

Bezpečný distribuovaný úložný prostor

Lukáš Hejtmánek, Luděk Matyska a Michal Procházka

Ústav výpočetní techniky, Masarykova univerzita, Brno a CESNET z.s.p.o

1 Úvod

Datová úložiště, propojená vysokorychlostní sítě, mohou sloužit jako uzly distribuovaného datového prostoru s vysokou kapacitou a přijatelnou cenou. Distribuovaný úložný prostor začíná být důležitou součástí mnoha aplikací. Příkladem plně distribuovaného prostředí, a to jak výpočetně distribuovaného, tak i datově distribuovaného, jsou Gridy. V rámci Gridů byly a jsou realizovány projekty, například DataGrid, EGEE, LCG a jiné, které se zaměřují na výzkum dlouhodobého distribuovaného ukládání dat.

V prostředí Gridů jsou uživatelé obvykle organizováni v rámci takzvaných Virtuálních organizací (VO) [1]. Virtuální organizace se stává jednotkou správy členství uživatelů a správy zdrojů. Uživatel může být členem několika Virtuálních organizací, samotné Virtuální organizace pak identifikují skupiny uživatelů. Současné Gridy používají více přístupů ke správě dat, jsou to Storage Elements, které se chovají jako datová úložiště, k nimž se přistupuje pomocí aplikačních nástrojů pro uložení a nahrání dat (obvykle označováno jako stage-in/stage-out), a dále to jsou síťové a distribuované souborové systémy jako NFS, AFS, GPFS a další.

Logistické sítě [2] se v podstatě podobají zmíněným Storage Elements, ale přináší zároveň nový přístup k problematice ukládání dat. Logistické sítě poskytují univerzální rozhraní pro ukládání dat, díky němuž je možné vybudovat robustní, škálovatelné a vysoce výkonné distribuované systémy ukládání dat. Na základě logistických sítí je možné postavit zmíněné Storage Elements nebo distribuované systémy souborů. Původní verze logistických sítí ale není připravena na použití v prostředí Gridů, kde je kladen důraz na řádnou autentizaci a autorizaci uživatelů.

Cílem naší práce je poskytnout variantu logistických sítí, která by byla vhodná pro nasazení v prostředí Gridů. Náš přínos spočívá v bezpečnostních rozšířeních tak, že logistické sítě budou podporovat plnou autentizaci a autorizaci uživatelů. Tyto mechanismy jsou slučitelné se standardním přístupem k autentizaci a autorizaci v prostředí Gridů. Naše řešení je založeno na infrastruktuře tajných a veřejných klíčů (PKI, X.509 certifikáty) a na VOMS službě [3], kterou využíváme pro snadnější identifikaci uživatelů. Řešení jsme propojili s jednoduchou federativní autentizační službou používanou v rámci projektu Eduroam. Uživatel se může svým Eduroam účtem prokázat online certifikační autoritě, která mu vydá časově omezený certifikát, s nímž pak přistupuje k jednotlivým komponentám logistických sítí.

2 Logistické sítě

Logistické sítě [2] přináší obecný koncept ukládání dat založený na obecně nespolehlivé službě ukládající pouze bloky dat. Logistické sítě dále popisují vyšší vrstvy, které nad touto nespolehlivou službou staví naopak spolehlivý systém ukládání souborů. Námi popisované logistické sítě využívají pět síťových vrstev: IBP, L-Bone, eXnode, LoRS a aplikační vrstvu.

Vrstva IBP je páteří logistických sítí, představuje základní vrstvu, která se stará o ukládání dat v podobě datových bloků bez jakékoliv informace o celkové struktuře ukládaných dat. Obdobně jako IP protokol v sítích, i IBP je nezaručená služba nízké úrovně, o spolehlivost se starají vyšší vrstvy. Řízení přístupu je založeno na systému oprávnění (capabilities). Pouze uživatel disponující správnými oprávněními je schopen ukládat nebo číst data. Oprávnění jsou reprezentována řetězcem, který obsahuje jméno serveru, na němž je datový blok uložen, a náhodný řetěz, jenž identifikuje datový blok v rámci serveru. Před samotným ukládáním dat si klient od úložného serveru musí vyžádat oprávnění k uložení určitého množství dat. Na základě tohoto oprávnění je následně klient schopen uložit data do daného rozsahu a posléze je schopen tato data přečíst. Aby klienti postupně nevyčerpali veškerou kapacitu úložných serverů, je obvykle možné ukládat data jen po omezenou dobu. Každý datový blok na serveru s sebou nese informaci o tom, kdy může být serverem uvolněn (tedy smazán). Klient může server požádat o prodloužení trvanlivosti datového bloku, server ovšem nemá povinnost takové žádosti vyhovět. Klient musí data přesunout na jiný server. Vrstva IBP nabízí klientům čtyři základní funkce: Allocate, Store, Load a Copy. Funkce Allocate slouží pro alokování místa na nějakém úložném serveru, tzv. depotu. Funkcí Store je možné do alokovaného prostoru uložit data. Funkcí Load lze uložená data zpět načíst. A funkce Copy slouží ke kopírování dat přímo mezi IBP depoty, klient předá lokaci zdrojových dat a lokaci alokovaného prostoru, IBP depot pak provede synchronně přenos.

