УДК 004.056(075.8)
DOI: 10.31673/2412-9070.2019.051318

В. М. АХРАМОВИЧ, канд. техн. наук, доцент;
Ю. О. ТИХОНОВ, канд. техн. наук, доцент;
В. І. СТЕПАНЕНКО, ст. викладач,
Державний університет телекомунікацій, Київ

ДОСЛІДЖЕННЯ РОЗПОДІЛЕНИХ СОЦІАЛЬНИХ МЕРЕЖ З ТОЧКИ ЗОРУ СПЕЦИФІЧНИХ ХАРАКТЕРИСТИК БЕЗПЕКИ

Проведено аналіз розподілених Інтернет соціальних мереж (ОСМ) (Persona, Safebook, PeerSoN Wie Concentric nodes, Vis-à-Vis) з погляду безпеки конфіденційності, інформаційного самовизначення, довірчих відносин, підтримання мобільності.

ОСМ Persona — це децентралізована соціальна мережа (СМ), концепція безпеки якої базується на поєднанні традиційного асиметричного та атрибутного шифрування (АШ).

ОСМ Safebook — децентралізована СМ, заснована на структурованій версії P2P, сприяє захисту конфіденційності своїх членів та їх захисту від супротивників.

ОСМ PeerSoN Wie Concentric nodes на основі ОСМ PeerSoN на P2P. Концептуально безпека та конфіденційність базуються на використанні асиметричного шифрування.

ОСМ Vis-à-Vis Vis-à-Vis — це децентралізована СМ, заснована на структурованій P2P.

Зазначено, що жодна з досліджених ОСМ не забезпечує комплексного захисту персональних даних користувача та інших параметрів безпеки.

Ключові слова: соціальні мережі; Інтернет; процеси; безпека; персональні дані; конфіденційність; інформаційне самовизначення; довірчі відносини; підтримання мобільності користувачів; друзі; групи; ключ; атрибути; асиметричне шифрування; централізовані; децентралізовані пристрої; контроль доступу; мережа P2P; індентифікація; хеш-таблиця; пошук.

Вступ

Значний вплив соціальних мереж на особистість та процеси, що відбуваються в державі, визумовлює потребу в подальшому дослідженні захисту персональних даних користевачів та інших параметрів мереж.

Аналіз літературних джерел [2; 4; 7; 9; 10] показує, що всі підходи мають на меті надати користувачеві більше безпеки та конфіденційності в Інтернет соціальних мережах (ОСМ). Захист особистих даних користувачів розглядається у багатьох концепціях недостатньо. Необхідні подальші дослідження щодо безпеки конфіденційності, інформаційного самовизначення, довірчих відносин, підтримання мобільності користувачів та інших параметрів в ОСМ.

Основна частина

1. ОСМ *Persona* [1] — це децентралізована соціальна мережа (СМ), концепція безпеки якої базується на поєднанні традиційного асиметричного та атрибутного шифрування (АШ). Причина поєднання полягає в підвищенні гнучкості для керування групами користувачів. На думку авторів, інші відомі методи групового шифрування [8; 11] обмежені тим, що авторизований доступ до персонального контенту для розподілу членів кількох груп дуже громіздкий. Концепція ***Persona*** розрізняє дві категорії об'єктів. Є користувачі, які генерують вміст і програми та надають користувачам послуги маніпулювання вмістом. Кожний користувач взаємодіє з Persona через розширення браузера, який обробляє всі криптографічні операції. Програми включають в себе додаток *служби зберігання даних* і *службу документів*. ***Служба зберігання*** використовується для забезпечення особистого контенту, зашифрованого друзям. Надаються лише операції з отримання та збереження інформації. ***Служба документів*** слугує для реалізації спільних пропозицій, таких як персональна дошка. Користувачі можуть призначити доступ для запису до своєї служби документів іншим учасникам або групам. Єдиною вимогою для служби зберігання або документообігу є реалізація заданого інтерфейсу програмування, кожний користувач може самостійно вирішити, якою частиною з його особистої інформації він поділиться з кимось із своїх друзів. Кожний користувач керує доступом своїх друзів та груп. Приналежність до групи грунтується на загальних атрибутах, які користувач поділяє з членами цієї групи. Кожний користувач генерує відкритий ключ (ВК) і загальний ключ (ЗК). Окрім шифрування, ВК застосовується як ідентифікатор користувача і може повідомлятися друзям із групи. Разом із тим, є один друг, який має секретний ключ (ASK, секретний ключ ABE). Він генерується за допомогою ЗК. ASK базується на наборі атрибутів, що визначають групу, до якої повинен належати друг. Для шифрування об'єкта має бути визначено структуру доступу у вигляді логічного виразу атрибутів. Якщо інформація надається, наприклад, зашифрованою структурою

