Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 1-11 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

NOVEL SYSTEM FOR HARDWARE-BASED VULNERABILITIES RECOGNITION

აპარატურულ უზრუნველყოფაზე დაფუძნებული სისტემებში უსაფრთხოების პრობლემების გამოვნელის ნაივური სისტემა

გიორგი იაშვილი კავკასიის უნივერსიტეტი, პაატა საკაძის ქ.1, 0102, თბილისი, საქართველო
Giorgi Iashvili Caucasus University, Paata Saakadze st.1, 0102, Tbilisi, Georgia

ABSTRACT. Hardware-based security mechanisms are becoming increasingly popular, but implementing these mechanisms correctly has proved difficult, thus undermining the root of security. This work introduces an effective way to formally verify important properties of such hardware security mechanisms and, consequently, determine the optimal mitigation strategies for each particular use case.The goal of the research that is reported in this paper was to understand the weaknesses of hardware-based devices and related software systems, in order to improve the necessary security mechanisms. The goal of the work is the creation of modern recognition system to identify hardware-based vulnerabilities and provide users with corresponding recommendations. This paper describes an integrated software system that analyzes the potential security threats that may affect a certain hardware-based system, and consequently suggests the optimal solutions. The result of our research is prototype of the system, which is able to collect information about modern hardware-based vulnerabilities and provide user with corresponding recommendations according to concrete scenario. Controlled test of the system was made in the frame of the research. Furthermore, in order to optimize the usability of the reports that the system generate, and the end users overall experience, the algorithmic core will be complemented with relevant machine learning elements. Thus, dedicated analysis routines will analyze the data that is stored in the database, also considering the newly entered data, will combine the available data and eventually add the required supplementary data to the database.

აბსტრაქტი. აპარატურზე დაფუძნებული უსაფრთხოების მექანიზმები სულ უფრო პოპულარული ხდება, მაგრამ ამ მექანიზმების სწორად რეალიზაცია რთული ამოცანაა. ეს ნამუშევარი წარმოადგენს ეფექტური ტექნიკის უსაფრთხოების ამგვარი მექანიზმების მნიშვნელოვანი თვისებების ოფიციალურად გადამოწმების ეფექტურ გზას და, შესაბამისად, თითოეული კონკრეტული სცენარ შემთხვევაში შემსუბუქების ოპტიმალური სტრატეგიების შემუშავებას. კვლევის მიზანი იყო აპარატურული უზრუნველყოფის სისუსტეების გაგება და მასთან დაკავშირებული პროგრამული სისტემების უსაფრთხოების აუცილებელი მექანიზმების გაუმჯობესება. სამუშაოების მიზანია თანამედროვე სისტემის შექმნა, აპარატურაზე დაფუძნებული სისუსტეების დასადგენად და მომხმარებლებისთვის შესაბამისი რეკომენდაციების მიწოდება. ამ ნაშრომში აღწერილია ინტეგრირებული პროგრამული სისტემა, რომელიც აანალიზებს უსაფრთხოების პოტენციურ საფრთხეებს, რომლებმაც შეიძლება გავლენა მოახდინონ გარკვეულ აპარატურულ სისტემაზე დაფუძნებულ მექანიზმებზე და, შესაბამისად, გვთავაზობს ოპტიმალურ გადაწყვეტილებებს. კვლევის შედეგია სისტემის პროტოტიპი, რომელსაც შეუძლია შეაგროვოს ინფორმაცია თანამედროვე აპარატურული მოწყვლადობის შესახებ და მომხმარებელს მიაწოდოს შესაბამისი რეკომენდაციები კონკრეტული სცენარის შესაბამისად. კვლევის ფარგლებში გაკეთდა სისტემის კონტროლირებადი ტესტი. გარდა ამისა, სისტემის მიერ წარმოქმნილი ანგარიშების გამოყენებასა და საბოლოო მომხმარებლების საერთო გამოცდილების ოპტიმიზაციის მიზნით, ალგორითმული ბირთვი დაკომპლექტდება შესაბამისი მანქანური სწავლების ელემენტებით. ამრიგად, სპეციალური ანალიზის სქემები დამუშავებენ

მონაცემთა ბაზაში შენახულ ინფორმაციას, და ასევე მიაქცევენ ყურადღებას ახლად შეყვანილი მონაცემების ნაკადებს. სისტემა მოახდენს ახალი მონაცემების დამატებას ბაზაში და შედეგად მივიღებთ რეკომენდაციების უკეთეს და უფრო დეტალურ ვარიანტს რაც დადებითად იმოქმედებს მომხმარებლის უსაფრთხოების დონეზე.

