Cesta k digitální identitě

Naše osobní údaje jsou uloženy v mnoha informačních systémech a jejich bezpečná správa není právě jednoduchou úlohou. Autentizační systémy se stávají složitějšími, podniky zase otevřenějšími.

Internet se stal hlavním zdrojem informací, pracovním nástrojem, zábavním podnikem a stále více i zdrojem příjmů „elektronické" společnosti. Z původně jednoduché sítě s několika uzly vyspěl ve složitý organický systém. A jak tomu u takových systémů bývá, se stoupající složitostí rostou i nároky na bezpečnostní systémy.

Tradiční bezpečnostní systémy

Nejrozšířenějším autentizačním prostředkem, používaným prakticky od okamžiku vzniku počítačových systémů, byla a stále jsou statická hesla. Autentizace hesly je s dnešními informačními systémy natolik spjatá, že její náhrada za jiné, silnější autentizační metody je většinou velmi pracná a bolestivá. Ale i tak se touto nelehkou cestou vydává stále více organizací.

Dalším z podstatných problémů při tvorbě moderních informačních systémů je integrace. Tento problém má vážný dopad na oblast informační bezpečnosti . Jednotlivé informační systémy dnešních organizací byly většinou budovány nezávisle na sobě a spolupráce dílčích aplikací je minimální. Jako příklad může sloužit databáze uživatelů systému: ve všech systémech má téměř stejný obsah, ale její struktura a komunikační rozhraní jsou většinou diametrálně rozdílná. Zejména v oblasti bezpečnosti představuje tento stav značné riziko, neboť případné nekonzistence velmi lehce přerostou do bezpečnostních problémů.

Public Key Infrastructure

V prostředí Internetu se v podstatné míře využívá infrastruktura veřejného klíče (PKI), založená na doporučení X.509. Nejběžnějším příkladem je použití certifikátů X.509 pro jednostrannou autentizaci SSL spojení, využívané hlavně u protokolu HTTPS. Mezi další možnosti použití patří vzájemná autentizace uzlů komunikujících protokolem IPsec, podepisování apletů atd. Z těchto příkladů je jasně vidět, že PKI se v praxi používá hlavně pro autentizaci neživých entit, jako jsou například servery, síťová zařízení atd., a jen málo se využívá pro autentizaci uživatelů.

Jedním z důvodů nízké akceptace PKI je její značná složitost; plná implementace X.509 a doprovodných specifikací je dosti náročná. Problematické je hlavně získávání certifikátů, ověřování jejich platnosti a zneplatňování. Mezi další komplikace patří nízká úroveň standardizace obsahu certifikátu. Pro použití v některých systémech sice existují specifikace profilů certifikátů, avšak implementace PKI je naplňují jen zřídka.

Mezi hlavní problémy PKI však patří soukromí uživatelů. Důležitá je především otázka, kolik a jaké osobní údaje má certifikát obsahovat. Bude-li jich málo, bude certifikát použitelný jen v jednom uzavřeném systému, pokud by jich bylo mnoho, nemuseli by uživatelé být ochotni certifikát z důvodů ochrany svého soukromí prezentovat.

Lze očekávat, že jedním z podstatných důvodů pro nasazení PKI dle X.509 bude předpokládaná právní závaznost elektronického podpisu, ovšem přesto zde zůstává řada otevřených otázek.

Pro zaručení nepopiratelnosti (angl. *non-repudiation*) elektronického podpisu je nutné vzít v úvahu mnohem více faktorů nežli jen samotný algoritmus elektronického podpisu. Nutnou podmínkou je důvěryhodná služba časových razítek, spolehlivá možnost ověření aktuálního stavu certifikátu, ale i způsob vytvoření elektronického podpisu, který je pro důvěryhodnost celého systému kritický. Například tvorbu elektronického podpisu v běžném osobním počítači typu PC není možné považovat za dostatečně bezpečnou a to ani v případě, že pro vlastní kryptografické operace slouží speciální zařízení typu kryptografická čipová karta apod. Výpočetní systém, ve kterém je podpis vytvářen, lze modifikovat prostřednictvím počítačového viru nebo i jinak a uživateli mohou být zobrazeny odlišné údaje než ty, které ve skutečnosti podepíše. Takový podpis může být ve většině právních systémů zpochybněn.