доступу («climber» (альпініст) або «Neighbour» (сусід)), то інший користувач може розшифрувати його тоді і тільки тоді, коли він належить до групи, яку було призначено щонайменше одним із двох атрибутів. Попередньо визначених груп не існує. Вони генеруються неявно тільки тоді, коли дані шифруються на основі відповідного ASK. Знання ВК та його пов'язаних атрибутів є достатнім для шифрування інформації з бажаною структурою доступу. Єдиний спосіб привести учасників з групи — це створити нові запити для кожного члена групи. Для того щоб заперечити групу майбутнім друзям, структури доступу можуть бути забезпечені, наприклад, такими нерівностями, як (дата < 2019).

Обговорення. Завдяки централізованому керуванню даними через служби зберігання та документування, ***Persona*** відповідає вимогам щодо постійного доступу до даних. Користувачі можуть отримати доступ до особистого вмісту члена групи, навіть якщо в даний час він відсутній у СМ. Призначені Persona застосування надзвичайно складні. Кожна нова заявка вимагає реалізації авторизації для дотримання відповідних списків контролю доступу, а знання ВК і ASK достатньо для обмеження доступу до інформації для членів групи. Що ж до інформаційного самовизначення, то тут існує серйозна проблема: члени групи неявно визначаються списком атрибутів ASK. Проте тільки виробник ASK знає призначення атрибутів членам групи. Не всі члени СМ можуть знати про свою спільну приналежність до групи. Існує ризик того, що учасники невідомої групи можуть ненавмисно прочитати зашифрований вміст. Крім того, ідентифікація користувача заснована на одному ВК. Деанонімізація користувачів можлива персональна. ВК обмінюються особисто безпосередньо між користувачами поза зоною. Це означає сильну довіру до дружби. Persona також досліджувалася для використання на мобільних пристроях. Атрибутне шифрування мА\недоліки. У порівнянні з RSA, операція АШ проводиться в кілька разів повільніше.