L-Bone vrstva představuje adresář úložných serverů, které jsou dostupné pomocí IBP protokolu. Tato služba navíc úložné servery průběžně monitoruje a kromě informací o adresách serverů a jejich geografické lokaci udržuje informace o jejich dostupnosti. Klient je schopen prostřednictvím L-Bone vrstvy získat např. geograficky nejbližší úložné servery a samozřejmě je schopen získat seznam serverů omezen pouze na ty, které jsou v provozu.

Vrstva eXnode se stará o mapování jednotlivých datových bloků do souborů. Jedná se o analogii k I-uzlům v souborových systémech ve světě UNIXu. Mapování, které nazýváme metadaty, je reprezentováno XML souborem. Tento soubor obsahuje oprávnění k jednotlivým datovým blokům, dále je ke každému datovému bloku udržována jeho velikost a jeho pozice v souboru.

Vrstva LoRS představuje aplikační rozhraní určené pro programování logistických sítí, poskytuje abstrakci ukládání a čtení souborů, využívá přitom předchozích vrstev. Pomocí této vrstvy mohou uživatelé snadno ukládat nebo číst soubory. Nevýhoda LoRS rozhraní je v tom, že převádí na uživatele správu metadatových souborů.

Zmíněna nevýhoda rozhraní LoRS znesnadňuje nasazení logistických sítí do prostředí Gridů. Uživatelé jsou sami zodpovědní za ukládání metadat. V případě, že uživatel o metadata přijde, nemá možnost získat uložená data. Úložné servery tato data časem uvolní (přesněji je uvolní po vypršení jejich platnosti, bez metadat nelze platnost dat prodlužovat). Z tohoto důvodu jsme vyvinuli vlastní metadata manažer, který na sebe přebírá úlohu správy metadat. Metadata manažer [4] tak přirozenou cestou rozšiřuje původní model logistických sítí.

3 Logistické sítě v kontextu virtuálních organizací

Virtuální organizace [3] je uskupení uživatelů nebo institucí, které se nějakým způsobem dohodly na sdílení svých zdrojů. V rámci dohod si instituce či uživatelé definují politiku sdílení (obvykle ve smyslu jaké zdroje kdo může využívat a kolik jich může využívat), která je technicky realizovatelná. V tomto článku se zaměříme pouze na sdílení diskových kapacit, jenz jsou založeny na logistických sítích.

Předpokládáme, že každý úložný server (IBP depot) má nějakého vlastníka, se kterým si virtuální organizace může dohodnout sdílení diskového prostoru pro své členy. Obvykle jde o jednostranné sdílení, tedy majitel IBP depotu je v roli poskytovatele služby a členové dané virtuální organizace tuto službu využívají. Přirozeným požadavkem je, aby majitel IBP depotu byl schopen své služby nabídnout několika virtuálním organizacím najednou a zároveň, aby byl schopen s různými organizacemi dohodnout různou politiku. Navíc bychom chtěli umožnit, aby majitel IBP depotu dokázal zjmenit politiku sdílení na úroveň jednotlivých uživatelů, tedy aby mohl definovat politiku sdílení jak pro celé organizace, tak pro jednotlivé členy v rámci organizace. Oba typy politik sdílení vyžadují, aby se uživatelé dokázali řádně identifikovat, ať už musí prokázat členství v nějaké virtuální organizaci nebo identifikují sebe přímo jako uživatele. Rozhodli jsme se využít identifikace pomocí PKI infrastruktury a služby VOMS (služba příslušnosti k virtuální organizaci).

Virtuální organizace obvykle nejsou neměnná uskupení, virtuální organizace se mohou slučovat a rozdělovat, mohou měnit své členy a v neposlední řadě i poskytovatelé služeb mohou měnit přístup k daným virtuálním organizacím. Navržené řešení musí akceptovat takovéto změny.

