УДК 004.75:004.056

DOI: 10.18372/2073-4751.69.16809

Давиденко А.М., д.т.н.,
orcid.org/0000-0001-6466-1690,
Гільгурт С.Я., д.т.н.,
orcid.org/0000-0003-1647-1790,
Душеба В.В., к.т.н.,
orcid.org/0000-0002-8929-3625

ЗАСОБИ ДОДАТКОВОГО ЗАХИСТУ ІНФОРМАЦІЇ КОРИСТУВАЧІВ У РОЗПОДІЛЕНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

davidenkoan@gmail.com
hilgurt@ipme.kiev.ua
vdusheba@ukr.net

Вступ

Розподілені високопродуктивні інформаційно-обчислювальні системи, що базуються на грід-технологіях, активно розбудовувалися останні півтора десятки років, в тому числі в Україні [1] і сьогодні стало займають певні ніші в технологічному забезпеченні наукової та господарської діяльності людини. Так, наприклад, система моніторингу однієї з найбільш розповсюджених грід-систем на базі проміжного програмного забезпечення ARC від північноєвропейського консорціуму Nordugrid (роботу якої можна передивитися в реальному часі за посиланням http://www.nordugrid.org/monitor/loadmon.php) наочно свідчить про ефективне використання обчислювальних ресурсів європейської грід-інфраструктури [2].

Разом с тим посилення загроз безпеки інформації, що спостерігається останнім часом, вимагає розробки нових методів та створення додаткових засобів захисту інформації, що зберігається та обробляється у подібних розподілених суперкомп'ютерних мережах.

Аналіз останніх досягнень і публікацій по зазначеній темі показує, що механізми безпеки, які використовуються в сучасних грід-мережах, орієнтовані насамперед на протидію зовнішнім по відношенню до грідівської інфраструктури суб'єктів. У той же час залишаються відкритими питання захисту програмного забезпечення грід-вузлів, а також інформації грід-користувачів від зловмисних дій інших авторизованих користувачів грід-системи, включаючи технічний персонал, що обслуговує грід-вузли. Однак, деякі дослідження стверджують, що від 80% до 90% атак інформаційної безпеки ініціюється саме користувачами всередині комп'ютерної системи [3]. Важливим моментом, який теж необхідно враховувати, є ймовірність злому штатного кіберзахисту грід-вузлів зовнішніми зловмисниками, в наслідок чого неавторизовані особи також можуть отримати доступ до приватних даних користувачів грід-системи.

Додаткові труднощі також виникають при обробці великих обсягів даних у зв'язку з тим, що стандартні засоби кібербезпеки грід-системи (зокрема, механізм відкритих ключів, заснований на використанні асиметричних алгоритмів) здатні істотно завантажувати комп'ютер користувача, що відправляє дані в грід-систему, так само, як і віддалені обчислювальні потужності.

В роботі запропоновано принципи створення додаткових засобів захисту інформації, які дозволяють доповнити і розширити штатні можливості захисту інформації стандартних сервісів гріду, зокрема, ввести додаткові функції закриття даних, що підлягають віддаленій обробці, а також підвищити показники швидкодії при рішенні задач закриття великих обсягів інформації, які передаються в грід-мережу.

Використання реконфігуровної платформи (на базі ПЛІС) дозволяє синтезувати цифрові схеми довільної складності [4-5], наприклад, високопродуктивні спеціалізовані процесори закриття інформації, які в тому числі, можуть реалізувати нестандартні алгоритми закриття інформації.

Постановка задачі

У попередніх роботах авторів [6-7] було закладено методологічні основи побудови систем внутрішньої безпеки грід-мережі. На основі аналізу відомих загроз у комп'ютерних системах та розроблених для них засобів протидії з урахуванням специфіки грід-середовища сформовано функціонал таких систем, який має реалізуватися підсистемами:

- контролю за цілісністю інформації;
- виявлення вторгнень сигнатурного типу;
- протидії мережевим хробакам;
- додаткового криптографічного захисту інформації грід-користувачів.

