Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 29-33 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

მანქანური მეთოდების გამოყენება სარეკომენდაციო სისტემებში
USE OF MACHINE LEARNING IN RECOMMENDER SYSTEMS

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 მანქანური სწავლება და ხელოვნური ინტელექტი დღეს სულ უფრო გავრცელებული ხდება. ისინი გამოიყენება სხვადასხვა სფეროში, მათ შორის ენერგეტიკის, სამედიცინო და ფინანსური სექტორების, სხვადასხვა ამოცანების შესასრულებლად და ძირითადი არჩევანის დასახმარებლად. სხვა გამოყენებასთან ერთად, მანქანათმცოდნეობა და ხელოვნური ინტელექტი გამოიყენება მძლავრი სარეკომენდაციო ძრავების შესაქმნელად, რათა მომხმარებელს მიაწოდოს შესაბამისი რეკომენდაციები სხვადასხვა მიმართულებით, როგორიცაა ფილმების რეკომენდაციები, მეგობრების წინადადებები სოციალურ ქსელებში და მრავალი სხვა. ამ ნაშრომის მიზანი არის აპარატურაზე დაფუძნებული სისტემების და მასთან დაკავშირებული მექანიზმების მოწყვლადობის იდენტიფიცირება და გაგება, უსაფრთხოების შესაბამისი ზომების გასაუმჯობესებლად. ნაშრომის მიზანია განახლებული ამოცნობის სისტემის მოდელის შემუშავება, რათა გამოავლინოს აპარატურაზე დაფუძნებული ხარვეზები და მიაწოდოს მომხმარებლებს საჭირო რეკომენდაციები.

საკვანძო სიტყვები: *მანქანური სწავლება, კონტენტზე დაფუძნებული, დაუცველობის იდენტიფიკაცია;*

ABSTRACT Machine learning and artificial intelligence are becoming increasingly common today. They are used in a variety of fields, including the energy, medical and financial sectors, to perform a variety of tasks and assist with key choices. Among other applications, machine learning and artificial intelligence are used to build powerful recommendation engines to provide users with relevant recommendations in a variety of areas, such as movie recommendations, friend suggestions on social networks, and much more. The objective of this paper is to identify and understand the vulnerabilities of hardware-based systems and related mechanisms in order to improve appropriate security measures. The aim of this paper is to develop an updated detection system model to detect hardware-based faults and provide users with necessary recommendations.

KEYWORDS: *machine learning, content-based, vulnerability identification;*

შესავალი:

მანქანური სწავლება და ხელოვნური ინტელექტი დღეს სულ უფრო გავრცელებული ხდება. ისინი გამოიყენება სხვადასხვა სფეროებში, მათ შორის ენერგეტიკის, სამედიცინო და ფინანსური სექტორებში, სხვადასხვა ამოცანების შესასრულებლად. სხვა გამოყენებასთან ერთად, მანქანური სწავლება და ხელოვნური ინტელექტი გამოიყენება მძლავრი სარეკომენდაციო სისტემების შესაქმნელად, რათა მომხმარებელს მიაწოდოს შესაბამისი რეკომენდაციები სხვადასხვა მიმართულებით, როგორიცაა ფილმების რეკომენდაციები, მეგობრების წინადადებები სოციალურ ქსელებში და მრავალი სხვა. კომპიუტერულ მეცნიერებაში არსებობს მრავალი გზა და მექანიზმი, რომლებიც იყენებენ კომპიუტერის ცენტრალურ პროცესორს (CPU). CPU-ს არქიტექტურა ასევე გადამწყვეტია კიბერუსაფრთხოების პროცესის შესრულების თვალსაზრისით. შედეგად, დღევანდელი პოპულარული ავტომატიზაციისა და

დაშიფვრის პროცედურები ეყრდნობა პროცესორის სიმძლავრეს კიბერუსაფრთხოების სხვადასხვა საკითხთან დაკავშირებით.

ეფექტური კიბერუსაფრთხოების მექანიზმების შემუშავება და დანერგვა არსებითად ეყრდნობა სათანადო ალგორითმული ბირთვების განხილვას. ამიტომ, უსაფრთხოების ალგორითმების შემუშავების მიზნით, რომლებიც უფრო ეფექტური და გამოსაყენებელია, განიხილება სხვადასხვა მიდგომები. ამრიგად, ავტომატიზაციის მექანიზმების ეფექტურობისა და უსაფრთხოების გაუმჯობესება შეიძლება განხორციელდეს მანქანის ცენტრალური დამუშავების ერთეულის ერთდროულად მუშაობისას სისტემის ზოგიერთ ასპექტზე შესაბამის პროგრამულ კომპონენტებთან ერთად. ამრიგად, CPU-ს ეფექტური გამოყენება შესაბამისი კიბერუსაფრთხოების მექანიზმების ოპტიმიზაციის მიზნით, გულისხმობს რამდენიმე ფაქტორის გათვალისწინებას.

