Bezpečnost v distribuovaném prostředí

Daniel Kouřil, ÚVT MU

V současných vědeckých disciplínách lze najít řadu oblastí, které se neobejdou bez ohromné výpočetní síly, kterou dnešní počítače nabízejí. Příkladem může být oblast výpočetní chemie, fyziky vysokých energií nebo biomedicíny. Některé úlohy jsou však tak rozsáhlé, že jejich řešení by na běžně používaných počítačích zabralo velmi dlouhou dobu, proto se často používají superpočítače nebo clustery, které nabízejí výrazně vyšší výkon. Protože s jídlem roste příslovečná chuť, uživatelům často nestačí ani výkon těchto systémů a hledají ještě výkonnější varianty, které by byly schopné efektivně zpracovávat jejich náročné úlohy.

Oblast náročných výpočtů dnes směřuje k budování a podpoře tzv. *Gridů*[1]. Zjednodušeně lze říci, že gridy umožňují uživatelům využít výpočetní kapacity z různých institucí a přitom uživateli vytvářejí jednotné prostředí a skrývají rozdíly mezi jednotlivými systémy. Jednotlivé systémy zapojené v gridu jsou však stále autonomní a jejich administrátoři mají nad nimi plnou kontrolu. Gridy jsou charakteristické dynamickým prostředím, kdy připojení i odpojení zdrojů je velmi dynamický proces. Stejně tak se může část gridové infrastruktury stát dočasně nedostupná, například kvůli problémům se síťovou konektivitou. Gridová infrastruktura se však snaží zajistit, aby takové dynamické změny minimálně ovlivnily práci uživatele i zpracování jeho úloh.

Takové rozsáhlé a dynamické prostředí přináší nové bezpečnostní problémy, pro které je nutné najít spolehlivá řešení. Na následujících řádcích se snažím zprostředkovat čtenáři pohled na problematiku bezpečnosti v dnešních systémech pro řešení náročných úloh, zejména s důrazem na rozsáhlé projekty, které spojují mnoho různých institucí a často přesahují území jednotlivých států, či kontinentů.

[1] jazykové puristy odkazuji na diskusi o správném českém překladu tohoto termínu na `http://meta.cesnet.cz/cs/grid.html`

1 Autentizace

Autentizace je proces ověření identity uživatele nebo služby. Nejčastěji používanou metodou autentizace v dnešních počítačových systémech je kombinace uživatelského jména a hesla, které se ověřuje proti nějaké databázi. Vzhledem k organizačním a geografickým vzdálenostem, ve kterých se gridové projekty realizují, ale tato metoda není vhodná. Bylo proto potřeba najít autentizační metody, které budou dostatečně jednoduché na používání, ale přitom škálovatelné a interoperabilní a které bude snadné administrovat. V gridech se proto používají technologie založené na PKI (*Public Key Infrastructure*), kdy každý uživatel a služba vlastní certifikát veřejného klíče podepsaný některou důvěryhodnou certifikační autoritou (CA). Tento certifikát spolu s odpovídajícím soukromým klíčem pak používá pro svou autentizaci. Technicky je tento mechanismus léta znám a používán, zejména v menším měřítku. V gridovém prostředí je ale potřeba stabilní produkční prostředí, které zajistí maximální interoperabilitu mezi zúčastněnými stranami. Bylo proto potřeba definovat pravidla, která musí splňovat každá certifikační autorita a mechanismy, které ověří, že tato pravidla jsou opravdu dodržována. Minimální požadavky jsou nastaveny tak, aby zajišťovaly důvěru v informace v certifikátu, zejména v to, že fyzický majitel certifikátu je skutečně osoba nebo služba v certifikátu uvedená. Mezi minimální požadavky na CA patří zejména nutnost předložení osobních dokladů žadatele při podávání žádosti o certifikát, dále tyto požadavky vyžadují, aby počítač, na kterém se provádí operace s podepisovacím klíčem CA, nebyl připojen k žádné počítačové síti, vyžadují aby všechny operace s tímto klíčem byly logovány, kladou důraz na včasné vydávání revokačních listů apod.

