Ахрамович В. М.
канд. техн. наук, доцент.
Державний університет телекомунікацій

СТВОРЕННЯ СТРУКТУРИ РОЗПОДІЛЕНОЇ СОЦІАЛЬНОЇ МЕРЕЖІ PROTECTEDBOOK

Akhramovych Volodymyr Mikolayevich
Ph.D., associate Professor,
State University of Telecommunications

STRUCTURE CREATION OF THE PROTECTEDBOOK DISTRIBUTED SOCIAL NETWORK

Анотація. Protectedbook складається з вузлів. Вузли концентричних сфер організовані в кілька концентричних сфер, а саме шарів (оболонок), і кілька шляхів ведуть від вузлів у найглибшому шарі до вузлів у самому зовнішньому шарі.

Субстрат P2P Protectedbook - це розподілена Хеш-таблиця, аналогічна KAD, який відповідає за зберігання та отримання посилань на вхідні пункти всіх користувачів концентричних сфер. Така підкладка складається з усіх вузлів користувача і дозволяє будь-якому вузлу надіслати запит пошуку, щоб дістатися до концентричних сфер будь-якого користувача.

Довірена послуга ідентифікації СНІД - третя сторона, яка довіряє, генерує та надає для кожного користувача Protectedbook пару ідентифікаторів: ідентифікатор вузла v, однозначно ідентифікуючи V як рівень P2P, та ID користувача v однозначно ідентифікує V як користувача в соціальній мережі.

Основні функції Protectedbook можна розділити на три основні категорії: управління даними; управління ключами; управління зв'язком.

Protectedbook забезпечує конфіденційність даних завдяки традиційній криптографії з відкритим ключем та симетричній криптографії. Доступ до вмісту може бути обмежений декількома визначеними користувачами.

Спілкування між двома користувачами V та U може відбуватися як синхронно, так і асинхронно. Кожен користувач зберігає такі повідомлення у своєму власному РПЗД та при необхідності ділиться ним з надійними контактами.

Abstract. Protectedbook consists of nodes. Nodes of concentric spheres are organized into several concentric spheres, namely layers (shells), and several paths lead from nodes in the deepest layer to nodes in the outermost layer.

The P2P Protectedbook substrate is a distributed KAD-like hash table that is responsible for storing and retrieving inbound links for all users of concentric spheres. This substrate consists of all user nodes and allows any node to send a search query to get to the concentric spheres of any user.

Trusted service of reliable identification data (SRID) Identification Service - third side that trusts, generates and provides a pair of IDs for each Protectedbook user: node identifier v, definitely identifying V as a P2P layer, and user v definitely identifying V as a social network user.

Protectedbook's main features can be divided into three main categories: data management; key management; communication management.

Protectedbook provides data privacy with traditional open-key cryptography and symmetric cryptography. Content access can be restricted to several identified users.

Communication between two V and U users can be synchronously and asynchronously. Each user saves such messages in his or her own RPD and shares them with trusted contacts if needed.

Ключові слова: концентричні сфери, вузли, користувач, структура, ядро, шари, оболонка, дзеркало, призма, субстрат P2P, ключі, шифрування, ідентифікація, автентифікація, сертифікат, IP-адреса, сервер, конфіденційність, цілісність, захист, дані, управління, атрибут, хеш-функція, ключ, протоколи, комунікації, доступ, перехід, обліковий запис.

Keywords: concentric spheres, nodes, user, structure, kernel, layers, shell, mirror, prism, P2P substrate, keys, encryption, identification, authentication, certificate, IP address, server, privacy, integrity, security, data, management , attribute, hash function, key, protocols, communications, access, transition, account.

Вступ.

Як відмічалося в попередніх роботах, захист персональних даних користувачів, залежить в значній мірі від типу соціальної мережі. Перевагу треба віддати розподіленим соціальним мережам, оскільки вони виключають зловживання з боку адміністрації мережі, власників та адміністраторів.

В даній статті автори формулюють структуру такої мережі з її устроєм, та устроєм складових, функціональні можливості, служби, протоколи, взаємодією користувачів, управління даними, ключами, комунікаціями, проблему створення, налаштування та обслуговування мережі.

Основна частина.

Концентричні сфери

Концентричні сфери - це структура друзів, яка надає користувачеві послуги зберігання даних та зв'язок. Концентричні сфери користувача V

складається з групи вузлів, що оточують вузол користувача. Вузли концентричних сфер організовані в кілька концентричних сфер, а саме шарів (оболонок), і кілька шляхів ведуть від вузлів у найглибшому шарі до вузлів у самому зовнішньому шарі ΩV. Оскільки Vє вузлом у j-й шарі, а j, кожне концентрична сфера додатково має такі властивості:

1. Вузол V^0 розташований у центрі Концентричних сфер і називається ядром;

2. якщо пара вузлів V_v^j, VV_v^{j+1} з'єднана, стосунки дружби між ними існують у шарі соціальної мережі;

3. кожен вузол V_v^{dz}, розташований на внутрішньому шарі λ_v і називається дзеркалом, є надійним контактом ядра V і зберігає дані V у зашифрованому вигляді;