KEYWORDS*: hardware-based attacks, side-channel, hardware security, modern system, hardware vulnerabilities.*
საკვანძო სიტყვები: *აპარატურული, აპარატურული დაცვა, გვერდითი არხი, თანამედროვე სისტემა, აპარატურული სისუსტეები*

შესავალი

თანამედროვე კიბერ სამყაროში სარეკომენდაციო სისტემები ხელოვნური ინტელექტის მექანიზმების ყველაზე თვალსაჩინო მაგალითია. ჩვეულებრივ, ასეთი პროგრამები იქმნება მომხმარებლისთვის უკეთესი გამოცდილებისთვის სხვადასხვა სისტემებში. მაგალითად Facebook, რომელიც შეიცავს „ადამიანები, რომელბსაც შეიძლება იცნობდეთ" მოდული და YouTube, რომელიც გთავაზობთ
შესაბამის ვიდეოს ინტერესების მიხედვით, რაც დგინდება დათვალიერების წინა ისტორიის საფუძველზე. ეს ყველაფერი შეიძლება ჩაითვალოს მომხმარებელზე ორიენტირებული სარეკომენდაციო სისტემების საკმაოდ კარგ მაგალითებად. ვებ პლატფორმები მომხმარებლებს საშუალებას აძლევს მიიღოს რეკომენდაციები სხვადასხვა კრიტერიუმების საფუძველზე. ალგორითმებს, რომლებიც გამოიყენება
ასეთი პროგრამებს მიერ უწოდებენ სარეკომენდაციო სისტემებს. დღეს ალგორითმები გამოიყენება სხვადასხვა სარეკომენდაციო სისტემა, მაგრამ შინაარსზე დაფუძნებული შემოთავაზებების მეთოდი ერთ-ერთი ყველაზე ორიენტირებულია მომხმარებელზე. სარეკომენდაციო სისტემები ფართოდ
გამოიყენება შინაარსის ფილტრაციისთვის სხვადასხვა ვებ პლატფორმებში, როგორიცაა ონლაინ მაღაზიები, ფილმების ან მოგზაურობის მონაცემთა ბაზა, საგანმანათლებლო მიმართულებები და მრავალი სხვა. შინაარსის ფილტრაციის სისტემები (content filtering systems) მომხმარებლებს ეხმარება მაქსიმალურად კარგად იპოვონ შესაბამისი შინაარსი, მათი საჭიროებებიდან და ინტერესებიდან
გამომდინარე. დღეს ნებისმიერი თანამედროვე სისტემისთვის მომხმარებლის უსაფრთხოებაა უაღრესად მნიშვნელოვანია. ჰაკერები ასრულებენ შეტევას სხვადასხვა ტექნიკისა და მიდგომის გამოყენებით. აპარატურულ უზრუნველყოფაზე დაფუძნებული სისტემები ხშირად ხდება სხვადასხვა
თავდასხმების სამიზნეები. გვერდითი არხი (side-channel), ცენტრალურ პროცესორზე ორიენტირებული (central processor unit) და ფიზიკური შეტევები გარჩევის ან კრიტიკული ინფორმაციის მიღების დღეს თავდასხმის მოდელის ერთ-ერთი ყველაზე პოპულარული მეთოდია. აღსანიშნავია, რომ სხვადასხვა პროგრამული მექანიზმები სამუშაოდ დღეს იყენებენ აპარატურულ სისტემას. ასეთი სისტემების უსაფრთხოების ხარვეზებმა შეიძლება სერიოზული პრობლემები შეუქმნას მთლიანობაში მექანიზმებს. სისტემა უზრუნველყოფს მომხმარებელს რეკომენდაციებს შესაბამის ინტერესებზე და პარამეტრებზე

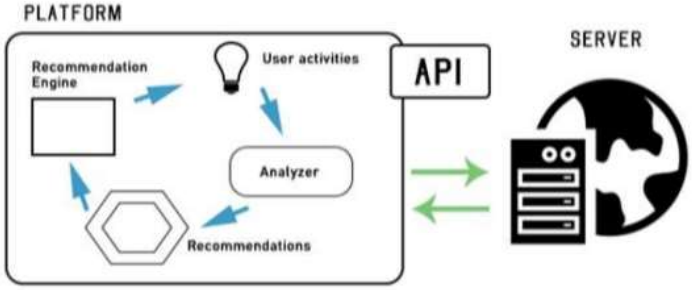
დაყრდნობით. სარეკომენდაციო სისტემის პირველი ვერსია ეყრდნობა ცნობილ ღია წყაროებს, მოწყვლადობის მონაცემთა ბაზებს და მუშაობს თითოეული მომხმარებლის შეყვანისთვის ნდივიდუალურად. მანქანური სწავლების მექანიზმების გამოყენებით, რომლებიც ჩაწერილია არსებულ რეკომენდაციების სისტემაში უკეთესი შედეგების მისაღწევად. ასეთი მიდგომა მნიშვნელოვნად გაიზრდის უსაფრთხოების დონის აპარატურულ სისტემებში.

