УДК 004

О.Кузь, магістр гр. КН-22М-2
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ НАВІГАЦІЇ ТА МОНІТОРИНГУ ФАЙЛОВОЇ СИСТЕМИ IOS

У статті розроблено програмне забезпечення, яке призначено для системи навігації та моніторингу файлової системи iOS. Метою розробки є дослідження та програмна реалізація системи навігації та моніторингу файлової системи iOS. Об’єктом дослідження є процес навігації та моніторингу файлової системи iOS. Предметом дослідження є методи навігації та моніторингу файлової системи iOS. Методи дослідження базуються на методах побудови файлових систем, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи навігації та моніторингу файлової системи iOS. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Історія обміну файлів між комп'ютером і телефоном не нова. На наше століття довелося багато всіляких програм. Громіздкі й гальмові пакети, що містять тонни помилок, перетаскування пісень папками на SD-картку, спеціальні кабелі й не менш спеціальні драйвери до них, у порівнянні із цим, зараз, у другому десятилітті XXI століття, усілякі операції відновлення виробляються тривіально. З 2011 року iOS-пристрою взагалі можна не підключати до комп'ютера, або синхронізуючи їх по Wi-Fi, або користуючись винятково iCloud. Однак потреба у файлових менеджерах для iOS-пристроїв поки що не відпала остаточно, особливо це стосується тих з них, на яких зроблений джейлбрейк. На сьогоднішній день у магазині App Store, є величезна кількість додатків, які асоціюються із клієнтами для соціальних мереж за типом twitter або vk, є файлові менеджери, різні клієнти, що працюють із відеороликами й фотографіями на інших сервісах. Однією фразою можна сказати, що додатків досить. Однак, далеко не всі з них можуть заслужити належної оцінки від користувача. Десь інтерфейс не дуже гарний, десь багато багів, малий функціонал та інші тому подібні проблеми. У прихильників Android завжди є в арсеналі головний аргумент проти iOS-користувачів – довід про закритість платформи. Мол, не можна файли по папках розкидати, не можна без джейлбрейку файлову систему подивитися. Так, папки /var, /root і їм подібні – не можна, однак це не заважає існуванню файлових менеджерів в App Store. Наприклад, після установки iFiles ви одержуєте практично повну файлову систему на iOS-пристрої без усяких джейлбрейків, нехай і в рамках одного додатка.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні Системи навігації та моніторингу файлової системи ios.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи навігації та моніторингу файлової системи iOS.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем навігації та моніторингу файлової системи iOS.
- Дослідження системи навігації та моніторингу файлової системи iOS.
- Програмна реалізація системи навігації та моніторингу файлової системи iOS.

Об’єктом дослідження є процес навігації та моніторингу файлової системи iOS.

Предметом дослідження є методи навігації та моніторингу файлової системи iOS.

Методи дослідження базуються на методах побудови файлових систем, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Структура папок і файлів iPhone. Власники джейлбрейкнутих iPhone мають доступ до файлової системи свого апарата, що відкриває перед ними додаткові можливості – змінювати налаштування, недоступні офіційним користувачам, установлювати зламані програми й т.д. По суті, працювати із джейлбрейкнутим iPhone можна як із флешкою. Тільки от файлова система його не так проста. І часом досить складно знайти потрібний файл. У цьому розділі з усім цим розберемося.

Почнемо із установлених додатків. На прошиваннях 1.x.x з ними все було набагато простіше. Програми попадали в private/var/mobile/Applications і залишалося тільки знайти папку виду Proga.app. Але це було ще до відкриття App Store, коли програми завантажувалися з Installer. Нині цей пакетний менеджер втратив свою актуальність. Причому справа не тільки у відкритті онлайн-магазину від Apple. Для установки сторонніх додатків, що не потрапили в App Store, зараз набагато переважніша Cydia.

Втім, у цьому випадку це не так важливо. Програми із Cydia й Installer попадають в одну папку із передвстановленими додатками. Тільки тепер шлях до неї небагато інший – private/var/stash/Applications.Gg5Ly. При цьому набір букв і цифр, що випливає за словом Applications для кожного апарата різний.

