УДК 651.2:004.38

ПАРАМЕТРИЧНЕ УПРАВЛІННЯ ПРІОРИТЕТАМИ ОБСЛУГОВУВАННЯ WEB-ДОДАТКА СЕРВЕРОМ

А.Л. Єрохін, О.П. Турута

Харківський національний університет внутрішніх справ, м. Харків, Україна, ayerokhin@ukr.net
Харківський національний університет радіоелектроніки, м. Харків, Україна, science.ukraine@gmail.com

Розглядається вирішення задачі покращення обслуговування web-додатка в мережі Інтернет за допомогою параметричного управління пріоритетами обслуговування сервером. При цьому за рахунок використання механізмів пріоритетів сервера забезпечується можливість ізоляції web-додатка.

УПРАВЛІННЯ ПРІОРИТЕТАМИ, WEB-СЕРВЕР, ОБСЛУГОВУВАННЯ WEB-ДОДАТКА, ПАРАМЕТРИЧНЕ УПРАВЛІННЯ

1. Вступ

Сучасний Інтернет стає все більш складним та набуває яскраво виражених ознак інтелектуальної розподіленої системи. Користувачі звертаються до сучасних web-сервісів Інтернету як до системи, яка вирішує інтелектуальні задачі людини. Тому розроблення принципів, методів й архітектурних багатоагентних систем та засобів управління обслуговуванням є актуальною задачею.

Динамічний розвиток технологій розробки web-сайтів призводить до того, що прості web-сторінки заміняються web-додатками. Усе більше завдань виконується на стороні клієнта. Заміна архітектурних принципів проектування додатків викликає наступні проблеми:

– складність керування пріоритетом обслуговування процесів;

– визначення границь web-додатка;

– можливий вплив небажаного коду, іншого web-додатка;

– неможливість ізолювання програм у браузері одна від одної;

– виникнення передумов втручання в роботу web-додатка, підміна та аналіз даних, у тому числі в межах сесії.

Вказаними проблемами активно займається світова науково-технічна спільнота. Так, у роботі [1] представлені проблеми ізоляції web-додатків, у роботах [2,3,4] розглядаються моделі роботи web-сервісу і принципи проектування web-додатків, у роботі [5] описані методи формування web-додатка, критерії створення безпечних додатків охарактеризовані в [6, 7].

2. Постановка задачі

Виходячи з аналізу попередніх розробок, необхідно вирішити наступні задачі:

1) дослідити модель процесу авторизації користувача на основі існуючого підходу параметричного управління пріоритетами обслуговування сервером;

2) розробити метод покращення обслуговування web-додатка. Під час розробки методу необхідно забезпечити можливість ізоляції web-додатка, для чого будемо використовувати механізми розподілу пріоритетів сервера;

3) розробити метод формування маркерів для захисту сесії web-додатка;

4) забезпечити захист даних автентифікації під час передачі неконтрольованими каналами зв'язку;

5) розробити спосіб розподілу загального пріоритету web-додатком на дочірні процеси.

3. Розподіл пріоритетів обслуговування агентів сервером

Процес авторизації агента відповідно до [6] виконується в три етапи (рис. 1):

1. Функції, дозволені агентові до ідентифікації (I) і вибір моменту ідентифікації (FIA_UID.1).

2. Функції, що реалізують ідентифікацію агента (FIA_UID.2), функції дозволені до автентифікації (II), вибір моменту автентифікації (FIA_UAU.1).

3. Функції, що реалізують автентифікацію (FIA_UAU.2) і сам процес роботи користувача після авторизації (III).

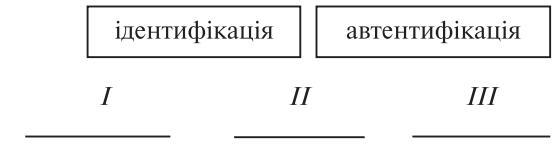


Рис. 1. Схема авторизації агента

Клас (FIA) і підкласи (FIA_UAU, FIA_UID) відповідають стандарту [7].

Пропонується використовувати номер етапу авторизації користувача як ознаку для формування сервером пріоритету обслуговування агентів. Модифікуємо відому модель [8] параметричного керування пріоритетами обслуговування:

$$W_{t+1} = \begin{cases} W_t - 1, & A_t(l) = 1 \wedge A_t(l) = 2 \vee (\beta - D_t^l) * P_t < 0 \\ W_t, & A_t(l) = 2 \wedge (\beta \le D_t^l \vee A_t(l) = 3) \wedge \\ & \wedge (P_t > \alpha \vee A_t(l) = 1) \\ W_t + 1, & A_t(l) = 3 \vee (\beta - D_t^l) > 0, \end{cases} \quad (1)$$

де $A_t(l)$ – функція авторизації агента сесії l у момент часу t; D_t^l – значення функції довіри агентові сесії l у момент часу t; α – граничні значення продуктивності сервера; P_t – стан сервера в момент часу t; β – нормоване значення рівня довіри, а різниця $\beta - D_t^l$ – визначає знак виразу.

