Scientific and Practical Cyber Security Journal (SPCSJ) 9(2): 41 – 43 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ATTACKING PASSWORDS USING AI
პაროლებზე შეტევა AI-ს გამოყენებით

Sergei Simonovi[1,2], Andria Adamia[1], Nikoloz Kadagishvili[1], Nikoloz Sanikidze[1]
[1]University of Young Penetration Testers, 1 Paata Saakadze St, Tbilisi 0102, Georgia
[2]Caucasus University, 1 Paata Saakadze St, Tbilisi 0102, Georgia

ABSTRACT: Passwords are a fundamental barrier protecting our personal and professional security in today's digital world. They safeguard our online accounts, banking information, social networks, and vast amounts of sensitive data. However, passwords are often weak or easily exposed, making them prime targets for attacks. Recently, artificial intelligence (AI) has significantly transformed the methods hackers use to crack passwords, increasing the complexity of security challenges. AI enables more sophisticated, efficient, and adaptive attack techniques, posing new risks to individuals and organizations alike. This paper explores traditional password attack methods, the evolving role of AI in password cracking, its consequences, and effective defense strategies to mitigate these emerging threats.

KEYWORDS: *AI, Password attacks, hacking*

ანოტაცია: პაროლები დღევანდელ ციფრულ სამყაროში ჩვენი პირადი და პროფესიული უსაფრთხოების მთავარი ბარიერია. ისინი გვიცავენ ჩვენს ონლაინ ანგარიშებს, საბანკო მონაცემებს, სოციალურ ქსელებს და უამრავ მნიშვნელოვან ინფორმაციას. მიუხედავად ამისა, პაროლები ხშირად სუსტია ან ადვილად გამჟღავნებადი, რაც მათ თავდასხმების სამიზნედ აქცევს. ბოლო წლებში ხელოვნურმა ინტელექტმა (AI) მნიშვნელოვნად შეცვალა ის მეთოდები, რომლითაც ჰაკერები ცდილობენ პაროლების გატეხვას, რაც უსაფრთხოების გამოწვევებს კიდევ უფრო რთულს ხდის.

საკვანძო სიტყვები: *AI, პაროლით შეტევები, ჰაკერული შეტევები*

1. შესავალი

პაროლები ჩვენს ციფრულ ცხოვრებაში უმნიშვნელოვანეს როლს თამაშობს. ისინი არის პირველი ბარიერი, რომელიც იცავს ჩვენს პერსონალურ და პროფესიულ ინფორმაციას. თუმცა, ხშირია შემთხვევები, როდესაც პაროლები სუსტია ან მარტივად გამოიცნობა, რამაც შეიძლება ჩვენი უსაფრთხოება სერიოზულად შეაზიანოს. ტრადიციულად, პაროლებზე შეტევა ძირითადად ორი გზით ხორციელდებოდა: ბრუტფორსით და სოციალური ინჟინერიით. ბრუტფორსი გულისხმობს ყველა შესაძლო კომბინაციის ავტომატურ მოძიებას, რაც დიდ დროსა და რესურსებს მოითხოვს, განსაკუთრებით გრძელ და რთულ პაროლებზე. სოციალური ინჟინერია კი გულისხმობს ადამიანური შეცდომების გამოყენებას, მაგალითად, ფიშინგის გზით, რათა მომხმარებელი თავად გამჟღავნდეს თავისი პაროლი. ხელოვნურმა ინტელექტმა კი მნიშვნელოვნად გაამარტივა და გააუმჯობესა პაროლების გატეხვის პროცესი.

