**УДК 004.056.53**

Г.В. БАБІЙ, В.Ю. ШАДХІН, С.О. КОВБАСЕНКО
Черкаський держаний технологічний університет

# АНАЛІЗ СИСТЕМ ЗАХИСТУ ХМАРНИХ ОБЧИСЛЕНЬ НА ОСНОВІ ВИКОРИСТАННЯ ОДНОРАЗОВИХ ПАРОЛІВ КОРИСТУВАЧА

*Метою даної роботи є розробка методу двофакторної автентифікації на основі використання одноразових паролів. Це дозволяє покращити процедуру автентифікації в хмарному сховищі. Метод реалізований на базі SMS повідомлень, які надходять на мобільний номер користувача і містять в собі одноразовий пароль.*

*Ключові слова: токен, автентифікація, мобільний пристрій, хмарне середовище, інформація, одноразовий пароль, двофакторна автентифікація.*

G.V. BABIY, V.U. SHADHIN, S.O. KOVBASENKO
Cherkasy State Technological University

**ANALYSIS OF PROTECTION CLOUD COMPUTING THROUGH THE USE OF ONE-TIME PASSWORD USER**

*Abstract - The aim of the work is development a method of two-factor authentication on the base use one-time passwords. This provides to enhance authentications procedure in the cloud storage. The method is realized on received SMS-messages those arrive to user phone number and include one-time passwords in it.*

*Keywords: token, authentication, mobile, cloud depository, the information, one-time password, one-time password, two-factor authentication.*

## Вступ

Зі зростанням попиту на хмарні обчислення збільшуються і вимоги до захисту та зберіганню інформації в них. Тому у провайдерів виникають питання про підвищення надійності й безпеки в хмарному середовищі. Обсяги даних, що генеруються компаніями по всьому світу й зберігаються в хмарі щороку зростають приблизно на 60%, тому все актуальнішими стають вимоги до захисту даних і їх постійному доступу. Все це підвищує цінність інформації як економічного активу. Особливу гостроту набуває проблема автентифікації до хмарного сховища.

## Постановка завдання

Щоб користувач хмарного сховища отримав доступ до інформації, яка там зберіться, йому необхідно пройти процедуру автентифікації. Найчастіше реалізується ця процедура через форму «ім'я користувача – пароль», яку заповнює власник зберігаємої інформації. Але щоб зробити цей метод більш надійний необхідно ввести додатковий фактор – одноразовий пароль, який треба ввести в спеціально відведене поле для підтвердження раніше введених даних. Саме на розробку й огляд методів надходження одноразових паролів спрямована дана стаття.

## Аналіз останніх публікацій

За інформацією виконавчого директора Symantec Енріке Салема, чим більше даних переміщається в загальнодоступну хмару, тим більш актуальною стає проблема захисту інформації. Основні загрози, що створюються при передаванні інформації до хмарного середовища:

- Втрата контролю над ресурсами хмари.
- Витік цінної інформації. Контролювати виток даних із хмари, яка до того ж постійно взаємодіє із зовнішніми сервісами, значно важче, ніж в корпоративній мережі, обнесеній по периметру міжмережевими екранами
- Несанкціонований доступ. Комунікаційна хмара, на відміну від хмари обчислювальної, не є монолітним і часто не має єдиної системи управління - для нього важливо вирішити завдання не тільки надійної автентифікації користувачів, а й обладнання, з якого користувач отримує доступ до ресурсів хмари.

Токени були створені для того щоб доповнити собою введення ім'я та пароля користувача певним цифровим кодом, який генерується хеш-функцією. За даними Commonwealth Bank of Australia 80% їх клієнтів використовують токени або одноразові смс-паролі для підтвердження своїх дій.

## Виклад основного матеріалу

Розглянемо типові методи захисту хмарного середовища.

Найкращий спосіб зберегти розміщенні в сховищі дані – використовувати шифрування. З метою запобігання неправомірного доступу провайдер повинен шифрувати інформацію клієнта, яку він зберігає на своїх серверах.

Самим поширеним способом автентифікації є захист паролем. Хмарні комунікаційні сервіси багато в чому засновані на SIP-протоколі. Деякі провайдери для підвищення надійності використовують такі засоби як сертифікати та токени [2].