Ще складніше із програмами, придбаними в App Store. Вони попадають у папку private/varmobile/Applications, але відкривши її, ви побачите купу додаткових папок з назвами виду: 2BF2F 8878-4846-B6E 7-019D0B5AE9B5. Шукати потрібну програму вам доведеться, клкаючи на них по черзі. У кожній з них є папка з ім'ям додатка, що ви шукайте:

– Стандартні додатки перебувають в /Applications.
– Додатки з App Store перебувають у папці /private/var/mobile/Applications.
– Фото з камери перебувають у папці: /private/var/mobile/Media/DCIM/100APPLE.
– AddressBook, SMS і Mail розташовані в папці /private/var/mobile/Library/
– Теми розташовані в папці /Library/Themes.

Якщо ви не хакер, то залазити в неї вам, швидше за все, і не знадобиться, а от звернути увагу на сусідню папку Documents іноді може бути корисно. У ній зберігаються файли, які можуть бути цікаві. Скажемо, диктофони зберігають тут аудіо-записи, інтернет-пейджери – відправлені файли, а програми для роботи з документами – ті файли, які ви в них записали й т.д.

З відео, піснями й фотографіями справа простіша. Пісні зберігаються за адресою private/var/mobile/MediaiTunes_Control/Music. Правда, вам ще прийдеться їх пошукати по папках виду F00, F01, F02 і т.д. А шляхи для відео й фото наступні:

– Фотографії: private/var/mobile/Media/DCIM/100APPLE.
– Аудіозаписи диктофона: private/var/mobile/Media/Recordings.
– iPhoneVideoRecorder: private/var/mobile/Mediai/PhoneVideoRecorder.
– Cycorder: private/var/mobile/Media/Videos.

Якщо ви встановили нове прошивання, то буде набагато корисніше, якщо ви настроїте телефон як новий, а відновлювати дані будете не через резервне копіювання, а вручну, щоб не залишилися баги старого прошивання. Для цього вам потрібно знати, де зберігається ваша особиста інформація:

– Контакти: private/var/mobile/Library/AddressBook (у папці два файли, потрібно зберегти обидва).
– СМС: private/var/mobile/Library/SMS.
– Пошта: private/var/mobile/Library/Mail.
– Замітки: private/var/mobile/Library/Notes.
– Календар: private /var/mobile/Library/Calendar.
– Safari (закладки й історія): private /var/mobile/Library/Safari.

– Історія дзвінків: private /var/mobile/Library/CallHistory.

Якщо ви хочете встановити на свій iPhone оффлайн карту вашого міста, то файл із ім'ям MapTiles.sqlitedb потрібно залити в директорію private/var/mobile/Library/Caches/Maps/MapTiles (у залежності від версії прошивання), а файл для пошуку вулиць Bookmarks.plist у директорію private/var/mobile/Library/Maps. Не забудьте, що перед цим потрібно хоча б раз відкрити додаток "Карти" на вашім місті.

У висновку приведемо ще кілька шляхів, які можуть вам знадобиться:

– Рингтони – private/var/stash/Ringtones.tQjbOo.
– Шпалери – private/var/stash/Wallpaper.kPDEMH.
– Файли настроювань – private/var/mobile/Library/Preferences.
– Налаштування Wi-Fi:
private/var/preferences/SystemConfigurationcom.apple.wifi.plist,
– Завантажені файли – private/var/mobile/Library/Downloads, private/var/mobile/Documents.
– Файли Кукі – private/var/root/Library/Cookies.
– MobileInstallation:
System/Library/PrivateFrameworks/MobileInstallation.framework
– Посилання "Додому" (збереження на робочий стіл) розміщаються в папці:
/private/var/mobile/Library/WebClips

Для джайлбрейкнутого телефону адреса папок буде починатися з /private/var/stash, тобто тут у джайбрейкнутому телефоні зберігаються стандартні додатки, шпалери й теми, рингтони, програми з Cydia.

Розробка структурної схем

Структурна схема розробленої системи зображена на рисунку 1. На ній показано структуру розробленого програмного забезпечення системи навігації та моніторингу файлової системи iOS.

Структурно розроблена система навігації та моніторингу файлової системи iOS складається з наступних основних блоків:

– Операційна система IOS.
– Система навігації та моніторингу файлової системи iOS.
– Пам’ять.
– Комунікації.
– Вбудовані додатки.