ეს უფრო ფართო სამეცნიერო სფერო გულისხმობს რამდენიმე კვლევის თემის განხილვას, როგორიცაა ცენტრალური დამუშავების განყოფილების ფიზიკური განხორციელება, მონაცემთა ეფექტური გამოთვლა და მონაცემთა გადაცემის მეთოდები პროგრამულ კომპონენტებთან ან საბოლოო მომხმარებელთან კომუნიკაციის დროს. ნაშრომი სტრუქტურირებულია შემდეგი სექციების მიხედვით: მეორე განყოფილებაში განხილულია უსაფრთხოების მექანიზმი, რომელიც ჩამოყალიბებულია ცენტრალური პროცესორის დონეზე. გარდა ამისა, წარმოდგენილია თანამედროვე თავდასხმების ძირითადი ელემენტები, რომლებიც მიზნად ისახავს ცენტრალური პროცესორის სიმძლავრის გამოყენებას. გარდა ამისა, წარმოდგენილია უსაფრთხოების შესაბამისი მექანიზმი, რომელიც ეხება IoT-ის საზღვრებს, რის შემდეგ წარმოდგენილია აპარატურაზე დაფუძნებული დაუცველობის ამოცნობის ახალი სისტემა და შეფასებულია მისი პრაქტიკული შესრულება.

დღევანდელი მექნიზმების განხილვა

უსაფრთხოების თანამედროვე მექანიზმების განვითარების მიუხედავად, კიბერშეტევები სხვადასხვა სისტემაზე თითქმის ყოველდღე ხდება. თავდამსხმელები ცდილობენ გამოიყენონ ყოველთვის უფრო რთული და კრეატიული მეთოდები თავიანთი მიზნების მისაღწევად. შესაბამისად, დაუყოვნებლივ უნდა აღინიშნოს, რომ თანამედროვე პროგრამული უზრუნველყოფის და ტექნიკის დაცვის სქემების შემუშავებასთან ერთად იქმნება ახალი თავდასხმის ვექტორები, რომ ცნობილი ორგანიზაციებიც კი ხდებიან ჰაკერების სამიზნე. დღესდღეობით არსებობს უამრავი აპარატურაზე ორიენტირებული შეტევა სხვადასხვა კატეგორიაში. ამრიგად, ყველაზე გავრცელებული შეტევები, რომლებიც ძირითადად ეხება ცენტრალურ პროცესორს, არის DoS შეტევები და CPU-ს გვერდითი არხის შეტევები.

DoS შეტევები - DoS შეტევების კლასი აჯგუფებს უსაფრთხოების საფრთხეებს, რაც თითქმის შეუძლებელს ხდის ცენტრალური პროცესორის სწორ მუშაობას. ამრიგად, DoS შეტევა გულისხმობს, რომ გამოყენებულია ხელმისაწვდომი გადამამუშავებელი რესურსების მნიშვნელოვანი რაოდენობა, ისე, რომ ცენტრალური დამუშავების ერთეულის მოქმედება მნიშვნელოვნად მცირდება. თავდამსხმელს შეუძლია აიძულოს CPU მთლიანად შეწყვიტოს მუშაობა მთელი DoS შეტევების დროს. ასეთი მკვეთრი ეფექტი მიიღწევა პროცესორის რესურსების მეშვეობით, როგორიცაა რეგისტრების, ფუნქციური და ლოგიკური ერთეულების აქტიურ მდგომარეობაში შენახვით. შესაბამისად, ცენტრალური პროცესორის განყოფილება დაკავებულია და ვერ ასრულებს დამატებით დავალებებს. ზოგიერთ შემთხვევაში, ასეთი შეტევა ხელს უწყობს სტრუქტურის ხარვეზებს, რომლებიც ეხება ცენტრალური პროცესორის განყოფილების არქიტექტურას. ამრიგად, ასეთი შეტევები ხორციელდება გარე მოწყობილობების ენერგიის გამოყენებით.