ლიტერატურის მიმოხილვა

აპარატურულ უზრუნველყოფაზე ორიენტირებული თავდასხმები ძალიან პოპულარულია დღეისთვის. არსებობს წარმატებული ჩატარებული თავდასხმების მთლი რიგი, რომელიც ორიენტირებულია კიბერ უსაფრთხოების ამ კონკრეტულ მიმართლებაზე [1-3]. ასევე, აპარატურაზე ხშირად ფიქსირდება ე.წ. side-channel თავდასხმები, რომელიც ხორციელდება მათ შორის პროგრამულ რეალიზაციაზე და ზოგ კრიპტოგრაფიულ ალგორითმზე [4-7]. ამ პერიოდისთვის პოპულარული სისტემებიც კი შეიძლება იყოს მოწყვლადი აპარატურაზე ორიენტირებული თავდასხმების წინაშე [8-10]. აღსანიშნავია, რომ არსებობს ე.წ. კომბინირებული თავდასხმების მიდგომები, რომელიც წარმატებით ხორციელდება არსებულ უსაფრთხოების მექანიზმებზე [11-13]. განხორციელებულია ამ მიმართულებით ახალი უსაფრთხოების მექანიზმების შემუშავება და ავტორები სთავაზობენ არსებული სისტემების გაუმჯობესებულ ვარიანტებს [14-16]. ერთ-ერთი მნიშვნელოვანი მიმართულება კიბერ უსაფრთხოებაში გახლავთ IoT (ნივთების ინტერნეტი) და ე.წ. ჭკვიანი მოწყობილობები, რაც იმას ნიშნავს, რომ მუდმივად იქმნება თავდასხმების ახალი ვექტორები [17-19].

შინაარსზე დაფუძნებული სისტემების მუშაობა

უსაფრთხოების სცენარის ანალიზისთვის შინაარსზე (content-based) დაფუძნებული რეკომენდაციების სისტემას სჭირდება მომხმარებლის მიერ მოწოდებული მონაცემები და სპეციალური ჩარჩოები, რომელიც ინახება მონაცემთა ბაზაში, მაგალითად შინაარსზე დაფუძნებული პარამეტრები, შეფასება, უკუკავშირი და
მომხმარებლის სხვა აქტივობები. ამ შემთხვევაში კიბერ უსაფრთხოებაზე და ტექნიკაზე დაფუძნებულ სისტემებში, მონაცემები კონკრეტული რეკომენდაციით გაანალიზებულია სისტემის მიერ. მონაცემების შეყვანა ხდება სპეციალური ინტერაქტიული ჩაშენებული ფორმის გამოყენებით. ამ მონაცემებზე დაყრდნობით, სისტემა ქმნის მომხმარებლის პროფილს, რომელიც გამოიყენება შესაბამისი უსაფრთხოების რეკომენდაციების შესაქმნელად. ეს პროცესი ხდება მომხმარებლის მხრიდან დამატებითი ინფორმაციის შეყვანის საშუალებით. სისტემას შეუძლია ამ დამატებითი ინფორმაციის დამუშავება, რის შედეგადაც ეს მექანიზმი ხდება უფრო ზუსტი.



სურ.1. კონტენტზე დაფუძნებული სისტემის მუშაობის პრინციპი

როგორც ნაჩვენებია გრაფიკულ გამოსახულება 1-ზე, პლატფორმის შიგნით სისტემა მიუთითებს მომხმარებლის საქმიანობაზე - მონაცემებსა და პრეფერენციებზე, აანალიზებს მათ და გარდაქმნის მათ რეკომენდაციებად. მიღებული რეკომენდაციები კი იგზავნება სარეკომენდაციო ძრავასთან. პლატფორმა ქმნის კავშირი სერვერთან და გაცვლის მონაცემებს სპეციალური არხით ან სპეციალური API - თ. ყოველი ახალი იტერაცია გვაძლევს უფრო ზუსტ და მომხმარებელზე მორგებულ შედეგს, გამომდინარე იქიდან, რომ ხდება მომხმარებლის უფრო მეტი მონაცემების მოგროვება და ხდება ცნობილი მისი პრეფერენციები და სხვა აქტივობა სისტემასთან მიმართებაში.