Z předcházejícího textu je zřejmé, že možnosti nasazení technologie PKI jsou u reálných systémů značně omezeny [1] a většinou se lépe hodí na řešení dílčích problémů v relativně uzavřených systémech.

Identity Management

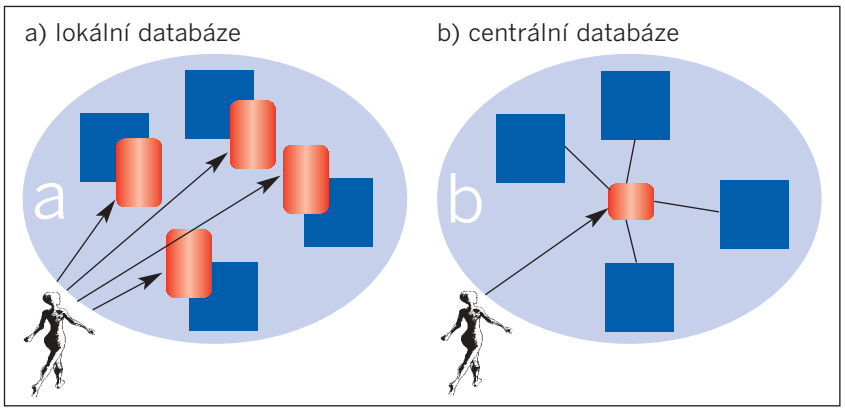
Technologie náležející do skupiny *Identity Management* přistupují k řešení podobných problémů z jiné strany. Cílem managementu identit je co nejvíce zjednodušit správu uživatelů, jejich atributů, autentizačních mechanismů atd. Takto vybudované mechanismy je potom možné využít jako službu i v jiných systémech nebo dokonce u jiných organizací.

Vezměme si modelový případ běžného podnikového informačního systému. Každá jeho aplikace má vlastní databázi uživatelů (viz obr. 1a). Záznamy o uživatelích se musí udržovat v každé databázi zvlášť, velmi lehce tedy vznikají nekonzistence či chyby a bezpečnostní audit se stává noční můrou příslušných pracovníků.

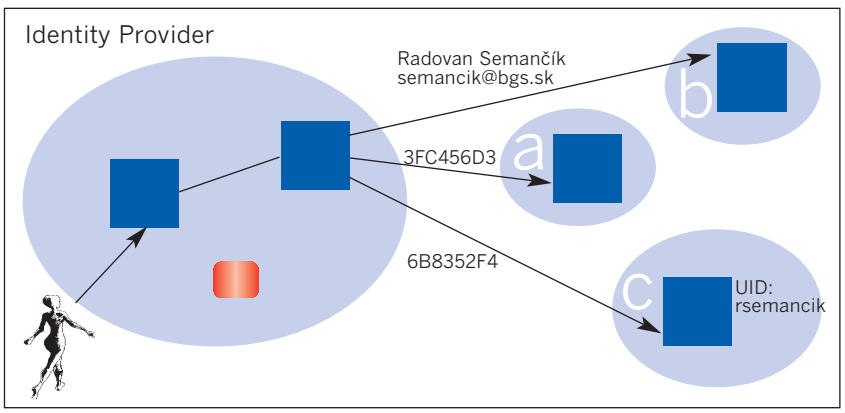
Prvním krokem k zlepšení situace bývá nasazení systému jednotné správy uživatelů. Databáze uživatelů se vede jen v jediném systému a ostatní ji využívají (viz obr. 1b). Jako jednotící prvek většinou slouží adresářový server LDAP, komunikaci s ostatními systémy řeší různé metadirectory a „provisioning" servery. Tímto způsobem je možné správu systému urychlit, zefektivnit a v neposlední řadě i snížit provozní náklady.

Avšak i toto řešení má však své nevýhody. Adresářové servery se výborně hodí k ukládání uživatelských údajů, pro autentizační nebo jiné bezpečnostní účely však nebyly navrhovány. Je zřejmé, že pro poskytování dalších služeb, jako například zjednodušené přihlášení (angl. *simplified sign-on*), je nutné rozšířit funkčnost adresářových serverů o nové vlastnosti. Takto rozšířený server se nazývá identity server a poskytuje okolním systémům službu managementu uživatelů.

