Bezpečnost internetového bankovnictví

Bezpečnost internetového bankovnictví je založena na několika málo základních principech a asi sto tisíci detailech. Prvním je bezpečnost počítače, na němž provádíme bankovní transakce, a který je připojen do Internetu. Druhým je bezpečnost samotného Internetu a třetím bezpečnost a fungující infrastruktura veřejných klíčů (PKI).

Kolaps PKI

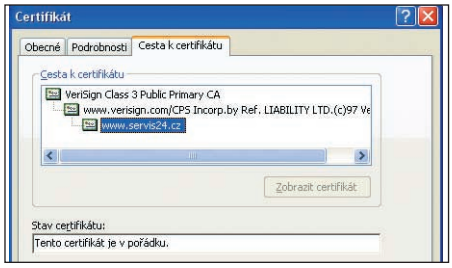
Určitě znáte pohádku o bezpečnosti internetového bankovnictví: „komunikace je šifrována pomocí protokolu SSL/TLS“, což poznáte podle adresy webové stránky, která má v názvu místo obvyklého http://www.banka.cz písmeno navíc (https://www.banka.cz) a podle ikony zámečku kdesi na obrazovce. Jedná se o idealizovanou koncepci, vyžadující spolupráci příliš velkého množství jednotek – celosvětové infrastruktury PKI, správně reagujících prohlížečů, bezpečných operačních systémů a proškolených uživatelů. Na klady a zápory této koncepce by nám nestačil celý časopis, proto v článku zobecňujeme a uvedená tvrzení platí pro obvyklé případy. K té obehrané pohádce: (a) komunikace může být šifrována, ale také nemusí, a ani zkušený „počítačník“ a uživatel Internetu to není schopen zjistit, (b) i když je šifrována, není jasné, s kým si to vlastně šifrujete, (c) velmi málo lidí je schopno si toto zjistit nebo ověřit, (d) uživatelé, kteří si zkontrolují alespoň ty dvě věci, které se jim vtloukají všude do hlavy (adresa a zámeček), jsou zcela jistě ostatními považováni za přehnaně paranoidní bezpečnostní mágy. A přesto mohou místo banky komunikovat s útočníkem (Man in the middle, MITM), který pouze zprostředkovává jejich komunikaci bance a zpět. Příčinou je PKI, které nemůže fungovat v době, kdy uživatel posuzuje míru důvěry podle počtu obtěžujících varovných hlášení na obrazovce, které musí odkliknout. Kolaps PKI nezpůsobila geniální myšlenka objevu veřejných klíčů, ale uživatelé, které ta infrastruktura kolem obtěžuje, nerozumí ji, a proto ji ignorují.

Když vše funguje

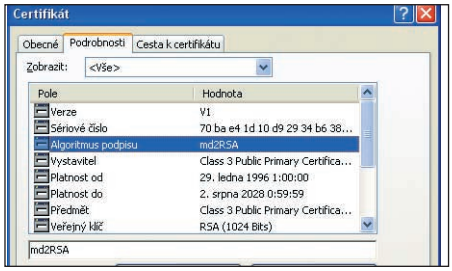
Když všechno funguje a je bezpečné, Internet zajistí, že se spojíme s bankou, se kterou se chceme spojit, PKI zajistí, že obdržíme její skutečný certifikát a internetový prohlížeč pomocí SSL/TLS zajistí, že komunikace s bankou je šifrována. To nám nakonec bezpečný prohlížeč v bezpečném počítači opravdu zprostředkuje tím, že vidíme ikonu zámečku a adresu banky https://. Avšak nic z toho, co je popsáno jako předpoklady, nemusí fungovat a také mnohdy nefunguje.