4. кожен вузол V_v^{dz} V, розташований на самій зовнішній оболонці Ω_v і називається вхідною точкою, виступає шлюзом для всіх запитів, призначених V;

5. кожен вузол $V_v^j, j\epsilon\,[2\ dz-1]$, розташований на оболонці між λ_v та Ω_v, називається призмою V;

6. множину призм позначають як . ∇_v

Підсумовуючи V_s Концентричні сфери θ_v - це об'єднання множини дзеркал Δ_v, безліч призм ∇_v, набір вхідних точок θ_v і серцевина V, кількість дзеркал V представляє кількість доступних розділів профільних даних V_s , хоча є стільки вхідних точок, скільки доріжок, які можуть провести до дзеркала. Кожне i^{th} дзеркало $\lambda_i \in \Delta_v$ являє собою корінь піддерева з гілками, що лежать у самій зовнішній оболонці θ_v. Розгалуження всіх підмножин, проміжного коефіцієнта, встановлюється V. Можливість множини θ_v внаслідок цього $\|\Omega_v\| = \|\Delta_v\| КП\|^{dz-1}$

Субстратна підкладка

Субстрат P2P Protectedbook - це PXT, аналогічний KAD, який відповідає за зберігання та отримання посилань на вхідні пункти всіх користувачів концентричних сфер. Така підкладка складається з усіх вузлів користувача і дозволяє будь-якому вузлу надіслати запит пошуку, щоб дістатися до концентричних сфер будь-якого користувача. PXT визначається як: PXT={K,N,R,$id_n(.), id_r(.)$, p(.)}

Де: K - простір ключів PXT, N і R відповідають набору відповідно вузлів і набору ресурсів, а $id_n: N \to K, id_r: R \to K,$ позначають функції, що уособлюють вузол та ресурс для їх ідентифікатора відповідно. Нарешті, p: K→ $\{N\}$ позначає функцію відображення, яка виводить набір користувачів, відповідальних за ресурс, заданий ідентифікатором ресурсу IPP. Ресурс складається з переліку посилань на вхідну точку цільового користувача концентричних сфер. Відповідний ідентифікатор ресурсу IPк представлений ідентифікатором користувача IPP або хешем атрибутів користувача, таких як його повне ім'я, день народження тощо. Надмірні копії пар (ключове значення) (IPк, ресурс) можуть зберігатися на вузлах, ідентифікатор яких відповідає IPк за попередньо визначеною кількістю перших бітів. KAD, Protectedbook реалізує оптимальну маршрутизацію, мінімізуючи відстань, виміряну в метриці XOR між IPк для пошуку та ідентифікатором вузла сусідніх вузлів. Через обмеження конфіденційності щодо структури, на відміну від KAD, запити пошуку не завжди обробляються ітеративно: Protectedbook використовує рекурсивну обробку з анонімізацією стрибків як основну техніку для забезпечення непростежуваності запитів сторін у випадку, якщо список вхідних точок посилань запитується.

Довірена послуга ідентифікації СНІД - третя сторона, яка довіряє, генерує та надає для кожного користувача v Protectedbook пару ідентифікаторів: ідентифікатор вузла IB_v, однозначно ідентифікуючи V як рівень P2P, та ID користувача $IК_v$ однозначно ідентифікує V як користувача в рівні соціальної мережі. Обидва ідентифікатори обчислюються, починаючи з набору властивостей V_s, таких як повне ім'я, день народження, місце народження тощо. Пара сертифікатів посилає кожен ідентифікатор на відповідний відкритий ключ, наданий V. Відповідні приватні ключі відомі V і нікому більше. Оскільки система P2P дозволяє отримати IP-адресу вузла з ідентифікатором вузла, розділення ідентифікаторів вузлів та користувачів це потрібно, щоб запобігти зловмисним користувачам отримувати IP-адресу жертви. Тільки надійні контакти вузла здатні зв'язати ці два ідентифікатори, оскільки вони служать дзеркалами. СНІД є винятком, оскільки це єдина система Protectedbook , яка може зв'язати ідентифікатор користувача та ідентифікатор вузла користувачів, окрім їхніх власних довірених знайомих. У разі порушення, крім місця розташування користувачів, СНІД також може розкривати участь користувачів у Protectedbook . Однак СНІД не має приватних ключів будь-якого користувача, тому вона не може представити себе жертвою, а також отримати його набір довірених контактів або отримати доступ до вмісту даних, опублікованого з обмеженнями. Хоча СНІД є централізованою інфраструктурою і, як наслідок, може здатися, що порушиться парадигма децентралізованої архітектури Protectedbook , але це on-line сервіс, який використовується лише один раз кожним користувачем Protectedbook , і, на відміну від центрального сервера OCM, вона не загрожує конфіденційності користувачів, оскільки не бере участі в будь-якій операції зв'язку або управління даними серед користувачів. Погодження СНІД з постачальником послуг Інтернету обходило б концепцію відокремлення ідентифікаторів. Однак ця атака є успішною лише в тому випадку, якщо Інтернет-провайдер контролює доступ до всіх користувачів Protectedbook ,

оскільки може бути розкрита лише конфіденційність користувачів, які використовують безпосередньо відстежувані Інтернет-з'єднання. Повний захист конфіденційності від зловмисного провайдера можливий лише за умови використання набагато складніших понять анонімізації, які заради ефективності не використовуються. Protectedbook справді не забезпечує анонімний зв'язок на рівні мережі.

