МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

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

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина І.

Одеса

21-22 квітня 2020 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Частина І. Одеса, 21-22 квітня 2020 р. - Одеса, Видавництво ОНАХТ, 2020 р. - 240 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані по секціях кафедри інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

СЕКЦІЯ № 1

Комп'ютерні науки

Тематичні напрями:

МАТЕМАТИЧНЕ І КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СКЛАДНИХ ПРОЦЕСІВ

УПРАВЛІННЯ, ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНИХ КОМПЛЕКСІВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

ОДЕСЬКОЇ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ХАРЧОВИХ ТЕХНОЛОГІЙ

Список
скорочень організацій, представники яких взяли участь у конференції

Таблиця 1

Скорочення	Повна назва організації
АУПРБ	Академия управления при Президенте Республики Беларусь
БГЄУ	Белорусский государственный экономический университет
ВНТУ	Вінницький національний технічний університет
ДДПУ	ДВНЗ «Донбаський державний педагогічний університет»
УДХТУ	ДВНЗ «Український державний хіміко-технологічний університет»
ДДТУ	Дніпровський державний технічний університет
ДДМА	Донбаська державна машинобудівна академія
ДНТУ	Донецький національний технічний університет
ДНУ	Донецький національний університет ім. Василя Стуса
ІФНТУНГ	Івано-Франківський національний технічний університет нафти і газу
ІІТЗН	Інститут інформаційних технологій і засобів навчання НАПН України
ІТТНАН	Інститут технічної теплофізики НАН України
КНУ	Київський національний університет імені Тараса Шевченка
НТУУ "КПІ"	Національний технічний університет «Київський політехнічний інститут»
КПАІТ	Коледж промислової автоматики та інформаційних технологій ОНАХТ
КДПУ	Криворізький державний педагогічний університет
НУ"ПП"	Національний університет «Полтавська політехніка імені Юрія Кондратюка»
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"
ОНПУ	Одеський національний педагогічний університет ім.Ушінского
ОНАХТ	Одеська національна академія харчових технологій
ОНПУ	Одеський національний політехнічний університет
ОНУ	Одеський національний університет імені І. І. Мечникова
ПДАТУ	Подільський державний аграрно-технічний університет
РДГУ	Рівненський державний гуманітарний університет
СКХП	Сумський коледж харчової промисловості НУХТ
ТЛіАЛ	Технічний ліцей імені Анатолія Лигуна, Національний технічний університет «Дніпровська політехніка»
УАД	Українська академія друкарства
УДПУ	Уманський державний педагогічний університет імені Павла Тичини
ХНУ	Хмельницький Національний Університет
ХНУРЕ	Харківський національний університет радіоелектроніки
ЦУНТУ	Центральноукраїнський національний технічний університет
ЧНУ	Чорноморський національний університет ім. Петра Могили
IAE	Institute of Automation and Electrometry of the Siberian Branch Russian Academy
VNTU	Vinnytsia National Technical University

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ANDROID

Деревінський Ю.В., магістрант, науковий керівник – Бобровнікова К.Ю., к.т.н.
Хмельницький національний університет, м. Хмельницький

Останнім часом зловмисне програмне забезпечення (ЗПЗ), таке як бекдори, шпигунське програмне забезпечення, дроппери, криптомайнери, банківські трояни, орієнтовані на мобільні пристрої, стають все більш актуальною загрозою [1]. При цьому застосовуються як нові методи інфікування мобільних пристроїв (наприклад, перехоплення DNS), так і перевірені схеми розповсюдження (наприклад, SMS-спам). Тим часом Android залишається найбільш популярною мобільною операційною системою для користувачів мобільних пристроїв [1].

Сьогодні в наукових джерелах широко представлені різноманітні підходи до виявлення ЗПЗ для Android. В [2] представлено підхід виявлення ЗПЗ, який класифікує шкідливі програми на основі зворотного зв'язку з користувачами мобільних програм. Однак у випадку чутливих мобільних ресурсів, які потребують значної частини дозволів, підхід може призвести до збільшення кількості хибних тривог. В [3] запропоновано підхід, який для виявлення ЗПЗ використовує комбінацію дозволів та намірів, доповнених декількома етапами класифікаторів. Таблиці рішень, багатошаровий персептрон та дерева рішень об'єднані за допомогою трьох схем: визначення середнього значення ймовірностей, добутку ймовірностей та більшості голосів.

У роботі [4] запропоновано метод виявлення ЗПЗ на основі аналізу журналів системних викликів. Результати експериментів показали високу точність виявлення, проте автори не врахували здатність деяких додатків ідентифікувати середовище типу пісочниці. В [5] запропонована система виявлення ЗПЗ, яка використовує глибоку згорткову нейронну мережу (CNN). Класифікація ЗПЗ проводиться на основі статичного аналізу необробленої послідовності коду з дизасембльованої програми. В [6] запропоновано підхід виявлення ЗПЗ, який для формування векторної моделі використовує набір ознак, таких як апаратне забезпечення, дозволи, компоненти додатку, відфільтровані наміри, опкоди та рядки, що витягуються із зразків додатків. Працездатність підходу аналізується за допомогою таких класифікаторів, як випадковий ліс, ліс, що обертається, метод опорних векторів (SVM).