Certifikát neplní svou úlohu

Základním nástrojem PKI je certifikát, který vydávají certifikační autority, neboť právě a pouze certifikát banky říká, že komunikujeme s bankou, a nikoli s útočníkem. Certifikát může být formálně platný, kryptograficky zkontrolovaný, a přesto nebude patřit bance! Certifikát vydává bance certifikační



Obr. 1 Certifikační cesta (u 1. autora)



Obr. 2 Na vrcholu bezpečnosti sedí „MD2“

autorita (CA). Její verifikaci provádí jí nadřízená CA a jí opět nadřízená CA atd. Víte, kolik je ve vašem prohlížeči důvěryhodných certifikačních autorit? Víte kolik je bank na světě, kterým byly vydány nějaké certifikáty a kolik je takových certifikátů? A abychom si byli jisti, že komunikujeme se svojí bankou na adrese https://www.třebabanka.cz, muselo by PKI fungovat absolutně jednoznačně. V celé síti propojených desítek „známých“ důvěryhodných a tisíců soukromých certifikačních autorit se nikdy nesmí objevit žádná, která by vydala certifikát na jméno https://www.třebabanka.cz někomu jinému (útočníkovi) než skutečně mojí „třebabance“. Jakmile to nastane, útočník může komunikaci s bankou odklonit k sobě (tzv. únosem spojení) a provést útok MITM. Internetový prohlížeč přijme jeho platný certifikát (s falešnou identitou) ze sítě důvěry a my komunikujeme s ním místo s bankou. Kdo zaručí, že si útočník za padesát dolarů na Hawajských ostrovech nekoupí certifikát „třebabanky“ nebo rovnou certifikát pro vlastní certifikační autoritu? Pro příklad: Verisign vydal v roce 2001 certifikát pro Microsoft, a přitom to nebyl Microsoft [1].

Co certifikát zaručuje?

Skutečné pravé certifikáty, které používáte jako důvěryhodné, toho zaručují opravdu velmi málo! Můžete si najmout právníka v oblasti mezinárodního práva, předložit mu certifikát, po delší době pátrání k němu najít certifikační politiku a nechat si vyložit, co garantuje. To ovšem nestačí, protože pokud se spojujete s nějakým subjektem na Internetu, certifikáty se mohou předkládat dynamicky, tedy museli byste si nechat prověřit všechny certifikáty z celé sítě důvěry. Ovšemže prohlížeče disponují pro tento případ nastavitelnými výstrahami (že daný certifikát není v jakémsi seznamu…, že vydavatel certifikátu je neznámý…). Výstrahy ale problém neřeší, jen na něj upozorňují. Uživatelé nemají na výběr. Buď hlášku vezmou vážně a pak spojení (třeba s bankou) ani nenáváží, mohou jít hledat právníka nebo to risknou a hlášku odklepnou. V takovém případě je úplně jedno, zda je certifikační autorita důvěryhodná či nikoliv a PKI jako základ svojí bezpečnosti zcela pohřbívají. To je převažující ohromná množina uživatelů Internetu.

Fungující PKI

Pokud se k certifikátům budeme stavět my, náš prohlížeč i náš počítač jako k něčemu posvátnému, na čem závisí osud našich dat, pak PKI bude fungovat. Takové systémy PKI existují a jsou to podnikové certifikační autority. Důvěru zprostředkovává nikoli anonymní síť certifikačních autorit, ale jedna podniková autorita. Uživatelé opět nemají na výběr, neboť bezpečný počítač, síť, správně nainstalované a chráněné certifikáty pro ně zajišťuje tým, který se stará o bezpečnost, a ten jim prostřednictvím jiných mechanismů nedovolí se systémem důvěry něco dělat. Pak je možné takovou PKI využít k ochraně informací, a kryptografie s asymetrickými systémy pro podpisy a výměnu klíčů krásně plní svoje poslání důvěrnosti, autentičnosti a právní neodmítnutelnosti zodpovědnosti. Před soud zde můžeme postavit konkrétního útočníka. Zkuste ale před soud postavit nějaký server na Internetu! Nebo hawajského provozovatele CA za vydání certifikátu „třebabanky“.

Závěr

Odborníci již ví, že masové PKI zkolabovalo, ale nijak se to nepropaguje, jen se od zavedené písničky „zámeček na displeji vše zaručí“ bude ustupovat. Proč, začíná být jasné. Kam se bude ustupovat, to si ukážeme příště. Bude to jednoduché a bezpečnější.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, tomas.rosa@rb.cz

LITERATURA

[1] http://www.verisign.com/support/advisories/authenticodefraud.html