Správa soukromých klíčů pomocí hardwarových tokenů

Daniel Kouřil, ÚVT MU

PKI (*Public Key Infrastructure*) nabízí velmi bohaté možnosti pro realizaci silných autentizačních mechanismů a je také základem řady rozšířených protokolů používaných pro zabezpečení síťové komunikace (jako je např. SSL). Vedle svých silných stránek však také model PKI trpí neduhy, které plynou z principů, na kterých je založen a mohou velmi často snižovat celkovou bezpečnost systémů založených na tomto modelu. Tento článek se zabývá problémy, které se týkají správy klíčů v PKI a popisuje jejich možné řešení pomocí specializovaných HW zařízení.

Základním principem PKI je použití dvojice soukromého a veřejného klíče, kterou každý zúčastněný uživatel či služba vlastní a spravuje. Soukromý klíč se používá pro vytváření elektronických podpisů, které lze následně pomocí odpovídajícího veřejného klíče ověřit a zkontrolovat tak, že data skutečně pocházejí od majitele dvojice klíčů a že nebyla nijak modifikována při přenosu. Naopak pomocí veřejného klíče je možné zašifrovat data tak, že je lze dešifrovat pouze pomocí odpovídajícího klíče a je tak zaručeno, že je může přečíst opravdu pouze určený adresát, tj. majitel dotyčného páru klíčů. Jak plyne z názvu i popisu, soukromý klíč je určen pouze pro použití svým majitelem, který jej musí držet v tajnosti. Naproti tomu veřejný klíč je distribuován v rámci celé komunity a je volně k dispozici komukoliv, kdo má zájem navázat bezpečné spojení s majitelem tohoto klíče. Veřejné klíče se nejčastěji distribuují ve formě certifikátů veřejného klíče vydávaných certifikačními autoritami. Certifikáty obsahují identifikaci majitele klíče a další informace, které jsou důležité pro komunikaci, jako je doba platnosti klíče, adresa seznamu revokovaných certifikátů, emailová adresa uživatele či síťová adresa služby ad. Samotný proces vybudování kvalitní a důvěryhodné certifikační autority, definování certifikačního procesu a vytvoření systému důvěry mezi certifikačními autoritami a uživateli je zcela klíčový pro nasazení PKI, ale je mimo rozsah tohoto článku. Více informací o současných trendech v oblasti certifikačních autorit lze nalézt např. v minulém čísle Zpravodaje [1].

Správa soukromých klíčů je jedním ze základních problémů, se kterými se oblast PKI potýká. Klíče používané v PKI jsou velmi dlouhé řetězce znaků a na rozdíl od hesel si je člověk nemůže zapamatovat. Musí být proto uloženy v nějaké elektronické podobě tak, aby jej mohla přečíst aplikace, kterou uživatel používá. Nejčastěji se dnes klíče ukládají na lokální disk počítače, buď ve formě samostatného souboru nebo ve specializovaném úložišti, které poskytuje aplikace, příp. operační systém. Vždy se ale jedná o data, která jsou uložena na disku počítače a tudíž čitelná komukoliv, kdo má oprávnění číst příslušnou část disku. Pro ochranu před neoprávněným přístupem k těmto datům se používá šifrování souborů heslem, které musí uživatel zadat při přístupu k soukromému klíči. Navíc, pokud to použitý souborový systém dovoluje, bývá přístup k datům na disku chráněn proti přístupu jiných uživatelů na úrovni operačního systému. Úroveň takové ochrany soukromé klíče je ale velmi křehká, zejména pokud se případnému útočníkovi podaří získat práva majitele soukromého klíče nebo administrátora příslušného systému. Technik jak získat příslušná data z lokálního disku je celá řada, od použití počítačových virů, přes zneužití různých chyb v aplikacích běžících na daném počítači, až k technikám sociálního inženýrství, které zřejmě právě zažívají renesanci v podobě tzv. *rhybaření*[1]. Pokud se útočníkovi povede získat soubor se soukromým klíčem, může se pokusit najít správné heslo k rozšifrování tohoto souboru. Jelikož má data plně pod kontrolou a může je libovolně zpracovávat, např. nasadit klasické techniky pro lámání hesel, které známe z jiných oblastí – jako je hádání hesel hrubou silou nebo slovníkový útok.