Функціональні можливості

Основні функції Protectedbook можна розділити на три основні категорії:

• управління даними;
• управління ключами;
• управління зв'язком.

Управління даними

Функціональні можливості управління даними дозволяють користувачам генерувати, змінювати та видаляти конфіденційну інформацію в OCM. У Protectedbook об'єкти даних, які також називаються елементами даних, - це згенеровані користувачем фрагменти інформації, що описують інформацію користувача. Елемент даних D представлений у вигляді кортежу (DId, тип, значення, версія), де тип описує характер даних, таких як особисті контактні дані, зв'язок, інтереси тощо; значення становить його вміст, і версія його -поточна версія. Ідентифікатор елементу даних $ІД_d$ однозначно ідентифікує D серед усіх об'єктів даних та дозволяє здійснювати основні операції зберігання, пошуку або видалення елемента. SV для розподіленого простору зберігання даних (РПЗД) визначено для кожного користувача на основі його дружніх стосунків. Дозвіл на зберігання вмісту на такому просторі походить із реальних життєвих відносин дружби V, а тому надається лише V. Розмір S_V S_V є динамічним: при встановленні дружби кожен друг F_i з V резервує довільну кількість власного простору місцевого зберігання даних (МЗД) ПМЗД і для V. Сума МЗД кожного друга, виділена для V, формує РПЗД V.

Через розподілену природу РПЗД дані поділяються на n блоків, і для заданої кількості надмірності ці блоки кодуються у n + l фрагментах, так що будь-які n фрагментів є достатніми для реконструкції вихідного об'єкта. Перш ніж розділити, операції шифрування вони можуть бути виконані на D, щоб гарантувати його конфіденційність та обмежити доступ до нього.

Управління ключами

Як було зазначено раніше, дані користувача можуть бути зашифровані на основі бажання власника. Основні функції управління дозволяють користувачам обмежувати доступ до своїх спільних конфіденційних даних. Protectedbook забезпечує конфіденційність даних завдяки традиційній криптографії з відкритим ключем та симетричній криптографії. Доступ до вмісту може бути обмежений декількома визначеними користувачами. Для того, щоб мінімізувати накладні витрати на зберігання даних в РПЗД, дані шифруються лише одним ключем, а саме ключем шифрування даних (КШД). Цей КШД потрібно поширювати серед усіх користувачів, які мають право розшифровувати дані. Розподіл КШД вимагає шифрування його за допомогою ключа шифрування (КШ), який раніше розподіляється між членами під час встановлення дружби.

Користувачі не покладаються на будь-яку третю сторону для здійснення розподілу ключів; вони надсилають матеріали усім членам групи, якими вони керують. Друзі V доступу до Sv в межах політики контролю доступу (ПКД), визначеної V. В основному, користувачі в Protectedbook створюють групи контактів, визначаючи кілька атрибутів, таких як "Сім'я", "Колеги" тощо. пов'язати їх із кожним контактом. Дані, захищені під цими атрибутами, будуть доступні для всіх контактів, пов'язаних лише з відповідними атрибутами. У Protectedbook атрибути визначаються через знаки. Користувачі в Protectedbook знають, які знаки вони надали, яким контактам, але не можуть знати, скільки знаків вони отримали від даного контакту, а також опису пов'язаного атрибута. Наприклад, V може надати U значок "Відвідувач", не розкриваючи атрибут " Відвідувач " і не розкриваючи, хто з контактів Vs також має цей знакU. З точки зору системи знак b відповідає набору КШД, використовуваних для шифрування даних, доступних для всіх контактів, наданих цим значком. Такий набір визначається як:

$D_b^n = \{h^i(s_b): i \in \{1 \dots n\}\}$ позначає добре відому односторонню хеш-функцію h (), яка послідовно застосовується s^b. Ідея послідовного хешування паролів спочатку була запропонована в [79], а потім використовується для створення одноразових систем автентифікації паролів, таких як S / Key [72]. Protectedbook не виконує автентифікацію запитів користувачів і використовує кожен хеш як 1. У рівнянні позначення двокрапка (`: ') означає" така, що " КШД, а не разовий пароль. Коли v надає U знак, b, U отримує КШД посилання $h^i(s_b)$, яке не розкриває нічого про атрибут знака, а також про список друзів Vs, які також отримали цей знак. Після прийому $h^i(s_b)$U може отримати всі ключі $\{h^j(Sb) : j \in \{1 \dots n\}\}$ і отримати доступ до всіх даних, що зберігаються в SV, зашифрованих такими КШДs. Protectedbook не забезпечує зворотну таємницю: в контексті соціальної мережі фактично користувачі можуть дозволити новому члену групи отримати доступ до раніше розподілених даних для цієї групи. Коли V відкликає b від U, V рекламує $h^{i-1}(s_b)$ для всіх контактів, раніше наданих з b, один за одним, крім U. Майбутні дані, доступні раніше контактам, наданим з b, будуть зашифровані V за допомогою КШД $h^{i-1}(s_b)$. Раніше опубліковані дані, зашифровані за допомогою $h^j(s_b)$ (будучи j ∈ {i, ..., n}), не будуть зашифровані знову, тому вони все ще будуть доступні U.