IBP depoty jsou registrovány v adresáři úložných serverů (L-Bone vrstva). V kontextu virtuálních organizací se přímo nabízí, aby L-Bone server byl součástí virtuální organizace a registroval tak pouze IBP depoty, které mají dohodnutou nějakou politiku sdílení s touto virtuální organizací. L-Bone server pak lze chápat jako přirozené rozšíření VOMS služby. Uživatelé kontaktující L-Bone server tak mohou snadno získat pouze IBP depoty patřící do jejich virtuální organizace a zároveň správci virtuálních organizací mohou snadno zpřístupňovat nové IBP depoty v rámci své virtuální organizace jejich zaregistrováním u příslušného L-Bone serveru.

V rámci virtuální organizace je obvykle definována množina uživatelských jmen a skupin, které slouží pro identifikaci uživatele. Na základě této identifikace další služby případně autorizují uživatele k jejich využívání. Označení uživatelů a skupin je ovšem platné pouze v rámci jedné virtuální organizace, v jiné organizaci mohou mít tatáž označení jiný význam. Z tohoto důvodu nemohou služby logistických sítí spoléhat čistě na označování uživatelů a skupin, mohou-li být sdíleny mezi několika virtuálními organizacemi. Základní službou, která autorizuje uživatele, je metadata manažer. Metadata manažer udržuje ke každému souboru autorizační informace a rozhoduje o přístupu individuálních uživatelů. Autorizační informace je v podstatě seznam uživatelů a skupin, které mají s daným objektem právo manipulovat (číst, měnit, mazat, atd.). Pokud v těchto autorizačních informacích udržujeme pouze označení uživatelů a skupin s implicitním přiřazením virtuální organizace, pak není možné tyto autorizační informace sdílet mezi rozdílnými virtuálními organizacemi a následně tedy není možné sdílet metadata manažer mezi organizacemi, měl-li by poskytovat globální jmenný prostor. Druhou možností je zahrnout do označení uživatelů a skupin i explicitní identifikaci virtuální organizace. Předpokladem této možnosti je, že názvy virtuálních organizací se liší. V naší práci využíváme druhého způsobu, tedy zahrnování názvu virtuální organizace do autorizačních informací, protože nezpůsobuje problémy při slučování těchto organizací.

Pro snazší využívání našich virtuálních organizací jsme vytvořili službu, která virtuální organizace propojuje s federativními službami. Uživatel se tak může autentizovat vůči nějaké federaci a naše služba mu na základě této autentizace vydá certifikát, kterým se následně autentizuje na službách logistických sítí. Tímto propojením je možné anonymizovat uživatele. Uživatelé v rámci virtuální organizace mohou být anonymní, jejich pravou identitu pak zná pouze federace, vůči které se autentizují.

3.1 Požadavky na přístup k datům

Distribuovaný systém pro ukládání dat musí splňovat následující požadavky, aby mohl být nasazen v rámci virtuálních organizací:

1. Uživatel musí být řádně autentizovaný na všech službách
2. Uživatel musí být řádně autorizován pro využití každé služby
3. Autorizace musí být odvolatelná

Aplikujeme-li tyto požadavky na logistické síť, znamená to, že každý uživatel musí být autentizován na metadata manažeru, L-Bone serveru a na IBP depotech. Tohoto můžeme dosáhnout pomocí certifikátů s VOMS atributy. Dále metadata manažer musí poskytovat metadata pouze autorizovaným uživatelům, obdobně L-Bone server může vydávat seznam IBP depotů pouze autorizovaným uživatelům a nakonec i IBP depoty nabízí své služby rovněž pouze autorizovaným uživatelům. Bod číslo tři vyžaduje odvolatelnost autorizace. Zde se nabízí dvě možnosti, buď používat revokačních listů a serverů nebo s každým autorizačním oprávněním svázat časové omezení platnosti. V druhém případě je nutné, aby si uživatel periodicky obnovoval autorizační oprávnění. Tento případ se nám jevil jako výhodnější oproti revokačním listům, které vyžadují fungující systém aktualizací, proto jsme jej použili.

4 Architektura

Navržené bezpečnostní rozšíření logistických sítí zaručuje řádnou autentizaci uživatelů a autorizaci uživatele na všech vrstvách logistické sítě. Uživatelé si mohou dočasně uchovávat autorizační oprávnění, aby je nebylo nutné neustále znova získávat. Naším požadavkem bylo, aby tato autorizační oprávnění byla kdykoliv revokovatelná. Revokovatelnost je dosaženo díky časovým limitům spojených se samotným autorizačním oprávněním. Jakákoliv služba, která vydává autorizační oprávnění, je schopna toto oprávnění vydat sama o sobě, nemusí kontaktovat jakoukoliv jinou službu.