2. ОСМ *Safebook* [4; 5], децентралізована СМ, заснована на структурованій версії P2P, сприяє захисту конфіденційності своїх членів та їх захисту від шкідливих супротивників. Підхід полягає в забезпеченні конфіденційності в комунікаціях, контролі доступу до особистої інформації, їх постійній доступності та цілісності. Концепція ***Safebook*** розділена на три шари. *Рівень соціальної мережі* містить цифрові представлення користувачів і їх взаємозв'язків. *Прикладний рівень служби* (ПРС) — середовище, яке предметно розвивається, описує інфраструктуру програми оператора. *Рівень зв'язку та транспорту* (РЗТ) включає в себе комунікаційні та транспортні послуги мережі. При реалізації Safebook Інтернет слугує як РЗТ-шар. Зловмисники з'являються як зловмисні користувачі на шарі СМ, як шкідливі оператори на шарі ПРС (предметно-розвиваного середовища), або як шкідливий третій учасник на шарі СТ. Трьома основними компонентами Safebook є *концентричні кола, P2P* та *довірча служба ідентифікації* (ДСІ). Розподілена структура Safebook використовується для конфіденційного спілкування та зберігання особистого вмісту. Вона складається з кількох логічних концентричних кіл навколо одного користувача. Внутрішнє коло включає в себе мережу користувача. Це контакти, яким довіряє користувач. Вузли на колі рівня $n + 1$ є кожним з найближчих контактів вузлів на рівні n. Кожен користувач реплікує свій особистий вміст на вузлах свого внутрішнього кола. Якщо повідомлення має бути перенаправлено користувачеві u, то воно спочатку досягає вузла зовнішнього кола *Concentric nodes u*. Внутрішні кола повідомлення послідовно передають u. Конфіденційність забезпечується тим, що вузли спілкуються виключно зі своєю електронною роботою. Жоден вузол на шляху до u не має безпосереднє знання фактичного одержувача повідомлення. Усі учасники організовані у вигляді P2P накладання. VIS допомагає знайти інформацію про інших користувачів, і для кожного користувача він, швидше за все, зареєструється у вузлах свого зовнішнього кола в PXT (*Distributed Hash Table* — росподілена хеш-таблиця). Шлях пошукового запиту від u до користувача v визначається спочатку PXT, а потім *Concentric nodes v*. Якщо пошук потрапляє в один із найбільш зовнішніх вузлів Safebookv, він делегується v через одного користувача концентричних кіл. Відповідь передається назад на u по тому самому шляху. ДСІ гарантує, що тільки реальні існуючі особи можуть зареєструватися в Safebook, а поза цим кожний користувач має унікальну пару ключ/значення, що складається з ідентифікатора вузла і псевдоніму.

Ідентифікатор вузла генерується на основі вибраних атрибутів користувача, таких як ім'я, день народження та місце народження: користувач реєструється з псевдонімом в накладенні P2P перед встановленням власної мережі та концентричних кіл. Починаючи з цього моменту, користувач може отримати профікційний та інший особистий контент з v через зовнішні вузли Safebook.

Обговорення. Із ноутбуком функціонує структурована система P2P, особистий контент якого зберігається безпосередньо на пристрої користувача. Незважаючи на тиражування в СМ, вимога щодо постійної доступності виконується лише частково. Якщо всі вузли мережі відкриті, то неможливо отримати доступ до особистого вмісту користувача. Реплікація особистого контенту здійснюється

в зашифрованому вигляді, однак користувач не впливає на те, коли сусід видаляє його вміст. Використання TIC як центральної інстанції порушує право на інформаційне самовизначення. Користувачі повинні зареєструвати там конфіденційну інформацію, наприклад ім'я, день народження або адресу. Таким чином, ДСІ займає аналогічну позицію, як і оператор централізованої ОСМ. ДСІ має забезпечувати взаємну довіру користувачів. Однак це третя сторона. Криптографічні ключі дійсно обмінюються з ДСІ поза зоною. Проте вимога щодо міцних довірчих відносини безпосередньо між користувачами не виконується. Немає інформації про використовувані криптографічні методи. Крім того, не існує припущень щодо технічних характеристик пристроїв, що беруть участь, тому оцінити продуктивність мобільних терміналів неможливо. Однак використання на основі PXT P2P накладання показує, що велика частка користувачів мобільного зв'язку має дуже негативний вплив на ефективність та надійність системи в цілому. Підтримання для мобільних користувачів строго обмежене ефектом Churn (відтоку з мережі).

3. ОСМ *PeerSoN Wie Concentric nodes* на основі ОСМ PeerSoN [2; 3] на P2P. Концептуально безпека та конфіденційність базуються на використанні асиметричного шифрування. Концепція PeerSoN використовується як накладання на PXT, кожний вузол представляє користувача і відповідає за розподілене зберігання персональних даних усіх користувачів. Для пошуку користувачів використовуються *глобальні унікальні ідентифікатори* (ГУІ). PeerSoN використовує як ГУІ значення хеш-адреси електронної пошти користувача. Система базується на таких протоколах: вхід, отримання протоколу і асинхронні повідомлення. За допомогою протоколу входу користувач реєструється з відповідними метаданими в мережі.