Оскільки визначення хеш-функції h () для обчислень практично нездійсненно, Protectedbook забезпечує передачу секретності, оскільки майбутня комунікація не буде доступною члену U, який залишає СМ. Взагалі кажучи, V де-не-його ПКД, вказавши набір правил знаків r ∈ R_v та призначає основному Sr кожне правило. Коли контакт U надається набором значків $B_v^u\, E^u :=$ $\{h^i\,(SrUj)\colon R_j^u\ \forall j\ \in \{1,\dots,||R_v||\}, \in \{1,\dots,\mathrm{n}\}\}$

від V, набір КШД, що відповідає правилам R_v^u, та відповідає U, надсилається йому. У таблиці 1 показаний приклад АКТ. При відкликанні значка b від U , V рекламує новий набір КШДs E^x кожному контакту X, що задовольняє одному або більше правилам U, також задовольняє при відкликання b від нього. З цього моменту V шифрує свої дані новими КШДs.

Управління комунікаціями

Функціональні можливості управління комунікаціями дозволяють користувачам встановлювати непомітні зв’язки дружби та спілкуватися між собою, забезпечуючи при цьому конфіденційність та цілісність повідомлення. Спілкування між двома користувачами V та U може відбуватися як синхронно, так і асинхронно. Кожен користувач зберігає такі повідомлення у своєму власному РПЗД та при необхідності ділиться ним з надійними контактами. У другому випадку V генерує повідомлення для U та зберігає його у своєму РПЗД Sv. Як тільки U шукає нові доступні дані Vs, він отримує повідомлення. Щоб відповісти, U виконує ті самі кроки: він зберігає відповідь у власному Su, потім V отримує цю відповідь, запитуючи про нові Vs дані. Цілісність повідомлення гарантується використанням цифрового підпису, тоді як конфіденційність зв'язку досягається зашифруванням повідомлень із симетричним КШД, обчисленим (у разі синхронного зв'язку) або раніше спільним (у разі асинхронного) між відправником та одержувачем. Зв'язок перешкоджає багаторазовій маршрутизації повідомлень за ланцюжками друзів таким чином, що інформація про запитувача даних не може бути отримана. У разі синхронного зв'язку приховується IP-адреси комунікаційних сторін, а отже, і їх місце знаходження. У разі асинхронного зв’язку це також заважає приятелю Vs користувача Fi зберігати дані Vs виводити довірчі відносини між V та запитувачем даних U.

Таблиця 1

Приклад ПКД на основі встановлених операцій між контактами, наданими користувацькими знаками

Правило r	Список $\boldsymbol{s_r}$	Поточний компонент i
B_{Prof}	$\boldsymbol{s_{r1}}$	n-3
B_{Family}	$\boldsymbol{s_{r2}}$	n-2
B_{Team}	$\boldsymbol{s_{r3}}$	n-1
$B_{Prof} \vee B_{Family}$	$\boldsymbol{s_{r4}}$	n-3

Основні протоколи.

Основні функції Protectedbook реалізують три основні групи операцій:

• створення, коли особа користувача створюється за допомогою сертифікатів, виданих СНІД;

• налаштування та обслуговування ОСМ, коли вузол користувача бере участь у розподіленій архітектурі ОСМ Protectedbook ;

• управління комунікаціями та відносинами СМ, де користувач отримує переваги від ОСМ.

Кожна операція вимагає виконання серії захищених протоколів, спрямованих на отримання облікових даних, створення та збереження послідовності накладок Protectedbook та створення безпечних каналів зв'язку. У всьому описі цих протоколів $П_{kx}$ позначає повідомлення М, яке підписується приватним ключем користувача Xs позначає повідомлення Ку $E_{ky}\{П\}$, яке шифрується з відкритим ключем користувача K_y^+. Ідентифікатор користувача d в Protectedbook асоціюється з клавішами: в той час, як $N_x = N_x^-, N_x^+$ позначає клавішу для ідентифікатора вузла, $U_x = U_x^-, U_x^+$ позначає ключ ключа для ідентифікатора користувача вузла X. Для забезпечення цілісності та конфіденційності всі повідомлення при кожному переході підписуються приватним ключем ідентифікатора вузла відправника (X) і шифруються відкритим ключем ідентифікатора вузла (Y). Для наочності термін $E_{ny}\{П\}S_{nx}$, позначається як П.

