МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXIII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

20-21 квітня 2023 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р**.** - Одеса, Видавництво ОНТУ, 2023 р. – 449 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області IT, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямами і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Редактор збірника Котлик С.В.

© Одеський національний технологічний університет

діляться. OSINT, за умови ефективного використання, може скомпрометувати внутрішні мережі персоналу, надаючи червоним командам і чорним капелюхам доступ до особистих даних тих, хто може бути потенційною ціллю. Оскільки OSINT допомагає зібрати відповідні цільові дані, фішингова атака, створена за допомогою OSINT, повинна мати ефективніші результати.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] F. Ansari, M. Akhlaq, A. Rauf, *Social networks and web security: Implications on open source intelligence*, 2nd National Conference on Information Assurance (NCIA), 2013, С. 79-82.
[2] B. J. Koops, J. H. Hoepman, R. Leenes, *Open-source intelligence and privacy by design*, Computer Law & Security Review, №. 6, 2013, С. 676-688.
[3] F. Tabatabaei, D. Wells, *OSINT in the Context of Cyber-Security*, Open Source Intelligence Investigation: From Strategy to Implementation, 2016, С. 213-231.

УДК 004.89: 004.3

ДОСЛІДЖЕННЯ ФАКТОРІВ ВПЛИВУ НА БЕЗПЕКУ МОБІЛЬНИХ ЗАСТОСУНКІВ НА ПРИКЛАДІ КЛІЄНТСЬКОЇ ЧАСТИНИ КІБЕРФІЗИЧНОЇ СИСТЕМИ РОЗУМНОЇ ПАРКОВКИ

ПАВЛОВА О.О.(pavlovao@khmnu.edu.ua), **АВСІЄВИЧ В.Р.** (kovalleonid4@gmail.com)
КУЗЬМІН А.А.(andriy1731@gmail.com)
Хмельницький національний університет

Розглянуто фактори, які впливають на безпеку мобільних застосунків на прикладі клієнтської частини кіберфізичної систем розумної парковки. На основі проведеного аналізу запропоновано способи їх усунення, одним з найефективніших є додавання проміжного програмного забезпечення (middleware) для перевірки запитів від клієнта до сервера.

Зараз ми не можемо уявити наше повсякденне життя без смартфона та численних додатків, які ми використовуємо для різних цілей. Сьогодні люди все більше покладаються на мобільні додатки для всіх аспектів свого життя та використовують їх безліч разів на день. Apple App Store і Google Play Store пропонують більше 8 мільйонів різних програм. Але ми не можемо бути впевнені, що програма надійшла з авторитетного джерела та що вона абсолютно безпечна. За статистикою [1] лише на початок 2018 року було зафіксовано 312 випадків уразливості додатків Android і 87 випадків уразливості додатків iOS. Відповідно до порівняльного тестування NowSecure [2], 85% досліджуваних програм мали одну або більше загроз безпеці. Понад 50% досліджених програм мали вузькі місця, які призводили до проблем захисту даних під час передачі. Близько третини протестованих програм мали проблеми з вихідним кодом. Зокрема, програми Android мали проблеми з кодом, які могли призвести до зворотного проектування та інших загроз. Відповідно до [3], коли йдеться про безпеку мобільних додатків, основні проблеми, які найчастіше виникають, це неправильне використання платформи, незахищене зберігання даних, незахищений зв’язок клієнт-сервер, незахищена автентифікація, незахищена авторизація, недостатнє шифрування даних, низька якість коду, підробка коду, ризик зворотного проектування та сторонні функції. Частота впливу цих прецедентів на безпеку мобільних додатків показана на рисунку 1.

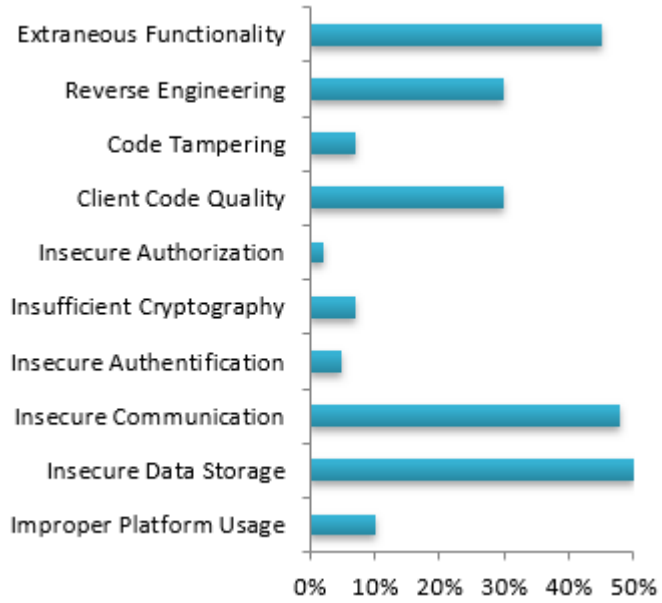

Рисунок 1 – Частота прояву факторів, що впливають на безпеку мобільних додатків [3]

Попередньо у [4] була представлена схема роботи кібезфізичної системи для розумної парковки та концепція інтерфейсу користувача для клієнтської частини пропонованої системи у вигляді мобільного застосунку. Тому дослідження факторів, які впливають на безпеку мобільних застосунків наразі є актуальним завданням.