Різні розташування/термінали зберігаються разом із поточним статусом з'єднання користувача. Якщо користувач *u* бажає з'єднатися з користувачем *v*, *u* викликає відповідний набір даних через ГУІ *v* у PXT. Із цього *u* витягує поточне розташування *v*. Дані про користувача можуть бути отримані за допомогою протоколу отримання. Для кожної дати пара ключ/вартість депонується в PXT. Пара ключ/значення повідомляє, які вузли в якій версії зберегли відповідний файл. Користувач отримує доступ до файла за допомогою пари ключ/значення, щоб ідентифікувати адресу вузла з поточною версією, а потім підімкнутися безпосередньо до цього вузла. Усі файли захищені відповідним контролем доступу. Якщо *u* захоче спілкуватися з *v*, то обмін повідомленнями здійснюється безпосередньо. Після того, як повідомлення з'явиться, використовується асинхронний протокол повідомлень. Спочатку *u* зберігає повідомлення під спеціальним ключем у PXT. Після того як *v* увійде назад у більш пізній час, *v* може отримати повідомлення за допомогою ключа. До кожного обміну даними додатково виконується протокол рукостискання. З одного боку, це запобігає будь-яким проблемам зі спамом, з другого боку, це допомагає вказати розмір даних, які потрібно передати. Наприклад, якщо користувач у даний момент увійшов через свій смартфон, він може динамічно вирішити, чи слід здійснювати передавання даних негайно або тільки при встановленні широкосмугового з'єднання.

Обговорення. Зберігання особистого контенту повністю зашифровано та децентралізовано в PeerSoN, однак, на відміну від ноутбука, користувач не може вирішити, якому вузлу повинен довіряти і в якому зберігати. Видалення особистого вмісту не може бути виконано користувачем. Окрім того, атаки на Concentric nodes можливі. Право на інформаційне самовизначення лише частково виконується. Оскільки PeerSoN спирається виключно на P2P під час зберігання особистого контенту, постійна доступність профілів користувачів і особистого контенту не гарантується. Для PeerSoN характер шифрування та процедури контролю доступу є дуже нечіткими: якщо відкриті ключі передавалися поза діапазоном, то, принаймні, було б забезпечено потребу в міцних довірчих відносинах. Анонімність користувачів не гарантується з можливістю одночасного входу в мережу з кількома пристроями, а також із використанням асинхронних повідомлень і протоколів рукостискання. PeerSoN забезпечує основу для підтримання мобільних абонентів, а також має розширення, яке дає змогу користувачам обмінюватися даними навіть без підімкнення до Інтернету через мобільні спеціальні мережі, такі як Bluetooth або WLAN.

Висока частка користувачів мобільного зв'язку негативно впливає на ефективність та надійність системи в цілому.

4. ОСМ *Vis-à-Vis Vis-à-Vis* (сервер і сервер) [10] — це децентралізована СМ, заснована на структурованій P2P. Зберігання особистого контенту здійснюється виключно на власному сервері. Це виконується у віртуальній машині (ВМ) в інфраструктурі хмарних обчислень (ІХО), наприклад Amazon EC2 [11]. Користувачі також можуть зберігати особистий контент на своїх кінцевих пристроях.