Операційна система IOS складається чотирьох рівнів абстракції, розглянутих нижче, а також наступних структурних блоків:

– Jailbreak – API доступу до файлової системи.
– Трьохмірний графічний інтерфейс користувача Cover Flow.
– Інтерфейс користувача Cocoa Touch з мультисенсорним екраном.
– Технологія Multitouch.

Технологія iPhone представлена у вигляді шарів. Основний шар – це Core OS. На його вершині перебуває шар Core Services. На вершині шару Core Services перебуває шар Media. І на самій вершині перебуває шар Cocoa Touch. Взагалі можна ще більше спростити цю технологію. Можна розділити й об'єднати їх в 2 шари – це шар мови C і шар Cocoa мови Objective C.

Пам’ять буває наступних видів:

– RAM.
– Flash.

Комунікації використовуються наступні:

– Wi-Fi.
– Bluetooth.
– USB 3.0.
– GSM/EDGE.

– GPS, A-GPS.

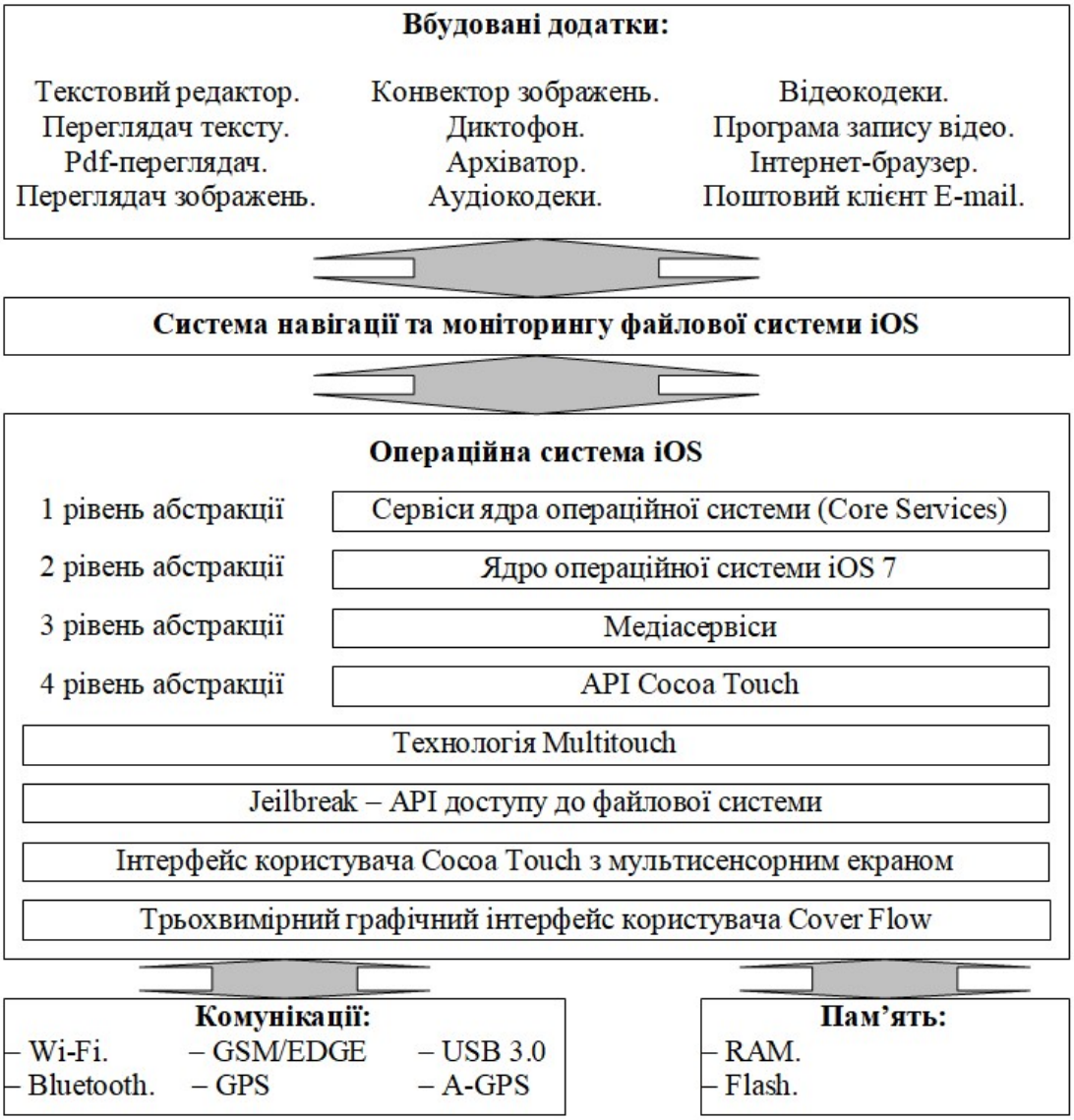

Рисунок 1 – Структурна схема системи

Джейлбрейк (злом) – це процес використання вразливостей заблокованого пристрою для встановлення програмного забезпечення, відмінного від наданого виробником цього пристрою. Джейлбрейк дозволяє власнику пристрою отримати повний доступ до операційної системи та всіх функцій. Цей процес також називається зломом, оскільки він має на увазі "звільнення користувачів з в'язниці обмежень" пристрою.

Термін «джейлбрейк» найчастіше використовується щодо iPhone, оскільки iPhone вважається «заблокованим» мобільним пристроєм з наявних на ринку. У ранніх версіях iPhone не було магазину програм, і інтерфейс iOS вважався більш обмеженим для користувачів, ніж зараз. У США перша версія iPhone була доступна тільки в мережі оператора AT&T, і користувачі, які хотіли перейти до інших операторів зв'язку, не могли цього зробити, не зламавши iPhone.

Підхід Apple до програмного забезпечення характеризується як закрита екосистема телефону, тоді як Android доступна налаштування безлічі опцій. Основна мотивація багатьох хакерів – зробити iOS більш схожим на Android. Джейлбрейк був і залишається способом встановлення додатків, не схвалених Apple, а також способом налаштування інтерфейсу.

