Захист файлів в операційній системі Android

Куперштейн Л. М.[1], Прокопчук С. О.[2], Буда А.Г.[3]

[1]К.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна,kupershtein.lm@gmail.com
[2]студент кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, prokopchukserhii@gmail.con
[3]к.т.н., доцент кафедри екології та екологічної безпеки, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна

Анотація **–У даній роботі розробляється програмний засіб для захисту файлів в операційній системі android.Програмний засіб даватиме можливість виконати захист двома способами: шифрування виконуваних файлів і приховування від файлових менеджерів.**

Ключові слова:Android, шифрування файлу, приховування файлу, пароль, зловмисник.

File security in operation system Android

Kupershtain L. M.[1], Prokopchuk C. O.[2], Byda A.G.[3]

[1]Ph.D., associateprofessorofInformationSecurityDepartment,VinnytsiaNationalTechnicalUniversity Khmelnytskeshossestr., 95, Vinnytsia, Ukraine, kupershtein.lm@gmail.com
[2]Student, InformationSecurityDepartment, VinnytsiaNationalTechnicalUniversity Khmelnytskeshossestr., 95, Vinnytsia, Ukraine, prokopchukserhii@gmail.com
[3]Ph.D., associateprofessorofEcologyandEnvironmentalSafety,VinnytsiaNationalTechnicalUniversity Khmelnytskeshossestr., 95, Vinnytsia, Ukraine

Abstract **–Application to protect file system in android.Application make it possible to perform protection in two ways: Encrypt and hide executable files from file managers.**

Keywords: Android, file encryption, information security,hidefiles, password, wrecker.

ВСТУП

Розвиток технологій дійшов до того, що мобільні пристрої дають змогу вміщати в собі великі обсяги пам'яті та працювати з доволі великою продуктивністю. В даний час мобільний пристрій стає все більш в центрі вашої роботи і життя та дають змогу вільно працювати з файлами різних типів. На більшості підприємств, як малих так і великих для роботи використовують планшети. Вони зручні для роботи і їх можна завжди носити з собою. Звичайно, це означає, що мобільні пристрої використовується для доступу до конфіденційної інформації.Також велика ймовірність того, що мобільний пристрій може бути викрадений зловмисником або переглянутий допитливим співробітником.Тому виникає потреба у захисті важливих файлів на мобільних пристроях [1].

ПРИХОВУВАННЯ ФАЙЛІВ

Операційні системи Android є аналогом Linux, тому методи приховування файлів та папок, що реалізовані у файлових менеджерах повинні спрацювати на Android. Приховування можна виконати двома способами [2].

Перший спосіб присвячений приховуванню папок. Потрібно просто при створенні нової папки поставити символ "." перед її іменем. Ця крапка в основному говорить Androidпро те, що потрібно забути цю папку і переглядати її вміст. Це означає, що файли які знаходяться в папці не будуть відображатись в галереї, мультимедійних програвачах, поштових клієнтах, офісних редакторах тощо.

Другий спосіб присвячений приховуванню мультимедійних даних в рамках вже існуючих папок шляхом створення .nomediaфайлу в середині них. Цей файл не матиме розширення або якогось вмісту. Це просто порожній файл який називається ".nomedia". Наявність такого файлу говорить операційній системі Androidне відображати всі файли (фотографії і відео) для будь-якої програми, яка намагатиметься взаємодіяти з ними.

Ці два методи доволі прості в реалізації і допоможуть надійно приховати файли з конфіденційною інформацією від зловмисниківале не від досвідчених користувачів. Якщо надати мобільному пристрою root-права, то це дасть змогу користуватися програмними засобами, які надають доступ до прихованих файлів.

Тому доцільно додати шифрування файлів, як одного з додаткових рівнів захисту на випадок

знаходження зловмисником прихованих файлів та папок.

ЗАХИСТ ФАЙЛІВ ШИФРУВАННЯМ

Пропонується виконувати шифрування з закритим ключем. Найбільш стійкими протоколами шифрування з закритим ключем є: AES таDES [3].

DES є блочним шифром - дані шифруються блоками по 64 біти - 64 бітний блок тексту подається на вхід алгоритму, а 64-бітний блок шифрограми отримується в результаті роботи алгоритму. Ключем може бути довільна 64-бітна комбінація, яка може бути змінена у будь-який момент часу. Частина цих комбінацій вважається слабкими ключами, оскільки може бути легко визначена. Безпечність алгоритму базується на безпечності ключа[4].

