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

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

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

21-22 квітня 2022 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 21-22 квітня 2022 р**.** - Одеса, Видавництво ОНТУ, 2022 р. – 251 с.

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

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

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

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНТУ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНТУ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц., Київський національний університет імені Тараса Шевченка

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНТУ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНТУ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНТУ,
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 та англійською мовами.
Редактор збірника Котлик С.В.

hackers than users, as they can detect all IoT devices outside the local network. Therefore, it is better to completely disable UPnP.

5. Constant updating of firmware and installed software. Updating your device's IoT software ensures that your device has the most up-to-date security settings. In addition, it helps the system eliminate security flaws in older versions of software.

Despite the risks, it is unlikely that IoT will cease to spread in homes, offices, etc. Because of this, hackers will not go anywhere. Therefore, the most important thing is to remember the safety of your devices. Understanding their vulnerabilities and using the right protection tools is necessary to counter threats in the changing world of IoT.

Referens

1. Cyber Threats Haunting IoT Devices in 2021 [Online]. Available: https://securityboulevard.com/2021/09/cyber-threats-haunting-iot-devices-in-2021/.

2. Reo J. DDoS Hackers Using IoT Devices to Launch Attacks [Online]. Available: https://www.corero.com/blog/ddos-hackers-using-iot-devices-to-launch-attacks/.

3. Swamini K. How to secure IoT devices and protect them from cyber attacks [Online]. Available: https://internetofthingsagenda.techtarget.com/post/How-to-secure-IoT devices-and-protect-them-from-cyber-attacks.

UDC 004.491.22

TYPES OF INTERNET FRAUD

MELNIK M.V., KIM YE.R. (e.kim@turan-edu.kz)
Turan University, Kazakhstan

In the modern world, in connection with the development of mobile and Internet communications, new “social” relations have been built. Every day, more and more people prefer to buy goods or services online. Thanks to online shopping, people save a lot of time, since there is no need to go for the goods, there is a home delivery function. With non-cash payment, bonuses are accrued, which can later be used to purchase a particular product. But with the development of the World Wide Web, there are such unpleasant phenomena as fraud in its various forms.

Scams on the Internet have grown in scope, going beyond the banal mailing list. There are scammers in almost all spheres of human activity. With the advent and development of the worldwide network, their activities have acquired new forms of fraud.

Fake online stores, various charitable fundraisers, phishing, viral content are some of the most popular methods of online deception.

Since purchases through online stores are in great demand, scammers create fake pages on social networks, under the guise of one-day shops. After making a certain number of purchases, these stores disappear, or the purchased goods are radically different from those declared.

Today, phishing attacks are still relevant. Proof of this is the statistics of Kaspersky Lab. In 2019, there were 492,432,555 activations of the Anti-Phishing system by Kaspersky Lab users when they tried to navigate to phishing sites. This is 245,626,777 attempts more than in 2018. In general, 19.34% of computer users of Kaspersky Lab were attacked [1].

Phishing attacks have new targets. During the period 2018-2019, 142 phishing attacks were registered against universities in 17 countries around the world. Of these, more than half of higher education institutions are located in the US - 83, in the UK - 24, and 9 each in Canada and Australia. Fraudsters mainly stole a large number of important documents, including a study in the field of nuclear energy.

For seven months of 2020, 11 thousand cyber attacks were recorded in Kazakhstan. This is 23.4% less than in the same period last year (14.4 thousand). It should be noted that this decrease is

primarily due to a decrease in the number of cyberbotnets. During the reporting period, 853 phishing attacks were committed in Kazakhstan, which is 12.1% more than a year ago (761 cyber attacks). Phishing attacks are punishable by law [2].

The number of Distributed Denial of Service attacks (DDoS attacks) is also growing significantly. In eight months of 2020, 206 people were registered, which is 39.2% more than in the same period last year (148 attacks). Recall that in September 2020, when monitoring incidents in the field of information security of Internet resources, state bodies of the Republic of Kazakhstan recorded DDoS attacks on educational platforms Khun Derek and Birimurando [2].

A popular form of online scam is fundraising for charity. This form of deception is carried out by sending letters or SMS with a request for help to people or animals in need. People transfer money to left-handed accounts that do not belong to charitable foundations, and as a result, their money is stolen.

Attackers generally rarely change their details when creating fake sites. Therefore, if you copy their payment details and drive them into a search engine, you can check if there are fraud warnings.

"Fake" applications are one of the new methods of Internet fraud. Often, a “fake” pretends to be popular apps, games, or instant messengers. Also, one of the new methods of stealing information is the use of a digital twin. This type of fraud is associated with the banking sector. There is a market on the dark web called "Kinesez" that sells digital masks, operating systems, browsers, etc. [3].