Розробка функції D детально буде розглядатися в наступній роботі, а тут визначимо, що остаточна повна оцінка довіри агентові з боку системи визначається успішністю автентифікації. Однак існує багато видів атак на процес автентифікації з метою спрацювання в системі помилки I-го роду, коли доступ до системи отримає той, хто такого права не має, або спрацювання в системі помилки II-го роду, коли доступ до системи не зможе отримати той, хто має право на це та намагається його отримати. Необхідно зменшувати ймовірність виникнення помилок I-го та II-го роду відповідно P_I , P_{II} . Однак посилення правил політики безпеки призводить до збільшення ймовірності P_I , послаблення правил безпеки призводить до збільшення ймовірності P_{II} , а використання функції D оцінки довіри агентові дозволить покращити відношення $\frac{P_I}{P_{II}}$. D визначається від P^1 , P^2 , де P^1 – ознаки агента; P^2 – ознаки стану системи.

4. Метод формування маркера

Для забезпечення надійної роботи сесії на етапі III необхідно сформулювати множину маркерів – M^l для сесії l, де елемент M_k^l ($M_k^l \subset M$, $k = \overline{1, M(M^l)}$) – маркер k-го запиту в сесії l.

Ідентифікатор агента є несекретним та може передаватися відкрито, проте дані автентифікації є секретними, тому передача їх неконтрольованими каналами зв'язку є небажаною. Наприклад компрометація біометричних даних є проблемою для подальшої роботи системи захисту [6].

В [9] відзначено високу ефективність використання одноразового блокноту, тому для реалізації автентифікації і захисту сесії пропонується сформувати множину маркерів M^l . Кожен маркер, як і шифрограми одноразового блокноту, буде використаний один раз.

На рис. 2 наведено схему проведення безпечної автентифікації та формування множини M^l .

Послідовність SA генерується сервером з урахуванням ознаки клієнта, сесії та випадкової величини. Номер SN вказує, який елемент множини M^l використовується для формування відповіді SB. Відмітимо, що з послідовностей SA, SB математично важко отримати образ даних автентифікації (паролю) – S. Клієнт знає (володіє) даними авторизації, web-додаток за відомим алгоритмом знаходить S-образ, а сервер зберігає замість даних автентифікації його S-образ.

Розглянемо метод формування множини маркерів M^l для сесії l.

Нехай SN – кількість маркерів, яку необхідно сформувати, значення SN вибирається випадково в інтервалі $L2 \geq L1 \geq SN$. У [10] вважається для Інтернет-сесій достатнім L1=500 та L2=1000.

Використаємо послідовність SA та образ даних автентифікації S для формування останнього елемента множини

M^l : $M_{L2}^l = sha1(SA + S)$.

Кожний попередній елемент знаходиться за формулою

$M_j^l = sha1(M_{j+1}^l)$,

де $j = \overline{L2-1, 1}$.

На сервері випадковим чином вибирається SN ($L1 \geq SN$), формується послідовність SA, далі формується множина M^l . M_{SN}^l зберігається у сесії l, а клієнту відправляється SA, SN.

