kódy obou počítačů dva fatální následky. Prvním bylo to, že překladač pro MSP byl neúměrně velký – spotřeboval téměř celé jedno kolo děrné pásky. Po jeho zavedení snímačem děrné pásky se podlaha kolem počítače zaplnila nekonečnými papírovými „špagetami", jejichž opětné namotávání ničilo nervy a ukrádalo čas. Nemluvě o statické elektřině, kterou se namotávající pravidelně nabil, aby pak při prvním dotyku s uzemněným předmětem dostal nečekaný „kopanec". Druhým následkem byla nízká rychlost výpočtů v pohyblivé čárce – dělení dvou čísel probíhalo „rychlostí" asi 120 operací za sekundu! Není proto divu, že jedním z našich prvních programátorských cílů bylo napsat překladač znovu a lépe. To se také nakonec podařilo, rychlost se zvýšila téměř stokrát a velikost kotoučů děrné pásky (kromě překladače se používal i tzv. „interpret", něco jako dnešní real-time knihovny základních funkcí) se zmenšila na polovinu. Druhým naším programátorským cílem pak bylo napsat program pro ovládání počítače (tehdy se říkalo *monitor*), který by usnadnil veškerou manipulaci obsluhy s ním.

Přes počáteční problémy bylo přece jen výhodou, že počítač byl tak řečeno „doma" – k dispozici bylo takřka libovolné množství strojového času a studenti oboru matematika měli k počítači neomezený přístup. Hned první ročníky studentů, které se na MSP „vyučily", se blýskly vytvořením několika překladačů, z nichž některé byly přijaty do základního programového vybavení počítače. Vzpomínám si na návštěvu profesora Reichla, autora knihy o Algolu 60 a jednoho z prvních skutečných odborníků na výpočetní techniku u nás. Když mu docent Hořejš u počítače předváděl, co vše studenti vytvořili za jediný rok v rámci svých diplomových a ročníkových prací, nevěřil svým očím a jen udiveně kroutil hlavou. Myslím si, že už nikdy od té doby asi neměli studenti k počítači blíž.

Kromě již uvedených periferních zařízení jsme k MSP 2A připojili také souřadnicový zapisovač Benson, na kterém bylo možné vykreslovat výsledky numerických výpočtů – grafy, průběhy funkcí a podobně. To se až dosud napodobovalo na rychlotiskárně ve značně nižší kvalitě. Na tomto plotteru pak také vzniklo množství gra-

fických motivů, které se později objevily na různých materiálech prvních seminářů a počítačových konferencí.

Vzhledem ke svému nevhodnému fyzikálnímu principu byl počítač MSP 2A značně nespolehlivý, a také jeho údržba byla stále pracnější. Přesto vydržel v provozu více než osm let, než se někdy po roce 1976 definitivně rozpadl a už se jej nepodařilo oživit. V té době už pokroky ve výpočetní technice (stejně jako nároky na množství a rychlost výpočtů) běžely velmi rychle kupředu a bylo načase poohlédnout se po lepším stroji.

RNDr. Jiří Franek, CSc., dlouholetý pracovník ÚVT MU, nastoupil na univerzitu v roce 1968 jako programátor tehdy nově zřizovaného Vědeckometodického střediska pro výpočetní techniku při Katedře matematických strojů Přírodovědecké fakulty UJEP. Podílel se na tvorbě základního i aplikačního vybavení prvního univerzitního počítače MSP 2A. Po vzniku ÚVT se zabýval mj. vývojem systému Sirael pro disketová pracoviště Consul a vývojem aplikací v oblasti automatizovaných systémů řízení ASŘ (mzdové a ekonomické systémy). Vedle svých odborných aktivit proslul také jako vynikající kreslíř a grafik. Vytvářel obrázky, grafiky a plakáty s počítačovou tematikou pro konferenci SOFSEM, ilustroval řadu počítačových textů, skript i knih, a samozřejmě využil svého výtvarného nadání i ke zpestření každodenního života na ÚVT. Do důchodu odešel koncem roku 2006. □

Obsah

Editor: Miroslav Bartošek • Vydavatel: Masarykova univerzita • Žerotínovo náměstí 9, 601 77 Brno, CZ
tel.: 549 492 100 • e-mail: zpravodaj@muni.cz • WWW: http://www.ics.muni.cz/zpravodaj/
Sazba systémem LaTeX 2ε písmem LucidaBright • Tisk: Grafex Blansko • *Neprodejné* • ISSN: 1212–0901