В [7] автори пропонують систему на основі статичного аналізу, яка функціонує в чотири етапи. Спочатку вона будує граф викликів для кожної програми, потім отримує послідовності API-викликів, використовуючи всі

унікальні вузли, після чого відносить кожен виклик до певного класу, пакету чи сімейства. Третій етап передбачає моделювання поведінки кожного додатку шляхом побудови ланцюгів Маркова з послідовностей API-викликів, при цьому ймовірності переходу, використовувані як вектор ознак, надають можливість класифікувати додаток як доброякісне або зловмисне програмне забезпечення.

В [8] розроблений фреймворк, який для ранжування додатків з урахуванням їх потенційного ризику використовує тріаж. Підхід поєднує ймовірнісну модель для прогнозування існування інформаційних потоків із показником того, наскільки значний потік у доброякісних та шкідливих додатках. Результати експериментів показують, що підхід здатний досить точно передбачити наявність інформаційних потоків і забезпечує значну економію ресурсів.

Огляд літератури показав, що проблема виявлення зловмисного програмного забезпечення для Android є надзвичайно актуальною. Згадані вище методи виявлення ЗПЗ в мобільних пристроях показали високий рівень ефективності, але також демонструють високий показник хибних спрацювань. Загальною слабкістю вищезазначених підходів є потреба у великих обсягах обчислювальних ресурсів та те, що вони не здатні адаптивно реагувати на відомі та невідомі атаки, здійснені ЗПЗ на мобільні пристрої. Також розглянуті підходи мають деякі загальні недоліки, які полягають в ігноруванні упакованого ЗПЗ та неможливості захистити пристрій від загроз нульового дня і зловмисних програм, здатних модифікувати себе.

Список літератури

12. McAfee Mobile Threat Report Q1, 2020. [Електронний ресурс] – Режим доступу: https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf. – 9.12.2019 р.

13. Amro, B. Personal Mobile Malware Guard PMMG: a mobile malware detection technique based on user's preferences / B. Amro. – International Journal of Computer Science and Network Security, 2018. – Vol. 18, No. 1. – pp. 18–24.

14. Idrees, F. Pindroid: a novel android malware detection system using ensemble learning methods / F. Idrees, M. Rajarajan, M. Conti, T. Chen, Y. Rahulamathavan. – Computers & Security, 2017. – Vol. 68. – pp. 36–46.

15. Chaba, S. Malware Detection Approach for Android systems Using System Call Logs / S. Chaba, R. Kumar, R. Pant, M. Dave. – arXiv preprint arXiv:1709.0880, 2017.

16. McLaughlin, N. Deep android malware detection / N. McLaughlin, J. Martinez del Rincon, B. Kang. – Proc. of the Seventh ACM on Conference on Data and Application Security and Privacy, 2017. – pp. 301–308.

17. Varsha, M. Identification of malicious android app using manifest and opcode features / M. Varsha, P. Vinod, K. Dhanya. – Journal of Computer Virology and Hacking Techniques, 2016. – Vol. 13, Issue 2. – pp. 125–138.

18. Mariconti, E. MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Model / E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro. – ACM Trans. Priv. Sec., 2019. – Vol. 1, No. 1. – pp. 1–33.

19. Mirzaei, O. Triflow: Triaging android applications using speculative information flows / O. Mirzaei, G. Suarez-Tangil, J. Tapiador, J. M.de Fuentes. – Proc. of the 2017 ACM on Asia Con-ference on Computer and Communications Security, 2017. – pp. 640-651.

ВИБІР СПОСОБУ ТЕСТУВАННЯ ВІДПОВІДНО ДО ОСОБЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Джус І. А., студентка, Вовк Р. Б., к.т.н., доцент
Івано-Франківський національний технічний університет нафти і газу

З швидким розвитком галузі інформаційних технологій невпинно зростає інтеграція продуктів програмного забезпечення (ПЗ) у такі сфери, як наука, медицина, економіка, бізнес, мистецтво та інші. Швидкі темпи розвитку технологій та конкуренція на ринку ПЗ провокують скорочення термінів на такі етапи процесу розробки, як проектування, дизайн і тестування. Але саме вони відіграють не менш важливу роль, ніж сама розробка. В той же час нехтування якісним тестуванням може призвести до значних фінансових затрат на етапі впровадження програмного продукту. Відомо, що одним із принципів тестування ПЗ є термін, що "вичерпне тестування системи неможливе" [1], а тому для кожного програмного продукту необхідно підбирати таку концепцію, яка б забезпечила максимальну якість та оптимізацію ресурсів, витрачених на розробку в цілому. В той же час вибір концепції тестування ПЗ залежить від призначення, обсягу, факторів ризику та його архітектури.

Відповідно до степені знання тестувальником структури програмного продукту виділяють три типи тестування [1]:

1. Тестування "чорного ящика" (black-box testing), при якому тестувальник взаємодіє безпосередньо з системою через її інтерфейс, не знаючи внутрішньої структури системи, її компонентів та зв'язків між ними;

2. Тестування "білого ящика" (white-box testing), за яким відома внутрішня структура системи, що безпосередньо підлягає тестуванню. Тестувальником у цьому випадку виступає розробник, який відповідає за імплементацію певного функціоналу;

3. Тестування "сірого ящика" (grey-box testing) є поєднанням двох попередніх типів, при частково відомій внутрішній структурі, чи, до прикладу, наявності доступу під час тестування до бази даних та проведення певних операцій з нею.

За базовою моделлю тестування програмного забезпечення виділяють чотири рівні тестування [1]:

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

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

ОДЕСА
21-22 квітня 2020 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Артеменко С.В., Ольшевська О.В.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.