Jazyk, kterým identity server komunikuje s okolím, se nazývá Security Assertion Markup Language (SAML) [2] a je založen na XML. Tento jazyk definuje tzv. *bezpečnostní tvrzení*, která poskytují informaci o provedené autentizaci, atributech nebo o provedeném autorizačním rozhodnutí. Využitím autorizačních tvrzení je možné snadno implementovat otevřený systém zjednodušeného přihlášení. V tomto případě při změně autentizačního mechanismu už není třeba měnit všechny aplikace, ale stačí jen modifikovat konfiguraci identity serveru. Možností využití identity serveru je však mnohem více a jeho schopnosti přesahují hranice podniku.



Obr. 1: Jednotná správa uživatelů.



Obr. 2: Poskytování identity služeb.

Identita v globálním prostředí

Řešení managementu identit v podnikovém prostředí přinese nesporně řadu výhod, zůstane-li však omezeno jen pro jednu organizaci, nebude dostatečně komplexní. Podniky se stále více otevírají světu, vyměňují si obchodní informace i jinak spolupracují. Podobně jako se otevírají podnikové informační systémy, musí se otevírat i jejich bezpečnostní jádro – systém managementu identit.

Velmi lákavá je i perspektiva „identity outsourcingu". Některé firmy vložily prostředky do moderních autentizačních systémů pro své zákazníky, ať již šlo o nasazení PKI, čipových karet nebo bezpečnostních tokenů. V každém případě se však nejednalo o malou investice a možnost sdílet náklady na autentizační systém s obchodními partnery je nesporně zajímavá.

Představme si organizaci, která má silný autentizační systém nasazený pro své zákazníky (*identity provider*). Tato organizace chce svým partnerům poskytnout možnost autentizovat uživatele systému aniž by partneři věděli, o kterou konkrétní osobu se jedná. Tuto službu může identity provider poskytnout pomocí jazyka SAML. Zprávu o úspěšné autentizaci uživatele pošle jako *bezpečnostní tvrzení* cílové organizaci (viz obr. 2), toto tvrzení připomíná jednoduchý certifikát zapsaný v jazyku XML, vytvořený ale jen pro jedinou transakci.

Jestliže uživatel povolí zveřejňování části osobních údajů, tyto budou poskytnuty cílovému systému (obr. 2, případ A) a uživatel si tak ušetří zdlouhavé vyplňování registračních formulářů. Jestliže cílový systém nemá dostatečnou důvěru uživatele, pošle se jen náhodně vygenerovaný identifikátor (obr. 2, případ B). Tento identifikátor stačí, aby si uživatel mohl personalizovat stránku, anonymně předplatit službu, atd. Může se také stát, že uživatel už má na cílovém systému vytvořený přístupový účet (obr. 2, případ C). Při prvním pří-

stupu přes identity providera mu cílový systém může nabídnout sdružení (angl. *federate*) jeho starého účtu s identity providerem. Pokud uživatel přistoupí k údajům příště, nemusí se již přihlašovat k cílovém systému, ale stačí mu přihlášení k identity provideru. Identity provider však o uživateli žádné nové informace nezíská, ty jsou stále udržovány lokálně na cílovém systému.

Technologie digitální identity se vůči systémům X.509 PKI liší v několika podstatných směrech. V první řadě mají bezpečnostní tvrzení používaná v systémech digitální identity relativně krátkou platnost (minuty) oproti platnosti certifikátů X.509 (roky). Kratší platnost umožňuje mnohem větší flexibilitu a lépe vyhovuje dynamickým údajům, vyžaduje však striktně on-line přístup. Identity server provádí autentizaci a udržuje uživatelské informace, čímž se staví do bezpečnostně velmi citlivé pozice. V systémech PKI jsou uživatelské informace a klíčový materiál uloženy v počítači uživatele, přičemž se zde provádí i vlastní kryptografické operace. Při nízké bezpečnosti běžných počítačů však tento přístup nemusí být ideální a vhodnější může být centralizované řešení digitální identity.