Управління ідентифікацією, або Identity and Access Management (IAM). Дана система потрібна для захисту звичайних хмар, проте в багатошаровій структурі комунікаційної хмари без неї взагалі неможливо ефективно працювати. У типового користувача хмарних сервісів відсутня система управління обліковими записами, а спроби провайдера впровадити певні політики внутрішньої безпеки зазвичай ігноруються. Вихід можливий в наданні хмарних послуг IAM оператором зовнішнього хмари [3]. Потреби в таких послугах

зростають по мірі того, як компанії будуть інтегрувати свої IT-системи в хмарних сервісів.

Контроль мобільних пристроїв. Хмарними сервісами найбільш зручно користуватися з мобільних пристроїв, які зараз можуть бути постійно на зв'язку. Підключивши такий пристрій до загальної корпоративної мережі підприємства, співробітник може виконувати свої службові обов'язки навіть не перебуваючи на робочому місці. Причому сам пристрій може бути використано не тільки для визначення місця розташування співробітника, але і для вибору методу зв'язку з ним.

Велике значення представляє ізоляція користувачів один від одного. Кращим варіантом для рішення цієї задачі є використання кожним клієнтом індивідуальної віртуальної машини (ВМ) та віртуальної мережі. Розділення між віртуальними машинами й між користувачами забезпечує гіпервізор.

Компанії повинні мати можливість самостійно перевіряти цілісність інформації. Провайдер аналізує журнали, тобто збирає та аналізує журнали роботи операційної системи й програм на предмет подій безпеки. Існують програми, які дозволяють компанії спостерігати як використовуються його веб-ресурси й запобігати негативному впливу вторинного трафіку. (як приклад WIRe, розроблена компанією ScanSafe). Але потрібно вважати і той факт, що інформація, яка зберігається в хмарі повинна також бути захищена від працівників провайдера. Таким чином організується захист від обслуговуючого персоналу шляхом надання різних прав доступу до тих чи інших даних.

На відміну від реального комп'ютера віртуальна машина може бути скомпрометована чи заражена навіть тоді, коли виключена. Для захисту від вірусних програм потрібно використовувати спеціальні програмні інтерфейси, які забезпечує гіпервізор для захисту активних та неактивних віртуальних машин.

Потрібно вважати, що спеціалізовані ресурси є більш захищеними, ніж колективні ресурси. Відповідно, атакована система повністю чи частково-колективна повинна бути більша і знаходиться під більшою загрозою. Брандмауер зменшує ризики для атаки на систему віртуалізованих серверів в хмарному середовищі [2].

Пропонується в майбутньому замінити токени на одноразові паролі. Для підтвердження того, що доступ до інформації отримує власник, а не зловмисник, надсилати на мобільний номер власника унікальний пароль, який також буде надсилатися при будь-яких змінах в ВМ – для підтвердження цих дій. Також вважаємо, що потрібно реєструвати мобільний номер в базі даних провайдера, в хмарі якого користувач використовує місце. Гарний приклад підтвердження дій й особистості на базі зареєстрованого номеру телефону ми можемо бачити на прикладах інтернет-банкінгу [3].

На відміну від токенів, які потрібно завжди мати при собі щоб пройти автентифікацію, мобільний телефон завжди знаходиться у власника і це не потребує додаткових затрат. Якщо розглянути в цьому аспекті Російську Федерацію, де номер мобільного телефону прив'язується до паспорта власника - це є гарною практикою, що даний номер не буде належати ще одній людині [5]. Додатковим рівнем захисту може бути пароль від акаунта в хмарі чи пін-код від мобільного телефону, які знає тільки власник. Якщо в токені ключ генерує хеш-функція, то її, а також сам ключ, легше вирахувати зловмиснику, ніж одноразовий код, що поступає на мобільний номер та генерується окремо випадковим чином. При умові, що даний код буде дійсний лише певний проміжок часу, наприклад 5 хвилин, його буде важче отримати для перехвату доступу. Досліди Gartner показують, що від 10% до 30% дзвінків в технічну допомогу компанії – це прохання про відновлення пароля, який користувач випадково забув. Кожен такий дзвінок коштує організації в середньому 25 доларів. В випадках, коли власник токена загубить його чи нанесе невиправних ушкоджень, при яких токен не буде генерувати вірні ключі, або його буде неможливо підключити до комп'ютера, то відновлення даного пристрою буде коштувати дорожче як компанії, так і користувачеві. В таблиці 1 приведено порівняння пристроїв, які використовуються для отримання одноразового пароля.

