Технічні науки

УДК 004.75

Аулов Іван Федорович
м. н. с. кафедри Безпеки інформаційних технологій
Харківський національний університет радіоелекроніки
Аулов Иван Федорович
м. н. с. кафедры Безопасности информационных технологий
Харьковский национальный университет радиоэлектроники
Aulov I.
junior researcher in Department of Information Technology Security
Kharkiv National University of Radio Electronics

МЕХАНІЗМИ, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ОСОБИСТИМИ КЛЮЧАМИ КОРИСТУВАЧІВ В ХМАРІ
МЕХАНИЗМЫ, МЕТОДЫ И СРЕДСТВА УПРАВЛЕНИЯ ЛИЧНЫМИ КЛЮЧАМИ ПОЛЬЗОВАТЕЛЕЙ В ОБЛАКЕ
MECHANISMS, METHODS AND MEANS FOR USERS PRIVATE KEYS MANAGEMENT IN THE CLOUD

Анотація: *Запропоновано новий механізм генерації та встановлення єдиної ключової пари в хмарі без передачі особистого ключа. Вдосконалено реалізацію алгоритму автентифікації користувачів в хмарі за протоколом OAuth, шляхом застосування алгоритму електронного цифрового підпису ДСТУ 4145-2012 та апаратних засобів захисту.*
Ключові слова: *управління ключами, OAuth, апаратні засоби захисту, хмара.*

Аннотация: *Предложено новый механизм генерации и установления единой ключевой пары в облаке без передачи личного ключа.*

Усовершенствована реализация алгоритма аутентификации пользователей в облаке по протоколу OAuth, путем применения алгоритма электронной цифровой подписи ДСТУ 4145-2012 и аппаратных средств защиты.

Ключевые слова: *управления ключами, OAuth, аппаратные средства защиты, облако.*

Summary: *Proposed a new generation mechanism and the establishment of a private key pair in the cloud without private key transfer. Improved implementation of user authentication algorithm in the cloud using OAuth, by applying the algorithm of digital signature DSTU 4145-2012 and hardware protection.*

Key words: *key management, the OAuth, hardware protection, cloud.*

Вступ

В Україні, як і в більшості держав світу, знаходять своє застосування хмарні сервіси. В провідних державах світу вже прийнято ряд законів та стандартів, що визначають поняття хмарних сервісів та регулюють захист інформації в хмарному середовищі. В Україні також ведеться розробка в цьому напрямку та 24.03.2016 подано законопроект 4302 «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень» до Верховної Ради України.

Впровадження хмарних технологій в світі виявило ряд проблем та питань з захисту інформації в хмарі. Особливо проблемними питаннями при використанні хмарних сервісів, на наш погляд, є управління ключами користувача в середовищі хмарних обчислень [1, 2].

Таким чином дослідження механізмів та засобів управління ключами користувача для України є важливим і актуальним завданням.

1. Механізм генерації та встановлення єдиної ключової пари між *N*-вузлами в хмарі

Нехай в хмарі необхідно встановити єдину ключову пару між N з'єднаними між собою вузлами. Кожний з вузлів повинен володіти ключовою парою для підпису (k_{sign}, Q_{sign}) та ключовою парою для направленого шифрування (k_{env}, Q_{env}) . Відкритим ключам повинні відповідати сертифікати – $Cert_{sign}$, $Cert_{env}$. Ключі підпису використовуються для автентифікації вузлів, забезпечення цілісності даних, а також підпису відкритих ключів користувача для відправки на сертифікацію до центру сертифікації ключів (ЦСК). Ключі шифрування призначені для забезпечення захищеного каналу передачі інформації між вузлами.

Запропонований механізм дозволяє забезпечити генерацію та встановлення ключової пари в системі з N вузлами при використанні якої забезпечується встановлення ключів по відкритому каналу зв'язку.