Проблема створення

Протокол створення особистих даних відповідає за надання новому користувачу V даних, необхідних для участі в Protectedbook. Щоб приєднатися, новий вузол V повинен запросити зареєстрованого користувача A, з яким повинен бути знайомим у реальному житті. Спочатку A надсилає (рис. 1) поза діапазоном V запит на запрошення ЗЗ, підписаний за допомогою приватного ключа K_a^- . Він містить впорядковані $Name_A$ властивості, які є клавішами сеансу і використовуються для шифрування корисного навантаження. Такі ключі рекламуються на початку повідомлення, зашифрованого відкритим ключем id цільового вузла. Кожен приватний ключ, асоційований з ідентифікатором вузла або користувача, генерується власником ідентифікатора IPp і невідомий нікому іншому. Визначає користувача A, сертифікат Cert (h($Name_A$), K_A^+), який надається СНІД, та ключ K^+ + СНІД. Повідомлення ЗЗ - це єдине повідомлення, яке надсилається чітким текстом, оскільки загальнодоступні ключіVs-вузлів та

ідентифікаторів користувача ще не сформовані та не сертифіковані, і все одно надсилаються поза діапазоном. Після отримання повідомлення ЗЗ, V генерує дві клавіші $IB_v -$ і IK_v згодом він запускає інший позадіапазонний процес: створює свій власний кордон NameV разом із підтвердженням права власності на NameV та передає обидва разом із відкритим ключем K_v^+ у повідомленні П до СНІД.

Потім СНІД генерує ідентифікатор користувача Vs і ідентифікатор ID IK_vвузла IB_v, застосовуючи дві різні ключові хеш-функції $h_{Mk1}(.)h_{Mk2}(.)$та на $Name_v$. Крім того, він генерує та підписує реєстраційні ключі VIPк шляхом хешування та підпису всіх перестановок елементів у $Name_v$. СНІД реагує на повідомлення із записом П поза діапазоном, з генерованими ідентифікаторами та клавішами РХТ разом із відповідними сертифікатами: Cert (IK_v, K_v^+), Cert (IB_v, K_{nv}^+), Cert $(IP_{кv}, K_v^+)$. На прийом в П, V приєднується до Protectedbook , а отже, P2P може почати створювати власні концентричні сфери. Згодом усі повідомлення, надіслані та отримані V у накладенні P2P, підписуються за допомогою N- відправника та шифруються за допомогою N + приймача.

Налаштування та обслуговування служб соціальних мереж

Після створення облікового запису користувач V може налаштувати свої концентричні сфери та отримати доступ до інших користувачів. Протокол налаштування Концентричних сфер дозволяє створити Концентричні сфери. Під час першого виконання цього протоколу ініціюючий вузол V надсилає запрошення вузлу A, запит на створення шляху Ш. Це повідомлення містить маркер реєстрації MP, структуру даних СД щодо кількості переходів на створених шляхах, коефіцієнт прольоту КП для дерева через Концентричні сфери та підписане випадкове число ВЧ. Маркер реєстрації включає ключі РХТ, які потрібно зареєструвати, для того, щоб Vs можна було знайти в OCM, сертифікат ідентифікатора користувача Vs, автентифікацію IK_v та весь час ExpireTime реєстрації IPkv. СД являє собою рекурсивно підписану структуру даних, що генерується V включаючи набір зменшених значень часу на основі бажаної довжини стрибка від ядра до однієї з вхідних точок. Кожен вузол при отриманні Ш видаляє один або більше підписів СД, таким чином потенційно спричиняючи постійне зменшення значення TTL при кожному переході. Значення в проміжку вказує дзеркалам і призмам, скільки наступних стрибкових вузлів слід вибрати для того, щоб гарантувати бажану доступність даних, які публікуються. Після отримання повідомлення Ш кожне дзеркало перевіряє цілісність маркера реєстрації, перевіряючи його підпис ключем, що міститься в сертифікаті СНІД. Потім він видаляє один або кілька підписів з СД і вибирає наступний перехід B зі свого списку друзів для шляху і передає оновлений Ш. У випадку, якщо в ядрі

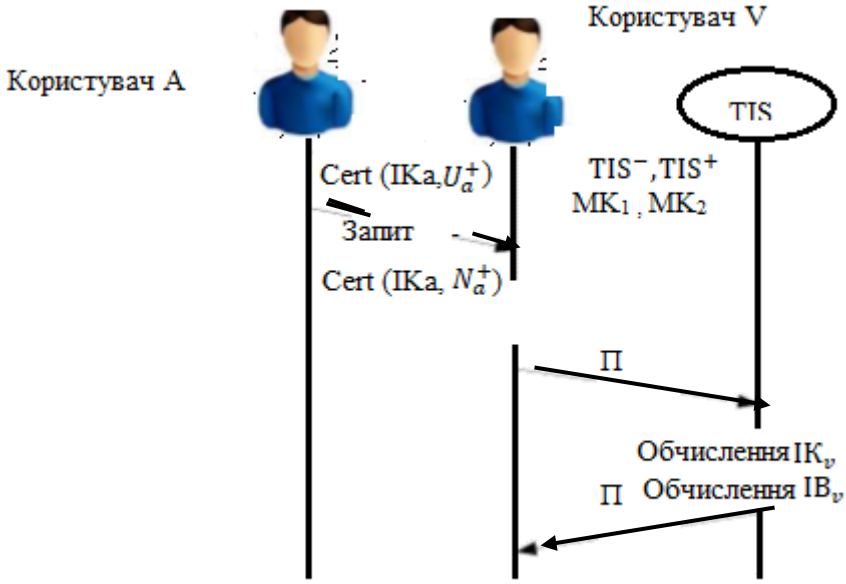

Рис. 1 Створення облікового запису для користувача V.