Dostáváme se tak k další problematické oblasti správy klíčů, kterou je fakt, že zabezpečení souboru s klíčem je z velké části v rukách samotného uživatele. Navíc v oblasti PKI neexistují me-

[1] rhybaření (*phishing*) je technika, kterou se útočníci snaží z uživatelů vylákat citlivé informace (čísla kreditních karet nebo hesla) pomocí podvržené komunikace tvářící se, že opravdu přichází od oficiální instituce (jako je banka, administrátor systému). Viz také `http://en.wikipedia.org/wiki/Phishing`

chanismy, které by spolehlivě zajistily, že soubor s klíčem je patřičně ochráněn, tj. že použité heslo je dostatečně silné, aby odolalo běžným útokům, že jsou správně nastavena přístupová práva k souboru s klíčem apod. Uživatelé také mohou (a často tak také činí) libovolně manipulovat se souborem s klíčem, např. jej kopírovat na jiné počítače, kde klíč potřebují a při těchto operacích může také dojít k prozrazení obsahu soukromého klíče. Důsledkem zneužití těchto problematických míst pak může být velmi oslabený systém.

Výrazné zvýšení bezpečnosti by přineslo uložení soukromých klíčů na bezpečnější místo tak, aby neležely přímo na disku stroje, ale místo toho byly na nějakém jiném médiu, které se použije pouze v případě potřeby.

Hardwarové tokeny

Pro bezpečnější ukládání soukromých klíčů existuje několik alternativ, které se liší ve způsobu práce s nimi i v zabezpečení, které uloženým klíčům poskytují.

Nejjednodušší možností je použít nějaký typ vyjímatelného média, jako je např. disketa, CD-ROM nebo populární USB flash disk, na které se soukromý klíč uloží místo pevného disku. Po dobu práce je médium s klíčem zapojeno do počítače a aplikace s klíčem pracují stejně, jako by byl přímo na pevném disku počítače, tj. přistupují k souboru na výměnném médiu. Po ukončení práce uživatel vyjme médium z počítače a klíč tak není v počítači nadále dostupný a nemůže se stát předmětem útoku. Tento postup je sice jednoduchý, ale neposkytuje žádnou ochranu pro klíč v okamžiku, kdy je médium s klíčem připojeno k počítači. Navíc se zvyšuje riziko prozrazení klíče, protože médium je přenosné a může se ztratit nebo být ukradeno. Naopak výhodou tohoto přístupu je fakt, že jej lze začít používat okamžitě a nejsou potřeba žádné změny v aplikacích.

Další možností je použití *čipových karet* a příbuzných technologií, které obsahují jak chráněný prostor, do kterého lze uložit soukromý klíč s certifikátem, tak i samostatný procesor, který je schopen s těmito klíči pracovat a provádět s nimi základní kryptografické operace. Karta je k počítači připojena pomocí čtečky zapojené přes USB nebo sériový port, pomocí které komunikují aplikace s kartou. Aplikace tak nepoužívají přímo soukromý klíč, ale předávají kartě data, která jsou zpracována procesorem na tokenu a výsledek je vrácen zpět aplikaci. Klíč tak nikdy neopustí kartu a není jej možné nijak zkopírovat. Přístup ke kartě je autentizován, tj. aplikace se musí procesoru na kartě nejprve prokázat znalostí příslušného PINu, který zadá uživatel. Je tak zabráněno zneužití informací z karty v případě její ztráty. Většina karet je konstruována tak, že se po zadání určitého počtu chybných PINů zablokuje a jedinou možností jak ji zprovoznit je její nová inicializace, která však nevratně smaže všechny informace na kartě. Vedle čipových karet s čtečkami také existují *čipové tokeny* připojitelné do USB, které kombinují funkcionalitu karty a čtečky v jednom kusu hardware. Vzhledem se podobají USB flash diskům, ale vnitřní architektura je totožná s čipovými kartami, tj. obsahují vlastní procesor a není možné přistupovat přímo k citlivým datům na tokenu. Výhodou tokenů je jejich vyšší mobilita, protože není potřeba s sebou nosit kartu i čtečku. Další výhodou je jejich tvar, protože vzhledem k jejich malé velikosti je lze připojit např. ke svazku klíčů, takže se snižuje riziko, že zůstanou zapomenuté v počítači.

Technologie čipových karet a tokenů výrazně zvyšují ochranu soukromých klíčů, protože umožňuje jejich bezpečné uložení a přístup k nim. Zavádí pojem tzv. dvoufaktorové autentizace (*two-factor authentication*), kdy uživatel musí prokázat znalost nějakého tajného kódu (tj. PINu k tokenu) a také fyzické držení tokenu.