З моменту появи термін «джейлбрейк» також використовувався для визначення адаптації коду на інших пристроях, від телефонів до ігрових консолей. Іноді він

використовується для позначення встановлення спеціального програмного забезпечення на мобільні пристрої або зняття обмежень на управління цифровими правами (DRM) для перегляду фільмів. Однак зазвичай термін "джейлбрейк" відноситься до продуктів Apple. Крім iPhone, він також застосовується до iPad та iPod Touch.

Термін "джейлбрейк" іноді використовується як синонім термінів "злом" (щодо програмного забезпечення) та "рутинг" (щодо телефонів). Рутінг можна описати як "джейлбрейк для Android", оскільки він спрямований на обхід засобів захисту, встановлених виробниками, для встановлення альтернативних мобільних операційних систем. Також часто зламують мережеві медіаплеєри Amazon Fire Stick та Roku для запуску мультимедійного програмного забезпечення замість вбудованих додатків та комутатори Nintendo для запуску емульованих ігор.

При зломі основні функції пристрою не змінюються. Зі зламаного iPhone або iPad, як і раніше, можна купувати і завантажувати програми з App Store. Однак для завантаження програм, відхилених Apple, та для використання додаткових функцій, отриманих внаслідок злому, використовуються незалежні магазини програм. Найпопулярнішим із них є Cydia – магазин для зламаних iOS-пристроїв, який зазвичай встановлюється у процесі злому.

Код злому зазвичай надається безкоштовно на форумах і сайтах спільнот зломщиків, які просувають необмежену користування пристроями. Більшість кодів злому супроводжується докладними інструкціями та інструментами застосування, але корисно мати деякі технічні знання.

Щодо джейлбрейка іноді використовуються терміни «прив'язаний» та «неприв'язаний».

– **Прив'язаний джейлбрейк** вимагає, щоб iOS-пристрій було підключено до комп'ютера під час увімкнення. Якщо не підключений до комп'ютера iPhone завантажуватиметься за допомогою спеціальної програми, він не перейде в стан злому.