встановлено коефіцієнт, що більший за 1, він вибирає подальші вузли для пересилання оновленого Ш для досягнення потрібного розгалуження. Цей процес є рекурсивним: B видаляє підпис з СД і пересилає оновлений Ш на номер КП вибраних довірених контактів, і залучення більшої кількості підписів дозволяє ланцюгам Концентричні сфери мати різну довжину. Однак значення СД ніколи не можна збільшувати для захисту від DOS-атак і так далі, поки на одному вузлі D не буде видалений останній підпис з СД. D стає, як наслідок, точкою входу для Концентричних сфер з V. Для цього він спрямовує один запит на реєстрацію для кожного ключа в IPк через систему P2P.

Оскільки посилання Ds як точки входу θ_{vs} буде інформацією у загальнодоступному доступі, D може ідентифікувати вузол K, чий ідентифікатор вузла є найбільш близьким до реєстраційного ключа: D вибирає із своїх сусідів вузол N_1 з ідентифікатором вузла, найближчий до реєстраційного ключа, вимірюється за допомогою показника XOR для наступного переходу. N_1 надає D посилання до (один або більше) найближчого вузла N_2 тощо, поки не буде досягнуто належного близького вузла K. Такий вузол K, який називається доком, відповідає за збереження асоціації (IPк, EPTentry) у системі P2P. Потім D надсилає K регістрове повідомлення, що містить $EPTentrus_{Np}$ та випадкове число Rnd_{Suv}, представляє собою авторизацію, і D може претендувати на роль дійсної точки входу для V.

K додає в свою таблицю вхідних даних (EPT) і містить маркер реєстрації MP, сертифікат ідентифікатора вузла Ds, -адресу IP та час відмітки. Потім K оновлює свій EPT і відповідає на повідомлення П, яке пересилається назад до $\mathcal{V}$ за зворотним шляхом. Крім того, схожий на KAD, у Protectedbook K зберігає всі зареєстровані значення в k вузлах навколо цільового вузла запиту на реєстрацію RespArea доків для реєстраційного ключа.

Концентричні сфери відіграють основну роль у гарантуванні конфіденційності зв'язку до V та наявних даних V для всіх інших користувачів, без необхідності V бути в мережі. З цієї причини структура θ_v завжди автоматично має бути дійсною, використовуючи протокол оновлення Концентричних сфер, навіть у випадку появи та виходу вузла, останнє, можливо, обумовлено вибором (користувач виходить із Protectedbook) або збій (Інтернет-проблема з підключенням). Враховуючи, що вузол B залишає Protectedbook , він надсилає повідомлення про вихід вузла сусідам всередину (A) та назовні (C, ...) на шляху через Концентричні сфери. Повідомлення містить ідентифікатор користувача $ІД_d$ Концентричних сфер і передається до всіх точок входу, обрізаючи таким чином піддерево, укорінене в B. Точки входу відправляють незареєстроване повідомлення для всіх доків K, раніше адресованих на етапі реєстрації. A одночасно надсилає повідомлення Ш і надсилає його новий вибраний контакт é, не вимагаючи, щоб V знаходився в мережі. З цього моменту процес оновлення аналогічний створенню шляху.

Комунікація та управління відносинами у соціальних мережах

Концентричні сфери дозволяють користувачам отримувати доступ до засобів OCM. Далі ми детально розглянемо протоколи, відповідальні за пошук цільових даних для пошуку друзів / пошуку даних, знайомства з установою дружби користувачів та збереження даних у сховищі даних вузлів друзів. Протокол пошуку дозволяє отримати список вхідних точок користувача $\mathcal{V}$'s Концентричних сфер θ_v. Користувач, що запитує U, ініціює рекурсивний пошук у системі P2P шляхом обчислення IPкv. Як тільки повідомлення про пошук epLook досягає одного з доків Vs, док відповідає на повідомлення epRep, що містить запис EPT, відповідний IPкv :

epRep = {EPTentry(IPкv), Cert (IB_k , K_k^+)}s_{xk}

Записи EPT кешуються під час прийому, щоб уникнути декількох зайвих запитів.

Протокол пошуку даних

Після виявлення вхідних точок Концентричних сфер користувача V протокол пошуку даних дає змогу користувачеві U отримувати профільні дані $Prof_v$ у зашифрованому вигляді. Перш за все, U делегує один із найпотаємніших вузлів оболонки Z, щоб надіслати повідомлення про запит Зп для даних Vs до D, однієї з вхідних точок Концентричних сфер Vs. Цей запит рекурсивно передається через Концентричні сфери до A, одного з дзеркал V, що зберігає $Prof_v$ A. Потім надсилає відповідь на відповідне повідомлення Пв, що містить перелік зашифрованих підписаних елементів даних V. Це повідомлення доходить до U, слідуючи тим же шляхом у зворотному порядку. Відповідно до своїх привілеїв, U згодом може розшифрувати та отримати доступ до певних частин цих даних.