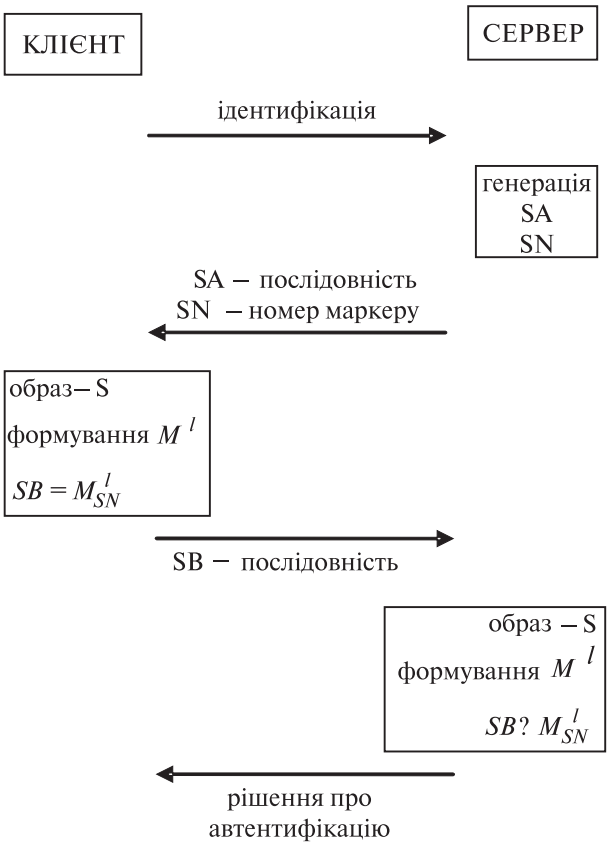


Рис. 2. Схема проведення безпечної автентифікації

Web-додаток аналогічно формує множину M^l , та зберігає перші SN елементів, серверу повертає SB (SB = M_{SN}^l). Якщо клієнт і сервер мають однакові образи S, то $SB = SB^{'}$, тобто автентифікація пройшла успішно, в іншому випадку – помилка.

Відмітимо, що на сервері немає необхідності зберігати всю множину маркерів M^l , достатньо зберігати останній успішно переданий маркер. Автентичність наступних маркерів перевіряється відповідно до способу побудови множини M^l : $M_j^l = sha1(M_{j+1}^l)$. За допомогою величини параметра SN-сервер може задавати довжину сесії, для якої формується одноразовий блокнот.

5. Особливості методу управління пріоритетами під час проектування web-додатків

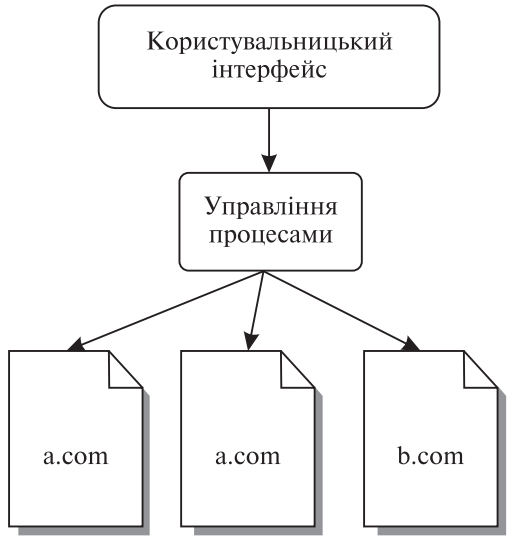
При проектуванні клієнтської частини [2,3] необхідно відзначити тенденцію заміщення статичних web-сторінок динамічними web-додатками, зростанням пропорції активного коду [1]. Отже, при проектуванні web-додатків виникають наступні проблеми:

– проблема перехресного впливу одних web-додатків на інші;

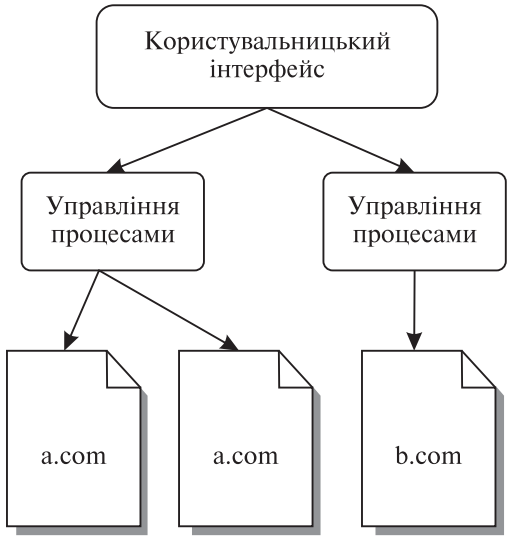
– розподіл обчислювальних ресурсів.

Розглянемо схему обслуговування браузером завантажених документів, які в загальному випадку браузер обробляє за схемою, представленою на рис. 3*а*.

При ізоляції додатків [1] обробка відбувається за схемою, що представлена на рис. 3*б*.



а



б

Рис. 3. Схеми обслуговування процесів браузером: *а* – схема обслуговування процесів звичайним браузером; *б* – схема обслуговування процесів браузером з функцією ізоляції процесу

У роботах [4,5] розглядаються способи формування вмісту додатка, наповнення різним контентом. Web-додаток обробляє декілька процесів, браузер обслуговує кілька web-додатків.

На рис. 3*б* показано браузер з функцією ізоляції; у такому випадку web-додаток може управляти деякими процесами.

Пропонується використовувати маркер M_k^l, який одержується від сервера, де l – ідентифікатор сесії, у якій працює агент, а k – номер запиту в групі запитів сесії l, $k = \overline{SN, L1}$.

