

МЕТОД АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ANDROID

Вінницький національний технічний університет

Анотація

Проаналізовано найпоширеніші методи автентифікації користувачів в ОС Android. Проведено аналіз переваг та недоліків кожного з методів, а також запропоновано власний метод автентифікації користувачів в ОС Android.

Ключові слова: ОС Android, автентифікація, символічний пароль, біометрична автентифікація, графічний пароль.

Abstract

This research paper describes a common user authentication methods in the Android OS. An analysis of the advantages and disadvantages of each method, as well as offer their own user authentication method on the Android OS.

Key words: Android OS, authentication, character password, biometric techniques, graphical password.

Вступ

Наразі все більше людей не може уявити свого життя без смартфона або планшета під рукою. А найпоширенішою операційною системою для смартфонів є Android [2].

Слід відзначити, що більшість смартфонів стали носіями конфіденційної інформації, важливих персональних або корпоративних даних. Разом з тим варто зазначити, що за допомогою смартфона легко отримати доступ до електронної пошти. Також за допомогою телефону власник може легко отримати доступ до своїх облікових записів в соціальних мережах таких як ВКонтакте, facebook, twitter, Instagram. А отже, всі ці дані повинні бути добре захищеними.

Захист цих даних може забезпечити процедура автентифікації. Існує низка методів автентифікації в ОС Android, які різняться своєю складністю, надійністю, вартістю та іншими показниками, однак їх спільним слабким місцем є те, що вони мають стандартний тип визначення факторів автентифікації, що породжує стандартні підходи до їх зламу.

Метою роботи є покращення системи автентифікації в ОС Android [1]. Виходячи з мети роботи, можна сформулювати низку задач, які необхідно розв'язати для її досягнення, а саме:

- Аналіз сучасних методів автентифікації користувачів в ОС Android
- Розробка власного методу автентифікації.

Аналіз відомих методів автентифікації

Серед вже відомих методів автентифікації найпоширенішими є символічні паролі, графічні паролі та біометричні паролі [4]. Кожний з цих методів має свої переваги та недоліки. Найбільшим недоліком символічних та графічних паролів є можливість підглядання їх під час введення, а також те, що більшість людей використовує занадто легкі паролі [2]. Біометричні паролі є більш надійними але вони потребують великих витрат на пристрої для введення біометричної інформації [3].

Проаналізувавши недоліки вже відомих методів автентифікації запропоновано власний алгоритм автентифікації користувачів в ОС Android. Представлений метод за об'єктом автентифікації базується на основі знання чого-небудь.

Суть метода полягає в тому, що користувач повинен буде розв'язати деякий елементарний математичний приклад. Але не знаючи алгоритму, знайти правильну відповідь буде майже складно. Даний метод дозволить збільшити час зламу автентифікаційних даних, не вимагаючи додаткових витрат апаратури, а також забезпечить захист від підглядання під час введення.

Алгоритм власного методу автентифікації

Оскільки всі вищеперераховані методи автентифікації в ОС Android мають низку недоліків, які суттєво впливають на захищеність даних користувачів, доцільно буде розробити власний метод автентифікації з урахуванням проаналізованих переваг та недоліків.

Нехай $\{a, b, c, d\}$ – множина випадкових цілих чисел; $\{+, -, /, *\}$ – множина можливих операцій над числами. Особливість методу полягає в тому, що оператори будуть виконувати невластиві їм операції, а будь-які інші, які користувач обиратиме сам. Також слід зазначити, що всі операції виконуватимуться послідовно, без будь-яких пріоритетів.

Наприклад нехай $+$ - виконуватиме операцію множення, $-$ - операцію ділення, $*$ - операцію додавання, $/$ - операцію віднімання, тоді приклад $(34-17*5/6+2)$ буде дорівнювати не 22, а 2. Адже насправді послідовно виконуватимуться такі дії $34/17+5-6*2$.

Даний метод автентифікації вирішує проблему підглядання пароля під час введення, притаманну символьним і графічним паролем. Адже внаслідок того, що числа випадкові, результат завжди буде різним.

Висновок

Таким чином, в результаті виконання роботи було проаналізовано відомі методи автентифікації користувачів в ОС Android, а також запропоновано власний метод, який має низку переваг над іншими методами автентифікації. Перевагою даного метода є також те, що він не потребує додаткових пристроїв, а отже вирішує головний недолік біометричних методів – високі витрати на реалізацію.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи/ Укладачі: А. О. Азарова, В. В. Карпінєць. – Вінниця: ВНТУ, 2013. – 44 с.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.
3. Графические пароли так же предсказуемы, как и пароли «1234567» и «password» [Електронний ресурс]. – Режим доступу: URL: <https://haker.ru/2015/08/21/alp-stat/> – Назва з екрану.
4. Методи автентифікації користувачів інформаційно-комунікаційних систем [Електронний ресурс]. – Режим доступу: URL: <http://www.stattionline.org.ua/vornka/44/5279> – Назва з екрану.

Вітович Максим Миколайович – студент групи БС-146, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vitovivh.max.1997@gmail.com.

Науковий керівник: **Юрій Володимирович Баришев** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна.

Maxim M. Vitovych – Department of Information Technology and Computer Engineering, Vinnytsia National Technical Univesity, Vinnytsia, email : vitovivh.max.1997@gmail.com

Supervisor: **Yurii Baryshev** – Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine.