Загорського, доц. А. В. Ліпенцева. - Львів : ЛРІДУ НАДУ, 2009. - С. 353-356. 33
6. *Селіверстов Р. Г.* Елементи теорії нечітких множин як засіб професіоналізації експертної діяльності в органах державного управління / Р. Г. Селіверстов // Ефективність державного управління : зб. наук. пр. ЛРІДУ НАДУ / за заг. ред. проф. В. С. Загорського, доц. А. В. Ліпенцева. - Львів : ЛРІДУ НАДУ, 2008. - Вип. 16/17. - С. 372-376.

Поступила 11.9.2013р.

УДК 004.056:004.75

М.Р.Шабан, м. Київ

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В GRID-СИСТЕМАХ

Abstract. We review different approaches to enabling security in Grid systems. We analyze such mechanisms as Globus GSI and message-level security. We also focus on the following aspects of Grid security: anomaly identification, and resource and data availability monitoring.

Актуальність

В останні роки світове наукове співтовариство відчуває все більшу необхідність у великих обчислювальних потужностях, що пов'язано з необхідністю проведення складних і ресурсномістких обчислень, при цьому потужні обчислювал ьні системи є досить дорогими. У зв'язку з цим стрімко розвиваються Grid-системи, які об'єднують існуючі обчислювальні центри, можуть просто і швидко масштабуватися і виконують розподілені додатки, використовуючи всі доступні їм ресурси.

Сучасні підходи до організації механізмів захисту інформації в комп'ютерних системах передбачають централізацію засобів захисту (сертифікаційні агенції, служби реєстрації та авторизації), що накладає значні обмеження на їх використання при динамічному масштабуванні Grid-систем. Таким чином, досить актуальною в даний час є проблема розробки засобів забезпечення захисту з розподіленою обробкою інформації.

Організація інформаційної безпеки Grid

У цілому засоби безпеки Grid повинні підтримувати наступні механізми захисту: аутентифікацію, передачу прав, одноразовий вхід, життєвий цикл мандатів і його оновлення, авторизацію, конфіденційність, цілісність даних, обмін політиками, рівень забезпечення безпеки, проникність мережевих екранів (firewall). Більшість з перерахованих вище вимог увійшли в стандарт

під назвою OGSA (Security Architecture for Open Grid Services), розроблений Open Grid Forum(OGF), і на сьогоднішній день Globus Toolkit (GT) - широко поширена реалізація цього стандарту[8].

Основними загрозами для інформації, що обробляється в Grid-системах є: загроза розкриття, загроза цілісності, загроза неналежного використання ресурсів, загроза відмови служб[5]. Забезпечення інформаційної безпеки Grid-інфраструктури передбачає вирішення як мінімум двох завдань: забезпечення стану конфіденційності, цілісності і доступності інформації організаційними і програмно-технічними засобами та забезпечення відповідності вимогам законодавства відносно захисту конфіденційної інформації і персональних даних.

Інфраструктура захисту Globus GSI

В даний час ПО середнього рівня Globus Toolkit є де-факто стандартом при розробці Grid-систем[4]. Для вирішення завдань забезпечення безпеки сучасні Grid-системи використовують інфраструктуру Globus Grid Security Infrastructure (GSI)[2]. Що базується на технології відкритих ключів протокол GSI здійснює аутентифікацію користувача в умовах одноразової реєстрації, комунікаційну захист і початкову підтримку обмеженого делегування повноважень.

Одноразова реєстрація забезпечує користувачеві можливість лише один раз пройти процедуру аутентифікації і, таким чином, створити проксі-сертифікат (proxy certificate), який може бути пред'явлений програмою будь-якої віддаленої службі для аутентифікації від імені користувача. Делегування робить можливим створення і передачу віддаленої службі делегованого проксі-сертифіката, який може бути використаний цією службою для виконання дій від імені користувача (можливо, з деякими обмеженнями); ця можливість виявляється важливою при виконанні операцій, мають вкладену структуру. В якості основи для ідентифікації користувача GSI використовує сертифікати X.509, широко поширеного стандарту для сертифікатів інфраструктури відкритих ключів. Для того щоб пристосувати X.509 на підтримку одноразової реєстрації та делегування повноважень, GSI визначає проксі-сертифікат X.509[9].