Praktické nasazení hardwarových tokenů

Tato kapitola popisuje prostředí vytvořené v průběhu řešení projektu „Univerzální autentizace pomocí hardwarových tokenů“, jehož cílem je nasazení tokenů v *META Centru*. *META Centrum*[2] je aktivita sdružení CESNET, která buduje a provozuje gridovou infrastrukturu v akademické síti CESNET2. Bezpečnostní infrastruktura *META Centra* je založena na autentizačním mechanismu Kerberos, kde se pro

[2] `http://meta.cesnet.cz/`

iniciální autentizaci uživatelů používá heslo. Vzhledem k popularitě a možnostem, které skýtá PKI jsme se rozhodli podporovat i tento mechanismus a zároveň vytvořit prostředí, které umožní vyřešit jednu z největších slabin PKI, kterou je správa soukromých klíčů. Vytvoření této podpory a vybavení aktivních uživatelů *META Centra* hardwarovými tokeny je cílem výše zmíněného projektu, který je řešen pod hlavičkou Fondu rozvoje sdružení CESNET a jehož řešiteli jsou MU v Brně, UK v Praze a ZČU v Plzni.

META Centrum vytváří virtuální organizaci, všichni jeho uživatelé jsou rozprostření po celé ČR a jsou primárně zapojeni v infrastruktuře svých domovských institucí. *META Centrum* nemá žádné nástroje (ani ambice), jak ovlivňovat lokální nastavení jednotlivých institucí. Naší hlavní snahou při řešení projektu HW tokenů proto bylo vybrat taková zařízení a programová vybavení, která všem uživatelům umožní hladké zapojení tokenů do stávajícího prostředí. Jednou z priorit proto bylo umožnit práci s tokeny na více platformách, nezbytnou podmínkou byla práce jak na MS Windows, tak i Linuxu. Vzhledem k tomu, že uživatelé i migrují mezi různými systémy, snažili jsme se najít řešení, které umožní přecházet mezi těmito platformami při zachování plné funkčnosti tokenu. Jelikož nezbytnou součástí projektu byly změny naší současné infrastruktury, zaměřovali jsme se především na použití open-source aplikací, které v případě potřeby umožňují provádět snadné zásahy do kódu.

Ve fázi výběru nejvhodnějšího typu tokenu jsme testovali několik vzorků jak čipových karet a čteček, tak i USB tokenů. Od začátku jsme sice preferovali spíše USB tokeny, zejména pro jejich snadnější fyzickou přenositelnost, ale chtěli jsme ověřit, že USB zařízení jsou skutečně ekvivalentní klasickým čipovým kartám. Mezi kritéria, která jsme vyhodnocovali, patřila zejména schopnost tokenu či karty provádět kryptografické operace a chránit soukromý klíč. Dále jsme se zaměřili na podporu příslušného typu tokenu v současných open-source produktech a možnosti používat zařízení na různých OS. Ověřovali jsme také podporu pro běžně používané standardy PKCS11 a PKCS15, které umožňují vyvíjet a používat aplikace nezávisle na konkrétním typu zařízení. Vyhodnocení ukázalo, že testované USB tokeny jsou skutečně funkčně zcela ekvivalentní čipovým kartám.

K dalšímu testovaní a pilotnímu provozu jsme vybrali USB token iKey 3000 od firmy Rainbow (nyní SafeNet). Každý token se dodává s ovladači a základním programovým vybavením pro OS Windows a Linux. Instalace na OS Windows byla bezproblémová, pro použití na OS Linux jsme se rozhodli nepoužívat dodávané ovladače a software, které byly dodávány pouze v binární verzi, nefungovaly ve všech Linuxových distribucích a zejména se nepodařilo je bezproblémově zaintegrovat do middleware *META Centra*. Pro tokeny iKey 3000 však existují kvalitní alternativní ovladače pro Linux i další open-source software. Pomocí těchto alternativních ovladačů lze bez problémů používat token, který byl inicializován originálním ovladačem a softwarem, takže jej lze snadno přenášet mezi různými systémy. Bohužel opačná možnost nefunguje, open-source nástroje nejsou schopny inicializovat token ve formátu, který by byl čitelný originálním softwarem. Nepovažujeme to však za významnou obtíž, protože uživatelé, kteří přechází mezi více systémy, mají vždy možnost inicializovat token v prostředí Windows pomocí originálního vybavení.

Bez výraznějších problémů se povedlo zprovoznit podporu tokenů ve frekventovaných aplikacích. V prostředí MS Windows jsme token testovali s aplikacemi Internet Explorer, Outlook, Mozilla Thunderbird a Mozilla FireFox. Lze tak snadno používat klientskou autentizaci při přístupu na chráněné www stránky, podepisovat, resp. dešifrovat emailovou komunikaci. Poslední tři aplikace spolupracují s tokeny i v prostředí Linuxu. Pro vzdálené přihlašování lze použít aplikace PuTTY nebo OpenSSH, které mají podporu pro hardwarové tokeny a lze je používat jak v prostředí MS Windows, tak i v Linuxu. V prostředí obou systémů také funguje balík OpenSSL, který umožňuje provádět kryptografické operace s tokenem. Obecně lze říci, že podporu tokenů lze zprovoznit ve většině aplikací, které podporují rozhraní PKCS11.