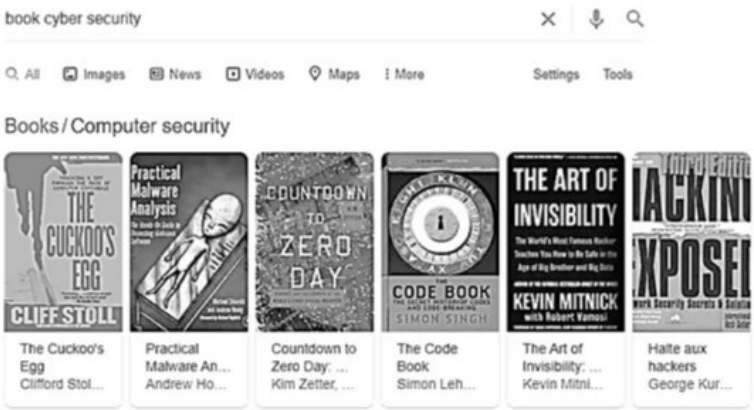
კონტენტზე დაყრდნობილ სისტემებში გამოყენებული კონცეფცია

შინაარსზე დაფუძნებულ მექანიზმებში გამოყენებული ცნებები ხშირად ეყრდნობა ინფორმაციის აღდგენის სისტემებს. ინფორმაციის მოძიების ეს სისტემები მომხმარებელს უზრუნველყოფს შესაბამისი ძიების შედეგებითა და ამავე დროს ისინი აანალიზებენ მომხმარებლის ქცევას. ეს აძლევს ამ სისტემებს შესაძლებლობას დაადგინონ, არის თუ არა მომხმარებლის ძებნის მოთხოვნა სასარგებლო. ეს პროცესი ემყარება განსხვავებული კომბინაციის ალგორითმებს, რომლებიც ხელს უწყობენ თითოეული მომხმარებლის მოთხოვნის ძიების პროცესს. ჩვენ ვხედავთ აღნიშნული ალგორითმების მუშაობას პრაქტიკაზე, როდესაც ვიყენებთ ძებნას ისეთი ძრავები, როგორიცაა Google ან Yahoo. ასეთი ტიპის საძიებო სისტემებში, ინფორმაცია აღდგენის სისტემები უფრო რთულია და მუშაობს უზარმაზარ მონაცემებთან, რაც ეყრდნობა ინტერნეტის მომხმარებლების მოთხოვნებს. საძიებო სისტემების მუშაობა შეიძლება ნათლად ჩანს, თუ შევადარებთ სხვადასხვა ძიების შედეგების შედეგებს (სურათი 2):

- Cyber security news;
- News on cyber security;

სურ2. საძიები სისტემის შედეგების დემონსტრაცია

როგორც ვხედავთ ორივე საძიებო მოთხოვნის (სურათი 2) შედეგები საკმაოდ მსგავსია. ასევე უნდა აღინიშნოს, რომ თუ ჩვენ შევასრულებთ ისეთ საძიებო მოთხოვნას, როგორიცაა მაგალითად „წიგნები კიბერ უსაფრთხოება", ჩვენ სულ სხვა შედეგს ვიღებთ. საძიებო სისტემა გვთავაზობს უსაფრთხოებასთან დაკავშირებული სხვადასხვა წიგნებს ინტერნეტში. და ასეთი შედეგი უკვე განსხვავებულია, მაგრამ საინტერესო ისაა, თუ როგორ შეუძლია საძიებო სისტემას ამოიცნოს საძიებო მოთხოვნა და მიაწოდოს მომხმარებელს შესაბამისი ინფორმაცია. საძიებო ძრავები აგროვებენ ინფორმაციას, რომელსაც მომხმარებლები აწვდიან საძიებო მოთხოვნების დროს და ამ შედეგის საშუალებით საძეობი სისტემას შეუძლია ანალიზი და შესატყვისი შინაარსში სხვადასხვა საძიებო ობიექტების პოვნა. შედეგი მიიღწევა ტექსტის მოპოვების ტექნიკის გამოყენებით. თანამედროვე საძიებო სისტემები განსხვავებული ტექსტის მოპოვების ტექნიკას იყენებენ. ყველაზე აშკარა ტექნიკა ტექსტის მოპოვებისთვის არის TF მატრიცა (ტერმინის სიხშირის მატრიცა). ამ ტექნიკის საფუძველზე კონტექსტში ყველაზე ხშირად გავრცელებულ სიტყვას უფრო მეტი აქტუალობა აქვს. საძიებო სისტემა იყენებს TF- ს მატრიცას, რომ გააანალიზოს თითოეული სიტყვის სიხშირე საძიებო სისტემაში, რომელსაც ითხოვს მომხმარებელი.