4.1 Identifikace uživatele

Certifikáty tak, jak je definuje PKI, nelze použít přímo pro identifikaci uživatelů. Uživatel může vlastnit několik různých certifikátů, ale přesto jde o stále stejného uživatele. Certifikáty tedy nepředstavují permanentní identifikaci uživatele, zvedli jsme proto označení uživatelů a uživatelských skupin pomocí VO ID. VO ID je uchováno v certifikátech pomocí extenzí (X.509v3). Uživatelská a skupinová VO ID musí být unikátní a neměnné v rámci virtuální organizace. Extenze nesoucí uživatelská a skupinová VO ID je podepsána důvěryhodnou autoritou (například VOMS server) a jsou nerozlučitelně spárována s uživatelským certifikátem. Uživateli, který do systému vstupuje poprvé, je vygenerováno jeho uživatelské VO ID a je asociováno s jeho současným certifikátem. Pomocí tohoto certifikátu může uživatel požádat o spárování VO ID i s jinými jeho certifikáty. Systém je takto schopen na základě VO ID jednoznačně identifikovat uživatele, i když uživatel používá různé certifikáty.

4.2 Autorizace uživatele

Proces autorizace má následující tři části:

1. Uživatel musí získat *proxy certifikát* s extenzemi pro jeho identifikaci (VO ID). Identifikace může být implementována prostřednictvím VOMS atributů, které vydává VOMS server v rámci virtuální organizace. Předpokládáme, že uživatel má nějaký svůj osobní certifikát podepsaný nějakou důvěryhodnou certifikační autoritou. Proces vytvoření proxy certifikátu má dvě části. Napřed si uživatel vytvoří dočasný proxy certifikát ze svého osobního certifikátu, tento dočasný certifikát je použit pro autentizaci vůči VOMS serveru, který následně vydá atributy obsahující VO ID uživatele a skupin, do nichž patří. V druhé části si uživatel vytvoří proxy certifikát, do kterého si vloží atributy vydané VOMS serverem. Předpokládáme, že VOMS server vydá VO ID atributy pouze autorizovaným uživatelům, tj. klientům patřícím do dané virtuální organizace. Proxy certifikát je časově omezený, obvykle má platnost několik hodin nebo dní.

Druhou možností, jak získat proxy certifikát, je využít jednoduché federativní služby. Uživatel, který se dokáže autentizovat v rámci nějaké federativní služby, může využít online certifikační autority, která mu vydá časově omezený proxy certifikát s VOMS atributy. Online certifikační autorita využije zmíněné federativní služby pro autentizaci uživatele.
2. Uživatel musí získat metadata (v případě přístupu k souborům). Metadata manažer řídí přístup k souborům. Pokud je uživatel autorizován číst soubor, metadata manažer mu vydá metadata. Autorizace je založena na VO ID attributech z proxy certifikátu a na ACL daného souboru. Tato část autorizace je založena pouze na VO ID attributech z proxy certifikátu, metadata manažer nekontaktuje žádnou další službu. Platnost metadat je časově omezená, i tuto autorizaci lze tedy revokovat. Architekturu revokovatelných metadat diskutujeme v sekci 4.3.
3. Uživatel musí získat seznam IBP depotů a seznam oprávnění k depotům. V případě čtení souborů stačí uživateli pouze seznam oprávnění k depotům, seznam depotů, na kterých jsou uložena data, je součástí metadat. Adresář úložných serverů (L-Bone server) vydává seznam IBP depotů a seznam oprávnění pouze autorizovaným uživatelům. Autorizace uživatele opět závisí pouze na jeho proxy certifikátu a příslušných VO ID attributech. Platnost oprávnění k depotům je opět časově omezená. Oprávnění jsou pevně svázána s uživatelským VO ID a jsou tak platná pouze pro konkrétního uživatele.

Uživatel, který přistupuje k IBP depotům, se musí prokázat patřičnou částí metadat a zároveň patřičným oprávněním ke konkrétnímu depotu. Metadata i oprávnění uživatel získal v krocích 2 a 3 při své autorizaci. IBP depot ověří platnost metadat a platnost oprávnění, které obdržel od uživatele. Pak je uživatel oprávněn číst data uložená na IBP depotu. V případě zápisu dat se uživatel prokazuje pouze oprávněním získaným v kroku 3, depot toto oprávnění ověří a případně dovolí uživateli ukládat data.