Реалізація функціональності останнього, четвертого типу набула сьогодні нової актуальності й потребує доопрацювання з урахуванням вимог сьогодення.

Аналізуючи особливості підсистеми безпеки грід-інфраструктури з точки зору закриття даних від авторизованих користувачів та від технічного персоналу грід-вузлів, приходимо до висновку, що найбільш уразливою інформація виявляється під час відносно довготривалого зберігання на дискових носіях у вигляді файлів даних у відкритому вигляді. Саме на даному етапі обробки приватні дані користувачів найбільш вразливі для зловмисних дій збоку авторизованих користувачів грід-системи, а також технічного персоналу, що обслуговує грід-інфраструктуру.

Таким чином, виникає необхідність у розширенні можливостей вбудованих у грід засобів інформаційної безпеки, а саме – у введенні додаткових функцій закриття даних під час їх віддаленій обробки, а також у підвищенні продуктивності виконання завдань закриття інформації в грід-мережі.

Отже, метою даної роботи є пошук можливостей та шляхів побудови засобів підвищення захищеності конфіденційних даних користувачів, як від зовнішніх, так і від внутрішніх по відношенню до грід-системи зловмисників, використовуючи в якості платформи реконфігуровні пристрої на базі ПЛІС.

Застосування реконфігуровних обчислювачів

Як свідчать дослідження, найбільш придатними в якості платформи створення засобів захисту інформації для мережевих застосувань на базі програмованої логіки є так звані реконфігуровні обчислювачів (РО) – приєднані пристрої на базі ПЛІС типу FPGA, які підключаються до серверів віддалених кластерів та локальних ПЕОМ користувачів за стандартними інтерфейсами обміну даних [8]. Сучасні ПЛІС дозволяють миттєво завантажити в себе (тобто, фактично, виготовити) довільну обчислювальну архітектуру, яка може сягати мільйонів логічних елементів. Використання РО дозволяє підвищити ефективність та гнучкість апаратних засобів захисту інформації, а також знизити загальну вартість технічного рішення.

Крім розвантаження центрального процесора апаратний захист із застосуванням РО підвищує безпеку обчислювальної системи в цілому. Це обумовлено, насамперед, тим фактом, що на виконання алгоритму шифрування не можуть вплинути шкідливі програми, оскільки він реалізується не в оперативній пам'яті комп'ютера, а на апаратному рівні, а також можливістю знизити ризик перехоплення секретної інформації по електромагнітному випромінюванню спеціальні схемотехнічними прийомами. Крім того, в апаратних засобах захисту інформації можуть бути реалізовані додаткові функції, такі як якісна генерація випадкових чисел, розрахунок контрольних сум для критичної інформації, авторизація процесу завантаження робочої станції та доступу до

зовнішніх накопичувачів і периферійних пристроїв.

Для досягнення найбільшої продуктивності при вирішенні поставленої задачі необхідно задіяти РО на обох кінцях каналу обміну даними, що захищаються, тобто як в складі ПЕОМ грід-користувача, так і в складі віддаленого обчислювального вузла.

Принципи реалізації додаткового захисту

Механізм реалізації згаданих вище додаткових функцій підсистеми захисту інформації грід-мережі в загальному випадку виглядає наступним чином. Перед запуском на виконання грід-завдання в ПЛІС реконфігуровного обчислювача на комп'ютері грід-користувача (в разі його наявності) завантажується структура спеціалізованого процесора, що реалізує необхідні алгоритми закриття інформації. Дані, що підлягають обробці, після перетворення – або апаратно в РО (центральний процесор комп'ютера користувача в такому випадку практично не навантажується), або програмним способом передаються комунікаційними каналами на цільовий грід-вузол і зберігаються там у закритому вигляді. Процедура зворотного перетворення даних ініціюється завданням користувача безпосередньо перед його виконанням і здійснюється або за допомогою РО, встановленого на цільовому грід-вузлі, або програмним способом, з використанням обчислювальних ресурсів кластера.

В системах додаткового захисту інформації, побудованих за запропонованими принципами, в залежності від ступеню "стандартності" можуть бути здійснені кілька варіантів реалізації розглянутого вище механізму закриття даних користувача, наприклад:

- "прозорий" режим – з максимальним використанням штатних засобів безпеки грід-інфраструктури і реалізацією на ПЛІС стандартних алгоритмів захисту;
- "прозорий розширений" режим – з можливістю завантажувати в ПЛІС нестандартні, зокрема, посилені алгоритми закриття інформації [9];
- "напівпрозорий" режим, при якому вбудовані засоби безпеки грід-інфраструктури використовуються тільки для забезпечення авторизації та доставки ключової інформації, а процедури власне закриття інформації реалізуються компонентами програмно-апаратної підсистеми захисту даних за безпосередньою участю користувача; тобто грід-користувач має можливість обирати спосіб закриття інформації та конфігурувати відповідні компоненти.

В останніх двох режимах ступень захисту додатково підвищується, тому що зловмисник в загальному випадку не має відомостей про алгоритм закриття інформації.

У кожному з перерахованих вище варіантів замість РО можливо використовувати програмну реалізацію, як на комп’ютері користувача, так і на віддаленому грід-вузлі. Але в цьому випадку знижується продуктивність системи і надійність закриття інформації.

Для створення повноцінної системи додаткового захисту розробникові необхідно мати відповідний інструментарій, що включає в себе бібліотечні компоненти, утиліти, конфігурації (bitstream) для ПЛІС, приклади використання, тестові додатки тощо.

Слід зауважити що грід-середовище може виступати не тільки в якості об’єкта захисту, але й ще як інструмент централізованого створення реконфігуровних компонентів системи додаткового захисту при наявності відповідного сервісу [10-11].

Використання сервісу віртуальних організацій

Поняття віртуальної організації (ВО) є основним у сучасних грід-системах [12]. ВО являє собою об'єднання користувачів і ресурсів грід для вирішення завдань у конкретній галузі наукових досліджень у рамках грід-інфраструктури у відповідності до встановлених для даної ВО правил. Ці правила регулюють доступ до всіх типів засобів, включаючи обчислювальні

ресурси, програмне забезпечення та дані. Склад ВО може динамічно змінюватися [13].

Технічно, щоб якийсь грід-вузол був доступний для віддаленого використання, він повинен надати свої ресурси хоча одній ВО. З іншого боку, кожен грід-користувач, для того, щоб мати можливість задіяти конкретний грід-ресурс, повинен бути зареєстрований хоча б в одній віртуальній організації, допущеній до його використання. Таким чином, членство у ВО є обов'язковою умовою роботи в грід-середовищі.

Беручи до уваги ключову роль віртуальних організацій у грід-системах, у цій роботі автори пропонують організувати централізоване управління засобами додаткової безпеки на рівні ВО. Доцільність такого рішення обумовлена наступними причинами.

По-перше, всіх учасників ВО об'єднують загальні цілі та інтереси, наприклад, єдина галузь наукових досліджень, або виробнича галузь, для якої ведуться розробки. Для вирішення подібних завдань, як правило, на всі обчислювальні елементи ВО, встановлюється одноманітне програмне забезпечення. Даний факт дозволяє спростити процеси управління додатковим захистом та підвищити їх ефективність.

По-друге, внаслідок подібності завдань, що розв'язуються, до інформаційних об'єктів грід-користувачів – учасників ВО пред'являються близькі вимоги щодо рівня безпеки. Так, якщо оброблена в межах віртуальної організації інформація є критичною і пред'являє підвищені вимоги щодо конфіденційності, то правила поведінки всіх членів даної ВО регламентуються відповідним чином.

Як важливий момент слід також відзначити наявність посад системного адміністратора ВО і системного адміністратора безпеки ВО. З одного боку, ці особи зацікавлені в успішному виконанні всіх грід-завдань, що запускаються в межах ВО, з іншого – вони не мають такі повноваження, як локальні адміністратори грід-вузлів. Зазначені причини обумовлюють доцільність надання їм повноважень з управління додатковим захистом.

Функціонування ВО здійснюються за допомогою служби членів віртуальної організації (англ. Virtual Organization Membership Service – VOMS), у базі даних якої зберігається інформація про членів віртуальної організації та їх права [14]. Використовуючи VOMS-сервер, адміністратор ВО має можливість керувати політикою безпеки ВО, змінювати права та ролі користувачів ВО, а також контролювати процес реєстрації нових учасників ВО. VOMS-сервер також бере безпосередню участь у процесі делегування прав грід-користувача процесам, що запускаються на грід-ресурсах. При цьому до базової інформації про автентифікацію користувача додаються відомості про його права і ролі у віртуальній організації.

Отже, при практичній реалізації механізмів додаткового захисту на рівні ВО, може бути ефективно використана функціональність VOMS-серверів. Зокрема, в їх базах даних може зберігатися і підтримуватися його конфігураційна інформація. До такої інформації можуть бути віднесені статуси безпеки грід-ресурсів, що входять до ВО і ключова інформація для сервісу додаткового захисту даних користувача.

Висновки

Створені в результаті виконання даного дослідження системи додаткового захисту приватної інформації дозволяють грід-користувачеві підвищити ступінь захищеності своїх програм і даних, що пересилаються в грід-мережі та зберігаються на віддалених серверах, а також прискорити процес перетворення великих обсягів інформації з метою її захисту.

Розглянутий механізм закриття даних користувача може бути реалізований в декількох варіантах, у кожному з яких замість РО можливе використання програмної реалізації.

Ґрунтуючись на ключовій ролі віртуальних організацій у гріді, а також з метою забезпечення максимальної прозорості використання створюваних сервісів

запропоновано для управління системою додаткового захисту даних використовувати функціональність вже наявних в грід-системі VOMS-серверів.

Література

1. *Петренко А.І., Свістунов С.Я., Кисельов Г.Д.* Практикум з грід-технологій: навчальний посібник. – К.: НТУУ «КПІ», 2011. – 580 с.

2. Advanced Resource Connector / Nordugrid. Grid Solution for Wide Area Computing and Data Handling [Електронний ресурс] – Режим доступу: http://www.nordugrid.org/middleware. – Загл. с екрану. – (Дата звернення: 07.07.2022)

3. Tulloch M. Microsoft Encyclopedia of Security. – Redmond, Washington: Microsoft Press, 2003. – 414 p.

4. Палагин А.В., Опанасенко В.Н. Реконфигурируемые вычислительные системы: Основы и приложения / К.: «Просвіта», 2006. – 280 с.

5. Hilgurt S.Ya. A Survey on Hardware Solutions for Signature-Based Security Systems // The 1st International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP-2021): Proceedings of the 1st International Workshop, Ternopil, Ukraine, 16-18 Nov. 2021. – Ternopil: Faculty of Computer Information Systems and Software Engineering, 2021. – P. 6-23

6. Давиденко А.Н., Гильгурт С.Я., Душеба В.В., Гиранова А.К. Анализ вопросов внутренней безопасности в распределенных компьютерных сетях // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2011. – Вип. 62 – С. 57-62.

7. Давиденко А.Н., Гильгурт С.Я., Душеба В.В., Евдина А.К. Развитие системы внутренней защиты информации в распределенных компьютерных сетях // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2012. – Вип. 63 – С. 3-9.

8. Гильгурт С.Я. Реконфигурируемые вычислители. Аналитический обзор // Электронное моделирование. – 2013. – Т.35. – № 4. – С. 49-72.

9. Гиранова А.К. Обобщенная структура реконфигурируемого процессора, реализующего симметричные алгоритмы закрытия информации // Зб. наук. праць ІПМЕ ім. Г.Є.Пухова НАН України. – Київ, 2010. – Вип. 57. – С. 113-119.

10. Evdokimov V., Davydenko A., Hilgurt S. Using GRID for Centralized Synthesis of FPGA-based Information Security Systems // Pattern Recognition and Information Processing (PRIP'2021): Proceedings of the 15th International Conference, Minsk, Belarus, 21-24 Sept. 2021. – Minsk: UIIP NASB, 2021. – P. 115-118.