Концепція Vis-à-Vis вводить концепцію віртуальних окремих серверів (VIS). Кожний користувач використовує свій власний екземпляр VIS для зберігання особистого вмісту. Виходячи з хеш-значення IP-адреси, кожен екземпляр VIS отримує унікальний ідентифікатор. Це слугує для організації всіх екземплярів VIS у багатошаровому

PXT. Верхній шар — це метагрупа, яка керує всіма екземплярами VIS і шукає інших користувачів. Vis-à-Vis дозволяє зберігати особистий контент на власному терміналі або на комбінації терміналу та екземплярі VIS, однак ексклюзивне використання екземпляра VIS має дві важливих переваги. З одного боку, ICH гарантує постійну доступність віртуальних машин, з другого боку, оператор бере на себе все адміністрування, наприклад імпортування останніх оновлень безпеки. Vis-à-Vis визначає дві категорії особистої інформації:

• обмежену інформацію, яку можна переглядати лише за допомогою надійних контактів;

• інформацію, яка доступна для пошуку, доступна для більшої спільноти користувачів і дозволяє шукати інтереси людей.

У разі доступу до обмеженої інформації екземпляр VIS діє як контрольний монітор. Тільки особи з відповідними правами доступу можуть переглядати ці дані. Конфігурація правил доступу здійснюється самим користувачем, окрім того, примірник користувача VIS зберігає загальний секретний ключ для кожного з його друзів разом із посиланням на примірник VIS відповідного друга. Цей ключ генерується, коли новий друг закривається, наприклад на основі протоколу Diffel-Hellman [6]. Він служить для створення безпечного каналу зв'язку між взаємно довірчими екземплярами VIS. Інформацію про пошук організовано у вигляді текстових груп, як ідентифікатор використовуються мета-групи, а рішення для одного елемента приймається локально асоційованим екземпляром VIS. Кожна набрана група складається з користувачів із загальними атрибутами або інтересами. Замість посилання на групу застосовується комбінація типу і відповідного ключа. Пошукові запити дають можливість усім членам уводити групові цифри, а коли вони створюються або приєднуються до іншої групи, хеш-значення посилання використовується як ідентифікований член групи. Ідентифікатор використовується для визначення екземпляра VIS, який зрештою обробить відповідний запит. Приєднання або запит на іншу групу автоматично регулюється згодою всіх членів поточної групи або невизначеним механізмом автентифікації. Можна також створювати приховані набрані групи. Про їх існування поінформовані лише члени цих груп. Додавання інформації до іншої групи здійснюється шляхом вставки відповідної пари ключ/значення в PXT.

Обговорення. Використання ICH гарантує кожному постійну доступність їхнього особистого контенту, однак при такій комбінації існують додаткові витрати на оренду та експлуатацію ВМ. Організація учасників є децентралізованою в Vis-à-Vis. Окрім того, кожний користувач керує та зберігає свою особисту інформацію виключно на власному екземплярі VIS. Проте право на інформаційне самовизначення не гарантоване. Оскільки шифрування не виконується на примірниках VIS, оператори мають можливість читати та копіювати особистий вміст. Vis-à-Vis не забезпечує адекватної анонімізації особистої інформації. Атаки деанонімізації все ще можливі завдяки інформації, доступній для пошуку. Атаки Сибіл [7] не виключені. Зловмисне функціонування невизначеної кількості екземплярів Vis дає можливість підробити будь-які ідентичності. Обмін криптографічними ключами відбувається у Vis-à-Vis поза зоною. Виконані передумови для міцних відносин довіри. Висока доступність IXO також надає мобільним користувачам швидкий і надійний доступ до ОСМ. Інформація про ефективність криптографічних операцій та операції мобільного зв'язку відсутня.

Висновки

Жодна з чотирьох децентралізованих ОСМ не повністю гарантує право на інформаційне самовизначення. Хоча несвідомий доступ до персонального контенту в Persona не може бути виключений, він зберігається незашифрованим в Vis-à-Vis.