AES— симетричний алгоритм блочного шифрування. Вважається, що використовується в AES ключ довжиною в 128 біт - досить надійний захист проти лобової атаки, тобто з математичної точки зору підібрати пароль важко. Незважаючи навіть на деякі недоліки AES, зламати захищену за допомогою цього алгоритму інформацію практично нереально [5].

В роботі пропонується виконувати шифрування бітового масиву введеним з клавіатури секретним ключем. Такий метод менш надійний,ніж шифри AESта DES, але він переважає над ними своїм часом виконання та апаратною складністю.Довжина ключа повинна бути в діапазоні 8-32 символи. Для ключа можна використовувати символи, літери та цифри клавіатури мобільного пристрою. Використання символів для паролю є дещо не стандартним для паролів та секретних ключів, тому збільшить складність зламу. Також при спробі підібрати значення ключа значно збільшиться кількість можливих варіантів.

ПРОГРАМНА РЕАЛІЗАЦІЯ

Програмний засіб розроблений в середовищі AndroidStudio. Середовище розробки адаптоване для виконання типових завдань, що вирішуються в процесі розробки застосунків для платформи Android.У тому числі у середовище включені засоби для спрощення тестування програм на сумісність з різними версіями платформи та інструменти для проектування застосунків, що працюють на пристроях з екранами різної роздільної здатності[6].

Програмний засіб включає в себе два модулі: hide і lock. Модуль hide виконує функцію приховування файлів та папоквід зловмисниківметодами додавання до імені символу “.” таперейменування медіа файлів в “nomedia”. Модуль lockвиконує функцію шифрування файлів з використанням секретного ключа введеного з клавіатури.Робота з програмним засобом починається з вибору файлу будь-якого типу, розширення та розміру із наступним введеннямсекретного ключа.

За допомогою модуля hidevиконується приховування файлу від файлових менеджерів, галерей та медіа-програвачів.

За допомогою модуля lockпрограмний засіб шифрує обраний файл. Введений ключ перетворюється в бітове значення. Обраний файл перетворюється в бітовий масив. Бітовий масив файлу ділиться на блоки по 1024 біти і для виконання шифрування до кожного елементу блоку додається бітове значення секретного ключа. Після шифрування кожного елементу, кожен з них записується у новий масив.Після завершення шифрування останнього блоку зашифровані дані перезаписуються в файлз такою ж назвою і типом. Так як в блоки бітового масиву було додане ще одне значення, то старий вміст файлу повністю заміниться на не зрозумілий для сторонніх осіб набір символів.

Таким чином програмний засіб зможе надавати два рівні захисту файлів та папок на мобільних пристроях, що забезпечуватиме більший захист.

ВИСНОВКИ

Досліджено методи приховування файлів від зловмисників в операційній системі Android. Для збільшення рівня захисту пропонується використовувати шифрування бітового масиву файлів з використанням ключів, що дозволить підвищити рівень захищеності даних на мобільних пристроях.

ЛІТЕРАТУРА REFERENCES

[1] Howto: Androidfileencryption. [Electronic resource]. – Access to resources: https://www.sookasa.com/resources/Android-file-encryption/ – name from screen.

[2] HowtohidefilesandfoldersonAndroidwithoutinstallingparanoid apps. [Electronic resource]. – Access to resources:http://www.phonearena.com/news/How-to-hide-files-and-folders-on-Android-without-installing-paranoid-apps_id57615 – name from screen.

[3] The story of Android, cryptography and a crippled 3DES [Electronic resource]. – Access to resources: http://blog.kotowicz.net/2010/09/story-of-android-cryptography-and.html – name from screen.

[4] Стандарт шифрування даних DES. [Електронний ресурс]. – Доступ до ресурсу: http://lib.mdpu.org.ua/e-book/kruptologiya/lect6.html – назва з екрану.

[5] Алгоритм шифрования AES. [Электронный ресурс]. – Доступ к ресурсу: http://www.opengsm.ru/blog/algoritm-shifrovaniya-aes/ – название с экрана.

[6] Знакомство с AndroidStudio. [Электронный ресурс]. – Доступ к ресурсу: http://startandroid.ru/ru/articles/listofarticles/284-znakomstvo-s-android-studio.html– название с экрана.