Ключі пошуку в шарах PXT для того самого цільового користувача можна обчислити, починаючи з різних властивостей, таких як: ім'я, день народження тощо, і подаватися з різних доків. Заснування дружби у Protectedbook , довірчі відносини не розглядаються як симетричні. Замість того, щоб просити дружбу з цільовим користувачем Vs, користувач Protectedbook U рекламує свою дружбу до V. Ця реклама проходить у три етапи:

- перш за все, U шукає всі загальнодоступні дані користувачів, що володіють набором властивостей відповідні кілька IPк;
- по-друге, серед усіх отриманих проектів U вибирає цільового користувача V, який рекламується;
- Нарешті, повідомлення про дружбу Д надсилається до V через Концентричні сфери V. Таке повідомлення включає IB_v та марку друзів, що складаються із засвідченої ідентичності U, їх вузлів та ідентифікаторів користувача, короткого повідомлення про дружбу та списку симетричних ключів, які використовуються для розшифрування захищених даних Us.

Оголошення про дружбу можуть бути неодноразово делеговані довіреному контакту Z у рекламодавця (або його друга), через повідомлення frDel, що містить Д разом зі списком вхідних даних Концентричні сфери Vs. У випадку, якщо V не є іншим, його дзеркало A буде виконувати роль поштової скриньки і зберігатиме рекламу про дружбу, поки V знову не з'явиться в мережі. Якщо V відповість U своєю рекламою дружби, стосунки довіри стають симетричними: U може стати новим дзеркалом V і навпаки.

Дані D користувача Us збирається в маркер разом із відповідними DId. Далі жетони підписуються з K_u^+ та шифруються за допомогою КШД. Такий зашифрований маркер ЗМ з підписами даних додатково зберігається у новому дзеркалі Us повідомленні DataStore разом із DId та ідентифікатором КШД IPP IPP DEKid, які використовуються V як літери під час відповіді на запит про дані даних на адресу U. Отримавши дані Store, $\mathcal{V}$ індексує ЗМ з Did, Dversion, DEKid, в РПЗД U, перш ніж відповісти на повідомлення storeConf. Після прийому підтвердження U може відслідковувати, на якому дзеркалі зберігається (розділений) (зашифрований) елемент.

Висновки.

У цій статті ми вказали на централізовану архітектуру існуючих он-лайн соціальних мереж як на ключове питання конфіденційності та розглянули рішення, яке спрямоване на те, щоб уникнути будь-якого централізованого контролю. Таке рішення, а саме Protectedbook - це он-лайн соціальна мережа, що базується на одноранговій архітектурі. Завдяки повному розповсюдженому характеру архітектура однорангових даних уникає централізованого контролю з боку будь-якого потенційно шкідливого постачальника послуг. Щоб впоратися з відсутністю довіри та відсутністю співпраці, яка є в централізованих мережах, використовуються однорангові системи для забезпечення базової конфіденційності серед користувачів соціальної мережі, Protectedbook використовує довірчі відносини, які є частиною самого додатка соціальної мережі. Конфіденційність в операціях з доступу до базових даних та обміну даними в соціальній мережі досягається завдяки техніці анонімізації, заснованій на багатосторонній маршрутизації між вузлами, які довіряють один одному в соціальній мережі. Співпраця між одноранговими вузлами налагоджується на основі довірчих відносин, які випливають із самої соціальної мережі.

Література

1. Ахрамович В.М. Проблеми відтворення атак на дані приватної особи та методи захисту в Інтернет-соціальних мережах. /- Sciences of Europe, Praha, Czech Republic.2019/ VOL 4, No 44. P. 31-38. www.european-science.org

2. Ахрамович В.М., Чегренець В.М. Постановка проблем захисту від загроз особистій інформації приватній особі в інтернет-соціальних мережах через дослідження їх функцій. Тези доповідей VIIIміжнародної науково-практичної конференції 1 частина: «Осінні наукові читання», м.Київ:–К.: Центр наукових публікацій, 2019. –с. 51-58. www.cnp.org.ua

3. Akhramovych V. M., Chegrenec V.M. The problem of the protection methods differences of the centralized and decentralized distributed social networks./ Perspectives of world science and education. Abstracts of the 3rd International scientific and practical conference. CPN Publishing Group. Osaka, Japan. 2019. Pp. . 217-225. URL: http://sci-conf.com.ua.

4. Ахрамович В.М., Чегренець В.М. Дослідження характеристик особистої інформаціїї користувача в інтернет-соціальних мережах. Тези доповідей Discovery science. Proceedings of articles the international scientific conference Czech Republic, Karlovy Vary – Ukraine, Kyiv, 6 December 2019 Pp 101-109. http://sci-conf.com.ua.

5. Ахрамович В.М., Чегренець В.М. , Зідан А. М. Деякі аспекти безпеки особистих даних в соціальних мережах. Science, society, education: topical issues and development prospects. Abstracts of the 1st International scientific and practical conference. SPC “Sci-conf.com.ua”. Kharkiv, Ukraine. 2019. Pp. 175-178. URL: http://sci-conf.com.ua.

6. A. Satsiou and L. Tassiulas. Reputation-based resource allocation in p2p systems of rational users. IEEE Transactions on Parallel and Distributed Systems, 21(4):466 -479, April 2010.

