POLTAVA UNIVERSITY OF ECONOMICS AND TRADE

ЗБІРНИК НАУКОВИХ СТАТЕЙ МАГІСТРІВ

Полтава
2022

УДК 339.1+640+664+37+657+005+004+80(062.552)
З-41

Друкується відповідно до Наказу по університету № 173-Н від 05 вересня 2022 р.

Збірник наукових статей магістрів. – Полтава : ПУЕТ, 2022. – 268 с.

З-41

ISBN 978-966-184-435-2

У збірнику представлено результати наукових досліджень магістрів спеціальностей: Готельно-ресторанна справа; Економіка; Комп'ютерні науки; Міжнародні економічні відносини; Облік і оподаткування; Освітні педагогічні науки; Філологія; Фінанси, банківська справа та страхування.

УДК 339.1+640+664+37+657+005+004+80(062.552)

ISBN 978-966-184-435-2

СПЕЦІАЛЬНІСТЬ ЕКОНОМІКА

Освітня програма «Управління персоналом та економіка праці»

СПЕЦІАЛЬНІСТЬ КОМП'ЮТЕРНІ НАУКИ

Освітня програма «Комп'ютерні науки»

Висновки. Дистанційна освіта допомагає людям отримувати знання де б вони не були. Знаходячись в Україні, ви можете переглядати лекції від MIT, Harvard, Stanford чи навіть отримувати повноцінну вищу освіти закордонного університету. У часи війни та пандемії багато людей були вимушені припинити очне навчання, тому актуальність альтернативного способу навчання зросла ще більше.

По об'єктивним причинам, дистанційна освіта в деяких моментах поступається очній, тому важливо забезпечити максимально якісний досвід користування. Важливою складовою досвіду користування є інтерфейс, якщо він погано реалізований, то студенти будуть довше підключатися до занять, знаходити домашні завдання, викладачу буде важче викладати матеріал та взаємодіяти з ними. Тому доступний інтерфейс є одним із ключів успіху цифрового продукту.

Список використаних джерел

1. Microsoft Word – 10560 // The Academic and Business Research Institute is a privately-owned, for-profit publishing corporation incorporated and operating in the state of Florida, United States of America [Електронний ресурс]. URL: http://www.aabri.com/manuscripts/10560.pdf.
2. 10 Usability Heuristics for User Interface Design [Електронний ресурс]. URL: https://www.nngroup.com/articles/ten-usability-heuristics/
3. Steve Krug Don't Make Me Think: A Common Sense Approach to Web Usability, 2nd Edition / Steve Krug. – 2005. – 201 с.

УДК 640.412(477.83):005.591.6

АНАЛІЗ ПРОГАЛИН БЕЗПЕКИ ПІРИНГОВИХ МЕРЕЖ

Орлова Д. І., *магістр спеціальності Комп'ютерні науки освітня програма «Комп'ютерні науки»*
Черненко О. О., *к. ф.-м. н., доцент, доцент кафедри комп'ютерних наук та інформаційних технологій*

Анотація. Було проаналізовано основні засади пірингових мереж. Розглянуто типи атак на пірингові мережі, які можуть виникнути. Наведено способи та заходи безпеки для всіх дослі-

джуваних атак. Проведене дослідження є основою для продовження дослідження проблем захисту піринговых мереж і побудові нових безпечних засобів обміну даними в децентралізованих структурах.

Ключові слова. Пірингова мережа, брандмауер, маршрутизація, вузол, центральний сервер, аутентифікація.

Abstract. The basic principles of peering networks were analyzed. The types of attacks on peering networks that can occur are considered. Methods and security measures for all investigated attacks are given. The conducted research is the basis for continuing research on the protection of peering networks and the construction of new secure means of data exchange in decentralized structures.

Keywords. Peer-to-peer network, firewall, routing, node, central server, authentication.

Постановка проблеми. Безпечна діяльність є однією з основних складових процесу забезпечення успішного функціонування піринговых мереж. Тому розгляд основних атак на пірингові мережі та способів захисту є наданням належного та надійного середовища використання цих мереж.

