

Bezpečnost internetového bankovníctví (3)

V internetu není zajištěna ani důvěrnost ani integrita přenášených dat. V návaznosti na články v předchozích dvou číslech ST se budeme věnovat východisku z této překerní situace.

Funguje-li to, je to dobré

Viděli jsme, že nástroje, které nám mají garantovat identitu protistrany a utajenost spojení, mohou fungovat (a pak mohou být velice silné) nebo nemusí (pak není garantováno nic), ale stěžejí se dobereme viníka. To je případ certifikátů a PKI. Další triviální podmínkou fungování internetového bankovníctví je, aby počítač nebyl prolezlý škodlivým softwarem. Problémů s bezpečností je ale nekonečně a my ani klient je nemůžeme vyřešit. Ba naopak, musíme připustit a předpokládat, že klient se nachází v nedůvěryhodném prostředí (osobní počítač, operační systém, internetový prohlížeč, internet). A východisko bylo vskutku nalezeno. Neřeší všechny problémy, ale řeší jich mnoho, dobře a efektivně.

Nezávislý bezpečný autentizační kanál

Východiskem je autentizace klientů a platebních příkazů prostředky (komunikačními kanály), které nezávisí ani na osobním počítači, ani na internetu. V podstatě se ujal dvě metody, a to autentizační kalkulačtor a SMS zprávy. To nutí útočníka ovládnout oba komunikační kanály, což (bohužel) možné je, ale útok je to velmi drahý a technicky náročný. Ze strany klienta je proto taková autentizace velmi vhodná pro ochranu masového internetbankingu, navíc účinná, uživatelsky jednoduchá a levná. V počátcích internetového bankovníctví tuto autentizaci zajišťovaly autentizační kalkulačtory, později jejich úlohu převzaly zprávy SMS. Mobilní telefony jako autentizační prostředky dokonce odsunuly do pozadí certifikáty (závisí na bezpečnosti PC i internetu) a částečně i autentizační kalkulačtory (znamenají většinou další výdaj a další nepohodlný předmět v kapse). Zkrátka uživatelé dostali do rukou hardware (mobilní telefon), který útočník obtížně spáruje s otevřeným komunikačním kanálem klient-banka na internetu v daném čase apod. Samotný mobilní telefon a samotný internet sice velkou bezpečností neoplyývají, ale dohromady vytváří ohromnou bariéru. Skutečně, současné útoky na klienty internetového bankovníctví (phishing nebo sociální inženýrství) jsou odborně na úrovni 1000 krát nižší.

Moderně: Chip Authentication Protocol

Trend nezávislé autentizace se bude dále prohlubovat. Do hry jistě vstoupí další

hardware, kterým je čipová platební karta. Klient ji už často má, pouze není plně využita. Málokdo si uvědomuje, že tento kousek silikonu umí operace asymetrické kryptografie, skrytý tajný klíč pro symmetric-



Obr. 1 Technologie CAP/DPA

ké šifry a ochránit soukromý podpisový klíč schématu digitálního podpisu. Ve skutečnosti je to další a opět nezávislý a velmi bezpečný kryptografický hardware, který už máme v kapse nebo peněžence. K využívání jeho nových funkcí postačí pouze klientovi doplnit čtecí zařízení, do něhož se čipová karta vsune. Toto „pouzdro“ se nazývá například „CAP reader“. Je to samostatná čtečka (s klávesnicí a displejem), která není propojena s počítačem ani internetem. Proto může garantovat vysokou bezpečnost příslušného komunikačního kanálu. Využití čipové platební karty pro autentizaci v internetovém bankovníctví se nazývá CAP/DPA (Chip Authentication Protocol/Dynamic Passcode Authentication). Může mít několik úrovní. Na té nejnižší úrovni čipová karta generuje jednorázové heslo pro přihlášení k účtu. Pak lze realizovat protokol challenge-response (bankovní web zašle klientovi výzvu, ten ji vloží do kalkulačtoru a odezvu kalkulačtoru opíše z jeho displeje do webového formuláře). Na té nejvyšší úrovni lze autentizovat důležité údaje z platební transakce, jak jsme tomu zvyklí u autentizačních kalkulačtorů. Ostatně, čipová karta zasunutá do CAP readeru se od současných autentizačních kalkulaček vůbec neliší. Jistěže i tato technika má své slabiny. Útočník může například internetové sezení unést a nechat uživatele pomoci technologie CAP autentizovat platební příkaz, ovšem do banky

ho neodeslat. Neprovedení platby může klientovi způsobit ve výjimečných případech škodu i větší než prozrazení detailů platby.

Další útoky a nástrahy

Dosud jsme nehovořili o kryptografických slabínách internetového bankovníctví. Patrně nejslofistikovanějším útokem je útok na samotný certifikát. V nedávné době byl díky známým slabínám v hašovaci funkci MD5 vytvořen platný certifikát, jež však certifikační autorita nikdy nevydala (<http://www.win.tue.nl/hashclash/rogue-ca/>). O chybě v Debianu (viz ST 8/08, str. 22) se ví už rok, a přesto existují internetové obchody (!), které provozují své SSL spojení s touto chybou, tedy klíči RSA, které jsou vybírány pouze z množiny o pár desetitisících prvcích (a tedy známými). Oblíbená sada útoků využívá phishing nebo sociální inženýrství, tj. vylákání číselných kódů nebo jiných údajů pro různé potřeby. Také současné praktiky telefonního bankovníctví jsou dosti středověké a vylákání nebo odposlech všech čísel bezpečnostního čísla (pod různými názvy u různých bank) není problém. S tímto číslem lze pak provádět nespočet útoků, třeba měnit číslo mobilu pro autentizaci nebo jiná nastavení, apod. Nedůslednost panuje i v oblasti autentizace příkazů. Například souhlas s inkasem někdy není potřeba autentizovat, a přitom ho útočník může zneužít stejně jako platební příkaz apod.

Závěr

Na bezpečnost internetu nebo počítače k němu připojeného by si málokdo vsadil, a přesto je to prostředí, kterému sdělujeme přístupové kódy a klíče k našim penězům. Hrajeme tichou hru s bankou, kdy ani jeden z nás nehovoří o bezpečnosti a doufáme, že až se něco stane, zaplatí to ten druhý. Naštěstí mezitím přišla vlna mobilních telefonů, která nabídla autentizační zprávy SMS jako přirozenou variantu k certifikátům a autentizačním kalkulačkám. Internetové bankovníctví může být a je díky těmto nezávislým kanálům přijatelně bezpečné. Navíc je tu velký potenciál v platební kartě, která je dalším bezpečným prvkem v rukou klienta. Nové možnosti skýtá také spojení čtečky nebo mobilu s touto platební kartou.

Vlastimil Klíma,
nezávislý kryptolog, v.klima@volny.cz

LITERATURA

[1] E-archivy článků z aplikované kryptologie
<http://cryptography.hyperlink.cz>, <http://crypto.hyperlink.cz>