7. David Chaum. Blind signature system. In D. Chaum, editor, Advances in Cryptology, CRYPTO '83, page 153, New York, 1984. Plenum Press.

8. David Chaum. Blind signatures for untraceable payments. In Ronald Linn Rivest, A. Sherman, and D. Chaum, editors, Advances in Cryptology, CRYPTO '82, pages 199-203. Plenum Press, 1983.

9. Leucio Antonio Cutillo, Re-k Molva, and Thorsten Strufe. Leveraging social links for trust and privacy in networks. In INetSec 2009, Open Research Problems in Network Security, Zurich, Switzerland, April 2009.

10. Leucio Antonio Cutillo, Re-k Molva, and Thorsten Strufe. Privacy preserving social networking through decentralization. In WONS 2009, 6th International Conference on Wireless On-demand Network Systems and Services, Snowbird, Utah, USA, February 2009.

11. Levente Buttyán and Jean-Pierre Hubaux. Enforcing service availability in mobile ad-hoc wans. In Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, MobiHoc '00, pages 87-96, Boston, Massachusetts, 2000. IEEE Press.

12. Mira Belenkiy, Melissa Chase, C. Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya, and Eric Rachlin. Making p2p accountable without losing privacy. In Proceedings of the 2007 ACM workshop on Privacy in electronic society, WPES '07, pages 31-40, Alexandria, Virginia, USA, 2007. ACM.

13. P. Dewan and P. Dasgupta. P2p reputation management using distributed identities and decentralized recommendation chains. IEEE Transactions on Knowledge and Data Engineering, 22(7):1000 -1013, July 2010.

14. P. Michiardi and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of IFIP Communication and Multimedia Security Conference, CMS 2002, Portoroz, SLOVENIA, 2002.

15. S. Buchegger and J-Y. Le Boudec. Nodes bearing grudges: Towards routing security, fairness and robustness in mobile ad hoc networks. In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, PDP 2002, Canary Islands, Spain, 2002.

16. V. Vishnumurthy, S. Chandrakumar, and E. Sirer. KARMA: A Secure Economic Framework for Peer-to-Peer Resource Sharing. In Workshop on the Economics of Peer-to-Peer Systems, P2PEcon, Berkeley, CA, USA, 2003.

Dragomirov S. G.
doctor of engineering, professor,
Vladimir State University, Russia
Eydel P.Ig.
engineer,
L.L.C. "STC "AutoSphere"
at Vladimir State University", Russia
Dragomirov M.S.
candidate of technical Sciences
L.L.C. "STC "AutoSphere"
at Vladimir State University", Russia
Gamayunov A.Y.
Engineer,
LLC "STC "AutoSphere"
at Vladimir State University", Russia

PROMISING APPROACH TO SOLVING THE PROBLEM HIGH-EFFICIENCY COOLANT FILTRATION IN ENGINES VEHICLES

Драгомиров Сергей Григорьевич
доктор технических наук, профессор кафедры двигателей
Владимирского государственного университета
им. А.Г. и Н.Г. Столетовых, Россия
Эйдель Павел Игоревич
инженер
ООО «НТЦ «АвтоСфера» при ВлГУ», Россия
Драгомиров Михаил Сергеевич
кандидат технических наук,
ООО «НТЦ «АвтоСфера» при ВлГУ», Россия
Гамаюнов Антон Юрьевич
инженер
ООО «НТЦ «АвтоСфера» при ВлГУ», Россия

ПЕРСПЕКТИВНЫЙ ПОДХОД К РЕШЕНИЮ ПРОБЛЕМЫ ВЫСОКОЭФФЕКТИВНОЙ ФИЛЬТРАЦИИ ОХЛАЖДАЮЩЕЙ ЖИДКОСТИ В АВТОТРАНСПОРТНЫХ ДВИГАТЕЛЯХ

Summary. The article analyzes the critical and still unsolved problem of contamination of the coolant and engine cooling systems in General. The assessment of existing filtration devices is given, and their principal disadvantages are given. A new concept of modified hydrocyclone coolant cleaning is proposed. Its advantages, features, results of laboratory studies and operational tests are given. The conclusion is made about the prospects of this approach to solving the problem of high-efficiency filtration of engine coolant.

Аннотация[*]**.** В статье анализируется критически острая и до настоящего времени не решенная проблема загрязнения охлаждающей жидкости и систем охлаждения двигателей в целом. Дана оценка существующих устройств фильтрации, приведены их принципиальные недостатки. Предложена новая концепция модифицированной гидроциклонной очистки охлаждающей жидкости. Даны ее преимущества, особенности, результаты лабораторных исследований и эксплуатационных испытаний. Сделан вывод о перспективности данного подхода к решению проблемы высокоэффективной фильтрации охлаждающей жидкости двигателей.

Keywords: coolant, pollution, motor vehicles, coolant filtration, hydrocyclone filters, separation, hydraulic resistance.

[*] Данное исследование выполнено в рамках реализации инновационного Проекта № 45450 “Разработка конструкции инновационного высокоэффективного фильтра для систем охлаждения автотранспортных двигателей и формирование научно-технического задела для развития его промышленного производства” Программы СТАРТ.