1.1 Протокол генерації та встановлення ключа в групі точок еліптичної кривої

Налаштування та генерація ключа

Загальносистемні параметри: еліптична крива - E , базова точка еліптичної кривої - G , порядок базової точки - n , розмір поля, який визначає базове кінцеве поле $-F(p)$. Алгоритм передбачає встановлення спільної пари ключів між двома вузлами за один прохід. Якщо $N > 2$ спочатку спільна пара генерується для двох вузлів, після чого спільна пара генерується між вузлами де вже встановлено ключ та новим вузлом.

Протокол встановлення ключа

1. Кожний з вузлів системи генерує особистий ключ - випадкове число $d_i\,(1 \le d_i < n)$, та обчислює відкритий ключ Q_i:

$$Q_i = d_i G (\mathrm{mod}\ p) \qquad (1)$$

2. Відкритий ключ кожного з вузлів Q_i підписується за допомогою особистого ключа вузла та передається іншим вузлам.

3. Два вузли обчислюють загальний секрет S за протоколом Діффі-Гелмана:

$$S_1 = d_1 Q_2 (\text{mod } p) \quad (2)$$

$$S_2 = d_2 Q_1 (\text{mod } p) \quad (3)$$

$$S = d_1 d_2 G (\text{mod } p) \quad (4)$$

4. Отриманий спільний секрет S перетворюється за допомогою функції вироблення ключа H, в псевдовипадкове число d ($1 \le d < n$). Відкритий ключ Q, обчислюється згідно виразу 1.

5. Якщо в системі $N > 2$ відкритий ключ Q підписується особистим ключем вузла та передається наступному вузлу для формування спільної пари.

6. Отримане значення ключової пари (d, Q) на останньому кроці – є спільною ключовою парою для всіх вузлів. Відкритий ключ Q відправляється на сертифікацію.

1.2 Протокол вироблення спільної пари в полях Галуа

У випадках, коли застосування математики ЕК або спарювання точок ЕК не можливе, а вимоги стійкості до атак типу «повне розкриття» дозволяють використовувати криптографічні алгоритми з субекспоненційною стійкістю протокол може бути побудовано з використанням математичних примітивів в полях Галуа наступним чином.

Налаштування та генерація ключа

Загальносистемні параметри: просте поле Галуа $F(p)$, просте сильне число - P , первісний елемент поля – Θ . Алгоритм передбачає встановлення спільної пари ключів між двома вузлами за один прохід. Якщо $N > 2$ спочатку спільна пара генерується для двох вузлів, після чого

спільна пара генерується між вузлами де вже встановлено ключ та новим вузлом.

Протокол встановлення ключа

1. Кожний з вузлів системи генерує випадкове число $x_i (1 < x_i < p-1)$, та обчислює Y_i:

$$Y_i = \Theta^{x_i} (\text{mod } p) \quad (5)$$

2. Відкритий ключ кожного з вузлів Y_i підписується за допомогою особистого ключа вузла та передається іншим вузлам.

3. Два вузли обчислюють загальний секрет S за протоколом Діффі-Гелмана:

$$S_1 = Y_2^{x_1} (\text{mod } p) \quad (6)$$

$$S_2 = Y_1^{x_2} (\text{mod } p) \quad (7)$$

$$S = \Theta^{x_1 x_2} (\text{mod } p) \quad (8)$$

4. Отриманий спільний секрет S перетворюється за допомогою функції вироблення ключа H, в псевдовипадкове число k ($1 < k < p-1$). Відкритий ключ Q, обчислюється згідно виразу 5.

5. Якщо в системі $N > 2$ відкритий ключ Q підписується особистим ключем вузла та передається наступному вузлу для формування спільної пари.

6. Отримане значення ключової пари (k, Q) на останньому кроці – є спільною ключовою парою для всіх вузлів. Відкритий ключ Q відправляється на сертифікацію.

1.3 Аналіз протоколу

Для оцінки запропонованого криптографічного протоколу застосуємо набір критеріїв, що запропоновані в [3, с. 556-564, с. 611]. Відповідно до висунутих критеріїв в запропонованому протоколі:

1. Забезпечується взаємна автентифікація суб'єктів, оскільки вони володіють тимчасовими особистими та відкритими ключами, справжність яких підтверджена підписом вузла.