სურ 3. საძიები სისტემის შედეგების დემონსტრაცია წიგნების მაგალითზე

შინაარსობრივი ტერმინების წონა

სარეკომენდაციო სისტემებში გამოიყენება ორი ძირითადი მექანიზმი. ეს არის მექანიზმები ტერმინის სიხშირისთვის (TF) და ინვერსიული დოკუმენტის სიხშირისთვის (IDF). ჩვენ შეგვიძლია გამოვყოთ სხვადასხვა შინაარსის ვებსაიტებისთვის გამოყენებული სიტყვების სიხშირე. ჩემი კვლევის ფარგლებში დამუშავდა შემდეგი ორგანიზაციების ვებ – გვერდები:

1. სამეცნიერო კიბერ უსაფრთხოების ასოციაციის ოფიციალური ვებგვერდი;
2. Utoweb სტუდიის ოფიციალური ვებ – გვერდი;
3. საბავშვო კიბერ უსაფრთხოების უნივერსიტეტის ოფიციალური ვებ – გვერდი.

გამოსახულება 4 ასახავს თითოეული სიტყვის სხვადასხვა სიხშირის დათვლის შედეგებს ვებსაიტის შინაარსი:

	Frequency of the word					
Website	security	website	student	team	university	design
1	120	28	15	17	9	1
2	25	85	0	5	0	75
3	85	105	55	0	1	1

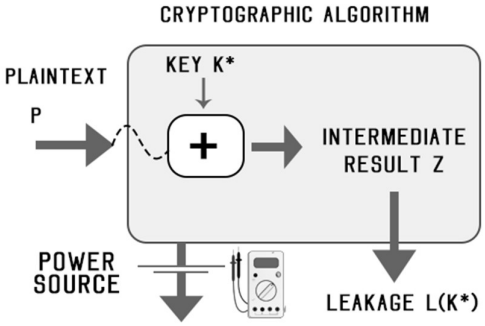
სურ 4. ტერმინების სიხშირე

ტერმინების სიხშირის შესამოწმებლად, ზემოთ აღნიშნულ ვებ – გვერდებზე უნდა დაითვალოს სიტყვების წარმოქმნის რაოდენობა. მაგალითად, ის ფაქტი, რომ კონკრეტული სიტყვა "X" პირველ ვებ – გვერდზე გვხვდება 20 – ჯერ, ხოლო მეორე ვებ – გვერდზე ოთხჯერ, არ ნიშნავს რომ სიტყვა „X“ პირველ ვებგვერდზე ხუთჯერ უფრო აქტუალურია, ვიდრე მეორეში. სხვაობა ამ შემთხვევაში გაცილებით ნაკლებია. "ტერმინი სიხშირე" - სთან ერთად უნდა გავითვალისწინოთ ”ინვერსიული დოკუმენტის სიხშირე” (IDF), რომელიც ზომავს რამდენად მნიშვნელოვანია კონკრეტული ტერმინი დოკუმენტში. ტერმინის სიხშირე (TF) ჩვეულებრივ იყოფა დოკუმენტის ზომაზე და გვიჩვენებს შინაარსის კონკრეტული პირობების საერთო რაოდენობას:

TF (A) = რამდენჯერ გამოჩნდება ტერმინი A დოკუმენტში და იყოფა ჯამზე ამ დოკუმენტის ტერმინების რაოდენობა. რადგან ინვერსიული დოკუმენტის სიხშირე (IDF) ზომავს ტერმინის მნიშვნელობას გასათვალისწინებელია, რომ ისეთი შემთხვევები, როგორიცაა "the", "of", "or", "is" შეიძლება აღმოჩნდეს ბევრი შინაარსში, მაგრამ ნაკლები წონა ექნება. ბალანსის მიღება შესაძლებელია შემდეგი ფორმულით:

IDF (A) = log_e (ყველა დოკუმენტის რიცხვი გაყოფილი დოკუმენტების რაოდენობაზე შინაარსით A). მაგალითად, ჩვენ გვაქვს ტერმინი A, რომელიც 3-ჯერ გვხვდება D დოკუმენტში, რომელიც ჯამში შეიცავს 100 სიტყვას, TF ტერმინისთვის გამოითვლება (3/100) = 0,03.

გვერდითი არხის თავდასხმა პრაქტიკაზე - დღეისთვის გვერდითი არხის თავდასხმები მიკროკონტროლერებზე არის ძალიან გავრცელებული სურათი 5 ახდენს ამ თავდასხმის პროცესის დემონსტრაციას. მაგალითში ნაჩვენებია თავდასხმა AES - ის პროგრამულ



რეალიზაციაზე.

