Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 23-28 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

სარეკომენდაციო სისტემების გამოყენება კიბერუსაფრთხოების მიმართულებით

RECOMMENDER SYSTEMS USE IN CYBERSECURITY FIELD

Giorgi Iashvili – Caucasus University, Tbilisi, Georgia
Roman Odarchenko – National Aviation University, Kyiv, Ukraine
Sergii Gnatyuk - National Aviation University, Kyiv, Ukraine
Avtandil Gagnidze - East West University, Tbilisi, Georgia

აბსტრაქტი. ნაშრომი აღწერს ვებ-ზე დაფუძნებულ ინტეგრირებულ სისტემას, რომელიც აანალიზებს უსაფრთხოების პოტენციურ საკითხებს, რამაც შეიძლება გავლენა მოახდინოს გარკვეულ აპარატურაზე დაფუძნებულ სისტემაზე და, შესაბამისად, გვთავაზობს ოპტიმალურ გადაწყვეტილებებს. შემუშავებული სისტემა ტესტირება ხდება რეალურ სამყაროში ინდუსტრიული და კორპორატიული შემთხვევების გამოყენებით და შეფასების პროცესის შედეგი ადასტურებს, რომ მას შეუძლია მნიშვნელოვნად გააუმჯობესოს სისტემების კიბერუსაფრთხოების დონე, რომელიც ეკუთვნის სხვადასხვა ორგანიზაციებს. კვლევის შედეგად შეიქმნა ვებ-სისტემის პროტოტიპი, რომელიც აგროვებს ინფორმაციას თანამედროვე აპარატურასთან დაკავშირებული მოწყვლადობის შესახებ და აძლევს მომხმარებლებს შესაბამის რეკომენდაციებს კონკრეტული სიტუაციიდან გამომდინარე.

საკვანძო სიტყვები: *სარეკონებდაციო სისტემა, თადასხმის ანალიზი, მონაცეცმებთან მუშაობა;*

ABSTRACT. The paper describes an integrated web-based system that analyzes potential security issues that may affect a certain hardware-based system and therefore suggests optimal solutions. The developed system is tested using real-world industrial and corporate cases, and the result of the evaluation process confirms that it can significantly improve the level of cyber security of systems belonging to various organizations. As a result of the research, a prototype of a web system was created, which collects information about vulnerabilities related to modern hardware and provides users with appropriate recommendations based on a specific situation.

KEYWORDS: *recommender system, attacks analysis, work with data;*

შესავალი

კიბერუსაფრთხოების პრობლემატიკის გათვალისწინებით, გამოთვლითი სიჩქარე არის ერთ-ერთი მთავარი პრობლემა, რომელიც უნდა გადაიჭრას. პროცესორის არქიტექტურა

განსაზღვრავს მონაცემთა დამუშავების მახასიათებლებს და ზოგიერთ შემთხვევაში მთელი აპარატის შესაძლებლობებს. სხვადასხვა ფიზიკური არქიტექტურის გათვალისწინებით, პროცესორებს შეიძლება ჰქონდეთ გარკვეული შეზღუდვები, რამაც შეიძლება გამოიწვიოს შეუთავსებლობა ზოგიერთ დაკავშირებულ სისტემასთან, მათ შორის უსაფრთხოების შესაბამის მექანიზმებთან. გარდა ამისა, მნიშვნელოვანია აღინიშნოს, რომ ცენტრალური გადამამუშავებელი განყოფილების კარგად შემუშავებული არქიტექტურა საშუალებას აძლევს ახალი აპარატურის დანერგვას თანამედროვე სისტემებში, როგორიცაა მიკროარქიტექტურები და ენერგიის დაზოგვის ცენტრალური გადამამუშავებელი ერთეული. ეს გულისხმობს, რომ არსებული პროგრამული უზრუნველყოფა შეიძლება იმუშაოს ახალ აპარატურულ პლატფორმებზე. მაგრამ დღესდღეობით აპარატურაზე ორიენტირებული შეტევები საკმაოდ პოპულარულია. აპარატურაზე დაფუძნებული სისტემების დიდი ნაწილი დაუცველია თუნდაც მარტივი ფიზიკური შეტევებისა და გვერდითი არხის შეტევების მიმართ.