2. Автентифікація ключів не передбачена, але може бути виконана за рахунок взаємодії сторін після встановлення спільної ключової пари.

3. Новизна ключів забезпечується за рахунок використання генератора випадкових чисел на етапі формування допоміжних ключів, що використовуються при встановленні спільного ключа.

4. Захист від атак типу «маскарад» та «модифікація» для відкритих ключів допоміжних ключів забезпечується за рахунок використання ЕЦП, з використанням особистого ключа вузла та посиленого сертифіката відкритого ключа вузла.

5. При виробленні розділюваного спільного ключа передачі особистого ключа не відбувається. Криптоживучість ключа не забезпечується у випадках компрометація одного з тимчасових ключів.

6. Гарантії з забезпечення послуг, конфіденційності, цілісності, доступності, справжності і неспростовності щодо інформації автентифікації та ключів забезпечуються вузлом та третьою довіреною стороною, що управляє сертифікатами відкритих ключів.

7. Складність криптоаналізу полягає в складності вирішення відповідної криптографічної задачі на якій базується математичний апарат асиметричного перетворення, що застосовується в протоколі Діффі-Хелмана, а також підбору особистого ключа, що засновано на недосконалості функції перетворення спільного секрету в особистий ключ.

8. Всі суб'єкти впливають на розділюваний таємний ключ за рахунок використання відкритих ключів.

9. При виробленні розділюваного спільного ключа передачі особистого ключа не відбувається.

10. При використанні протоколу необхідно звертатися до третьої довірчої сторони для виготовлення та підтримання життєвого циклу сертифікатів вузлів, а також сертифікатів відкритих ключів сформованих в результаті застосування протоколу.

11. При компрометації спільного особистого ключа в одному з вузлів, особистий ключ в інших вузлах також є скомпрометований.

12. При додаванні або зміні вузлів в системі потребує повторної генерації спільного ключа

2. Протокол автентифікації користувачів в хмарному середовищі

На сьогодні в світі в якості методів автентифікації користувачів в хмарі застосовується:

– однофакторна автентифікація на основі пароля;
– двофакторна автентифікація (Two-Factor Authentication, 2FA);
– багатофакторна автентифікація (Multi-Factor Authentication);
– єдиний пароль (SingleSign-On, SSO).

Методи автентифікації реалізуються за рахунок застосування таких протоколів, як OAUTH (Open authentication), FIDO (Fast IDentity Online), OpenID, XSSO (X/Open Single Sign-on) та Kerberos.

В якості засобів автентифікації може застосовуватися:телефонні дзвінки, SMS повідомлення, смарт-картки, ID-картки, токени, мобільні додатки, паролі OTP, модулі довіреної платформи (Trusted Platform Modules, TPM), пристрої з підтримкою NFC.

Найбільше розповсюдження сьогодні отримав метод автентифікації з використанням пароля. Також розповсюдження набуває метод з використанням протоколу OAuth [4], що дозволяє автентифікувати користувача не передаючи на сторонній сайт його дані автентифікації. Існуючий протокол OAuth, що використовує пароль користувача для

автентифікації має суттєвий недолік, а саме необхідність зберігання та передавання паролю користувача на сервер автентифікації.

Для вирішення цієї проблеми пропонується застосовувати кінцевими користувачами хмарних сервісів засоби веб-автентифікації користувачів на основі сертифікатів відкритих ключів, що застосовуються в національній системі ЕЦП України.

2.1 Структурна схема засобів веб-автентифікації

До складу засобів веб-автентифікації користувачів на основі сертифікатів відкритих ключів, що пропонується до застосування, входять: сервер веб-автентифікації, сервер прикладної системи, персональний комп'ютер (ПК) чи робоча станція (РС) користувача, ЦСК (рис. 1).