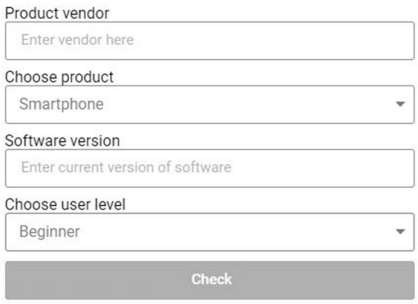
სურ 5. გვერდითი არხის თავდასხმა

ამ თავდასხმის მიზანია კრიპტოგრაფიული ალგორითმის ფარული $k*$ გასაღბის მიღება. თავდამსხმელს შეუძლია შეყვანილი p მონაცემების და მიკროკონტროლერის ელექტრომოხმარების გაანალიზება. შიფრაციის ალგორითმი ამ შემთხვევაში უკვე ცნობილია. ერთადერთი რამ, რაც არ არის ცნობილი ფარული გასაღები $k*$-ია. თავდამსხმელს შეყვანილი p-ს მიხედვით შეუძლია შუალედური z შედეგის მიღება. შუალედური შედეგი z ეფუძნება შეყვანილ p მონაცემებს და $k*$ ფარულ გასაღებს. გვერდითი არხის გაჟონვის გაანალიზებით ხდება ცნობილი შუალედური z და შეიძლება გაკეთდეს ჰიპოტეზური ტესტი $k*$-ზე. გაჟონილი ინფორმაცია რომელიც გამოწვეულია z - ით შეიძლება იყოს წარმოდგენილი ფუნქციით გასაღბის მნიშვნელობით $k*$.

$$L(k^*) = f_{k^*}(p) + \varepsilon \qquad (1)$$

ფუნქცია f_{k^*} დამოკიდებულია კრიპტოგრაფიულ ალგორითმზე და რეალიზაციის მეთოდებზე პროგრამულ და აპარატულ უზრუნველყოფაში. ფუნქციიდან ჩნდება შეცდომის ε რომელიც ხმაურის ცვლადს წარმოადგენს და არის დამოუკიდებელი.

შემუშავებული სისტემა



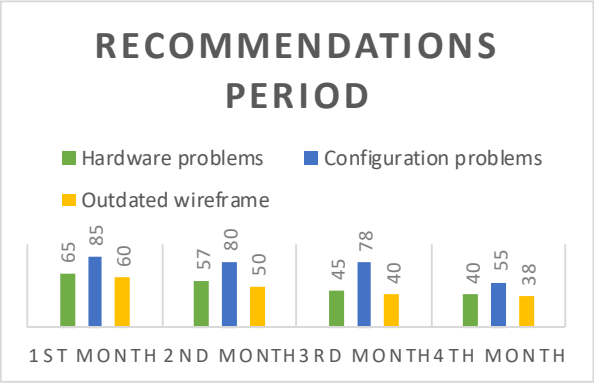
სურ 6. სისტემის ინტერფეისის ნაწილი

სისტემა, რომელიც შემუშავდა კვლევის ფარგლებში შეყვანილი მონაცემების საფუძველზე ახდენს აპარატურულ უზრუნველყოფაზე დაფუძნებული სქემების უსაფრთხოების დონის დადგენას. მსგავსი ტიპის შეფასება შეიძლება მოხდეს როგორც საოფისე, ასევე ინდუსტრიულ და IoT გარემოში. წარმოდგენილი სისტემა არის შექმნილი web აპლიკაციის სახით, რომელიც ვრცელდება ღია წყაროს მოდელით (open source). სისტემა თავის შეფასების მეთოდებში იყენებს სპეციალიზირებულ მონაცემთა ბაზებს, რომლებშიც ინახება ინფორმაცია თანამედროვე და აქტუალური უსაფრთხოების პრობლემების და თავდასხმების შესახებ. ამ პლატფორმებში შედის ისეთი რესურსები როგორიცაა AttackerKB, CVE MITRE და ExploitDB. სისტემაში ხდება ზემოაღნიშნული ბაზებიდან აქტუალური და განახლებადი ინფორმაციის მიღება. სისტემაში მონაცემები ნაწილდება რამდენიმე კატეგორიის მიხედვით: აპარატურული უსაფრთხოებაზე თავდასხმის ვექტორები, ახალი სისუსტეები არსებულ პროდუქტებში და მოწყვლადობა სისტემების განუახლებელ ვერსიებში. არსებული ინფორმაციის დამუშავების საფუძველზე, სისტემის მიერ ხდება შესაბამისი რეკომენდაციის გაცემა.
სისტემის სამუშაო მექანიზმი ეფუძნება ინფორმაციის მოგროვებას კონკრეტული აპარატურლი უზრუნველყოფის მიხედვით. ერთ-ერთი ყველაზე პოპულარული თავდასხმების ტიპი აპარატურულ უზრუნველყოფაზე არის ე.წ. გვერდითი არხის (side-channel) თავდასხმა. კვლევის ფარგლებში შექმნილ სისტემას აქვს შესაძლებლობა დაადგინოს გვერდითი არხის გაჟონვა საშუალო შედეგით z. ეს გაჟონვა შეიძლება იყოს წარმოდგენილი ფუნქციის სახით რომლის გასაღების მნიშვნელობაა k^*, სისტემას შეუძლია შეაფასოს გაჟონვის შესაძლებელი დონე შესაბამისი პარამეტრების გამოყენებით და ხმაურის დამოუკიდებელი ε ცვლადით.

