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

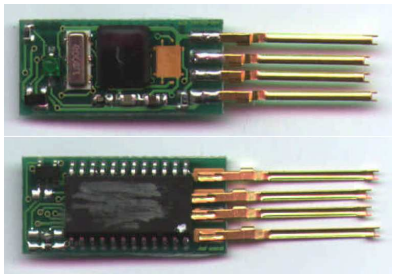
Aby mohl nějaký hardwarový token bezpečně poskytnout autentizaci uživatele a autorizaci jeho operací, je nutné, aby především on sám byl navržen s ohledem na požadovanou míru bezpečnosti. Ačkoliv se může zdát, že zařízení dostupná v současné době na trhu mají v tomto smyslu obdobné vlastnosti, ani zdaleka 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.

Obrázek 1: Čip obalů zbavený.



Obrázek 2: I takto může vypadat USB token uvnitř.

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 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.

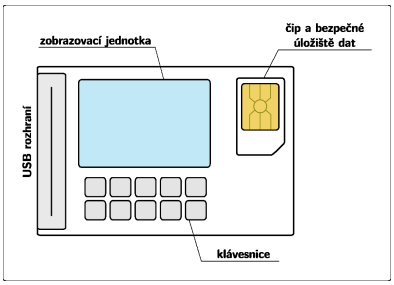
Situace se dále komplikuje v případě, že se jedná o používání HW tokenů v počítači pro potřeby nesouvisející s elektronickým bankovnictvím – např. pro autentizaci vůči firemní síti, ustanovení bezpečného připojení či pro podepisování a šifrování e-mailů. Tyto útoky, často automatizované, nevyžadují ani 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.



Obrázek 3: Návrh nového tokenu.

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. □