გვერდითი არხის შეტევების დროს, როდესაც შეყვანის სახით მიიღება შეტყობინება და გასაღები და გამოიყენება სტანდარტული კრიპტო ალგორითმი, ჩვენ მაინც შეგვიძლია მივიღოთ შიფრის გაჟონვა ტექნიკის პრობლემების გამო. სამუშაოს ამოცანა იყო არსებული აპარატურაზე ორიენტირებული შეტევების ანალიზი, ამ შეტევებით გამოწვეული მონაცემების გაჟონვის გამოთვლა და ტექნიკის შეთავაზება, რომელსაც შეუძლია შეამსუბუქოს ან აღმოფხვრა ეს გაჟონვა.

თანამედროვე მიდგომების განხილვა

კიბერუსაფრთხოებაში ცენტრალური პროცესორის გამოყენების საინტერესო მაგალითია Morpheus, რომელიც არის CPU-ის ახალი არქიტექტურა, რომელიც შეიქმნა მიჩიგანის უნივერსიტეტში 2019 წელს. Morpheus პროცესორის სპეციფიკური არქიტექტურის გათვალისწინებით, მას შეუძლია შეტევების დაბლოკვა მექანიზმის გამოყენებით, რომელიც მოიცავს დაშიფვრას და შემთხვევით გადაკეთებას საკუთარი კოდისა და მონაცემების გასაღების ბიტების წამში ოცჯერ. პრინციპში, ის უფრო სწრაფია, ვიდრე ყველაზე ეფექტური თანამედროვე ავტომატური ჰაკერების მექანიზმები და, ბუნებრივია, ბევრად უფრო სწრაფია, ვიდრე ნებისმიერ ადამიანს შეუძლია იმუშაოს. Morpheus არქიტექტურა შეიძლება გამოყენებულ იქნას სხვადასხვა პროგრამული და აპარატურის პლატფორმებისთვის, მათ შორის პორტატული და IoT მოწყობილობებისთვის. პროცესორის ეს არქიტექტურა ორიენტირებულია დეველოპერებზე და მომხმარებლებზე და დაფუძნებულია მონაცემების ბიტების რანდომიზაციაზე, რომლებიც ცნობილია როგორც განუსაზღვრელი სემანტიკა, რომელიც წარმოადგენს CPU არქიტექტურის სპეციალურ ნაწილებს, რომლებიც ეხება დაპროგრამებული აპლიკაციის კოდის ფორმატსა და შინაარსს. მორფეუსის არქიტექტურა ვერ აგვარებს კიბერუსაფრთხოების ყველა საკითხს, მაგრამ მისი არქიტექტურა ორიენტირებულია კონტროლის ნაკადის მთლიანობის შეტევებისგან დაცვაზე, როგორიცაა ბუფერული გადადინება.

დღევანდელი კიბერ სამყარო იცვლება ახალი ტენდენციებისა და მიმართულებების გავლენით. ამრიგად, კვლევისა და განვითარების ერთ-ერთი მნიშვნელოვანი მიმართულება წარმოდგენილია IoT ეკოსისტემით, რომელიც მნიშვნელოვნად განვითარდა ბოლო რამდენიმე წლის განმავლობაში. შესაბამისად, სმარტ მოწყობილობების მნიშვნელოვანი რაოდენობა გამოიყენება სხვადასხვა ინდუსტრიაში. ხშირ შემთხვევაში, ასეთი მოწყობილობები გამოიყენება ტექნიკური ან განმეორებითი ამოცანების შესასრულებლად, როგორიცაა მონაცემთა შეგროვება და ადეკვატური დახარისხება, ან შეტყობინებების გაგზავნა და მიღება. გარდა ამისა, არსებობს კომპლექსური ინდუსტრიული გარემო, რომელიც სარგებლობს IoT ქსელური ინფრასტრუქტურის საკმარისი სიმძლავრით და მრავალფეროვნებით, როგორიცაა თანამედროვე ავტომობილების ქარხნები, რომლებიც იყენებენ IoT-ზე დაფუძნებულ ჭკვიან სისტემებს მანქანების აწყობის პროცესში.

საინტერესოა აღინიშნოს, რომ მხოლოდ რამდენიმე წლის წინ, ინტეგრაციული კონცეფცია, როგორიცაა ჭკვიანი სახლი, აღიქმებოდა და მიდგომა მნიშვნელოვნად განსხვავებულად იქნა მიღებული, ვიდრე დღეს. ადრე ჭკვიანი მოწყობილობების კონცეფცია და იდეა უფრო ორიენტირებული იყო სხვადასხვა პროცესების ავტომატიზაციაზე. მიუხედავად ამისა, დღევანდელი IoT მოწყობილობები და მასთან დაკავშირებული ცნებები უფრო მეტად არის ორიენტირებული პრაქტიკული პრობლემების გადაჭრაზე უფრო ფართო მასშტაბით, როგორიცაა ბუნებრივი რესურსების გამოყენების შემცირების წვლილი.