На даний час розглядається заміна антивірусного ПЗ на хмарні антивірусні сервіси. Хмарний антивірус складається з двох частин – клієнтської і серверної. Клієнтська частина встановлена на комп'ютері користувача і має мінімальний розмір. Ця частина містить двигун. Двигун сканує дані і відправляє для аналізу, причому не самі файли, а лише контрольні суми файлів (хеш) на сервер. На сервері міститься база сигнатур (вірусна база). Сервер отримавши хеші файлів шукає аналоги у своїй вірусної базі. Якщо шкідливі програми будуть виявлені, то сервер відправляє на комп'ютер користувача скрипти (спеціальні команди), при виконанні яких комп'ютер очищається від вірусів та іншого шкідливого ПЗ.

В новій галузі на роль лідера висувається стартап CloudPassage, засновником і виконавчим директором якого є ветеран RSA Security Карсон Світ. Наприкінці січня 2013 р. компанія запустила в дію свій сервіс Halo Netsec – першу і єдину, за словами Карсона Світа, службу серверної безпеки з контролем дотримання регулятивних норм, яка безпосередньо забезпечує багаторівневий захист середовища еластичного хмари.

Halo Netsec забезпечує для хмарного сервісу двофакторну автентифікацію з використанням мережевого екрану і функцією виявлення вторгнень. Фігурально кажучи, це сервіс "безпечною безпеки".

Таблиця 1

**Порівняння пристроїв**

| Характеристики | Mobile-OTP (віртуальний токен) | Aladdin eToken PASS (апаратний токен) | RSA Mobile (SMS автентифікація) | OTM (одноразова матриця) |
|---|---|---|---|---|
| Кількість факторів | Двофакторна автентифікація | Однофакторна автентифікація | Однофакторна автентицікація (можливі варіанти з двофакторною) | Однофакторна автентифікація |
| Додатковий пристрій | Мобільний телефон | Пристрій токен | Мобільний телефон | - |
| Додаткове ПЗ (користувач) | Потребує установки спеціального java додатку | - | - | - |
| Open source | так | - | - | - |
| Алгоритм генерації одноразових паролів | Алгоритм MD5 для генерації необхідно: поточний час, PIN-код, код пристрою | Алгоритм HMAC і хеш-функція SHA-1 для генерації необхідно: початкове значення для генератора, кількість необхідних циклів генерацій | - | - |

**Висновок**

Отже з розвитком хмарних обчислень розвиваються методи захисту інформації. Дуже важливо щоб клієнт був впевнений в цілісності даних. Очевидно, що використання технології одноразового паролю - більш безпечний спосіб, чим використання статичного паролю та ключа, який генерує хеш-функції. Так як пароль, що надходить в смс-повідомленні є дійсним протяцjv деякого проміжку часу – власник акаунта більш впевнений у захисті своєї інформації. Провайдер, який надає хмарне сховище, має зробити все можливе для захисту файлів не тільки в самому сховищі, а й коли користувач зв'язується з ним для передачі інформації. Для передачі використовуються тунельні протоколи, автентифікація, управління ідентифікаціями, для зберігання дані шифруються криптографічними алгоритмами. Для розділення інформації різних користувачів та захисту її від вірусних програм використовуються віртуальні машини, брандмауери, антивіруси й інші програми захисту чи спостереження, які провайдер буде вважати використовувати за необхідне.

**Література**

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: Академия / В.Г. Грибунин, В.В. Чудовский, 2009. – 416 с.

2. Каторин Ю. Защита информации техническими средствами / Каторин Ю., Разумовский А., Спивак А. – НУИ ИТМО, 2012. – 416 с.

3. Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Горячая линия – Телеком / Афанасьев А.А. – 2012. – 550 с.

4. Карр Н. Великий переход. Революция облачных технологий / Карр Н. – 2013

5. Облачные сервисы: взгляд из России / Под ред. Гребнева. – 2011 – 282 с.

**References**

1. Hrybunyn VH, VV Chudovskyy - Complex protection system of information in the enterprise: Academy, 2009. - 416 p.
2. Katoryn Y, Razumovskyy A., Spivak A.- The protection of information by technical funds: Nui ITMO, 2012. - 416 p.
3. Afanas'ev.A.A. - Authentication. Theory and practice of secure access to information resources: Hotline – Telecom, 2012. - 550 p.
4. Nicholas Carr - Large switching. Revolution cloud computing technology. "Mann, Ivanov and Ferber", 2013
5. Ed. Ridge – Cloud services: VIEW from Russia. Cnews, 2011 - 282 p.

Рецензія/Peer review : 6.1.2014 р. Надрукована/Printed :6.2.2014 р.
Рецензент: проф. к.т.н. Тимченко А.А.