Pro programování vlastních aplikací, které používají token, jsme použili open-source knihovnu

OpenSC[3], která je dostupná ve verzích pro Linux i MS Windows. Tato knihovna nám umožnila vytvořit aplikace pro tokeny nezávisle na konkrétním operačním systému. Pro správnou funkci této knihovny je potřeba mít instalované ovladače konkrétního tokenu, ale protože knihovna umí komunikovat jak s originálními ovladači (na MS Windows), tak s alternativními ovladači (na Linuxu), mohli jsme se soustředit na vývoj vlastní aplikace a nezatěžovat se nižšími detaily komunikace s tokenem.

Nedílnou součástí projektu byla úprava stávající infrastruktury *META Centra* tak, aby umožnila hladké nasazení hardwarových tokenů. Vedle zprovozňování a konfigurace dodaného vybavení jsme se soustředili na vývoj vlastního software a potřebných nástrojů. Nejdůležitějším úkolem bylo připravit současnou autentizační infrastrukturu tak, aby umožňovala použití PKI autentizace pomocí hardwarových tokenů. Bezpečnostní infrastruktura *META Centra* je založena na mechanismu Kerberos, který podporuje autentizaci pomocí hesla a symetrické kryptografie. Jedním z prvních úkolů projektu tedy bylo upravit protokol Kerberos tak, aby umožňoval i autentizaci pomocí PKI certifikátů. Využili jsme aktivit standardizační organizace IETF a převzali tehdejší návrh úprav protokolu a podle tohoto návrhu jsme navrhli a realizovali změny do implementace protokolu Kerberos. Jednalo se o velmi komplexní zásah do kódu, ale výsledkem byla funkční a kompatibilní realizace tohoto rozšíření. Výsledná verze byla přejata do standardní distribuce a v současné době je dále vyvíjena a používána i dalšími organizacemi ve světě, které nasazují čipové technologie v prostředí s protokolem Kerberos.

Vedle zapojení tokenů do stávající infrastruktury *META Centra* jsme nachystali nástroje, které umožní použití tokenů v mezinárodním gridovém prostředí, které používá PKI a speciální tzv. proxy certifikáty (viz také [1]). Využili jsme vlastností, které pro manipulaci s proxy certifikáty nabízí knihovna OpenSSL a pomocí ní implementovali program, který pomocí tokenu generuje proxy certifikáty.

[3] `http://www.opensc.org/`

META Centrum vždy úzce spolupracovalo s certifikační autoritou sdružení CESNET. Certifikáty vydané touto CA jsou uznávány širokou komunitou v rámci celé Evropy a držitelé těchto certifikátů se tedy mohou snadno zapojovat do mezinárodních projektů. Pro podporu uživatelů *META Centra* jsme dohodli zřízení Registrační autority pro CESNET CA, která bude provozována na ÚVT MU a bude usnadňovat získání certifikátu jak pro uživatele *META Centra*, tak i MU.

V současné době je infrastruktura *META Centra* připravena k nasazení tokenů. Administrátoři byli vybaveni vybranými USB tokeny již dříve a v současné době je používají k administrátorským účelům. Připravili jsme nákup většího množství tokenů a připravujeme v brzké době jejich distribuci mezi cca 150 aktivních uživatelů.

Vedle přípravy technického zázemí bylo úkolem projektu vyřešit i logistické problémy s distribucí tokenů. Situace *META Centra* je odlišná od jiných prostředí, protože máme velmi distribuované uživatele, což velmi komplikuje fyzické předání tokenů. Nakonec jsme se rozhodli uspořádat krátké semináře s jednotlivými skupinami uživatelů, které se budou konat přímo v jejich lokálních institucích. V rámci těchto seminářů uživatelům předáme tokeny, předvedeme jejich funkcionalitu, jejich zapojení do *META Centra* a příp. gridových aktivit a zejména vyřešíme na místě otázky spojené s žádostí o certifikát od CESNET CA, protože k tomuto kroku je nutný fyzický kontakt s pracovníkem CESNET RA, který ověří identitu žadatele. Věříme, že výsledkem bude hladké zapojení tokenů do infrastruktury a tím zvýšení celkové bezpečnosti *META Centra*. Navíc výsledky a zkušenosti s touto netechnickou fází budou cenné do budoucna, protože řada velkých mezinárodních projektů se začíná zabývat myšlenkami na použití hardwarových tokenů a jejich distribuce rozsáhlém prostředí je samozřejmě klíčová.

Literatura

[1] D. Kouřil. „Bezpečnost v distribuovaném prostředí.“ *Zpravodaj ÚVT MU*. 2005, roč. 15, č. 4, s. 2–6. □