IoT მოწყობილობები წარმოადგენს განხილული თავდასხმების პროგნოზირებულ სამიზნეს. კლასიკური DoS შეტევების გათვალისწინებით, ჰაკერები აკონტროლებენ სხვადასხვა მოწყობილობას, მათ შორის IoT პარამეტრებს. თავდამსხმელები ქმნიან ლოგიკურ სტრუქტურებს დაზარალებული IoT მოწყობილობებიდან, რომლებსაც ბოტნეტებს უწოდებენ და ისინი უგზავნიან უამრავ მავნე მოთხოვნას მსხვერპლს, რითაც ეფექტურად ქმნიან DoS შეტევას. ადგილობრივი ცენტრალური დამუშავების

ერთეულების შემთხვევაში, თავდამსხმელებს ასევე შეუძლიათ გამოიყენონ სპეციალური მავნე პროგრამები, რომლებიც აიძულებენ CPU-ს არქიტექტურულ დაუცველობას ჰაკერისთვის.

CPU-ს გვერდითი არხის შეტევები - კლასიკური გვერდითი არხის შეტევები ეფუძნება კრიპტოგრაფიული მექანიზმების დარღვევას და ინფორმაციის მიღებას დაშიფვრის სისტემის ფიზიკური იმპლემენტაციისგან. გვერდითი არხის შეტევები იყენებს კრიპტოგრაფიული მექანიზმების გაჟონულ ინფორმაციას, როგორიცაა დროის ინფორმაცია, ელექტრომაგნიტური გაჟონვა ან ენერგიის მოხმარება. ჩვეულებრივი გვერდითი არხის შეტევის ტიპიური მაგალითია დაშიფვრის გასაღების მოპარვის უნარი, რაც შეიძლება მიღწეული იყოს ჰაკერის მიერ სამიზნე მოწყობილობის ენერგიის მოხმარებაზე თვალთვალის გზით. გვერდითი არხის შეტევებმა ასევე შეიძლება ჰაკერებს მისცეს საშუალება დააკვირდნენ კომპიუტერის ეკრანის ელექტრომაგნიტურ ველს ან განახორციელონ აკუსტიკური შეტევა სამიზნე მოწყობილობის კლავიატურის ხმის ჩასაწერად, რათა მიიღონ შესაბამისი ფრაზები.

ცენტრალური დამუშავების ერთეულზე ორიენტირებული გვერდითი არხის შეტევები, როგორიცაა საზღვრების შემოწმების შემოვლითი, შეუძლია გამოიყენოს CPU ქეში, როგორც გვერდითი არხი. ეს შეტევა შეიძლება განხორციელდეს Intel-ზე, IBM-ზე და ARM-ის ზოგიერთ ცენტრალურ დამუშავების ერთეულზე. ასეთი თავდასხმის დროს ჰაკერები იღებენ მონაცემებს პროცესორის ქეში მეხსიერებიდან. შესაბამისად, თავდამსხმელს შეუძლია მიიღოს წვდომა კრიტიკულ მონაცემებზე იმით, რომ ერთ პროცესს საშუალებას აძლევს ამოიღოს ინფორმაცია სისტემაში აქტიური სხვა პროცესის მეხსიერებიდან. გარდა ამისა, ცენტრალური დამუშავების ერთეულზე ორიენტირებული გვერდითი არხის შეტევა იყენებს თანამედროვე Intel პროცესორების Rogue Data Cache Load (RDCL) დაუცველობას. ეს დაუცველობა საშუალებას აძლევს თავდამსხმელს აიძულოს მომხმარებლის პროცესები წაიკითხოს ბირთვის დაცული მეხსიერება, რითაც ეფექტურად გადალახოს უსაფრთხოების საზღვრები [1].

ცენტრალური დამუშავების ერთეულზე ორიენტირებული გვერდითი არხის შეტევა არის ZombieLoad Attack, რომელიც ძირითადად მიზნად ისახავს Intel-ის მიერ გამოშვებულ პროცესორების უახლეს ვერსიებს. შეტევა ეყრდნობა მიკროარქიტექტურული მონაცემების შერჩევის დაუცველობას, რომლებიც გამოიყენებოდა ინტელის პროცესორების წინასწარი თაობების წინასწარი შეტევებისთვის. ZombieLoad თავდასხმის დროს თავდამსხმელი იღებს წვდომას და კითხულობს სენსიტიურ ინფორმაციას, რომელიც ინახება ცენტრალურ დამუშავების განყოფილებაში.