Залежність безпеки кіберфізичної системи розумного паркування можна відобразити у вигляді кортежу факторів, які впливають на безпеку клієнтської частини у вигляді мобільного застосунку:

$$Csec =< ef, re, ct, ccq, ia, ic, iac, icm, ids, ipu >,$$

де $ef -$ ризик стороннього функціоналу; $re -$ зворотнє проектування; $ct -$ крадіжка коду; $ccq -$ якість коду; ia – незахищена авторизація; $ic -$ недостатнє шифрування; $iac -$ незахищена аутентифікація; $icm -$ незахищене клієнт-серверне з'єднання; $ids -$ незахищене сховище даних; $ipu -$ неправильне використання платформи.

Було проаналізовано вплив факторів, зазначених на рисунку 1, на прикладі реальних випадків використання мобільних додатків мільйонами користувачів та наслідків, до яких призвела дія вищезазначених факторів. За результатами дослідження, було визначено множину наслідків, до яких призводять вказані вище фактори. Наслідки, які можуть бути спричинені цими факторами, зображені у вигляді діаграми на рисунку 2.

Рисунок 2 – Наслідки незахищеності мобільних додатків

У ході дослідження було виявлено, що один фактор може спричиняти декілька наслідків, так само як один наслідок може бути спричинений декількома факторами. Тому напрямками подальших досліджень є аналіз кореляції факторів, які впливають на безпеку мобільних застосунків та наслідків, до яких вони призводять для розробки ефективних методів підвищення безпеки мобільних застосунків.

Список використаних джерел:

1.CVEdetails.com the ultimate security vulnerability data source URL: https://www.cvedetails.com/ (Доступ 11.03.2023)

2.A decade in, how safe are your iOS and Android apps? URL: https://www.nowsecure.com/blog/2018/07/11/a-decade-in-how-safe-are-your-ios-and-android-apps/(Доступ 11.03.2023)

3.Understanding OWASP Mobile Top 10 Risks with Real-world Cases URL: https://appinventiv.com/blog/owasp-mobile-top-10-real-world-cases/(Доступ 11.03.2023)

4. Авсієвич В., Кузьмін А. Дослідження вразливостей системи розумної парковки та способи їх усунення. Актуальні Проблеми Комп'ютерних Наук (АПКН-2022), Хмельницький, Україна, 18-19 листопада 2022. Хмельницький: ХНУ, 2022. С. 11-14.

ПАРСИНГ ТЕКСТУ: ВИКОРИСТАННЯ ПОТУЖНОСТЕЙ NLP ЗАДЛЯ ПІДВИЩЕННЯ ТОЧНОСТІ ОТРИМУВАНИХ РЕЗУЛЬТАТІВ

ПЕЛОВИЧ Д. В, СМИШ О. Р.

Національний університет «Києво-Могилянська академія

Аналіз текстів судових рішень (далі — СР) є невіддільною частиною процесів оцінювання якості, ефективності та прозорості судочинної системи України — за різними параметрами. Утім, тексти СР, як і будь-яких інших правових документів, є доволі специфічними для сприйняття. У таких документах використовуються спеціалізована лексика й терміни, складні синтаксичні структури, а також існує певний стандарт в оформленні змісту, який є відмінним від звичних. Ці фактори ускладнюють мануальний процес аналізу подібних текстів. Наразі найбільш поширеним способом отримання сирих текстів СР з бази ЄДРСР [1] є відкритий офіційний ресурс ЄДРСР ДСАУ [2] (релевантні пошукові запити, що стосуються СР, надають попередньо згаданий ресурс першим у вибірці, що свідчить про його популярність).

Парсинг [3], як інструмент аналізу, може запропонувати можливість вичленення інформації з СР та подальше формування з неї певної уніфікованої структури (напр., у форматі JSON чи XML) задля отримання потрібної інформації з СР. Для *парсингу* використовуються різні підходи. Одним із таких підходів є *rule-based approach* [4], який орієнтується на певні закономірності в розташуванні слів у тексті, граматику тощо. Зазвичай, такі правила визначаються людьми емпірично після попереднього огляду певної вибірки текстів. У цьому випадку, проблема полягає в тому, що практично неможливо передбачити всі можливі комбінації розташування слів у реченні, словоформи, граматичні складові тощо. Цей чинник безпосередньо впливає на отримувані результати *парсингу* — менша кількість і досконалість визначених правил дає зменшення точності результатів.

З метою вдосконалення програми задля збільшення відсотка випадків отримування коректних результатів, пропонується інтеграція NLP [5]. Natural Language Processing (далі — NLP) передбачає розробку алгоритмів і обчислювальних моделей, які можуть обробляти, розуміти та відтворювати природну людську мову. NLP має широкий спектр застосування. Розглянемо саме такі субкатегорії NLP, як Named Entity Recognition (далі — NER) і Grammatical Tokenization and Tagging (далі — GTT).