ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ НАДІЙНОГО ДОСПУПУ ДО ГРІД-ІНФРАСТУКТУРИ

к. т. н. Гіоргізова-Гай В. Ш.,
Сулімов А. В.
ННК «ІПСА» НТУУ «КПІ», вул. Панаса Мирного 19, Київ 03056

Сьогодні Грід-технології все активніше входять у різні сфери життя суспільства, і спрямовуються на вирішення не тільки складних науково-технічних задач, а й власних задач бізнесу, промисловості, організації сховищ даних, тощо.

Доступ до ресурсів та сервісів є одним з найбільш важливих компонентів Грід системи, що називається User Interface (UI). Йому приділяється особлива увага, тому що він є ключовим сполучною ланкою між Грід середовищем і кінцевим користувачем.

User Interface зазвичай реалізується у двох видах: інтерфейс командного рядка (Command Line Interface — CLI) та графічний інтерфейс (Graphical User Interface — GUI) За характером реалізації GUI можна розділити на два типи: Java аплети та програми і Грід-портали — Web-орієнтовані обчислювальні портали.

Очевидними перевагами GUI є надання користувачам простого інтуїтивно зрозумілого засобу, який зробити складну інфраструктуру Грід прозорою для вирішення їх прикладних задач. В доповнення до цього GUI у вигляді Грід-порталу дозволяє використовувати у якості клієнтського ПЗ стандартний web-браузер. Web-портали, як і будь-які Web-додатки, уразливі до хакерських атак.

Сьогодні існує цілий ряд Грід-орієнтованих CMS систем — конструкторів створення і керування сайтом, наприклад, Gridsphere,Uportal, Clarens та багато інших. Завдяки їх використанню розробка, впровадження, підтримка і використання Grid-порталів стає все більш зручною. Ці засобами є достатньо зрілими продуктами, що забезпечують досить високу безпеку створених на їх основі порталів, але вони також підтримують експорт модулів сторонніх розробників і створення власних. Це може негативно вплинути на питання безпеки. Навіть, якщо злонавмисник не зможе отримає доступ до самих ресурсів Грід, а тільки до порталу, це все одно зашкодить надійному обслуговуванню користувачів.

Загальна концесія захисту Web-проекту повинна забезпечувати комплексний захист, який повинен включати надійну безпеку: безпеку Web-сервера (операційної системи, Web-сервера, середовища програмування, бази даних, засобів захисту Web-сервера), системи управління Web- порталу (CMS), інформаційного середовища адміністраторів Web-порталу, а також сторонніх Web-додатків. Важливими механізмами забезпечення інформаційної безпеки Web-проектів є: політика безпеки, аудит і протоколювання подій на всіх компонентах комплексного захисту Web-проекту [1].

Розглянемо більш детально питання пов'язані з безпекою CMS і аудитом безпеки порталу на прикладі експериментального Web-порталу SDGrid (System Development by Grid), створеного з метою надання доступу користувачам до обчислювальних можливостей і різних інформаційних ресурсів національної Grid-інфраструктури України [2].

Загальними вимогами порталу є:

- Універсальний доступ без додаткового ПО з боку клієнта.
- Наявність надійних інформаційних сервісів, зокрема про Grid ресурси.
- Використання відкритих стандартів і технологій Grid.
- Масштабована і гнучка структура, легкість додавання/видалення додатків порталів, програмних систем Grid, обчислювальних ресурсів, сервісів, користувачів і так далі.
- Підтримка стандартів Global Grid Forum.
- Підтримка розподілених клієнтських застосувань і порталів.

Також висуваються такі вимоги до безпеки системи управління порталом:

- Підтримка стандарту безпеки Грід Globus Security Infrastructure (GSI).
- Використання протоколів HTTPS/SSL, шифрування даних на всіх рівнях.
- Надійний механізм аутентифікації.
- Єдина система аутентифікації: використання одного облікового запису для доступу до різних ресурсів Grid.
- Використовувані інструментальні засоби повинні мати добре супроводження і постійне оновлення

Базовий портал SDGrid побудований на базі CMS Gridsphere 2. 1. 5 з використанням інструментарію: OGCE 2. 2 portlets і GridPortlets 1. 4. Проведена розробниками порталу SDGrid

порівняльної характеристики безкоштовних Grid орієнтованих CMS показала, що Gridsphere в даний час є найбільш зручною, популярною і поширеною платформою для створення як обчислювальних порталів, так і порталів користувача [3].

Gridsphere і додатковий інструментарій відповідають висунутим вимогам до системи безпеки порталу. Механізм аутентифікації порталу SDGrid заснований на передачі сертифікату, виданого центром сертифікації, приватного ключа користувача і отриманні на їх основі тимчасового прокси-сертифікату у сервера MyProxy. За допомогою порталу і отриманого прокси-сертифікату користувач авторизується і може посилати завдання в Грід і проглядати результати.

Для пошуку погроз інформаційній безпеці Web-додатків існує 2 методи: ручний пошук (виконуваний людиною) і автоматичний (виконуваний сканером безпеки). Для проведення об'єктивного дослідження техніки безпеки порталу SDGrid, спочатку був виконаний автоматичний аналіз безпеки, а потім — ручна перевірка з'ясованих погроз високого і середнього ступеню небезпеки.

Вибір автоматичних сканерів безпеки проводився на основі огляду ринку сканерів і результатів опитування.

Порівняння характеристика вибраних сканерів безпеки проводилося за їх характеристиками, які були заявлені розробниками. Було виділено 5 груп критеріїв порівняння, які найповніше охоплюють функціональні аспекти вибраних сканерів.

Загальна порівняльна характеристика сканерів по всіх групах критеріїв представлена у таблиці 1. Оцінка показує скільки критеріїв (можливостей) з максимальної кількості у групі підтримує даний сканер.

Таблиця 1 — Загальна оцінка по всіх групах критеріїв

Критерій порівняння	**Максимум балів**	**Nmap**	**Nessus**	**AWVS**	**SSS**	**XSpider**
Параметри сканування	15	9	13	9	10	10
Розгортання і архітектура	5	2	5	1	1	1
Управління результатами сканування і реагування	11	0	7	9	7	10
Оновлення і підтримка	4	0	2	2	2	3
Додаткові критерії	3	1	0	1	0	2
Разом балів	38	12	27	22	20	26

Таким чином, в наслідок порівняння найбільш важливих критеріїв 1 і 3 груп (функціональних можливостей), лідирують сканери Nessus і XSpider, непогано зарекомендували себе сканери AWVS і SSS, сканер Nmap отримав найменшу кількість балів головним чином через відсутність використання різних настройок і методів. У таблиці 2 представлена кількість знайдених класів загроз.

Таблиця 2 — Результати сканування порталу SDGrid

Критерій порівняння		**Nmap**	**Nessus**	**AWVS**	**SSS**	**XSpider**
Знайдено все класів погроз		4	2	4	2	4
Ступінь ризику	Високий	0	0	1	1	0
	Середній	0	0	1	0	1
	Низький	4	2	2	1	3

Слід відмітити, що сканери XSpide, AWVS і SSS показали в цілому сумірний час сканування, тоді як Nessus і Nmap працювали на порядок менше. З найшвидше провів сканування Nmap, а найдовше — AWVS.

Знайдені класи погроз безпеці високого і середнього рівнів ризику були перевірені ручним методом пошуку. Ручний метод підтвердив загрозу «Міжсайтове виконання сценаріїв» (Cross Site Scripting) високого ступеня ризику (її по різному класифікувавши виявили AWVS, SSS і XSpide) і «Фіксація сесії» середнього ступеня ризику (її виявив тільки AWVS). Таким чином найкраще зарекомендував себе сканер AWVS, який об'єктивно знайшов більшу кількість загроз, показав найбільш докладний їх опис, а також рекомендації по усуненню.

Механізми безпеки порталу SDGrid в цілому задовольняють поставленим вимогам до безпеки, проте мають ряд уразливостей. Для захисту від класу атак «Фіксація сесії» потрібно перейти на 3-у версію системи GridSphere. Причому успіх їх застосування багато в чому залежить від професіоналізму хакера і халатності адміністраторів безпеки порталу. Також істотним підвищенням загального захисту порталу може служити використання індивідуального міжмережевого екрану, наприклад, Chek Point FW-1 або CYBERWALLPLUS. Такий екран забезпечить додатковий рівень безпеки за рахунок запобігання відомим типам атак на сервер і своєчасних сповіщень адміністратора безпеки про підозрілу діяльність.

Література

1. Офіційний сайт організації Web Application Security Consortium. — Режим доступу: http://www. webappsec. org/.

2. Згуровський М. З. Створення національної Grid-інфраструктури для забезпечення наукових досліджень / Згуровський М. З., Петренко А. І., Кисельов Г. Д. // Інформаційні технології в освіті. — 2009. — № 4. — С. 12–17.

3. Киселев Г. Д. Использование платформы GridSphere для создания Grid-порталов / Киселев Г. Д., Зеленюк А. А., Киевский А. Г., Оленович Е. В. // Системный анализ и информационные технологии: Материалы 11-й международной научно-технической конференции «САИТ-2009». — К. : НТУУ «КПІ», 2009. — С. 440.

АДАПТИВНЕ ЗАСТОСУВАННЯ МАТРИЦЬ КВАНТУВАННЯ В АЛГОРИТМАХ ЗМЕНШЕННЯ НАДЛИШКОВОСТІ ДАНИХ НА ОСНОВІ ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ

Віталій Горєлов, Юрій Ілляш
Прикарпатський національний університет
імені Василя Стефаника,
вул. Шевченка, 57 м. Івано-Франківськ, 76025

Алгоритми зменшення надлишковості даних на основі одного із ортогональних перетворень — дискретного косинусного перетворення (ДКП) ґрунтуються на спектральній інтерпретації сукупності просторових хвиль [1]

$$S_{vu} = \frac{1}{4} C_u C_v \sum_{x=0}^{7} \sum_{y=0}^{7} s_{yx} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16}, \qquad (1)$$

де S_{vu} — результат обчислення ДКП для координат v, u матриці даних, C_u, $C_v = 1/2$ для u, $v = 0$ і C_u, $C_v = 1$ для інших значень, s_{yx} — зміщенні значення вхідної величини.

Існують аналоги дискретного косинусного перетворення, що дозволяють підвищити ефективність обчислень шляхом заміни значень косинусів числами, які отримують за допомогою операцій зсуву та додавання.

ДКП набуло широкого застосування завдяки можливості «ущільнення енергії».

Висока ефективність стиснення даних, якої досягають в алгоритмах з ДКП, базується на тому факті, що у матриці частотних коефіцієнтів, яка утворюється з вихідної матриці після дискретного косинусного перетворення, низькочастотні складові розташовані ближче до верхнього лівого кута, а високочастотні — до правого нижнього.

Людське око чутливе до низькочастотної складової сигналу. Таким чином, можна усунути високочастотні складові і значно зменшити кількість даних, призначених для зберігання та передачі. Зменшення надлишковості реалізують шляхом ділення значень елементів вихідної матриці на значення елементів матриць квантування. Подальшого ущільнення досягають за допомогою ентропійного кодування [1].

Як міру похибки відновлення можна прийняти різні величинами, зокрема, нормоване середньоквадратичне відхилення або критерій максимальної похибки оцінювання.

Вирішення задачі стиснення даних у такій постановці не передбачає проведення оцінки ефективності та управління нею. Оцінка ефективності у даному випадкові — процедура суб'єктивна. Ступінь відповідності числових показників якості та оцінки користувача («задовільно», «не задовільно») може визначатися цілим рядом параметрів і може ніколи не досягати бажаного з точки зору математики значення. Проте, вирішальне значення має рішення користувача.

Отже, існує необхідність забезпечити можливість адаптації процедури усунення надлишковості даних до потреб користувача, які не формулюються чітко.

Алгоритми типу jpeg реалізують ступінчасту зміну ступеню стискання, яка задається відповідними матрицями квантування.

Коефіцієнти матриць вибрані дослідним шляхом групою JPEG, проте вони можуть бути довільними, оскільки,у відповідності до стандарту,входять окремим блоком до файлу з даними.

У ряді випадків існує потреба у проведенні оптимізації розміру файлу у відповідності до особливостей його подальшого використання. Наприклад, для web-сторінок. Особливо актуальна задача у випадкові пакетної оброки. Встановлення ступеню стиску зазвичай покладається на користувача. При цьому процес має інтерактивний характер, що знижує ефективність роботи і збільшує затрати часу.

Таким чином, актуальною є задача розробки системи, здатної самостійно оцінити якість стиснутих даних і, у відповідності