დაუცველობა ეფუძნება პროცესორის მიერ შემოთავაზებულ ფუნქციას, რომელიც ცდილობს სისტემის მიერ გაცემული მომავალი ბრძანებების პროგნოზირებას და ამ მეთოდს ეწოდება სპეკულაციური შესრულება. ეს ფუნქცია საშუალებას აძლევს ცენტრალური დამუშავების ერთეულს უფრო სწრაფად იმუშაოს , მაგრამ ასევე შეუძლია თავდამსხმელებს საშუალება მისცეს ჩაჭრას მგრძნობიარე მონაცემები, როგორიცაა მომხმარებლის ინფორმაცია და პაროლები. შესაბამისად, Intel-მა გამოუშვა პატჩები, რომლებიც აგვარებენ მოწყვლადობას, მაგრამ ისინი ასევე აღიარებენ, რომ შესაბამისი შემარბილებელი ღონისძიებები სრულად ვერ აღკვეთს მგრძნობიარე მონაცემების გაჟონვას CPU-ზე ორიენტირებული გვერდითი არხის შეტევების დროს, როგორიცაა ZombieLoad Attack-ის ახალი ვერსია .

ფიზიკური თავდასხმების განხილვა

ფიზიკური შეტევები - ჰაკერისთვის მთავარი მიზანი წარმატებული შეტევის მიღწევაა, მაგრამ შეტევის შესაბამისი მეთოდები შეიძლება განსხვავდებოდეს. ფიზიკურ შეტევებს IoT მოწყობილობებზე ესაჭიროებათ უშუალო კონტაქტი მიზანთან. უმეტეს შემთხვევაში, ასეთი თავდასხმების შედეგი არის აპარატურის გატეხვა სხვადასხვა ფიზიკური ფაქტორების გამო. გარდა ამისა, ზოგიერთი IoT მოწყობილობა განთავსებულია შენობების გარეთ და ძალიან მგრძნობიარეა ფიზიკური შეტევების მიმართ.

სადაზვერვო შეტევები – IoT მოწყობილობებზე ასეთი თავდასხმის დროს ჰაკერები არ ახორციელებენ ავტორიზებულ მანიპულაციებს სისტემასთან ან ქსელთან მიმართებაში. ამრიგად, სადაზვერვო შეტევები შეიძლება შედგებოდეს პორტის სკანირებით, პაკეტების ამოცნობით და ქსელის ტრაფიკის ანალიზით.

Distributed Denial-of-Service (DDoS) თავდასხმები – თავდასხმის ყველაზე პოპულარული სახეობა, რომელიც ჩვეულებრივ ხორციელდება უკვე ინფიცირებული მოწყობილობების (ბოტნეტის) გამოყენებით და ორიენტირებულია ერთ კონკრეტულ სამიზნეზე. ასეთი თავდასხმების მიზანია სერვისის ან მოწყობილობის მიუწვდომელი გახადოს დიდი რაოდენობით არალეგიტიმური მოთხოვნების გაგზავნით, რაც ქმნის მავნე ტრაფიკის ნაკადს მიზნობრივი სისტემებისთვის.

წვდომის შეტევები – ამ კატეგორიის თავდასხმის გათვალისწინებით, ჰაკერი იძენს არაავტორიზებულ წვდომას გარკვეულ ქსელებსა თუ მოწყობილობებზე. წვდომის შეტევები შეიძლება განხორციელდეს ორი განსხვავებული გზით: სისტემაზე ფიზიკური წვდომით ან დისტანციურად. ცხადია, მეორე მეთოდი ნაკლებად სარისკოა თავდამსხმელისთვის, შესაბამისად, უფრო ხშირად გამოიყენება ვიდრე პირველი.

თავდასხმები კონფიდენციალურობაზე - კონფიდენციალურობის დაცვა IoT-ის კონტექსტში ძალიან რთულია ინფორმაციის დიდი მოცულობის გამო, რომელიც ადვილად ხელმისაწვდომია დისტანციური წვდომის არხებით. ამრიგად, კონფიდენციალურობაზე პოპულარული თავდასხმები წარმოდგენილია მონაცემთა მოპოვებით და კიბერ ჯაშუშობით.