შედეგების განხილვა

კვლევის ფარგლებში, მოხდა შექმნილი სისტემის შემოწმება სხვადასხვა მოწყობილობებზე და ტექნიკაზე ორიენტირებულ პროგრამულ პლატფორმებზე, რომლებიც სხვადასხვა ორგანიზაციას ეკუთვნის. ტესტირების პერიოდი იყო ოთხი თვე. ამრიგად, ჩართულმა ორგანიზაციებმა თვეში ერთხელ გამოსცადეს თავიანთი სისტემები, რათა მოგვაწოდონ მონაცემები, რომლებიც აუცილებელია უსაფრთხოების დონის გაუმჯობესების თვალსაზრისით. მოწყობილობები,

რომლებიც ყოველდღე გამოიყენება სხვადასხვა ორგანიზაციებში სხვადასხვა მიზნებისთვის, სადაც ტესტირება ხდება წარმოდგენილი სისტემის გამოყენებით. ამრიგად, იგი გამოიყენეს დარეგისტრირებულმა ორგანიზაციებმა და შეგროვებული მონაცემების საფუძველზე შეიქმნა რეკომენდაციების სრული სია, რომლებიც სინთეზურად არის წარმოდგენილი სურათზე 7.



სურ 7. სარეკომენდაციო პერიოდი

შეგროვებული მონაცემები ეხება კიბერუსაფრთხოებასთან დაკავშირებული სამი კატეგორიის პრობლემას: აპარატურის პრობლემებს, კონფიგურაციის პრობლემებს და მოძველებულ ქსელურ სტრუქტურებს. ამრიგად, აღმოჩნდა, რომ უსაფრთხოების ყველაზე გავრცელებული საკითხი ეხებოდა აპარატურის არასწორ კონფიგურაციას, რამაც შეიძლება მომავალში სერიოზული პრობლემები გამოიწვიოს. შესაბამისად, ჩართულ ორგანიზაციებს მიეწოდათ შესაბამისი რეკომენდაციები.

დღეს კომპიუტერული მეცნიერების თეორიასა და პრაქტიკაში სტანდარტული კრიპტოგრაფიული ალგორითმები უსაფრთხოდ ითვლება კლასიკური კომპიუტერების შეტევისგან. ხაზგასმით უნდა აღინიშნოს, რომ აპარატურაზე დაფუძნებულ გვერდითი არხების შეტევებმა შეიძლება გაჟონოს ინფორმაცია შიფრის შესახებ. ეს დღეს კომპიუტერულ მეცნიერებაში დიდი პრობლემაა. სისტემით, რომელსაც ამ კვლევის ფარგლებში ვთავაზობ, ამ პრობლემის მოგვარება შეიძლება. თანამედროვე ტექნიკაზე დაფუძნებული სისუსტეების ამოცნობის სისტემა იყენებს ახალ მიდგომას პრობლემის გასაანალიზებლად კონკრეტული სცენარის საფუძველზე. ახალი მიდგომა იყენებს ცნობილ ტექნიკურ მოწყვლადობის მონაცემთა ბაზებს, გაანალიზებული სისტემის მდგომარეობის გათვალისწინებით. ტექნიკურ ბაზაზე დაფუძნებული სხვადასხვა შეტევები წარმატებით ხორციელდება ბიზნესის, განათლებისა და ფინანსური სფეროების ცნობილ სისტემებზეც კი. ეს ფაქტი თანამედროვე რეკომენდაციების სისტემას უნიკალურ და არსებულ სიტუაციასთან შესაბამისობაში აქცევს. ეს ნიშნავს, რომ გათვალისწინებული მიდგომის საფუძველზე, მრავალ ორგანიზაციას, რომელიც მუშაობს სხვადასხვა მიმართულებით, შეუძლია შეავსოს უსაფრთხოების ხარვეზები ტექნიკურ სისტემებზე და, შესაბამისად, გაზრდის მათ უსაფრთხოების დონეს.

რეკომენდაციების სისტემაში გამოყენებული მეთოდები ემყარება პრაქტიკულ ანალიზის მიდგომებსა და პოპულარულ მონაცემთა ბაზებს. ეს ფაქტი რეკომენდაციებს შესაბამის და სასარგებლოს ხდის როგორც საბოლოო მომხმარებლებისთვის, აგრეთვე ორგანიზაციებისათვის.