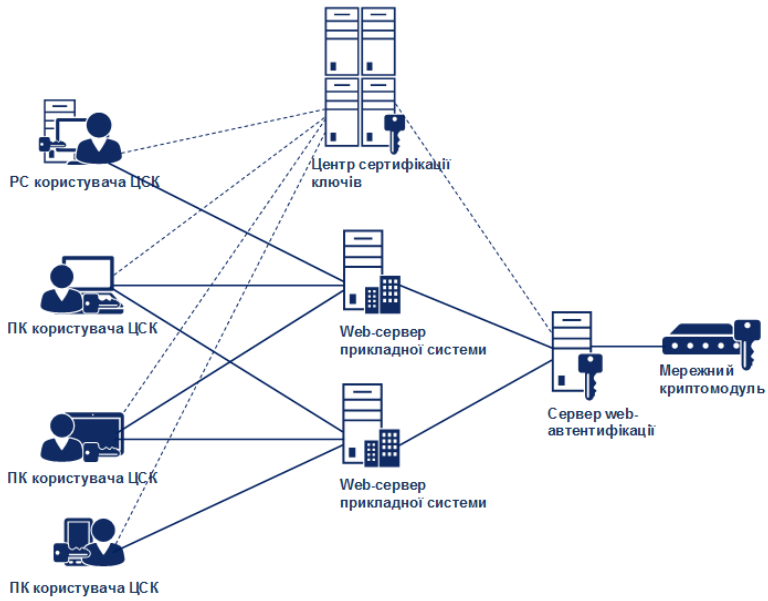

Рисунок 1 – Структурна схема засобів web –автентифікації

Сервер веб-автентифікації, реалізується на основі веб-сервера з інтерпретатором PHP, Java або C# та включає криптографічну бібліотеки для перевірки підписів з інтерфейсом PHP, Java, C#, а також за необхідності мережний крипто модуль.

Засоби у складі прикладних систем виконують функції:

– автентифікації прикладних систем за протоколом OAuth;

– автентифікації користувачів ЦСК з використанням особистих ключів та сертифікатів користувачів за запитами від автентифікованих прикладних систем за протоколом OAuth;

– передачу даних про автентифікованих користувачів ЦСК прикладним системам за їх запитами.

Зазначені функції засоби виконують шляхом застосування протоколу OAuth та механізмів криптографічного захисту інформації.

Автентифікація користувачів ЦСК здійснюється шляхом перевірки електронного цифрового підпису (ЕЦП), що накладається в процесі автентифікації з використанням їх особистих ключів та сертифікатів.

2.2 Функціональна схема засобів веб-автентифікації

На рисунку 2 зображена функціональна схема засобів веб-автентифікації.