Velkým úspěchem gridových aktivit je vytvoření prostředí, které takovou klasifikaci certifikačních autorit umožňuje. V současné době je v každém evropském státě, který má nějakého účastníka gridových aktivit, alespoň jedna certifikační autorita, která splňuje takové minimální požadavky. V České republice máme CA[2], kterou vybudovalo a provozuje sdružení CESNET a která

[2] `http://www.cesnet.cz/pki/`

umožňuje všem členům české akademické obce získat certifikát uznávaný všemi významnými gridovými projekty v Evropě. Protože podobné aktivity pro definování minimálních požadavků existují i v zemích severní Ameriky a Asie, lze čekat, že v horizontu několika let bude možné použít certifikát vydaný CA CESNET pro přístup ke gridovým službám na celém světě. Zároveň je snaha přenést tyto aktivity i do prostředí, které s gridy přímo nesouvisí, příkladem může být projekt TACAR[3], který pod záštitou sdružení TERENA buduje adresář důvěryhodných evropských CA a je z velké části založen na gridových autoritách. V budoucnu by tak mělo být možné používat certifikát od CA CESNET pro přístup k řadě akademických služeb v rámci celé Evropy, později i jinde ve světě.

Každý gridový uživatel tedy má certifikát, jehož odpovídající soukromý klíč má uložen na disku a zašifrován heslem. Aby uživatel nemusel zadávat toto heslo při každém přístupu k gridovým službám, nabízí gridová infrastruktura rozšíření klasické podoby PKI formou tzv. *proxy certifikátů*. Proxy certifikát je nově vygenerovaný certifikát, který není podepsaný žádnou CA, ale uživatelovým vlastním soukromým klíčem. Tento certifikát má platnost několik málo hodin (zpravidla deset nebo dvanáct) a jeho soukromý klíč je uložen na disku nešifrovaně v souboru, který je čitelný pouze majiteli certifikátu. Uživatel tak nemusí zadávat heslo ke svému privátnímu klíči při každém použití gridu. Krátká doba platnosti proxy certifikátu snižuje riziko plynoucí z případného ukradení takového nešifrovaného certifikátu. Gridová infrastruktura také poskytuje nástroje na automatické přenášení proxy certifikátů mezi různými počítači v sítí, které uživatel nebo jeho úloha pravě používá. Tato technika se obecně označuje jako princip *single sign-on* a umožňuje, aby se uživatel do gridu přihlásil pouze jednou a pak již po určitou dobu nemusel explicitně zadávat své autentizační údaje, protože lokální systém si jeho identitu pamatuje a umí ji použít transparentně. Výrazně se tím usnadňuje použití gridu a zvyšuje to i bezpečnost uživatelova certifikátu, protože se téměř po celou dobu pracuje pouze s krátkodobým proxy certifikátem.

Vedle PKI podporují gridy i jiné autentizační metody. Existuje například služba, která umožňuje integrovat PKI infrastrukturu s prostředím, kde je používán autentizační mechanismus Kerberos. Tato služba generuje certifikáty na základě kerberovských lístků a umožňuje tak snadnější připojení uživatelům z organizací, které používají Kerberos. Dalším trendem současné gridové bezpečnosti je zavádění jednorázových hesel, tj. hesel, která lze použít pro jedinou autentizaci.

2 Autorizace

Autorizace je proces, ve kterém služba ověřuje, že autentizovaný klient má oprávnění použít danou službu. Na rozdíl od oblasti autentizace, kde gridová infrastruktura od počátku stavěla na dostupných technologiích, se gridové autorizační služby začaly budovat na zelené louce. Žádná z dostupných autorizačních metod totiž neposkytovala funkcionalitu, která je pro gridy požadována. Jako příklad lze uvést autorizaci založenou na adresářové službě LDAP, která je hojně využívaná, zejména v organizačně uzavřených prostředích (např. v rámci jedné univerzity). V LDAPu lze definovat skupiny uživatelů, kteří mají právo použít určitou službu. Tato služba při každém přístupu klienta nejprve zjistí, zda klient je uveden v příslušné skupině a rozhodne tak, zda klientovi službu poskytne či ne. Tento způsob je jednoduchý a dobře funguje v relativně malém prostředí, postrádá však např. mechanismus delegování práv, kdy by uživatel mohl předat část svých oprávnění jinému uživateli (např. kolegovi, který by chtěl zpracovat data, která jsou čitelná pouze jejich majiteli), vyžaduje časté dotazy na LDAP server a není dostatečně škálovatelný.