IoT მოწყობილობების უსაფრთხოება. მთელ მსოფლიოში ჭკვიანი მოწყობილობების გამოყენების მნიშვნელოვანი ზრდის გათვალისწინებით, IoT-ზე დაფუძნებულ გამოთვლით გარემოზე მიმართული შეტევების რისკი მუდმივად იზრდება. IoT მოწყობილობებზე თავდასხმები დღეს ძალიან გავრცელებულია და ჭკვიანი მოწყობილობების ახალი მოდელებისა და მიდგომების შემუშავებით, თავდასხმები უფრო და უფრო ხშირი ხდება და, ასევე, უფრო მრავალმხრივი, იმის გათვალისწინებით, რომ მათ შეუძლიათ ადაპტირდნენ მიზნობრივი IoT მოწყობილობების სხვადასხვა პროგრამულ და აპარატურულ კონფიგურაციებთან. უმეტეს შემთხვევაში, ჭკვიან მოწყობილობებზე თავდასხმის მიზეზი არის მონაცემთა ცენტრების წვდომა, რომლებიც აკონტროლებენ მოწყობილობებს, რომლებიც ერთი ან მეტი ქსელის ნაწილია. სხვა გამოთვლითი სისტემების მსგავსად, IoT მოწყობილობები ასევე დაუცველია კიბერშეტევებისგან. შესაბამისი დაუცველობა შეიძლება დაიყოს სხვადასხვა კატეგორიად მათი განსხვავებული ბუნების მიხედვით. მაგალითად, ჩვეულებრივი შეჭრის ტექნიკა გულისხმობს ჰაკერის წვდომას ჭკვიან მოწყობილობაზე მოძველებული პროგრამული უზრუნველყოფის ან სპეციალური პროგრამული უზრუნველყოფის მიერ მართული აპარატურის შედეგად. ტექნიკის ხარვეზების აღმოჩენა და გამოსწორება ჩვეულებრივ ბევრად უფრო რთულია, ვიდრე პროგრამული ხარვეზები ან ხარვეზები. მნიშვნელოვანია თანამედროვე მოწყობილობებისთვის არსებული ტექნიკის უსაფრთხოების ზომების ყოვლისმომცველი ანალიზი. ახალი მიდგომები ამ მიმართულებით გაზრდის უსაფრთხოების არსებული საკითხების გაგებას და ხელს შეუწყობს ტექნიკის უსაფრთხოების მექანიზმების გაუმჯობესების მეთოდების შემუშავებას.

პოტენციური შეტევები IoT მოწყობილობებზე. დაკავშირებული ჭკვიანი მოწყობილობების ინფრასტრუქტურისა და მასთან დაკავშირებული სხვადასხვა ინდუსტრიების განვითარებამ ხელი შეუწყო სმარტ მოწყობილობების ინფრასტრუქტურაზე სხვადასხვა კიბერშეტევების სერიას, რომლებიც გამოიყენება სხვადასხვა ორგანიზაციაში. ბოლო რამდენიმე წლის განმავლობაში, ჰაკერებმა მოახდინეს დიდი რაოდენობით თავდასხმები IoT-ზე დაფუძნებულ ინფრასტრუქტურაზე მთელს მსოფლიოში. კვლევის ფარგლებში, რომელიც მოხსენებულია ამ ნაშრომში, ჩვენ გავაანალიზეთ ყველაზე გავრცელებული პოტენციური თავდასხმები IoT მოწყობილობებზე.

ინტერაქტიული ფორმა მოვლენების იდენტიფიცირებისთვის

სისტემა, რომელიც შემუშავებულია ჩვენი კვლევის ფარგლებში, აქვს შესაძლებლობა შეამოწმოს კონკრეტული კლასიკური, ინდუსტრიული, საოფისე ან IoT მოწყობილობების აპარატურა. წარმოდგენილი ამოცნობის სისტემა არის ვებ-აპლიკაცია, რომელიც ხელმისაწვდომია უფასოდ. შეფასების ნაგულისხმევი მეთოდი ეყრდნობა სანდო რესურსების სიის გამოყენებას, რომლებიც ინახება აპლიკაციის მონაცემთა ბაზაში. მონაცემთა ბაზა შედგება ინფორმაციისგან პოპულარული ონლაინ დაუცველობის აღმოჩენისა და მითითების პლატფორმებიდან, როგორიცაა AttackerKB , ExploitDB , CVE MITER და ეროვნული დაუცველობის მონაცემთა ბაზა.