From January to August 2020, Kaspersky Lab specialists identified 4,970 erroneous resources in the Kazakhstani segment of the Internet, created by scammers luring users out of money. Thanks to technical solutions, almost 690,000 attempts to access this site were blocked for Kazakh users [2]. In August, it was reported that the number of Internet deceivers had increased tenfold in a year. At the same time, Internet fraud using an electronic digital signature (EDS) is developing in Kazakhstan.

To authenticate a user, modern anti-fraud systems use a "digital" fingerprint. The transaction will be approved if the security system sees a mask that matches the one that the user applied earlier. Most banks in this case will not send a security code via SMS to confirm the transaction [3].

In our opinion, it is advisable to adhere to the following recommendations in order not to become another victim of an Internet scammer: - when making an online purchase, check all information about the seller;

- you can not send a deposit or the full amount for the goods until it is delivered to your door;
- it is not allowed to enter a phone number and a card number at the same time;
- you should not send your personal data and photos to an unfamiliar user on the network;
- you can not respond to messages about requests for money transfer;
- it is not allowed to download or save files from unreliable sources;
- it is necessary to configure the operating system in such a way that when working on the Internet or in social networks, all the necessary security rules are provided;
- it is desirable to install a licensed antivirus and use it correctly [3].

There are also many different ways to protect against online fraud, such as:

- complex username and password. For a secure login and password, you must use large and small letters, capital letters, various numbers and symbols;
- binding to a phone number. Most applications and programs have the function of linking a number to a phone. It must be attached to confirm
- updating antivirus and software (software). If new updated versions are released, you must immediately install the latest version of the system and antivirus, as this will better protect electronic resources;
- distrust and inattention. You need to be very careful and attentive to suspicious letters and links, preferably without opening them, and immediately delete them. It is also necessary to know and remember that the login and password from social networks should never be entered on unfamiliar sites [2].

In conclusion, I would like to say that Internet fraud is a phenomenon that has penetrated from the real world into the virtual one. Today, it poses a huge threat to the economic security of the country. Most users, to exchange information between accounts, use various sites and programs. For most people, virtual communication on the World Wide Web has become a commonplace in everyday life and has almost completely replaced communication in the real world.

REFERENCES:

1. Nazar'janc N.K. Moshennichestvo v Internete // Nacional'nye interesy: prioritety i bezopasnost', 2015. – №(5). – S.72-79.

2. Mihajlenko I.A. K voprosu o sposobah moshennichestva v seti Internet // Ugolovno-processual'nye i kriminalisticheskie chtenija, 2016. – №5(13). – S.98-104.

3. Kulmatova B.A. Sposoby zashhity ot internet-moshennichestva // Academy, 2019. – №12(51). – S.78-80.

UDC 004.021

FENWICK TREES AS REPLACEMENT FOR SEGMENT TREES IN THE "RANGE SUM QUERY PROBLEM WITH RANGE UPDATES"

R.MASALSKYI (masalskyi@stud.onu.edu.ua), I.MAZUROK (igor@mazurok.com)
Odesa I. I. Mechnikov National University

Keywords: data structures, algorithms, range sum query problem.

Introduction. Considering the problem where we have an array and we need to support two types of queries. The first query is to add some value to the continuous substring of the array. The second query is to find the sum of the continuous substring of the array. We will call it RSQM problem. This problem can be found as a base problem in several tasks such as: Finding the perimeter or area of parallel rectangles; a big amount of graph decomposition such as heavy-light decomposition [2]; some clustering algorithms. Including the algorithm of clustering of words in the document which has a block structure developed by Masalskyi Ruslan [3]. The main data structure to solve this problem is a Segment tree [1][5]. However, the solution based on the Segment tree, although is asymptotically optimal, has a sufficiently large constant inside. The purpose of the work is to provide a better solution to the RSQM problem.

Fenwick tree definition. Consume we have an initial array $a[i], i = 0 \ldots n-1$. Define two additional arrays $diff$, where $diff[i] = a[i] - a[i-1], i = 1 \ldots n-1, diff[0] = a[0]$. And the second one $wdiff$, where $wdiff[i] = diff[i] * (n-i)$. The solution of RSQM in this case can be splitted into two RSQ [1] (range sum query) problems, based on arrays $diff, wdiff$. The solution of RSQ based on Fenwick tree is the standard usage of Fenwick and could be found here[4].

Fenwick tree update range query. Query input l, r, x: $a[i] += x, l \le i \le r$. Having an array $diff$ the query updates only $diff[l], diff[r+1]$ as follows: $diff[l] += x, diff[r+1] -= x$. As $diff$ unambiguously determines $wdiff$ so: $wdiff[l] += x * (n-l), wdiff[r+1] -= x * (n-r-1)$.

Fenwick tree sum range query. Query input l, r: $\sum_{i=l}^{r} a[i]$. The sum could be found by formula:

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

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

21-22 квітня 2022 р

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

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

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

Відповідальний за випуск: Котлик С.В.