Proto vznikly a stále se vyvíjejí sofistikované gridové autorizační služby, které poskytují efektivnější nástroje pro řešení autorizační problematiky v oblasti gridů. Řada těchto služeb poskytuje funkcionalitu vypůjčenou ze světa PKI, kdy každý projekt spravuje jeden nebo více tzv. *atributových serverů* vydávající uživatelům atributové certifikáty, kde je zapsáno členství uživatele

[3] `http://www.terena.nl/tech/task-forces/tf-aace/tacar/`

ve skupinách, případně přímo aktuální role uživatele. Uživatel s administrátorskými právy tak může pracovat se svou běžnou identitou a oprávněním a pouze pro úkony související se správou použít administrátorský certifikát. Snižuje se tak riziko zneužití nebo chyby, kterou uživatel může udělat. Atributový certifikát je podepsán službou, která jej vydala a koncový server nemusí kontaktovat žádnou třetí službu, jen ověří podpis na atributovém certifikátu a zkontroluje příslušné atributy. Klient posílá svůj atributový certifikát jako součást autentizačního procesu, zpravidla je zakódován v uživatelově proxy certifikátu, takže nejsou potřeba ani žádné změny na úrovni komunikačního protokolu. Takové prostředí umožňuje flexibilní správu uživatelských oprávnění, uživatel si může vybrat jaké skupiny nebo role z přiřazených právě potřebuje pro svou práci. Příslušné atributové certifikáty lze často také delegovat i jiným uživatelům, kteří tak mohou používat služby, ke kterým má přístup původní uživatel. Tyto delegační certifikáty jsou zpravidla časově omezené.

V gridovém prostředí bývá také problém vůbec zapsat přístupovou politiku, protože faktorů, které ji ovlivňují, může být velmi mnoho a jsou velmi různorodé. Často nelze vystačit s jednoduchým statickým seznamem uživatelů, příp. skupin, který je zapsán v konfiguraci služby, ale výsledná přístupová politika je výsledkem vyhodnocení řady dílčích pravidel. Například vedoucí gridového projektu může definovat skupinu uživatelů, kteří mohou používat výpočetní prostředky přiřazené tomuto projektu, ale lokální správci těchto prostředků mohou definovat vlastní přístupovou politiku, která musí být vyhodnocena též. Častým příkladem může být situace, kdy lokální správce chce preferovat uživatele pocházející z lokální instituce před ostatními, kterým je přístup povolen pouze v okamžiku, kdy výpočetní prostředky nejsou zatížené. Takových pravidel může být celá řada, mohou být definovány na více místech a vyhodnocování přístupové politiky pak může být velmi složitý proces. Tyto problémy vyústily v definování jazyků založených na XML, které umožňují standardizovaným způsobem zapsat i složité přístupové politiky a rovněž nabízejí nástroje pro efektivní zpracování těchto pravidel.

V oblasti autorizace se gridový svět snaží přiblížit a využít výsledků, které jsou dostupné v oblasti webových služeb (*Web services*). Zejména zmíněné zpracování pravidel pro řízení přístupu je založeno na výsledcích z oblasti webových služeb a standardů, které odtud pocházejí.

Současná gridová řešení se v maximální míře snaží podporovat interoperabilitu mezi různými organizacemi. V oblasti autorizace se proto zkoumají přístupy, které jsou schopné využít autorizační mechanismy z různých institucí, pokud možno bez zásahu uživatele tak, aby uživatel mohl volně využívat různé služby nabízené různými organizacemi a přitom zůstalo zachováno požadované zabezpečení a princip single sign-on.

Tento přístup je velmi dobře využitelný i mimo gridové prostředí, jak ukazuje například projekt Shibboleth[4], který vznikl pro podporu digitálních knihoven a má řadu faktorů společných s gridovou problematikou. Shibboleth je orientován na prostředí webu a umožňuje, aby uživatel, který přistupuje k webovému serveru, byl autorizován pomocí informací, které jsou spravovány jeho domovskou institucí. Umožňuje tak, aby uživatel přistupoval k elektronickým zdrojům odkudkoliv bez potřeby dodatečného hesla. Organizace tak například nemusejí nutit uživatele, aby používali proxy servery pro přístup k digitálním knihovnám, ale uživatel může přímo přistupovat k serveru knihovny, který jménem uživatele kontaktuje uživatelův „domovský“ autorizační server a je schopný převzít a zpracovat výsledek autorizačního procesu. Z pohledu uživatele je důležité, že celý proces je maximálně transparentní. Vzhledem k podobným cílům, které Shibboleth a gridy mají, vznikl nový projekt GridShib, který se snaží o větší propojení gridů a principů, na kterých je Shibboleth založen.

3 A co uživatel?

Cílem systémových správců by měl vždy být spokojený uživatel, pro bezpečnost to platí dvojná-

[4] `http://shibboleth.internet2.edu/`

sob. Bezpečné totiž nemusí znamenat uživatelsky složité, naopak systém by měl být od počátku navržen tak, aby umožňoval snadné použití ze strany uživatelů. Průzkumy ukazují, že bezpečnostní incidenty jsou z velké části zapříčiněny uživateli a jejich nesprávným chováním, nikoliv problémy v infrastruktuře. Systém může používat i sofistikované bezpečnostní mechanismy, ale pokud uživatel nebude dostatečně opatrovat své autentizační údaje, bude celkově systém daleko zranitelnější.