სისტემა ეფუძნება ამ წყაროებიდან ყველაზე რელევანტურ ინფორმაციას. მონაცემთა ბაზაში შენახული მონაცემები ეხება შემდეგ კატეგორიებს: ახალი აპარატურაზე დაფუძნებული თავდასხმის ვექტორები, ახალი მოწყვლადობა არსებულ პროდუქტებში და უსაფრთხოების საკითხები Wireframes-ის მოძველებულ ვერსიებში. ამრიგად, შესაბამისი საძიებო მოთხოვნების გათვალისწინებით, სისტემა მომხმარებელს აწვდის ინფორმაციას აღნიშნულ პროდუქტში არსებული უსაფრთხოების საკითხების შესახებ, უსაფრთხოების დონის ამაღლების დეტალურ რეკომენდაციებთან ერთად.

ცნობილი დაუცველობისა და კიბერუსაფრთხოების მონაცემთა ბაზებიდან მოთხოვნებთან და ტენდენციებთან ერთად, სისტემა აგროვებს ინფორმაციას შიდა შემთხვევების შესახებ, სისტემის მომხმარებლების მიერ შესრულებული საძიებო მოთხოვნების საფუძველზე. სურათი 3 ასახავს რამდენიმე პოპულარულ საძიებო მოთხოვნას პლატფორმის ჩარჩოში და სისტემა ინახავს ადგილობრივ მონაცემთა ბაზაში. პლატფორმაზე მომხმარებლის ქცევის უკეთესი თვალყურის დევნებისთვის, მომხმარებლის შეყვანის ფორმა ხელმისაწვდომია მხოლოდ ავტორიზებული მომხმარებლებისთვის. თითოეულ მომხმარებელს აქვს პირადი პროფილი კონკრეტული სტატისტიკური მონაცემებით.

უპირველეს ყოვლისა, სისტემა ათავსებს ყველა ინფორმაციას აპარატურაზე დაფუძნებული პრობლემების შესახებ ზემოთ ნახსენები სანდო წყაროებიდან. შემდეგი ნაბიჯი არის შესაბამისი რეკომენდაციების გენერირება და შეგროვებული მონაცემების პრიორიტეტიზაცია. გათვალისწინებულია შემდეგი კრიტერიუმები: შესაბამისობა,

მითითების თარიღი, გავრცელება, ზოგადი ინფორმაცია და რისკის დონე. ყველა ეს პარამეტრი გამოიყენება კონკრეტული საკითხისთვის ყველაზე სასარგებლო და პრაქტიკული რეკომენდაციის შესაქმნელად. ჩვენ შევაგროვეთ მონაცემები, რომელიც ეფუძნება აპარატურულ თავდასხმებს შემდეგ კატეგორიებში: საოფისე აღჭურვილობა, სამრეწველო მოწყობილობები, IoT მოწყობილობები და კლასიკური მოწყობილობები, რომლებსაც იყენებენ საშუალო მომხმარებლები.

დასკვნა

მრავალი ბიზნესის ყოველდღიურ ოპერაციებში აპარატურაზე დაფუძნებული სისტემების მნიშვნელობის გათვალისწინებით, მოწყობილობის უსაფრთხოების მეთოდების გაძლიერება სისტემის შენარჩუნების სასიცოცხლო კომპონენტია. შედეგად, ჩვენ ვაპირებთ გავაძლიეროთ უსაფრთხოების საკითხების იდენტიფიკაციის სისტემის შესაძლებლობები ისეთი ვარიანტების მიწოდებით, რომლებიც მომხმარებლებს საშუალებას აძლევს აირჩიონ მომხმარებლის დონე. შედეგად, სისტემამ უნდა აირჩიოს შესაბამისი ტექნიკა აპარატურაზე დაფუძნებული სისტემის უსაფრთხოების არსებული პრობლემის გადასაჭრელად, მომხმარებლის განსაზღვრული უნარების დონის მიხედვით, გაზრდის ასეთი მეთოდის გამოყენებადობას კიბერუსაფრთხოების პრობლემების გადასაჭრელად ბიზნესის ფართო სპექტრში. გარდა ამისა, ალგორითმული ბირთვი დაემატება მანქანური სწავლების საჭირო ასპექტებს, რათა გააუმჯობესოს სისტემის მიერ გენერირებული ანგარიშების სარგებლიანობა, ისევე როგორც საბოლოო მომხმარებლების საერთო გამოცდილება.