6. Обслуговування ідентифікованих агентів

Відзначимо, що для ряду сервісів тривалість роботи агентів на етапі III найбільша, отже, функція (1) не може управляти пріоритетом доступу, тому пропонується метод для параметричного управління обслуговуванням сервера з урахуванням маркера M_k^l.

Для кожного запитуваного ресурсу оцінимо пріоритет обслуговування за формулою

$$W_{t+1}^{M_j^l} = \begin{cases} W_t^l + 1, \text{ для } j = k \\ W_t^l * (1 - \dfrac{1}{k-1}), \text{ для } j < k, \end{cases} \quad (2)$$

де $W_t^l = \dfrac{\sum_{i=1}^{k} W_t^{M_i^l}}{k}$ – середній пріоритет для сесії; $M_j^l \subset M$; l – ідентифікатор сесії; $i = \overline{SN, L1}$.

Таким чином, забезпечується можливість ідентифікації потоків одного агента та підвищення пріоритету обслуговування активної сторінки й зниження пріоритетів сторінок, які обслуговуються у фоновому режимі.

Висновки

У роботі проаналізовано стандартний метод параметричного розподілу пріоритетів обслуговування агентів в мережі Інтернет.

Запропоновано спосіб інтелектуального управління завантаженням web-додатка шляхом виділення пріоритету між своїми процесами.

Запропоновано метод захисту даних автентифікації та формування множини маркерів для ідентифікації web-додатка протягом сесії.

Удосконалено метод параметричного управління обслуговування web-додатків, який дозволяє інтелектуально змінювати параметри обслуговування в залежності від завантаження сервера й пріоритету потоку даних, а також етапу автентифікації.

Список літератури: 1. *Reis C., Bershad B., Gribble S., Levy H.* Using Processes to Improve the Reliability of Browser-based Applications // University of Washington Technical Report UW-CSE-2007-12-01. 2. *Быков М.Ю.* Модель процесса обработки запросов системой управления web-сайтами

// Вычислительные методы и программирование. – М. – 2005. Т. 6. Раздел 2. С. 52-56. 3. *Алиев Р.Т.* Методы управления трафиком в мультисервисных сетях // Научно-технический вестник СПбГИТМО (ТУ). Выпуск 6. Информационные, вычислительные и управляющие системы. – СПб.: СПбГИТМО(ТУ), 2002. С. 10–13. 4. *Kappel G.*, Proll B., Retschittzegger W., Schwinger W., Hofer T., Modeling Ubiquitous Web Application – A Comparison of Approaches // Journal of Network and Computer Application – 2001. 5. *Christos B., Giorgos K., Ioannis M.* A web content manipulation technique based on page Fragmentation // Journal of Network and Computer Application, 2006. 6. *Галатенко В.А.* Стандарты информационной безопасности / Под ред. Бетенина В.Б. – М.: Интернет-университет Информационных технологий, 2006. – 208с. 7. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных систем. Ч.2. Функциональные требования. Введен впервые. – М. Узд. стандартов, 2002. – 160 с. 8. *Коваленко А.А.* Методи та засоби підвищення оперативності передачі даних у мультисервісних мережах: Автореф. дис. на здобуття наук. ступеня канд. техн. наук // Харківський національний університет радіоелектроніки. –Харків. – 2008. – 19 с. 9. *Шеннон* К. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. 10. *Полянская О.Ю.* Инфраструктуры открытых ключей [електронний ресурс] – режим доступу http://www.intuit.ru/department/security/pki/.

Поступила в редколлегию 2.09.2008

УДК 651.2:004.38

Параметрическое управление приоритетами обслуживания web-приложения сервером / А.Л.Ерохин, А.П.Турута // Бионика интеллекта: научн.-техн. журнал. – 2008. – № 2(69). – С. 36-39.

Рассматривается подход к управлению загрузкой web-приложения путем выделения приоритетов между собственными процессами. Усовершенствован метод параметрического управления обслуживанием web-приложений, который изменяет параметры обслуживания в зависимости от загрузки сервера, приоритетов потоков данных и особенностей аутентификации.

Рис.: 3. Библиогр.: 10 назв.

UDC 651.2:004.38

Light devices for visualization of traffic management / A.L.Yerokhin, O.P.Turuta // Bionics of Intelligence: Sci. Mag. – 2008. – № 2 (69). – P. 36-39.

The approach to management loading web-applications by separations priority between own process is considered. The method of parametric management of web-applications service is improved, it changes the parameters of the service depending on loading the server, priority dataflow and particularities to authentifications.

Fig.:3. Ref.: 10 items.