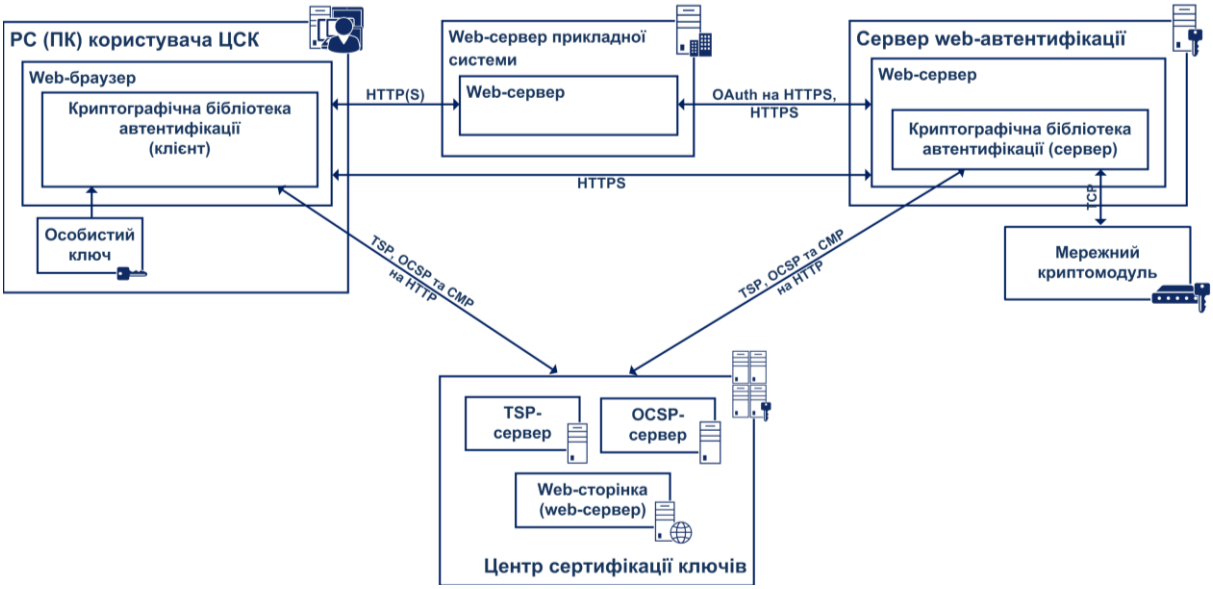

Рисунок 2 – Функціональна схема засобів веб –автентифікації

До складу PC (ПК) користувача входить:

– модуль веб-автентифікації, який завантажується автоматично з сервера web-автентифікації;

– носії ключів користувача, що підключаються до PC (ПК).

Веб-сервер прикладної системи повинен реалізувати логічні блоки взаємодії з користувачем ЦСК та сервером веб-автентифікації за

протоколом OAuth. Програмно-технічний комплекс ЦСК, є окремою складовою частиною, що не входить безпосередньо до складу засобів, але взаємодіє з ними.

Сервер веб-автентифікації у складі засобів призначений для:

– автентифікації веб-серверів прикладних систем за протоколом OAuth, що включає також ведення реєстру облікових записів прикладних систем (додавання, видалення та зміну реєстраційних даних);

– автентифікації користувачів ЦСК шляхом: надання відповідних web-сторінок автентифікації та модулю автентифікації, перевірки ЕЦП, що накладається користувачем на дані автентифікації в процесі автентифікації, перевірки статусу сертифікатів користувачів у ЦСК за протоколом OCSP та з використанням СВС;

– передачу даних про автентифікованих користувачів ЦСК web-серверам прикладних систем за їх запитами.

Мережний криптомодуль (за наявності) призначений для безпосередньої перевірки ЕЦП, що накладається користувачем на дані автентифікації в процесі автентифікації з метою зменшення навантаження на сервер web-автентифікації.

Модуль автентифікації користувача ЦСК використовується для:

– зчитування особистого ключа користувача та перевірки статусу сертифікатів користувача за протоколами OCSP та з використанням СВС;

– накладання ЕЦП на дані автентифікації з використанням зчитаного особистого ключа для передачі на сервер web-автентифікації.

Електронні ключі призначені для зберігання особистих ключів користувача та апаратної реалізації криптографічних перетворень усередині пристрою для забезпечення більш високого рівня безпеки.

2.3 Порядок взаємодії засобів веб-автентифікації

Порядок взаємодії засобів під час автентифікації користувача ЦСК на web-сервері прикладної системи реалізований відповідно до протоколу

OAuth [4]. Структурно-функціональна схема взаємодії засобів web-автентифікації наведена на рис. 3.