შედეგად, კონკრეტული ანალიზის პროცედურები შეისწავლის მონაცემთა ბაზაში არსებულ მონაცემებს, ასევე ახლად შეყვანილი მონაცემების გათვალისწინებით, გააერთიანებს არსებულ მონაცემებს და საბოლოოდ დაამატებს საჭირო დამატებით მონაცემებს მონაცემთა ბაზაში. საბოლოო მომხმარებლის პოპულარულ ძიებებზე დაფუძნებული მონაცემთა ახალი წყაროების ინტეგრირებით, ეს ტექნიკა ეფექტურად გაზრდის რეკომენდაციების შესაბამისობას.

კვლევის მიზანი, რომელიც მოხსენებულია ამ ნაშრომში, იყო გაერკვია აპარატურაზე დაფუძნებული მოწყობილობებისა და მასთან დაკავშირებული პროგრამული სისტემების სუსტი მხარეები, რათა გაუმჯობესებულიყო უსაფრთხოების აუცილებელი მექანიზმები. ამ პროცესში მომხმარებლის ჩართვა უსაფრთხოების მექანიზმის დაკალიბრებას უფრო ეფექტურს ხდის. საბოლოო მომხმარებლის უკეთესი განათლება უსაფრთხოების პრობლემებთან დაკავშირებით ზრდის მათი გამოვლენისა და შესაბამისი გადაწყვეტილებების პოვნის ალბათობას. შემუშავებული პროგრამული სისტემა დაეხმარება საბოლოო მომხმარებლებს უკეთ გააცნობიერონ უსაფრთხოების პრობლემების წყარო და სტრუქტურა , რათა მოხდეს სათანადო ზომების მიღება. თავდასხმის სტრატეგიები მუდმივად იცვლება და სისტემა, რომელიც წარმოდგენილია, შეუძლია დაეხმაროს მომხმარებლებს ოპტიმალური შემარბილებელი სტრატეგიების მიღებაში. გარდა ამისა,

სისტემა შესაფერისია უფრო დიდი ორგანიზაციების აპარატურული ინფრასტრუქტურის უზრუნველსაყოფად, რათა მკაცრი კანონებიც კი, როგორიცაა მონაცემთა დაცვის ზოგადი ევროპული რეგულაცია, სრულად იყოს გათვალისწინებული და ეფექტურად დანერგილი პრაქტიკაში.

ნაშრომი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის დაფინანსებით FR-22-14060 პროექტის ფარგლებში

გამოყენებული ლიტერატურა

1. Gagnidze, A., Iavich, M., & Iashvili, G. (2017). A Roman Version of the Merkle's Cryptosystem. Proceedings of the National Academy of Sciences of Georgia, 11(4), 28–33.
2. Deogirikar, J., & Vidhate, A. (2017). Security Breaches in IoT: A Study. In Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud (pp. 32-37). Coimbatore, India: IEEE.
3. Ronen, E., & Shamir, A. (2016). Extended Functional Attacks on IoT Devices: The Case of Smart Lights. In Proceedings of the European Symposium on Research in Computer Security (pp. 3-12). Zarrabrücken, Germany: IEEE.
4. Iashvili, G., Iavich, M., Gagnidze, A., & Gnatyuk, S. (2020). Increasing the Usability of the TLS Certificates Generation Process Using Safe Design, CEUR Workshop Proceedings, 2698, 35-41.
5. Lukova-Chuiko, N., Fesenko, A., Papirna, H., & Gnatyuk, S. (2021). Risk Management as a Method of Protection Against Cyber Threats, CEUR Workshop Proceedings, 2833, 103-113.
6. Iavich, M., Gnatyuk, S., Odarchenko, R., Bocu, R., & Simonov, S. (2021). The Novel System of Attacks Detection in 5G. In Lecture Notes in Networks and Systems (Vol. 226, pp. 580-591).