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.

7. Порівняльний аналіз сучасних шляхів діагностики складних технічних виробничих систем. **Лактіонов О.** (Національний університет «Полтавська політехніка)	93
8. Optimization of paths, taking into account the significance of intermediate points. **Мазурок І.Є., Веремйов К.В.** (Одеський національний університет ім. Мечникова)	95
9. Методика навчання фахівців із інформаційної безпеки соціальної інженерії з використанням OSINT і мови SIEVE. **Миронов І. В., Болтач С. В.** (Одеський національний технологічний університет)	97
10. Дослідження факторів впливу на безпеку мобільних застосунків на прикладі клієнтської частини кіберфізичної системи розумної парковки. **Павлова О.О., Авсієвич В.Р., Кузьмін А.А.** (Хмельницький національний університет)	98
11. Парсинг тексту: використання потужностей NLP задля підвищення точності отримуваних даних. **Пелович Д. В., Смиш О. Р.** (Національний університет «Києво-Могилянська академія»)	100
12. Захист підприємств від кібератак на корпоративні мережі. **Петрук Д. С.** (Волинський національни університет імені Лесі Українки)	102
13. Використання мобільних застосунків у роботі з документацією ТОВ "Аграна Фрут Україна". **Погоріла Ю. В.** (Донецький національний університет імені Василя Стуса)	103
14. Технологія HDR у моніторах. **Романюк О. Н., Захарчук М. Д., Романюк О.В., Коробейнікова Т. І.** (Вінницький національний технічний університет, Національний університет «Львівська політехніка»)	105
15. Проєктування інформаційної системи управління сегрегаційним комплексом збору відходів оперативної поліграфії. **Сторожук Д.І.** (Українська академія друкарства)	107
16. Дослідження методів перетворення повідомлень у бортових автомобільних системах. **Чайковський О.Р., Селіванова А.В.** (Одеський національний технологічний університет)	109
17. Процес безпечної передачі інформації у мобільному додатку “Студент ЧДТУ” з Використанням Spring Security на основі JWT. **Куницька С.Ю., Архіпов М.О., Чоповенко В.М.** (Черкаський державний технологічний університет)	110
18. Захист даних та вихідних файлів від несанкціонованого доступу та копіювання комп’ютерних відеоігор. **Шаповал В.В.** (Київський національний університет імені Тараса Шевченка)	112
19. Програмне забезпечення для забезпечення безпеки резервного архівування даних у хмарних системах. **Шевчук Р.П., Заріцький О.І.** (Західноукраїнський національний університет)	114
20. Вплив війни в Україні на кібербезпеку. **Шередега Р.О., Бутенко Т.А.** (Харківський державний біотехнологічний університет)	116
21. Дослідження застосування стандартів PAPERLESS у закладах вищої освіти. **Чіклікчі О.С., Лукашенко Д.О., Ольшевська О.В.** (Одеський національний технологічний університет)	117
22. 3-D візуалізація авторадіограмм радіоактивних частинок. **Новіков А.М.** (Інститут проблем безпеки атомних електростанцій Національної академії наук України)	119
Розділ 3: Нові інформаційні технології в освіті	121
1. Development of a methodology for evaluating the efficiency of ship operator model. **Nosov P.S., Masonkova M.M., Diahyleva P.S., Solovey O.S.** (Херсонська державна морська академія)	121
2. Optimization of management processes for maritime transport personnel qualification. **Nosov P.S., Ponomaryova V.P., Diahyleva O.S., Ben A.P.** (Херсонська державна морська академія)	123
3. Using SolidWorks in modern education and science. **Rudyk O.Yu., Baranov I.I., Gereta M.M., Dytynyuk V.O., Fedoryshyn S.I.** (Хмельницький національний університет)	125

УДК 004.056

МЕТОДИКА НАВЧАННЯ ФАХІВЦІВ ІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ З ВИКОРИСТАННЯМ OSINT І МОВИ SIEVE

МИРОНОВ І. В., БОЛТАЧ С. В.
(boltach.svetlana@gmail.com)
Одеський національний технологічний університет

В тезах розглядаються можливі вразливості систем та інструменти, що допомагають їх визначити. Особлива увага приділяється атакам в соціальній інженерії для оцінки безпеки. Серед інструментів виділяється OSINT, що передбачає збір, аналіз і використання даних із відкритих джерел для розвідувальних цілей. Фішингові атаки створені за допомогою OSINT мають ефективніші результати та можуть бути використані для навчання фахівців з інформаційної безпеки соціальної інженерії.

«Червоні команди» з кібербезпеки або «етичні хакери» наймаються організаціями спроб злому систем задля оцінки вразливості безпеки за допомогою тестів на проникнення або оцінки екосистеми мережі. Ці вразливості можуть бути засновані на широкому спектрі програмних точок безпеки або конкретних вразливих процесах і системах. Такими можуть бути відкриті мережеві системи, неналежно навчені співробітники та навіть неправильні методи фізичної безпеки. Роботою організації стає посилення або підвищення безпеки цих потенційних точок збою на основі інформації, зібраної червоною командою після тесту на проникнення. Обсяг тесту на проникнення визначається на початку цього процесу та підписується організацією та червоною командою. Документ про обсяг перевіряє роботу, яку дозволено виконувати червоній команді, і захищає її від звернення з боку компанії, якщо особа стає відчуженою через процеси соціальної інженерії, яких дотримується червона.

Сучасні тенденції у використанні соціальної інженерії майже експоненціально зростали з кожним роком і продовжують зростати такими ж темпами. Ця проблема ще більше ускладнюється тим, що атака соціальної інженерії зазвичай поєднується з іншою частиною зловмисного коду, як від програм-вимагачів або шкідливих програм. Через цю тенденцію до атак «чорних капелюхів» або зловмисних атак червоним командам частіше доручають використовувати атаки соціальної інженерії для оцінки вразливостей безпеки соціальної інженерії. Ця потреба потребує ефективного процесу, який червоні команди використовували б, щоб знаходити цілі в організації, яка наймає персонал, створювати спеціальні атаки та запускати атаки етично. Однак такий процес ще не розроблений і не випробуваний. Перш ніж червоні команди зможуть захистити свої організації, ці червоні команди потрібно навчити розпізнавати ці атаки, розуміючи найкращі практики, які використовують команди чорних капелюхів, піддаючи себе доступним інструментам і атакам.

Зараз доступно багато інструментів для створення атак соціальної інженерії. Найефективніші інструменти – безкоштовні та доступні для всіх осіб, які беруть участь у цих атаках (червоні команди, чорні капелюхи тощо). Розвідка по відкритим джерелам (OSINT) – це метод, який широко використовується в індустрії кібербезпеки на етапі розвідки ланцюжка кіберкількувань. Він визначається як інструмент, який передбачає збір, аналіз і використання даних із відкритих джерел для розвідувальних цілей.

Раніше OSINT використовувався як інструмент для відстеження та лову злочинців, моніторингу переміщень осіб і навіть для створення оглядів населення на основі публічних публікацій, але зараз він також використовується організаціями як інструмент збору даних для профілювання нових клієнтів або їхніх власних співробітників. Цей процес може бути використаний червоними командами для захисту своїх організацій або зловмисниками для компрометації своїх цілей. Проблема полягає в тому, що організації мають різні рівні ризику для соціальної інженерії через загальнодоступну інформацію, якою їхні співробітники

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.