– Для **відв'язаних джейлбрейків** комп'ютер не потрібен. Все необхідне переходу в стан злому міститься на iPhone. Перезавантаження без підключення до комп'ютера не впливає на джейлбрейк.

Зараз, коли програми для iPhone мають більший доступ до операційної системи, джейлбрейк став менш популярним. Оскільки Apple публічно не схвалює джейлбрейк, було впроваджено апаратні та програмні виправлення вразливостей, що використовуються під час злому. В результаті багато версій iOS не вдасться зламати швидко чи легко.

Чи легальний джейлбрейк?

Строго кажучи, джейлбрейк не є незаконним, але закони у всьому світі різняться, змінюються і часто не є однозначними, коли йдеться про джейлбрейк. Джейлбрейк або рутинг телефону є законним, якщо робиться для встановлення легально придбаних програм. Однак якщо його зроблено для встановлення незаконно придбаних додатків, то й сам процес стає незаконним.

У США джейлбрейк підпадає під дію Закону про захист авторських прав у цифрову епоху, який торкається питань авторського права на цифрові матеріали. Розділ 1201 закону забороняє обхід цифрового блокування доступу до матеріалів, захищених авторським правом, у тому числі до програмного забезпечення. Конгрес переглядає закон кожні кілька років та поступово розширює список винятків. У 2010 році дозволили зламувати телефони, у 2015 році – смарт-годинник та планшети. З того часу до списку винятків було додано більше пристроїв; список продовжує розширюватися у міру перегляду.

Закони можуть відрізнятися у різних країнах світу. У багатьох країнах Джейлбрейк ніколи не обговорювався в суді, тому точна правова позиція залишається неясною.

Хоча Apple не підтримує джейлбрейк, компанія зазвичай не загрожує застосуванням юридичних заходів до зломщиків. Apple навіть відомий своєю подякою співтовариствам, які займаються джейлбрейком, за виявлення слабких місць у системі безпеки.

Незалежно від закону, при зламі телефону гарантія анулюється, тому якщо при джейлбрейку щось піде не так, розраховувати буде нема на що. Джейлбрейк також робить пристрій схильним до цілого ряду проблем безпеки, описаних нижче.

Чи безпечний джейлбрейк?

Джейлбрейк телефону легальний, але не завжди безпечний. В результаті джейлбрейку телефону у кіберзлочинців з'являються можливості його злому.

При джейлбрейку телефону відмова від системи безпеки Apple. Програми, завантажені зі сторонніх джерел, не перевіряються в Apple App Store і тому становлять загрозу безпеці. Після джейлбрейку телефон перестане отримувати оновлення iOS, включаючи оновлення безпеки Apple, що робить його більш вразливими для загроз безпеки.

Apple вважає джейлбрейк iOS порушенням умов використання та інформує клієнтів, що це наражає телефон на наступні ризики:

- Уразливості у системі безпеки.
- Нестабільна робота.
- Можливі збої та зависання.
- Зменшення терміну служби батареї.

Тому Apple застерігає від джейлбрейків iPhone або інших пристроїв iOS. iPhone рідко заражається вірусами, але якщо це відбувається, причиною часто є злом телефону. Якщо щось трапиться з телефоном, його доведеться робити самостійно, оскільки джейлбрейк телефону анулює гарантію.

Слід враховувати, кому належить пристрій та яка інформація зберігається на телефоні. Наприклад, чи належить телефон роботодавцю? Чи синхронізується на телефоні робоча пошта? Будь-яка шкідлива діяльність ризикує не лише ваші дані, а й дані організації. Оскільки безпека зламаного телефону знижена, організація наражається на більший ризик кібератаки.

Організації, що надають співробітникам мобільні пристрої, зазвичай вживають заходів безпеки, що не дозволяють користувачам наражати на ризик дані компанії. Це може бути блокування телефону, яке дозволяє додавати або змінювати лише певні функції, підтримка пристроїв та програм в актуальному стані, встановлення агента мобільного пристрою, здатного виявити джейлбрейк.