Аналіз основних досліджень і публікацій. Дослідженням тенденцій розвитку піринговых мереж займалися такі люди, як Е. С. Таненбаум, Л. М. Куперштейн, М. Д. Кренцін, Фаріда Чоудхурі, Роджер Ваттенгофер, О. П. Войтович, Ю. В. Баришев, Е. І. Колібабчук.

Формулювання мети. Метою статті є проаналізувати основні засади піринговых мереж, надати їх класифікацію, проаналізувати типи атак на пірингові мережі, які можуть виникнути та виявити способи та заходи безпеки для всіх досліджуваних атак.

Виклад основного матеріалу дослідження. Основна ідея загального доступу до файлів у мережі P2P (Peer-to-Peer – рівнорангової мережі або піринговой мережі) полягає в тому, що безліч комп'ютерів разом об'єднують свої ресурси, щоби сформувати систему розподілу контенту.

Наразі використання піринговых мереж не обмежене обміном файлами. Також P2P мережі розповсюджені там, де є важливим обмін конфіденційними даними між людьми. Це системи інтер-

нет-телебачення, IP-телефонія, системи відеомовлення та відеозв'язку тощо.

Як і традиційний Інтернет, P2P мережі вразливі до загальних і специфічних мережевих атак.

Виявляють такі найбільш поширені атаки на пірингові мережі: «людина посередині» (man-in-the-middle – MITM), «атака забруднення» (pollution attack), «відмова в обслуговуванні» (danial of service – DoS) та її розподілена модифікація (distributed danial of service – DDoS), «поширення хробака» (worm propagation), «атака Сивілли» (Sybil attack), «атака затемнення» (eclipse attack), «раціональна атака» (rational attack), «отруєння індексу» (index poisoning) та ін. Ці атаки різняться складністю у реалізації і технологіями безпеки проти них.

Актуальним є аналіз знань про загрози P2P системам, засобів їх попередження та виявлення для оцінки їх потенціалу, також покращення та побудови нових перспективних запобігаючих механізмів.

Загальна характеристика піринговых мереж. За ступенем централізації P2P мережі бувають трьох типів:

- чисті peer-to-peer системи;
- гібридні peer-to-peer системи;
- федеративні.

Залежно від того, як вузли з'єднуються один з одним можна поділити мережі на структуровані та неструктуровані.

За функціями:

- розподілені обчислення;
- файлообмін;
- співпраця.

Класифікація атак на пірингові мережі.

1. DoS (аббр. англ. Denial of Service «відмова в обслуговуванні»)

2. Якщо атака виконується одночасно з великої кількості комп'ютерів, говорять про DDoS-атаку (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»).

Захист. Для захисту від мережевих атак застосовується ряд фільтрів, підключених до інтернет-канала з великою пропускною здатністю. Фільтри діють таким чином, що послідовно аналізують прохідний трафік, виявляючи нестандартну мережну активність та помилки.

3. Атака посередника, атака «людина посередині», MITM-атака (англ. *Man in the middle*).

Захист. Використовувати шифрування інформації.

4. Атака «Поширення хробака» (Worm propagation).

Захист. Проактивний захист. Також «кредити довіри». Ряд переваг дає застосування міжмережевих екранів та подібних до них утиліт.

5. Атака «Забруднення» (Pollution attack).

Захист. Користувачі повинні просто видалити шкідливий файл

6. Раціональні атаки (Rational attacks).

Захист. Алгоритм, що гарантує належний рівень взаємності вивантаження та завантаження. Ті вузли, які не вивантажують – їх «штрафують».

7. Атака «Сивілли» (Sybil attack)

Захист. Пряма перевірка – вирішення завдання, яке один користувач не може вирішити самостійно.

Непряма перевірка – можна заощадити власні ресурси, якщо делегувати завдання валідації вузлів іншим учасникам.

Плата за реєстрацію.

Соціальні графи.

Gate Keeper.

Доказ виконання роботи.

8. Атака «Затемнення» (Eclipse attack).

Захист. Застосовувати криптографічні протоколи. Ціноутворення також. Основний метод захисту – використання чистої пірингової мережі. Додатково ще гарно застосовувати рандомізацію при визначенні розташування вузлів.

9. Атака «Отруєння індексу» (Index poisoning attack).