Pokud například uživatel používá několik příbuzných webových stránek, kam je přístup chráněn různými hesly, velmi pravděpodobně uloží tato hesla do každého klienta, kterého použije, přes veškerá varování, že tak nemá činit. Pokud však tyto webové stránky budou podporovat princip single sign-on, kdy uživatel zadá heslo jen jednou a infrastruktura v pozadí zajistí, že jeho identifikace se bude předávat transparentně bez nutnosti opakovaného zadávání hesla, je pravděpodobné, že patřičně poučený uživatel heslo opravdu napíše pokaždé z klávesnice.

Pokud se taková infrastruktura navíc propojí i s newebovým prostředím, např. pomocí gridových technologií a uživatel tak skutečně bude své heslo zadávat pouze jednou za den, výrazně se tak zvýší nejen pohodlí uživatelů, ale zejména bezpečnost celého systému. Vybudování takového systému sice stojí více úsilí, ale vrátí se ve vyšší úrovni bezpečnosti a uživatelského pohodlí. Jedním z podstatných cílů gridových technologií je poskytnout nástroje pro vybudování takového prostředí.

Dalším problémem, který přímo souvisí s gridy, je správa soukromých klíčů uživatelů. Zatímco jméno a heslo si je každý uživatel schopen zapamatovat, privátní klíč o velikosti 1024 bitů si nezapamatuje nikdo. Musí být proto uložen na nějakém médiu, nejčastěji disku uživatelské stanice. To přináší riziko jeho prozrazení, zejména v dnešní době, kdy je k Internetu připojena řada počítačů, které nejsou aktualizovány, případně jsou napadeny nejrůznějšími viry, a soukromý klíč se tak může dostat do nepovolaných rukou útočníka. Současné gridy se proto snaží nabídnout řešení, které uživatelům umožní uložit svůj soukromý klíč na specializovaný server, který uživatelům vydává pouze krátkodobé proxy certifikáty. Přestože takový server obsahuje klíče řady uživatelů, což je v přímém rozporu s klasickým pohledem na PKI, ukazuje se, že je to bezpečnější řešení, než ponechávat klíče u uživatelů, kteří o jejich zabezpečení nemají vědomosti či zájem. Další možností, která umožňuje odstranění uživatelského klíče je použití čipových karet, které se postupně začínají v gridovém prostředí prosazovat.

4 Síťová kontrola aneb firewall

Slovo firewall je zaklínadlem, které se objevuje snad v každém článku o bezpečnosti, a proto mu nemůžeme nevěnovat aspoň krátkou zmínku ani zde. Firewallem máme na mysli zařízení umístěné mezi komunikujícími stranami, které monitoruje síťovou komunikaci a je schopno tuto komunikaci ovlivnit. Nejčastěji se tento prostředek používá pro izolování lokální sítě tak, aby např. lokální počítače nebyly dostupné z Internetu.

Firewall je často považován za synonymum pro zabezpečenou síť a bývá také automaticky doporučován téměř jako všelék na veškeré problémy s bezpečností. Zkušenosti z gridového prostředí však ukazují, že firewally nezřídka přinášejí více problémů než užitku, a proto by jejich nasazení mělo být vždy velmi pečlivě uváženo. Firewally zpravidla implementují politiku „co není povoleno je zakázáno“ která je však velmi nepřirozená pro gridové prostředí, protože povolení každé nové služby je dlouhotrvající proces, který špatně zapadá do dynamického gridového světa.

Řada gridových projektů dnes spravuje různé seznamy portů a IP adres, které musí být povoleny v konfiguracích firewallů, aby bylo možné vybudovat a udržet funkční infrastrukturu. Přestože definují minimální požadovanou funkcionalitu, jsou tyto seznamy zpravidla tak rozsáhlé, že v podstatě stírají význam firewallu. Stačí také drobná opomenutí v konfiguraci pro částečné, či úplné vyřazení určité funkcionality.

Firewally by proto měly být nasazovány jen v situacích, kdy opravdu mohou přinést zvýšení bezpečnosti i v reálném provozu a co nejméně omezovat legitimní uživatele. O to více úsilí by mělo být věnováno zabezpečení služeb samotných, než omezování přístupu k nim. □