Переваги джейлбрейку

Більше контролю за власним пристроєм

Apple прагне надати користувачам єдиний інтерфейс. Деякі користувачі вважають це обмеженням і хочуть персоналізувати свій телефон, додавши власні іконки, шпалери та меню. Джейлбрейк – це вирішення такого завдання. Після джейлбрейка ви, а не Apple або будь-хто, станете адміністратором свого пристрою з усіма відповідними правами. Наприклад, ви можете додавати іконки на домашній екран iPhone або встановлювати власні заставки. Джейлбрейк також розширює доступ до файлової системи та навіть розблокує можливість підключення інших пристроїв, що дозволяє підключити iPad до комп'ютера та забезпечує більший контроль.

Встановлення та використання неавторизованих додатків

Apple забороняє завантаження різних програм у свій магазин App Store з міркувань безпеки. Джейлбрейк дозволить встановлювати програми, яких немає в App Store. Cydia – найпопулярніший магазин програм для зламаних телефонів, до якого можна додавати неавторизовані програми, такі як ігри та мережеві інструменти. Емулятори ретро-ігор також є гарним прикладом: Apple забороняє їх завантаження до свого магазину додатків (оскільки вони дозволяють грати в старі комп'ютерні ігри, не купуючи оригінальні копії). Однак вони знаходяться у вільному доступі до Cydia.

Видалення встановлених програм

iOS не дозволяє змінювати або видаляти встановлені за промовчанням програми, такі як Apple Watch, Погода, Ігри та інші. Ці програми займають місце в пам'яті, що незручно для

людей, які не користуються ними. Джейлбрейк дозволяє видалити встановлені за промовчанням програми Apple і використовувати замість них сторонні програми. Це дозволить, наприклад, налаштувати голосовий помічник Сірі на використання Google Maps замість Apple Maps.

Доступ до додаткових функцій захисту від крадіжок

Деякі користувачі вважають, що джейлбрейк надасть їм доступ до покращених функцій захисту від крадіжки. Наприклад, у iPhone є функція «Знайти iPhone», але вона не працює, коли телефон перебуває в режимі польоту, вимкнено або не ловить мережу. Існують програми для зламаних пристроїв, які, як стверджують, працюють краще, ніж функція «Знайти iPhone», наприклад iCaughtU. Коли зловмисник вводить неправильний пароль, передня камера фотографує його та надсилає фото власнику пристрою електронною поштою.

Недоліки джейлбрейку

Припинення автоматичних оновлень

Більше не вдасться отримувати автоматичні оновлення безпосередньо від Apple. Потрібно буде чекати, поки співтовариство зломщиків виконає джейлбрейк кожної версії iOS. Злом оновлень вимагає часу, крім того, доведеться зламувати кожну версію iOS, що випускається Apple. Це означає, що оновити зламаний телефон не вдасться доти, доки не буде зламано останнє оновлення, що може статися не відразу. Виконання джейлбрейку після великих оновлень може виявитися досить проблематичним. Чи вартує джейлбрейк цих труднощів?

Неможливість інсталювати деякі програмні оновлення

Внаслідок деяких несанкціонованих змін iPhone може назавжди втратити працездатність після встановлення оновлень iOS, що постачаються Apple.

Анулювання гарантії на телефон

Apple заявляє, що несанкціонована зміна iOS є порушенням ліцензійної угоди для iOS. Через це Apple може відмовити в обслуговуванні iPhone, iPad або iPod touch, на якому встановлено неавторизоване програмне забезпечення. Таким чином, якщо в результаті джейлбрейку пристрій виявиться пошкодженим або несправним, Apple може відмовити в будь-якому сервісному ремонті.

Зменшення терміну служби батареї

Зламування програмного забезпечення може призвести до прискореної розрядки батареї, що скорочує час роботи iPhone, iPad або iPod touch від однієї зарядки акумулятора.

Телефон може «перетворитися на цеглу»

Телефон перестане завантажуватися, реагувати на команди та виконувати дзвінки – «перетвориться на цеглу». Сам собою джейлбрейк не блокує телефон, але існує ризик повної відмови функціонування телефону.

Втрата доступу до контенту та сервісу

Часто причиною злому телефону є бажання отримати доступ до більшої кількості контенту, але іноді це може виявитися неефективним, оскільки можна втратити доступ до інших сервісів, таких як iCloud, iMessage, FaceTime, Apple Pay, Погода та Stocks. Сторонні програми, які використовують сервіс Apple Push Notification, мають проблеми при отриманні повідомлень або отримують повідомлення, призначені для інших зламаних пристроїв. Інші сервіси, що використовують push-сповіщення, такі як iCloud та Exchange, стикаються з проблемами синхронізації даних з відповідними серверами. Існували повідомлення про те, що сторонні постачальники блокують зламані пристрої.

Збільшення ймовірності поломки телефону

Імовірність виходу з ладу зламаного iPhone або iPad може бути вищою. Програми, доступні для зламаних пристроїв, отримують доступ до функцій та API, недоступних для програм, схвалених Apple. Робота таких програм могла не тестуватися. Це може призвести до частих та несподіваних збоїв пристрою, збоїв та зависання вбудованих та сторонніх програм та втрати даних.

Ненадійна передача голосу та даних

Джейлбрейк може призвести до обриву дзвінків, повільних або ненадійних з'єднань для передачі даних, а також до затримок передачі даних про місцезнаходження або передачу неточних даних.

Витік даних

Сумно відомий інцидент зі зламаними пристроями стався, коли зловмисники отримали доступ до даних для входу в iCloud у 225 000 людей, які намагалися виконати джейлбрейк. Витоку сприяли вразливості системи безпеки, що утворилися в результаті джейлбрейку, що допомогло зловмисникам отримати доступ до пристроїв користувачів.

Проблеми з безпекою

Закритий характер iOS робить її однією з найбезпечніших мобільних операційних систем, оскільки забезпечується захист як особистої інформації, так і самої системи. Зламування телефону збільшує можливості зловмисників вкрасти особисту інформацію, пошкодити пристрій, атакувати мережу або впровадити шкідливі програми, шпигунські програми або віруси.

Ризики безпеки при джейлбрейку

Джейлбрейк телефону є загрозою безпеці. Джейлбрейк надає вам більше можливостей контролю над пристроєм, але також він надає більше можливостей контролю за всіма програмами, які працюють на пристрої. Найбільші загрози безпеці виникають через дозволи цим програмам запитувати root-доступ на пристрої. Якщо на пристрої встановлені шкідливі програми, вони можуть отримати доступ до root, тобто повний доступ до всіх даних на пристрої.

Під час злому порушується закрита екосистема пристрою, що забезпечується Apple для захисту користувачів від загроз безпеки. Зламані телефони набагато сприйнятливіші до вірусів і шкідливих програм, оскільки дозволяють не виконувати перевірку програм Apple, що забезпечує завантаження програм без вірусів. Джейлбрейк допускає встановлення піратських програм, що розповсюджуються безкоштовно додатків та ігор. Це означає, що довіреними стають розробники всіх додатків, що встановлюються, а не тільки розробники Apple.

Дані з банківських програм, збережені паролі та дані облікових записів соціальних мереж можуть опинитися під загрозою, якщо ця інформація стане доступною зі зламаного iPhone. Цей ризик розкрився, коли шкідлива програма для злому iOS, KeyRaider, вкрала 225 000 ідентифікаторів Apple ID та тисячі сертифікатів, закритих ключів та чеків про покупки. Внаслідок жертви повідомляли про незвичайну історію покупок додатків з боку вкрадених у них облікових записів. В інших випадках телефони жертв були заблоковані для отримання викупу.

Крім високого ризику зараження шкідливими програмами, зламані iPhone часто містять помилки, які можуть призводити до збоїв телефону та відключення важливих функцій. Зі зростанням використання смартфонів зростає і ризик мобільних злочинів. Тому важливо бути в курсі останніх загроз та шахрайських схем, а також встановлювати комплексний мобільний захист на пристрої.

Як полагодити зламаний телефон

Зламаний телефон можна відремонтувати, просто відновивши iPhone. Не потрібно вручну видаляти встановлені програми злому, оскільки в результаті з iPhone буде видалено все, і пристрій буде скинуто до заводських налаштувань Apple.

Перед початком переконайтеся, що ви здійснили повне резервне копіювання даних з iPhone або iPad. Це пов'язано з тим, що в процесі видалення джейлбрейка буде виконано повне очищення пристрою та відновлення до стандартної конфігурації. Тому необхідно заздалегідь створити резервну копію всіх файлів, які ви хочете зберегти. Найкраще зберегти файл резервної копії у двох місцях (локально та у хмарі).