Součástí naší architektury je mechanismus, který uživateli zabrání v obejití kteréhokoliv kroku autorizace. Tento mechanismus je založen na tom, že jsou uživateli vydávána oprávnění potřebná vždy pro další krok autorizace a uživatel je tedy nucen kontaktovat služby v daném pořadí. Všechna autorizační oprávnění jsou časově omezená a uživatel je musí periodicky obnovovat. Služba může obnovení autorizačního oprávnění odmítnout, čímž je dosažena jejich revokovatelnost.

4.3 Časově omezená metadata

Rozdělení metadata manažeru a úložných serverů do dvou nezávislých služeb přináší problém s ověřováním platnosti metadat. Pokud metadata manažer a úložný server nejsou online propojeni, pak úložný server nemůže ověřit platnost metadat (tj. zda uživateli nebyla odebrána práva přístupu). Důsledkem je, že práva přístupu nejsou revokovatelná (klient si může metadata uložit lokálně a měl by pak přístup k datům navždy), což porušuje jeden z primárních požadavků na přístup k datům v rámci virtuální organizace. Z tohoto důvodu musí metadata manažer vydat pouze časově omezená metadata tak, aby úložný server byl schopen časovou platnost nějakým způsobem (ovšem bez kontaktování další služby) ověřit. Základní myšlenkou řešení je podepsat metadata společně s časovým razítkem. Podpis pro metadata vydá uživateli metadata manažer. Problémem zůstává, jak vyrobit podpis tak, aby proces podepisování netrval neúměrně dlouho a aby byl podpis ověřitelný i bez znalosti kompletních metadat k jednomu souboru.

Řešení uvedeného problému spočívá ve vytvoření vazby mezi datovými bloky a odpovídajícími metadaty. Tuto vazbu lze snadno udržovat bez navýšení složitosti celého systému. Při vytvoření nového souboru si klient vygeneruje unikátní identifikaci (například UUID [5]), tato identifikace bude pevně svázaná s nově vytvořeným souborem. Následně klient ukládá data tohoto souboru na úložné servery a zároveň s požadavkem na uložení předá vygenerovanou identifikaci. Úložný server permanentně sváže uložený datový blok s klientem dodanou identifikací. Zároveň klient запиše danou identifikaci do metadat a pak je předá metadata manažeru. V případě přístupu k datům vydá metadata manažer klientovi metadata spolu s podpisem. Podpis obsahuje časové razítko spolu s identifikací souboru (UUID). Klient se musí úložnému serveru prokázat takto získaným podpisem. Úložný server snadno dokáže ověřit, že klient získal správná metadata a že platnost metadat (a zároveň podpisu) nevypršela. Identifikace v podpisu musí souhlasit s identifikací svázanou s datovým blokem. Metadata manažer je schopen zmíněný podpis snadno vyrobit, navíc je nutný pouze jediný podpis pro celý soubor a je platný nezávisle na jméne souboru. Díky časovému razítku je nutné podpis obnovovat a metadata manažer může obnovení odmítnout, čímž je platnost metadat revokovatelná.

Tento přístup ovšem mění sémantiku uložených datových bloků na IBP depotech. Zavedením identifikace příslušnosti datového bloku do souboru poskytujeme vodítko případnému útočníkovi, které datové bloky patří do stejného souboru. V původní verzi implementace IBP protokolu nebyla žádná spojitost mezi datovým blokem a nějakým souborem. Útočník, který získá přístup k IBP depotu tak, že je schopen číst libovolné datové bloky, může snadněji z těchto bloků sestavit soubory. Podle identifikací ví, které bloky tvoří jeden soubor. Pokud tento fakt způsobuje problém, doporučujeme šifrování dat na vyšší úrovni.

5 Experimenty s prototypovou implementací

Pro experimenty s prototypovou implementací jsme použili prostředí s jedním klientem a několika servery. Servery byly vybaveny dvěma procesory Pentium Xeon@3.0GHz, 3GB RAM, 1Gbps NIC a 400GB SW RAID 0 diskovým polem. Klient byl vybaven jedním procesorem Pentium Xeon@2.4GHz, 1GB RAM, 1Gbps NIC a lokálním IDE diskem. Na lokální disk bylo možno zapisovat rychlostí 35MB/sec, na diskové pole bylo možno zapisovat rychlostí 124MB/sec. Rychlost sítě měřená pomocí nástroje *iperf* [6] byla 940Mbps přes jedno TCP spojení. Klient i server používali operační systém Linux s jádrem 2.6.13.

Pro naše experimenty jsme použili jednoduchou federativní službu používanou v rámci projektu Eduroam. Uživatelé, kteří mají Eduroam účet, mohou získat časově omezený certifikát od naší online certifikační autority. Tento certifikát jsme použili pro otestování přístupu ke službám logistických sítí.