V praxi se ukazuje, že systémy PKI budou využity jako základ, na kterém se budou stavět systémy digitální identity. Digitální PKI certifikáty budou přiděleny jednotlivým serverům v systému a koncový uživatel se bude autentizovat vůči identity serveru libovolnou metodou (heslo, token, certifikát atd.). Informace o uživateli se budou pravděpodobně přenášet pomocí protokolu SOAP zapsané v jazyku SAML. Tento přenos bude chráněn protokolem TLS (SSL) autentizovaným pomocí X.509.

Jednou z důležitých iniciativ v oblasti digitální identity je Liberty Alliance Project [3]. Toto sdružení firem z oblasti IT průmyslu a jejich zákazníků usiluje o specifikaci systému digitální identity pro prostředí globálních sítí. V červenci roku 2002 byly zveřejněny specifikace první fáze projektu, které jsou zaměřeny hlavně na otevřený systém jednotného přihlášení (SSO). V době psaní tohoto článku jsou již k dispozici předběžné specifikace druhé fáze projektu, které dávají tušit mnohem širší možnosti využití technologií digitální identity.

Využití digitální identity v budoucnosti

Technologie digitální identity mají svůj základ v Internetu, jejich primární využití se však předpokládá v podnikové oblasti. Dnešní moderní podnikové prostředí se od Internetového liší už jen málo a s postupným rozšiřováním B2B a webových služeb se tento rozdíl stále více stírá. Identity server může sloužit jako centrální úložiště uživatelských údajů, zabezpečovat jednotné přihlášení a poskytovat další podobné služby. Tyto služby se s postupným otvíráním informačních systémů podniků přímo rozšíří i do Internetu.

Přímým přínosem pro uživatele Internetu bude možnost udržovat svůj uživatelský profil na serverech identity providerů. Tento profil potom bude možné použít pro řízené sdílení osobních informací s poskytovateli obsahu. To, čeho je dnes dosaženo pomocí nepohodlných registračních formulářů, bude moci být v budoucnosti automatizováno. Kromě pohodlí a lepší kontroly nad osobními údaji se však nabízí další využití. Atributy v osobním profilu totiž nemusí být statické, ale mohou se podle stavu uživatele měnit. Jestliže jste například na služební cestě, identity server může lokalizovat vaši polohu a s vaším svolením tento údaj sdílet s informačním portálem, který vám automaticky nabídne program kina ve městě, kde se právě nalézáte. Dynamický profil však lze využít i pro jiné služby, jako je například plánovací kalendář nebo stále populárnější systémy typu „instant messaging". Tyto rozšířené „identity-enabled" služby budou velkým přínosem hlavně pro podnikové uživatele, neboť dovolí jednodušší a lepší spolupráci mezi partnerskými organizacemi.

Závěr

Služby, které infrastruktura digitálních identit umožní, se snad ani nedají vyjmenovat. Již dnes jsou na trhu k dispozici konkrétní systémy vycházející z principů digitální identity, jejichž počet trvale roste. Momentální stav dané technologie umožňuje efektivně vytvářet pilotní i produkční řešení střední velikosti, která mohou v průběhu jednoho až dvou let představovat solidní základ rozsáhlejších infrastruktur.

Hlavní přínos „identity" technologií je však v jejich spojení s webovými službami. Identity technologie mohou poskytnout architektonickou vrstvu, která může doplnit webové služby o nový rozměr. Jestliže se tak opravdu stane, už jen málokdo bude pochybovat o tom, že identita je středem světa...

Radovan Semančík
semancik@bgs.sk

Odkazy:

[1] Ellison, C., Scheier, B.: Ten risks of PKI, Computer Security Journal, 2000, *http://www.counterpane.com/pki-risks.html.*

[2] Hallam-Baker, P., Maler, E.: Assertions and Protocol for the OASIS Security Assertion Markup Language, OASIS Standard, 2002.

[3] Liberty Alliance Project, *http://projectliberty.org/*.

Ing. Radovan Semančík
Pracuje jako Chief Information Officer ve společnosti Business Global Systems. Specializuje se na informační bezpečnost a distribuované systémy. Je absolventem Fakulty elektrotechniky a informatiky Slovenské technické university v Bratislavě.

MANAGEMENT SUMMARY

Článek sumarizuje přístupy k tvorbě bezpečnostních infrastruktur v podnikovém a Internetovém prostředí. Zvláštní pozornost je věnována technologiím digitální identity založeným na jazyku SAML.