Крок 1. Резервна копія в iCloud

– Підключіть iPhone, iPad або iPod touch до Wi-Fi.

– Перейдіть до меню Налаштування, виберіть [Ваше ім'я] та iCloud.

– Переконайтеся, що увімкнуто перемикач Резервна копія в iCloud.

– Натисніть кнопку Створити резервну копію та не відключайтеся від мережі Wi-Fi до завершення процесу.

Щоб перевірити хід виконання та підтвердити завершення резервного копіювання, перейдіть до меню **Налаштування**, виберіть **[Ваше ім'я]**, потім **iCloud** та **Резервна копія в iCloud.** Під кнопкою **Створити резервну копію** відображається **дата** та **час** створення останньої резервної копії.

Крок 2. Скасування джейлбрейку

1. Підключіть iPhone або iPad до комп'ютера або пристрою Mac за допомогою оригінального кабелю USB.
2. Запустіть iTunes на комп'ютері.
3. Розблокуйте пристрій та вимкніть функцію Знайти iPhone.
4. Перейдіть до меню Налаштування, виберіть [Ваше ім'я] та iCloud.
5. Переконайтеся, що перемикач Пошук iPhone вимкнено. Щоб вимкнути цю функцію, необхідно ввести Apple ID та пароль.
6. У iTunes на комп'ютері виберіть пристрій, коли він відобразиться.
7. На панелі Огляд натисніть кнопку Відновити. Запуститься процес видалення джейлбрейку.
8. Під час цієї процедури пристрій перезавантажиться. Пристрій запитає, чи потрібно відновити дані з резервної копії. Можна вибрати опцію iCloud, якщо потрібно відновити дані з файлу, створеного раніше.
9. Після завершення процесу iOS-пристрій повернеться до заводських налаштувань. З'являться стандартні кроки налаштування, які ви виконували під час першого увімкнення пристрою.

Якщо з будь-яких причин не вдається відновити зламаний iPhone, використовуйте режим відновлення, щоб видалити дані з пристрою.

На закінчення: уразливості програм на зламаних пристроях дозволяють зловмисникам легко викрадати конфіденційні дані, такі як платіжна інформація. Увага до небезпек допомагає захиститися під час роботи в інтернеті.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів навігації та моніторингу файлової системи iOS. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем навігації та моніторингу файлової системи iOS; Досліджена система навігації та моніторингу файлової системи iOS; На основі отриманих результатів досліджень створена програмна реалізація системи навігації та моніторингу файлової системи iOS. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання навігації та моніторингу файлової системи iOS. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
2. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
3. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019.

P.517-522.
4. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
5. Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P. 707-712.
6. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.701-706.
7. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
8. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
9. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
10. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
11. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
12. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
13. Смірнов, О.А., Усік П.С., Полігенько О.О., Одарченко Р.С., Терещенко Л.Ю. «Інформаційна технологія та програмне забезпечення для підвищення ефективності планування підсистеми базових станцій стільникового зв'язку». Проблеми телекомунікацій. № 1(26). С. 83-96. 2020.
14. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
15. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
16. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральноукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
17. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
18. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дрєєв О.М. Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 184-194, 2019.
19. Смірнов О.А., Котелянець В.В. Стійкі до колізій стохастичні моделі функціонування безпроводових сенсорних мереж. Вісник інженерної академії України, №3, с. 145-152, 2018
20. O. Smirnov, O. Kovalenko, A. Kovalenko, S. Smirnov, V. Vialkova. The mathematical model of the testing technology for Dom Xss vulnerabilities. Scientific & practical cyber security journal (SPCSJ) Vol 2 Issue 1, 22-28 pp. [Электронный Журнал]. Georgia. Tbilisi: SCSA – 2018.
21. Oleksii Smirnov, Oleksandr Kovalenko, Jamil Al-Azzeh, Anna Kovalenko, Serhii Smirnov. Qualitative risk analysis of software development. Asian Journal of Information Technology. – Volume 17(3). – Medwell Journals. – 2018. – P. 218-230.