Pro účely testování jsme použili vlastní implementaci L-Bone serveru tak, aby podporoval náš bezpečnostní model. Klient se autentizuje v rámci požadavku na seznam IBP depotů svým proxy certifikátem s VOMS atributy. L-Bone server ověří platnost klientského certifikátu a provede autorizaci na základě VOMS atributů. L-Bone server pomocí svého tajného klíče vyrobí podpis ke každému IBP depotu. Podpis obsahuje jméno IBP depotu, port, na kterém depot poslouchá, časové razítko a sériové číslo certifikátu klienta. Podpis spolu s jménem IBP depotu a portu je pak poslán již nešifrovaně zpět klientovi. Případný útočník může podpis ukrást (odposlechnout), nicméně pomocí takto získaného podpisu není schopen manipulace s daty na IBP depotu, protože při komunikaci s IBP depotem musí mít klient přístup k tajnému klíči od proxy certifikátu.

Obdobně jsme použili vlastní implementaci IBP depotu. Přidali jsme nový příkaz do IBP protokolu: `IBP_auth`, pomocí kterého se klient autentizuje. V rámci autentizace pošle klient svůj proxy certifikát a podpis získaný od L-Bone serveru. IBP depot ověří platnost podpisu a autorizuje klienta na základě VOMS atributů, následně pak vygeneruje 128 bitový klíč pro AES šifru, zašifruje ho pomocí klientova certifikátu a takto pošle klientovi zpět. Klient je schopen pomocí svého tajného klíče získat AES klíč, pomocí kterého jsou od této chvíle šifrovány oprávnění pro přístup k datovým blokům na IBP depotu a nebo i samotné přenosy dat. Klient si může zvolit, zda šifrovat jen oprávnění nebo i přenášená data. Zároveň s IBP depotem jsme modifikovali klientskou část. Zachovali jsme kompatibilitu s původní verzí IBP protokolu a přidali nové rozhraní pro použití našeho bezpečnostního modelu. Nové rozhraní si oproti původní verzi předdává autentizační kontext, pomocí kterého je schopno vytvářet nová šifrovaná spojení.

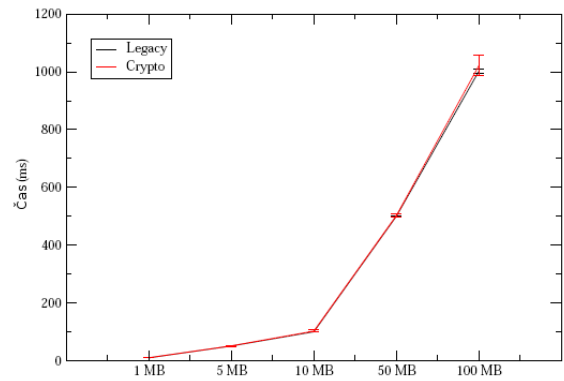
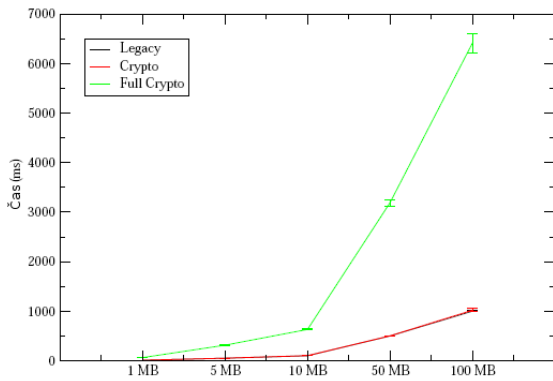
Pro vlastní testování jsme použili jednoho klienta, který volal sekvenci funkcí klientské knihovny pro práci s IBP. Cílem měření bylo zjistit dopad našich bezpečnostních rozšíření na výkon IBP. Porovnávali jsme tedy trvání původní funkce z IBP knihovny s námi modifikovanou funkcí. Použitá sekvence byla následující: `Allocate`, `Store`, `Load`, pak nová alokace na stejném IBP depotu a následně `Copy` do nové alokace. Tato sekvence byla opakována 500 krát. Velikosti datových bloků pro přenosy byly: 1MB, 5MB, 10MB, 50MB a 100MB. Porovnali jsme původní implementaci IBP (*Legacy*) s novou verzí, která šifrovala pouze posílaná oprávnění k datům (*Crypto*), a s novou verzí, která šifrovala oprávnění i přenášená data (*Full crypto*). Zároveň jsme změřili trvání funkce `IBP_auth`, která je pouze v nové verzi IBP protokolu a způsobuje jednorázové zpomalení při sestavování nového spojení.