ACKNOWLEDGEMENTS

ნამუშევარი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის მიერ დაფინანსებული PHDF-19-519 პროექტის ფარგლებში.

ბიბლიოგრაფია

1. Taehyun K. Reinforcing Meltdown Attack by using a Return Stack Buffer / K.Taehyun, S. Youngjoo // IEEE Access - 2019 - P. 186065 – 186077. DOI: 10.1109/ACCESS.2019.2961158
2. ZombieLoad: Cross-Privilege-Boundary Data Sampling / [M. Schwarz, M. Lipp, D. Moghimi, et al.] // ACM SIGSAC Conference on Computer and Communications Security, London, 11-15 November 2019: proceedings. ACM CCS 2019 - P. 753–768.
3. Clavier C. Differential power analysis in the presence of hardware countermeasures / C. Clavier, J-S Coron, N Dabbous // CHES – 2000, Worcester 17-18 August, 2000 - P. 252–263.
4. Schaumont P. Masking and dual-rail logic don't add up / P Schaumont, K Tiri // Cryptographic hardware and embedded systems, Vienna 10-13 September 2007: proceedings. CHES 2007 – P. 95–106.
5. Abomhara M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks / M. Abomhara, Geir M. Køien // Journal of Cyber Security and Mobility – 2015 – Vol. 4, Issue 1. - P. 65-68.
6. Ishai Y. Private Circuits: Securing Hardware against Probing Attacks / Y. Ishai, A.Sahai, D. Wagner. // Advances in Cryptology, Santa Barbara 17-21 August 2003: proceedings. CRYPTO 2003 - Vol. 2729 – P. 463-481.
7. Dan P. Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel / P. Dan // IACR Cryptology ePrint Archive. - 2002. – Vol. 169 – P. 170-184.
8. Samer M. Hardware attacks: an algebraic approach / M. Samer, G. Fayez, G. T. Aaron // Journal of Cryptographic Engineering. – 2006. – Vol. 6 – P. 325-337. DOI: 6. 10.1007/s13389-016-0117-6
9. Hardware attack risk assessment / [M. Samer, F. Gebali, T. Gulliver et al.] // ICES. – 2015. - Vol. 1109. DOI: 10.1109/ICCES.2015.7393073
10. Voyiatzis A. Active hardware attacks and proactive countermeasures / A.Voyiatzis , D. Serpanos // International Symposium on Computers and Communications, Taormina 1-4 July 2002 – Vol. 10 - P. 361 - 366. DOI: 10.1109/ISCC.2002.102170
11. Bouffard G. Combined Software and Hardware Attacks on the Java Card Control Flow / G . Bouffard, J .Iguchi-Cartigny, JL. Lanet // Prouff E. (eds) Smart Card Research and Advanced Applications. – 2011. - Vol. 10 – Issue 2. - P. 283-296. DOI: 10.1007/978-3-642-27257-8_18
12. Exploiting the analog properties of digital circuits for malicious hardware / [Y. Kaiyuan, H. Matthew, D. Qing et al.] // Communications of the ACM – 2017- Vol. 60 – P. 83-91. DOI: 10.1145/3068776

13. Hardware Trojan Attacks: Threat Analysis and Countermeasures / [S. Bhunia, M. S. Hsiao, M. Banga et al.] // International Conference on Communications (ICC), Sydney, 10-14 June 2014: proceedings. – IEEE ICC, 2014 - P. 1229-1247.
14. Lattice Based Merkle / [M. Iavich, G. Iashvili, A. Gagnidze et al.] // IVUS 2019, Kaunas 25 April 2019: proceedings. - CEUR-WS - 2019 – vol. 2470 – P.13-16.
15. Protection against Hardware Trojan Attacks: Towards a Comprehensive Solution / [S. Bhunia, M.Abramovici, D. Agrawal et al.] // IEEE Design & Test – 2013. - Vol. 30 - P. 6-17.
16. Gagnidze A. Novel Version of Merkle Cryptosystem / A. Gagnidze, M. Iavich, G. Iashvili // Bulletin of the Georgian National Academy of Sciences. – 2017. – Vol. 11, Issue 4. – P. 28 – 33.
17. Deogirikar J. Security attacks in IoT: A survey / J. Deogirikar, A. Vidhate // International conference IoT in Social, Mobile, Analytics and Cloud, Coimbatore 10-11 February 2017: proceedings. IEEE, 2017 – P. 32-37.
18. Ronen E. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights / E. Ronen ,A. Shamir // European Symposium on Security and Privacy, Saarbrücken 21-24 March 2016: proceedings. IEEE, 2016 – P. 3-12.