Зазвичай при виконанні аутентифікації GSI використовує протокол безпеки транспортного рівня (Transport Layer Security - TLS), що є модифікацією протоколу захищених сокетів (Secure Socket Level - SSL), хоча й інші протоколи аутентифікації на основі технології відкритих ключів можуть використовуватися для роботи з проксі-сертифікатами X.509. Протокол віддаленого делегування проксі-сертифікатами X.509 надбудований над рівнем TLS. Робоча група з проблем проектування Internet (Internet Engineering Task Force - IETF) затвердила попередній документ, що визначає розширення сертифіката X.509 для проксі-сертифіката[9]. Всесвітній форум Grid (Global Grid Forum - GGF) затвердив попередні документи, що

визначають протокол делегування для віддаленого створення проксі - X.509 і розширення GSS-API (Generic Security Services API – програмний інтерфейс уніфікованої служби безпеки), що дозволяють використовувати цей інтерфейс для програмування в Grid. Реалізації всіх алгоритмів захисту в термінах стандарту GSS-API дозволяє врахувати гетерогенність локальних доменів Grid-системи[7]. Розвинена підтримка для обмеженого делегування була продемонстрована в прототипах і є істотною складової пропонованого профілю проксі-сертифіката X.509. Обмежене делегування дозволяє одному об'єкту передати конкретнее підмножина «пулу» своїх привілеїв іншому об'єкту. Таке обмеження важливо в плані зменшення шкоди при навмисному або випадковому зловживанні делегованим сертифікатом.

Захист на рівні повідомлень

Захист транспортного рівня реалізується за рахунок використання самого транспортного механізму (хоча цей метод і забезпечує внутрішню захист сервісів Grid). При інтеграції Grid з Web-сервісами (Web-службами), системи Grid переходять до використання захисту на рівні повідомлень[6]. Оскільки остання передбачає індивідуальний контроль за кожним повідомленням SOAP (Simple Object Access Protocol - простий протокол доступу до об'єкта), вона дозволяє застосовувати протоколи транспортного рівня; таким чином, можна організувати захист на різних рівнях у залежності від важливості даних. Компанії IBM, Microsoft і VeriSign передали на затвердження до OASIS (Organization for the Advancement of Structured Information Standards) специфікацію захисту Web-сервісів, що отримала назву WSSecurity.

Вона пропонує платформу передачі повідомлень SOAP, що служить для інтеграції і підтримки існуючих моделей захисту, і набір розширень для SOAP, які забезпечують цілісність даних і конфіденційність. Розширення для заголовка повідомлень SOAP[1] забезпечує стандартний, що не залежний від платформи і мови механізм обміну захищеними завіреними повідомленнями. Security Assertion Markup Language (SAML). Коли організації спільно використовують ресурси, їм необхідний спільну мову, за допомогою якого суб'єкти Grid можуть обмінюватися інформацією про захист. SAML затверджений OASIS в якості стандарту, визначає мову і протокол для обміну даними про аутентифікацію і надання прав доступу. Твердження SAML містять інформацію про аутентифікаційні посилання, рішення про права доступу і атрибути, пов'язаних із зазначеним суб'єктом. Правила SAML можуть розміщуватися у зовнішніх сховищах правил, завдяки чому віртуальній організації буде простіше використовувати різноманітні правила, використовувані в локальних доменах. SAML визначає інтерфейс протоколу запитів/відповідей, який дозволяє клієнтам запитувати затвердження в уповноважених SAML[10]. Цей протокол, що складається з форматів

повідомлень на базі XML, можна легко пов'язати зі багатьма базовими комунікаціями і транспортними протоколами. Зараз SAML визначає лише один зв'язок - до SOAP через HTTP. Крім того, тимчасові мітки, встановлені для запитів і тверджень SAML, дозволяють адміністраторам Grid пов'язувати тимчасові обмеження зі станом віртуальної організації та користувацькими атрибутами. Тим самим відбувається динамічний характер формування довірчих відносин у середовищах Grid. Extensible Access Control Markup Language (XACML).

Узгоджене формування правил доступу на різних ресурсах є основою реалізації захисту. Стандарт Extensible Access Control Markup Language, затверджений OASIS, визначає базову схему для вираження правил надання прав доступу у форматі XML для різних пристроїв і додатків. Ця схема визначає елементи, необхідні для формулювання правил контролю за доступом, а також надає мову запитів і відповідей для передачі запитів та рішень. Крім того, XACML дозволяє використовувати різні традиційні алгоритми об'єднання правил для прийняття рішень про вибір політики і для об'єднання правил (можливо, одержуваних з різних джерел) в єдиний набір.