	IBP_auth	Allocate
<i>Legacy</i>	–	0.62
<i>Crypto, Full crypto</i>	14.5	1.10

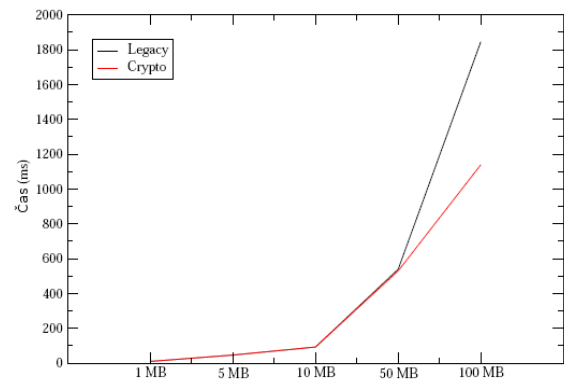
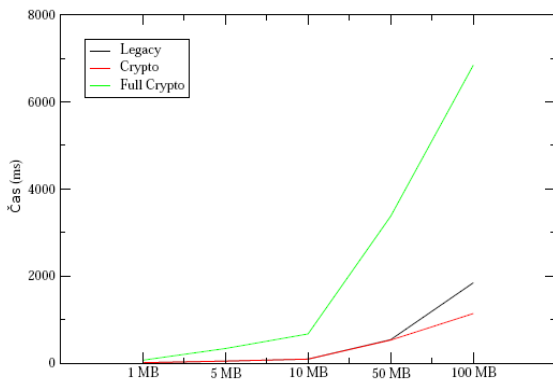
Tabulka 1: Trvání funkcí IBP_Auth a Allocate v milisekundách

Trvání operací `IBP_Auth` a `Allocate` je znázorněno v tabulce 1. Vzhledem k tomu, že operace `IBP_Auth` je vyžadována pouze jednou při sestavování nového spojení mezi klientem a IBP depotem, je její trvání konstantní a nezávislé na velikosti přenášených dat. Můžeme dobu jejího trvání prohlásit za bezvýznamnou. Funkce `Allocate` je zpožděna o zhruba 0.5ms. Tato ztráta je zanedbatelná v porovnání s trváním přenosů dat a navíc je nezávislá na velikosti přenášeného bloku (plné šifrování dat nemá žádný vliv na tuto funkci).

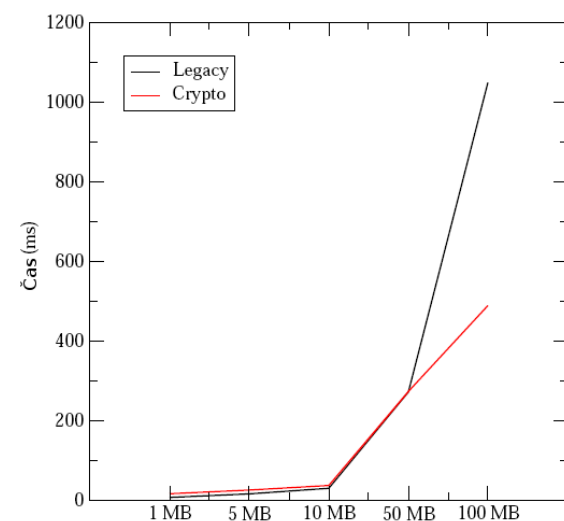
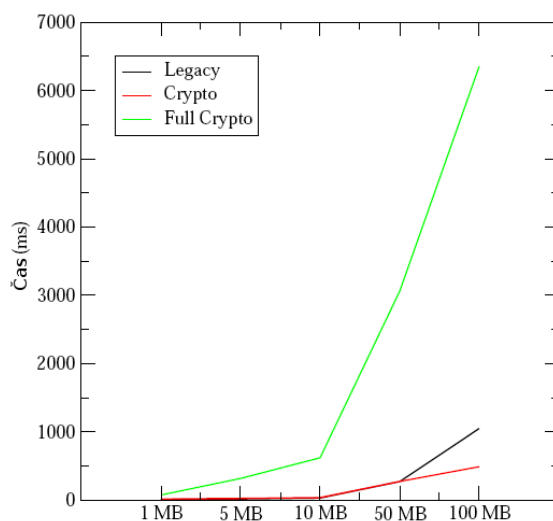
Trvání operací `Load`, `Store` a `Copy` je znázorněno na obrázcích 1 – 3. Levá část každého obrázku znázorňuje trvání dané operace ve všech režimech (tj. původní IBP – *Legacy*, pouze šifrování oprávnění – *Crypto* a plné šifrování – *Full crypto*). Vzhledem k tomu, že plné šifrování trvá podstatně déle než ostatní dva případy, dochází ke splývání rozdílů mezi původním IBP a šifrováním oprávnění. Z tohoto důvodu je na v pravé části každého obrázku znázorněno pouze původní IBP a šifrování oprávnění. Pokud šifrujeme pouze oprávnění, jsou funkce `Load` a `Store` plně srovnatelné bez větších rozdílů. U funkce `Store` je patrné, že v případě šifrování oprávnění bylo dosaženo lepších výsledků než v případě původní verze IBP. Tento jev si vysvětlujeme lepším rozložením zátěže, které vzniká díky zpomalení kvůli šifrování. V případě funkce `Copy` dochází k větší fluktuaci v měření, fluktuace je větší než rozdíly mezi původní verzí IBP a šifrováním oprávnění. V případě plného šifrování je rychlost funkcí omezena rychlostí AES šifry s 128bitovým klíčem. Funkce `Copy` vykazuje vyšší propustnost než funkce `Store`, protože v případě funkce `Copy` se přenáší data v rámci jednoho serveru, zatímco v případě funkce `Store` se přenáší data mezi klientem a serverem.