Читання вмісту та копіювання. Для Safebook і PeerSoN атаки не можна виключити. Обмін криптографічними ключами відбувається безпосередньо між користувачами поза групою. Це відповідає вимогам міцних відносин довіри. Для PeerSoN обмін ключами не вказано. Окрім того, в концентричних колах обмінюються криптографічними ключами між користувачами і ДСІ, а не безпосередньо між окремими абонентами. Використання окремих сервісів зберігання або віртуальних серверів забезпечує постійний доступ у Persona або Vis-à-Vis. У Safebook і PeerSoN зберігання виконується виключно в P2P. Обидві системи страждають від аномалій, таких як ефект відтоку користувачів. Вимога постійного доступу до профілю тут не виконується. Всі чотири системи мають потенціал для підтримання мобільних абонентів. Однак, завдяки P2P в Safebook, зі збільшенням участі користувачів мобільного зв'язку має дуже негативний вплив на ефективність та надійність системи в цілому. Незважаючи на реплікацію особистого контенту, PeerSoN також є вразливим до ефекту відтоку. З погляду ефективності та надійності всієї системи, Vis à Vismitters підтримує свою концепцію VIS для підтримки мобільних користувачів. Навряд чи є інформація про ефективність криптографічних методів, що використовуються на мобільних терміналах. Лише для PeerSoN можна сказати, що використання АШ призводить до набагато більших обчислювальних зусиль, ніж, наприклад, ОДА. Огляд виконання вимог у розглянутих децентралізованих СМ наведено в табл.

Огляд виконання вимог до розглянутих децентралізованих ОСМ

ОСМ	Інформаційне самовизначення	Сильні довірчі відносини	Доступ до постійного профілю	Підтримка мобільності
Persona	x	√	√	Θ
Safebook	Θ	x	x	x
PeerSoN	Θ	?	x	Θ
Vis-à-Vis	x	√	√	Θ

Умовні позначення: √ — виконано, x — не виконано,
Θ — частково виконано, ? — немає інформації

Список використаної літератури

1. ***Persona:*** *an online social network with user-defned privacy / R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin // SIGCOMM Comput. Commun. Rev. 2018. Vol. 39. P. 135–146.*

2. ***Buchegger S., Datta A.*** *A case for P2P infrastructure for social networks — opportunities & challenges: in WONS'09 //IEEE, Feb 2009. P. 161–168.*

3. ***Peerson:*** *P2p social networking: early experiences and insights / S. Buchegger, D. Schiöberg, L.-H. Vu, A. Datta: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, SNS '09, (New York, NY, USA) // ACM, 2015. P. 46–52.*

4. ***Cutillo L. A., Molva R., Strufe T.*** *Privacy preserving social networking through decentralization: Sixth International Conference on Wireless On-Demand Network Systems and Services (WONS), 2009 // IEEE, Feb. 2009. P. 145–152.*

5. ***Cutillo L. A., Molva R., Strufe T.*** *Safebook: Aprivacy-preserving on line social network leveraging on real-life trust // Communications Magazine, IEEE: Dec. 2009. Vol. 47. P. 94–101.*

6. ***Diffe W., Hellman M. E.*** *New directions in cryptography // IEEE transactions on Information Theory, 2017. Vol. 22.*

7. ***Lifesocial.kom:*** *A secure and p2p-based solution for online social networks / K. Graff, C. Gross, D. Stingl [et al.]: Consumer Communications and Networking Conference (CCNC), 2011 // IEEE, 2015. P. 554–558.*

8. ***NaorD., Naor M., Lotspiech J.*** *Revocation and tracing schemes for stateless receivers (J. Kilian, ed.): Advances in Cryptology — CRYPTO 2001, Springer Berlin Heidelberg. 2014. Vol. 2139 of Lecture Notes in Computer Science. P. 41–62.*

9. Narendula R., Papaioannou T., Aberer K. My3: A highly-available p2p-based online social network: The 2011 IEEE International Conference on Peer-to-Peer Computing (P2P). 2011. P. 166–167.