11. Євдокимов В.Ф., Давиденко А.М., Гільгурт С.Я. Свідоцтво про реєстрацію авторського права на твір № 105997; Комп'ютерна програма «Веб-сервіс централізованого програмування реконфігуровних засобів захисту інформації на базі гріду та хмарної інфраструктури STRAGS» («Веб-сервіс STRAGS») / Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, дата реєстрації 7.07.2021 р.

12. Foster I., Kesselman C., Tuecke St. The Anatomy of the Grid: Enabling Scalable Virtual Organizations // International Journal of High Performance Computing Applications, 2001. – Vol. 15. – №3. – P. 200-222.

13. Кирьянов А.К. Введение в технологию Грид: Учебное пособие. / А.К. Кирьянов, Ю.Ф. Рябов. – Гатчина: ПИЯФ РАН, 2006. – 39 с.

14. VOMS Usage Notes. [Електронний ресурс]. – Режим доступу: http://www.nordugrid.org/documents/voms-notes.html. – Загл. с екрану. – (Дата звернення: 07.07.2022).

Давиденко А.М., Гільгурт С.Я., Душеба В.В.

ЗАСОБИ ДОДАТКОВОГО ЗАХИСТУ ІНФОРМАЦІЇ КОРИСТУВАЧІВ У РОЗПОДІЛЕНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ

Робота присвячена питанням кібербезпеки в розподілених високопродуктивних середовищах, заснованих на використанні технології грід-обчислень. В розвиток попередніх робіт авторів, враховуючі нові обставини, що з'явилися останнім часом, запропоновані принципи побудови додаткових апаратно-програмних засобів захисту конфіденційних даних та програм користувачів, як від зовнішніх, так і від внутрішніх по відношенню до грід-системи зловмисників, включаючи технічний персонал, що обслуговує грід-вузли. При цьому запропоновані підходи не підміняють, а доповнюють та розширюють штатні можливості інформаційної безпеки гріду. Використання в якості апаратної платформи реконфігуровних обчислювачів на базі ПЛІС дозволяє забезпечити ефективність та гнучкість використаних засобів захисту інформації. Розглянуто декілька режимів реалізації механізму закриття даних користувача, що відрізняються ступенем використання штатних можливостей кіберзахисту грід-середовища. Кожний з режимів дозволяє задіяти замість апаратної програмну реалізацію алгоритмів закриття інформації – як на стороні персонального комп'ютера користувача, так і на обчислювальних вузлах розподіленої мережі. Для управління додатковим захистом даних запропоновано використовувати функціональність наявних в грід-системі VOMS-серверів, що забезпечують функціонування механізмів віртуальних організацій.

Ключові слова: *грід, захист інформації, ПЛІС, додатковий захист, VOMS.*

Davydenko A.M., Hilgurt S.Ya., Dusheba V.V.

TOOLS FOR ADDITIONAL PROTECTION OF USER INFORMATION IN DISTRIBUTED COMPUTER NETWORKS

The work is devoted to issues of cybersecurity in distributed high-performance environments based on Grid technology. In the development of the previous works of the authors, taking into account the new circumstances that have appeared recently, the principles of building additional hardware and software tools are proposed for protecting user's confidential data and programs, both from external and internal attackers, including personnel of Grid infrastructure. At the same time, the proposed approaches do not replace, but complement and expand the standard information security capabilities of the Grid. The use of FPGA-based reconfigurable accelerators allows ensuring the efficiency and flexibility of the information protection tools. Several modes of implementation of the mechanism of closing user data are considered which differ in the degree of use of the standard capabilities of cyberprotection of the Grid. Each of the modes allows hardware as well as software implementation of the encrypting algorithms – both on the side of the user's personal computer and on the computing nodes of the distributed network. To manage additional data protection, it is proposed to use the functionality of VOMS servers available in the Grid system, which provide the functioning the virtual organizations.

Keywords*: grid, information security, FPGA, additional protection, VOMS.*