Оцінювання доступності інформації

Важливим чинником ефективного виконання завдань Grid-системі є доступність ресурсів і даних. В останні роки лавиноподібно зростає кількість атак на доступність ресурсів та інформації в комп'ютерних системах: DoS (denial-of-service) атак та їх розподіленого варіанти - DDoS (distributed denial-of-service). Згідно з цим, на сьогоднішній день ефективного захисту проти подібних атак практично не існує [11]. Основним способом реалізації DDoS-атак є використання мереж так званих комп'ютерів-зомбі (botnets). За даними, на початок 2009 р. мережі botnets охоплювали близько 650 мільйонів комп'ютерів. Розподілені атаки, спрямовані на досягнення відмови в обслуговуванні (DDoS), представляють серйозну загрозу для багатьох інформаційних систем, та гарантованого захисту від них практично не існує. Це призводить до того, що авторизовані користувачі таких систем не можуть своєчасно отримати доступ до необхідної інформації. Подібні факти блокування роботи систем є причиною величезного збитку багатьох організацій в усьому світі, в тому числі і в Україні.

Одним з найбільш поширених підходів до оцінки доступності ресурсів і інформації є загальна теорія надійності [3], яка розвивається з середини 1950-х років в результаті широкого застосування методів і засобів автоматики і телемеханіки. У рамках теорії надійності розглядається поняття готовності системи, тобто стану працездатності пристрою в довільно вибраний момент часу. Очевидно, що в програмних системах в якості аналога пристрою може розглядатися деякий програмний компонент або сервіс (наприклад, Grid-сервіс в Grid-системах). У цьому випадку можна говорити про готовність чи доступності компонента або сервісу і оброблюваної їм інформації. На основі

цього підходу функціонує ПО GridView [12]. GridView являє собою систему моніторингу та візуалізації роботи Grid-сервісів. Одна з можливостей даного програмного забезпечення – моніторинг доступності Grid-сервісів і цілих віртуальних організацій. GridView дозволяє збирати інформацію про доступність окремих примірників Grid-сервісів, їх типів і організації в цілому. Інформація збирається кожну годину і агрегується по днях, тижнях і місяцях. Однією з метрик, що використовуються в GridView, є стан екземпляра Grid-сервісу, типу Grid-сервісу та організації в цілому. Стан визначається шляхом виконання набору тестів. До одного з недоліків GridView слід віднести недостатню частоту оновлення інформації (або виконання процедури тестування (тільки щогодини)).

Висновок

У статі розглянуті технології захисту інформації, що забезпечує Globus Toolkit і стандартні засоби middleware Advanced Resource Connector(ARC) NorduGrid 3.0.0.

Аналіз існуючих засобів захисту Grid-систем виявив слабкі місця у забезпеченні безпеки даних користувача розміщених у загальній дисковій пам'яті. У зв'язку з цим актуальною є розробка методу індивідуального захисту даних користувача.

1. Simple Object Access Protocol (SOAP) 1.1.W3C, Note 8, 2000.
2. CMS Requirements for the Grid : Proc. of the Int.Conf. on Computing in High Energy and Nuclear Physics (CHEP2001) / K.Holtman
3. *Синопальников В.А*. Надежность и диагностика технологических систем. / В.А.Синопальников, С.Н. Григорьев — М:. "Высшая школа", 2005. — 343 с.
4. *Foster I*. The Anatomy of the Grid. Enabling Scalable Virtual Organizations / I. Foster, C. Kesselman, S. Tuecke // Intern. J. Supercomputer Applications. — 2001. — 15, N 3. — P. 200–222.
5. *Рамакришнан Л.* Защита Grid / Л. Рамакришнан // Открытые системы. — 2004. — № 6. — С.63-68.
6. *Cornwall L.A.* Authentication and authorization mechanisms for multi-domain grid environments / L.A. Cornwall, J. Jensen, D.P. Kelsey // J. of Grid Computing. — 2004. — 9. — P. 301–311.
7. A security architecture for computational grids: Proc. of ACM Conf. on Computers and Security. / I.Foster, C. Kesselman, G. Tsudik, S. Tuecke —1998. — P. 83–91.
8. *Adams C*. Understanding PKI: concepts, standards, and deployment considerations. / C.Adams, S. Lloyd — London: Addison-Wesley, 2002. — 352 p.
9. IETF – Public-Key Infrastructure (X.509) (pkix), 2005. — www.tools.ietf.org/wg/pkix.
10. IETF – Transport Layer Security (tls), 2005. — www.tools.ietf.org.
11. *Tulloch M*. Microsoft Encyclopedia of Security / M. Tulloch— Redmond, Washington: Microsoft Press, 2003. — 414 p.
12. *Kalmady R.* GridView: a Grid monitoring and vizualization tool. / R. Kalmady, D. Sonvane, K.Bhatt —https://twiki.cern.ch/twiki/pub/LCG/GridView/.

Поступила 14.10.2013р.