10. ***Vis-à-vis:*** *online social networking via virtual individual servers / A. Shakimov, H. Lim, L. P. Cox, R. Caceres: tech. rep. Duke University, May 2016.*

11. ***Wong C. K., Gouda M., Lam S. S.*** *Secure group communications using key graphs: Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication, SIGCOMM'98 (New York, NY, USA) // ACM, 2018. P. 68–79.*

В. Н. Ахрамович, Ю. А. Тихонов, В. И. Степаненко

ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕННЫХ СОЦИАЛЬНЫХ СЕТЕЙ С ТОЧКИ ЗРЕНИЯ СПЕЦИФИЧЕСКИХ ХАРАКТЕРИСТИК БЕЗОПАСНОСТИ

Проведен анализ распределенных Интернет социальных сетей (ОСС) (Persona, Safebook, PeerSoN Wie Concentric nodes, Vis-à-Vis) с точки зрения безопасности конфиденциальности, информационного самоопределения, доверительных отношений, поддержки мобильности.

ОСС Persona — это децентрализованная социальная сеть (СС), концепция безопасности которой базируется на сочетании традиционного асимметричного и атрибутного шифрования (АШ).

ОСС Safebook, децентрализованная СС, основанная на структурированной версии P2P, способствует защите конфиденциальности своих членов и их защиты от противников.

ОСС PeerSoN Wie Concentric nodes на основе ОСС PeerSoN на P2P. Концептуально безопасность и конфиденциальность базируются на использовании асимметричного шифрования.

ОСС Vis-à-Vis Vis-à-Vis — это децентрализованная СС, основанная на структурированной P2P.

Указано, что ни одна из исследованных ОСС не обеспечивает комплексной защиты персональных данных пользователя и других параметров безопасности.

Ключевые слова: социальные сети; Интернет; процессы; безопасность; персональные данные; конфиденциальность; информационное самоопределение; доверительные отношения; поддержка мобильности пользователей; друзья; группы; ключ; атрибуты; асимметричное шифрование; централизованные; децентрализованные устройства; контроль доступа; сеть P2P; индентификации; хеш-таблица; поиск.

V. M. Akhramovych, Y. O. Tykhonov, V. I. Stepanenko

RESEARCH OF APPORTIONED SOCIAL NETWORKS IN TERMS OF SPECIFIC SECURITY FEATURES

The analysis of distributed Internet social networks (OSNs) (Persona, Safebook, 3 PeerSoN Wie Concentric nodes, Vis-à-Vis,) from the point of view of security privacy, information self-determination, trust relations, support of mobility is carried out. Existing OSNs have been evaluated.

OSN Persona is a decentralized social network (SN), the concept of security based on the combination of traditional asymmetric and attribute encryption (AE).

OSN Safebook, a decentralized SN based on a structured version of P2P, helps protect the privacy of its members and protect them from harmful opponents /

Despite the duplication in the SN, the requirement for permanent availability is only partially met. Replication of personal content is encrypted, but the user does not have influence when the neighbor removes its contents.

OSN PeerSoN Wie Concentric nodes based on OSN PeerSoN on P2P. Conceptually, security and privacy are based on the use of asymmetric encryption.

The right to information self-determination is only partially fulfilled. Because PeerSoN relies solely on P2P when storing personal content, the continued availability of user profiles and personal content is not guaranteed.

With centralized data management through storage and documentation services, Persona meets the requirements for ongoing access to data.

OSN Vis-à-Vis Vis-à-Vis (server and server) is a decentralized SN based on structured P2P.

The organization of participants is decentralized in Vis-à-Vis. In addition, each user manages and stores their personal information solely on their own VIS instance. However, the right to self-determination is not guaranteed.

Reading content and copying. For Safebook and PeerSoN, attacks cannot be ruled out. Cryptographic keys are exchanged directly between users outside the group.

It is stated that none of the investigated OSNs provides comprehensive protection of the user's personal data and other security parameters.

Keywords: social networking; Internet; processes; security; personal data; privacy; information self-determination; trusting relationships; support for user mobility; friends; groups; key; attributes; asymmetric encryption; centralized; decentralized devices; access control; P2P network; identification; hash table; search.