ექსპერიმენტები

არსებული პრობლემების გათვალისწინებით, რომლებიც დაკავშირებულია აპარატურულ ინფრასტრუქტურასთან, განსაკუთრებით დიდ ორგანიზაციებში, ძალზე მნიშვნელოვანია იმ მოწყობილობებზე თავდასხმების პრევენციის გზების პოვნა, რომლებიც უმეტეს შემთხვევაში კონფიდენციალურ ინფორმაციას ინახავს და გადასცემს. აპარატურაზე ორიენტირებული შეტევების განხორციელების შესაძლებლობა თუნდაც დისტანციურად აყენებს დიდი რაოდენობით სისტემებს რისკის ქვეშ. ბუნებრივია დავასკვნათ, რომ აპარატურა არის ძალიან მნიშვნელოვანი კვლევის მიმართულება კიბერუსაფრთხოების სფეროში, რომელსაც დიდი ყურადღება სჭირდება როგორც საბოლოო მომხმარებლების, ასევე მწარმოებლების მხრიდან. გარდა ამისა, აუცილებელია იმ პროცესების ეფექტური და ზუსტი მენეჯმენტის უზრუნველყოფა, რომლებიც მხარდაჭერილია სპეციალიზებული აპარატურით, როგორიცაა IoT-ზე დაფუძნებული სისტემები, რომლებიც აკონტროლებენ სამრეწველო მანქანებს ან ახორციელებენ მაღაზიების მენეჯმენტს. ამრიგად, რთული პროცესია უსაფრთხოების სტანდარტული მექანიზმის შექმნა, რომელიც გამოიყენება ნებისმიერი თანამედროვე აპარატურაზე ორიენტირებული სისტემისთვის. მწარმოებლები, რომლებიც იყენებენ არსებულ სტანდარტებს მიკრო სქემების და ტექნიკის ნაწილების შესაქმნელად, რომლებიც ძირითადად იმართება სპეციალური პროგრამული კომპონენტებით. პროგრამული უზრუნველყოფა შეიძლება შეიქმნას კონკრეტული სისტემის ან სისტემების ჯგუფისთვის.

დასკვნა

დღეისთვის არსებული სარეკომენდაციო მექანიზმები შესაძლებელია მოერგოს კიბერუსაფრთხოების მიმართულებას და იქნეს გამოყენებული სხვადასხვა ტიპის თავდასხმების ვექტორების იდენტიფიცირებისთვის და შემდგომი პრევენციისთვის.

საჭიროა მეტი მუშაობა ჩატარდეს ამ მიმართულებით. ერთ-ერთი რეალური ვარიანტი ამ სფეროს განვიტარებისა არის ახალი, კიბერუსაფრთხოების სფეროზე მორგებული სისტემის შემუშავება, რომელიც იქნება გამოყენებადი სხვადასხვა კიბერ თავდასხმების ან / და სხვა ინციდენტებზე რეაგირების თანამედროვე მეთოდი.

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

გამოყენებული ლიტერატურა

1. Taehyun, K., & Youngjoo, S. (2019). Reinforcing Meltdown Attack with the Use of Return Stack Buffer. IEEE Access, 2019, 186065–186077. DOI: 10.1109/ACCESS.2019.29
2. Schwarz, M., Lipp, M., Moghimi, D., et al. (2019). ZombieLoad: Cross-Privilege-Boundary Data Sampling. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (pp. 753–768). London, UK.
3. Clavier, C., Coron, JS., & Dabbous, N. (2000). Differential Power Analysis with Countermeasures against Techniques. In CHES Proceedings (pp. 252–263). Worcester, MA.
4. Schaumont, P., & Tiri, K. (2007). Masking and dual-rail logic don't add up. In Proceedings of Cryptographic Hardware and Embedded Systems (pp. 95–106). Vienna, Austria.
5. Abomhara, M., & Køien, G. M. (2015). Cybersecurity and Internet of Things: Challenges, Risks, Protection, and Safety Measures. Journal of Cybersecurity and Mobility, 4(1), 65-68.
6. Iavich, M., Gnatyuk, S., Odarchenko, R., Bocu, R., Simonov, S. (2021). The Novel System of Attacks Detection in 5G. In: Barolli, L., Woungang, I., Enokido, T. (eds) Advanced Information Networking and Applications. AINA 2021. Lecture Notes in Networks and Systems, vol 226. Springer, Cham. https://doi.org/10.1007/978-3-030-75075-6_47
7. Iavich, M., Iashvili, G., Gnatyuk, S., Tolbatov, A., Mirtskhulava, L. (2021). Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. In: Lopata, A., Gudonienė, D., Butkienė, R. (eds) Information and Software Technologies. ICIST 2021. Communications in Computer and Information Science, vol 1486. Springer, Cham. https://doi.org/10.1007/978-3-030-88304-1_15