Obrázek 1: IBP_load. Levá část porovnává původní verzi IBP (Legacy) s novou verzí, která šifruje pouze oprávnění (Crypto), a s novou verzí, která šifruje oprávnění i data (Full Crypto). Prává část porovnává pouze původní IBP s novou verzí, která šifruje pouze oprávnění. V tomto grafu je použit průměr naměřených hodnot.



Obrázek 2: IBP_store. Levá část porovnává původní verzi IBP (Legacy) s novou verzí, která šifruje pouze oprávnění (Crypto), a s novou verzí, která šifruje oprávnění i data (Full Crypto). Prává část porovnává pouze původní IBP s novou verzí, která šifruje pouze oprávnění. V tomto grafu je použit medián naměřených hodnot.



Obrázek 3: IBP_copy. Levá část porovnává původní verzi IBP (Legacy) s novou verzí, která šifruje pouze oprávnění (Crypto), a s novou verzí, která šifruje oprávnění i data (Full Crypto). Prává část porovnává pouze původní IBP s novou verzí, která šifruje pouze oprávnění. V tomto grafu je použit medián naměřených hodnot.

6 Shrnutí

Navrhli jsme distribuovaný systém pro ukládání dat založený na logistických sítích s bezpečností založenou na certifikátech a VOMS atributech. Takovýto systém je vhodný pro nasazení v Gridových virtuálních organizacích. Zároveň náš systém dokáže poskytovat zdroje několika různým virtuálním organizacím najednou. Náš vlastní přínos spočívá v přidání bezpečnostní vrstvy k tradičním logistickým sítím, která garantuje, že každý uživatel musí být řádně autentizován a k využití každé služby musí být řádně autorizován. Každé autorizační oprávnění je revokovatelné. Navržené řešení připouští sdílení úložných serverů několika virtuálními organizacemi.

Zároveň jsme provedli propojení našeho systému s jednoduchou federativní autentizační službou používanou v rámci projektu Eduroam. Uživatelé, kteří mají účet v rámci Eduroamu, jsou schopni od naší online certifikační autority získat dočasný certifikát. Tento certifikát mohou využít pro přístup k naší úložné infrastruktuře.

Provedli jsme prototypovou implementaci a udělali jsme základní testy výkonu navrženého řešení. Testy ukázaly, že i prvotní implementace podává velmi dobrý výkon v porovnání s původní implementací logistických sítí. Režie, kterou přidala bezpečnostní vrstva bez plného šifrování, je poměrně zanedbatelná.

Reference

1. I. Foster, C. Kesselman, and S. Tuecke. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. In *Grid Computing: Making the Global Infrastructure a Reality*, pages 171–197, 2003.
2. M. Beck, T. Moore, and J.S. Planck. An End-to-end Approach to Globally Scalable Network Storage. In *SIGCOMM'02*, 32(4):339–346, 2002.
3. R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. Lorentey, and F. Spataro: "VOMS, an Authorization System for Virtual Organizations." In *Grid Computing, First European Across Grids Conference*, volume 2970/2004, pages 33–40. Springer Berlin / Heidelberg, 2004
4. L. Hejtmánek. Distributed Data Storage with Data Versioning. In *CESNET Conference 2006*, pages 93–104, CESNET, z.s.p.o, 2006.
5. P. Leach, M. Mealling, and R. Salz. RFC4122: A Universally Unique IDentifier (UUID) URN Namespace, July 2005.
6. Iperf. <http://dast.nlanr.net/Projects/Iperf>.