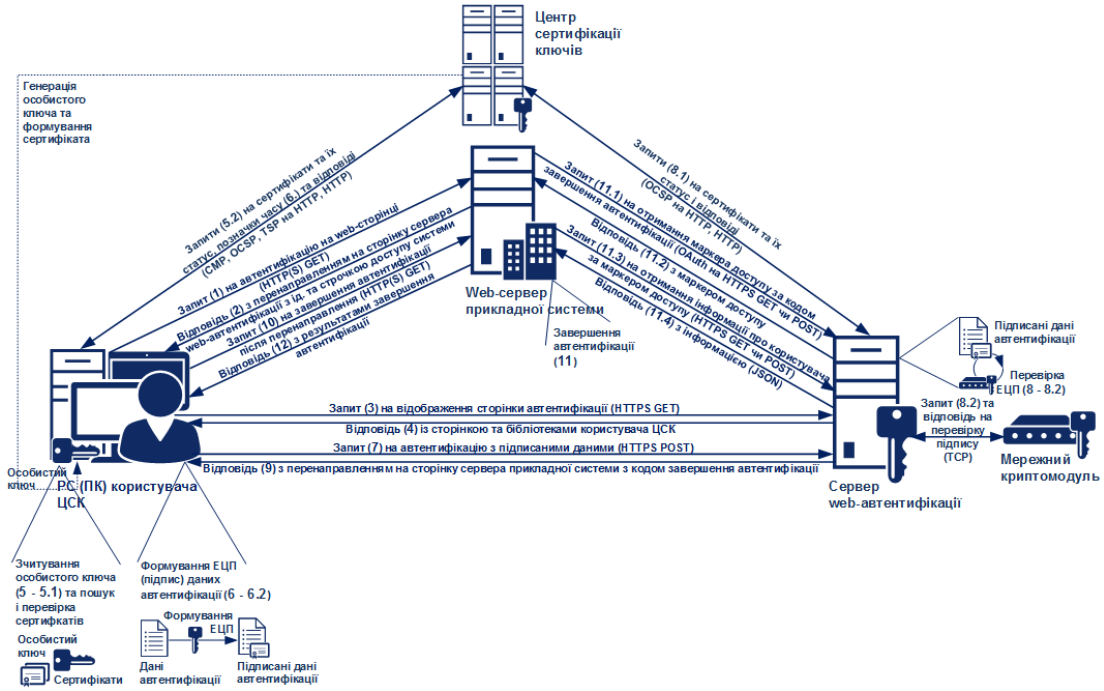

Рисунок 3 – Структурно-функціональна схема взаємодії засобів веб-автентифікації

Основними відмінностями запропонованого протоколу від існуючого є застосування ЕЦП, що накладається користувачем з використанням особистого ключа, замість логіна та пароля користувача, а також перевірці накладеного ЕЦП сервером веб-автентифікації.

Висновки

Запропонований механізм встановлення спільного ключа дозволяє встановлювати ключі в хмарному середовищі між N вузлами без передавання особистих ключів через недовірений канал зв’язку.

Застосування носіїв особистих ключів користувача, модулів криптографічного захисту дозволяють зменшити ризик реалізації загроз за рахунок використання сертифікатів відритих ключів користувача, хмарного ЦОД та апаратних засобів захисту.

Реалізація автентифікації користувачів в хмарі на основі протоколу OAUTH дозволяє здійснити автентифікацію користувачів за рахунок

використання сертифікату відкритого ключа на ресурсі, що захищається, без необхідності безпосереднього використання спеціалізованих бібліотек криптографічного захисту. Використання цього підходу дозволяє забезпечити, як мінімум, 3 рівень безпеки ключових даних, згідно ДСТУ ISO\IES 19790-2012.

Література:

1. Chandramouli, R. NIST Cryptographic Key Management Issues & Challenges in Cloud Services. / R. Chandramoli, S. Chokhani, M. Iorga, // [Електронний ресурс] – Режим доступу: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf. http://dx.doi.org/10.6028/NIST.IR.7956

2. Аулов І.Ф. Дослідження моделі загроз ключових систем хмари та пропозиції захисту від них / І.Ф. Аулов // Восточно-Европейский журнал передовых технологий. – 2015. – № 5/2 (77). – С. 4-13.

3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. Вид. 2-ге, перероб. і доп. – Харків: Видавництво «Форт», 2012. – 880 с.

4. RFC 6749 – The OAuth 2.0 Authorization Framework [Електронний ресурс] – Режим доступу: https://tools.ietf.org/html/rfc6749.