Захист. Аутентифікація версій. Вміст повинен модеруватися. І другий спосіб – рейтинг джерел.

10. Ботнети (Botnets).

Захист. Слід проводити моніторинг мережі та регулярно відстежувати її активність, щоб легко виявити неправильну поведінку мережі.

11. Атака підслуховування (Eavesdropping attack).

Захист. Міцна фізична безпека та шифрування інформації.

12. Маскарадна атака.

Захист. Фільтрація вхідних пакетів, які надходять із внутрішньої IP-адреси та фільтрація вихідних пакетів, які виходять з недійсної локальної IP-адреси.

Висновки. Аналіз розповсюдження піринговых мереж привів до підтвердження факту про розповсюдження використання децентралізованої мережевої технології. Виділено атаки загального та специфічного характеру. Атаки розрізнено за ступенем небезпеки та аспектом порушення рівня безпеки. Найнебезпечнішими атаками виявилися ті, що призводять до порушення цілісності даних, доступності і конфіденційності. До них належать: ботнети, «хробаки», «людина посередині» та ін. Попри виконання захисту від потенційних загроз атака нульового дня залишається актуальною. Таким чином завжди актуальним буде побудова нових і покращення існуючих способів захисту піринговых сервісів. Одержані результати дослідження ляжуть в основу розробки класифікації загроз P2P мереж.

Список використаних джерел

1. Комп'ютерні мережі. Таненбаум Е. С., Уезеролл Д. С.792–793.
2. Куперштейн Л. М., Кренцін М. Д. Аналіз тенденцій розвитку піринговых мереж. Вісник Хмельницького національного університету. 2021. № 4. С. 25–29.
3. Md. Sadek Ferdous, Farida Chowdhury, Md. Moniruzzaman. "A Taxonomy of Attack Methods on Peer-to-Peer Network" in Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security, India, 2007. P. 132–138.
4. Roger Wattenhofer. "Attacks on Peer-to-Peer Networks" in Semester Thesis of Swiss Federal Institute of Thechnolog, 2005, Zurich. P. 1–36.
5. Voitovych O. P., Baryshev Y. V., Kupershtein L. M., Kolibabchuk E. I. "Investigation of Simple Denial-of-Service Attacks", Third International

IEEE Conference “Problems of Infocommunications. Science and Technology”, 2016, Kharkiv, Ukraine. P. 1–4.
6. https://wiki.cuspu.edu.ua/index.php/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B0_P2P.

УДК 004+510.5

ПРО ТРЕНАЖЕР, ЩО НАВЧАЄ РОЗВ’ЯЗУВАННЮ ЗАДАЧ З ТЕМИ «НОРМАЛЬНІ АЛГОРИТМИ» АНГЛОМОВНОГО ДИСТАНЦІЙНОГО НАВЧАЛЬНОГО КУРСУ «ТЕОРІЯ АЛГОРИТМІВ»

Пилипченко В. С., *магістр спеціальності Комп’ютерні науки освітня програма «Комп’ютерні науки»*
Черненко О. О., *к. ф.-м. н., доцент, доцент кафедри комп’ютерних наук та інформаційних технологій*

Анотація. У статті розглядаються питання створення тренажеру з теми «Нормальні алгоритми Маркова».

Ключові слова: нормальні алгоритми маркова, теорія алгоритмів, тренажер.

Abstract. The article considers the issues of the creation of a training simulator as well as solving tasks using Normal Markov algorithms.

Keywords: normal algorithms of Markov, theory of algorithms, simulator.

Постановка проблеми. В наш час програми-тренажери зайняли важливу частину освітнього процесу. Онлайн навчання є частиною навчання та самонавчання студентів, особливо тих, хто знаходиться далеко за межами України. Враховуючи, що тренажера з теми «Нормальні алгоритми Маркова» в англомовному дистанційному курсі з дисципліни «Теорія алгоритмів» немає, виникла необхідність його розробки.

Формулювання мети. Метою написання статті є опис роботи тренажеру, а також демонстрація його програмної реалізації.

Виклад основного матеріалу дослідження. Під час створення тренажеру було розглянуто декілька тренажерів та їх реалізація [5–7]. Розроблено тренажер з теми «Нормальні алго-