AI-ს შეუძლია სწავლა და ადაპტაცია, რაც საშუალებას აძლევს მას დაადგინოს ყველაზე გავრცელებული პაროლები მომხმარებლის პირადი ინფორმაციის გათვალისწინებით და უფრო ეფექტურად მოახდინოს ჰაკერული შეტევები. ტრადიციული პაროლზე შეტევის მეთოდები,ტრადიციულად, პაროლებზე შეტევა ხორციელდებოდა ორ ძირითად მეთოდით:
ბრუტფორსი (Brute-force): ეს არის ყველა შესაძლო პაროლის კომბინაციების სისტემატიური შემოწმება, რაც დიდ დროს და კომპიუტერულ რესურსებს მოითხოვს, განსაკუთრებით, თუ პაროლი გრძელია და შეიცავს შემთხვევით სიმბოლოებს.
სოციალური ინჟინერია: ეს მეთოდი მიმართულია მომხმარებელზე, სადაც თავდამსხმელები ცდილობენ ფიშინგის გზით ან სხვა ხერხებით მიიღონ პირადი ინფორმაცია, რომლითაც შემდეგ პაროლებს გამოიცნობენ.

ხელოვნური ინტელექტის როლი პაროლების გატეხვაში ხელოვნურმა ინტელექტმა მნიშვნელოვნად შეცვალა პაროლებზე შეტევის მეთოდები. AI-ს შეუძლია დაადგინოს ყველაზე გავრცელებული და სუსტი პაროლები, გამოიყენოს პირადი ინფორმაცია მომხმარებლის შესახებ, რათა გამოიცნოს მისი პაროლი. ასევე, შეუძლია გამოიყენოს მანქანური სწავლების ალგორითმები, რომლებიც სწავლობენ გაჟონილი პაროლების მონაცემებს და ქმნიან პროგნოზირებად მოდელებს. ასევე შესაძლებელია შექმნას ფოკუსირებული და ეფექტური შეტევები, რომლებიც გაცილებით სწრაფად მუშაობენ ვიდრე ტრადიციული ბრუტფორსი. AI-ს დახმარებით, პაროლების გატეხვის პროგრამები აღარ მიმართავენ მხოლოდ ქვეით ბრუტფორსს, არამედ იყენებენ უფრო ჭკვიან და ფოკუსირებულ გზებს. ეს შეიძლება იყოს ნატურალიზებული ენის მოდელები, რომლებიც ახდენენ მომხმარებლის სოციალური მედიის ან საჯარო მონაცემების ანალიზს, რათა გამოიცნონ მისი პაროლი. მაგალითად, თუ ადამიანს უყვარს გარკვეული ფილმი ან სპორტული გუნდი, AI ამას გაითვალისწინებს პაროლის ვარიანტების გენერირებისთვის. AI ტექნოლოგიის გამოყენების მაგალითები პაროლებზე შეტევებში რამდენიმე ცნობილი ინსტრუმენტი უკვე იყენებს AI-ს პაროლების გატეხვისთვის, მაგალითად: DeepLocker და PassGAN იყენებენ გენერატიულ ნეირონულ ქსელებს, რათა შექმნან მეტად რეალისტური და ეფექტური პაროლების ვარიანტები. ეს მოდელები სწავლობენ პაროლების სტრუქტურასა და ქცევას, რაც საშუალებას აძლევს უფრო მიზანმიმართულ შეტევებში გამოიყენონ ისინი, ვიდრე ტრადიციული მეთოდები. ასეთი ალგორითმების გამოყენება გაცილებით სწრაფია და ეფექტურია, რაც ზრდის დაშვების რისკს როგორც ინდივიდუალურ, ისე ორგანიზაციულ დონეებზე.

2. შეტევის შედეგები და რისკები

AI-ს დახმარებით განხორციელებული პაროლებზე შეტევები მნიშვნელოვნად ზრდის უსაფრთხოების დარღვევის ალბათობას. ეს ნიშნავს, რომ ჰაკერები უფრო მარტივად აღწევენ პირად მონაცემებს, ფინანსურ ინფორმაციას და კომპანიის საიდუმლოებებს. შედეგად, როგორც კომპანიები, ისე მომხმარებლები განიცდიან ფინანსურ და რეპუტაციულ ზარალს.

3. დაცვის სტრატეგიები AI-დამყარებული შეტევების წინააღმდეგ

პაროლების დასაცავად AI-ტექნოლოგიისგან საჭიროა ახალ სტანდარტებზე გადასვლა. ერთ-ერთი ყველაზე ეფექტური გზა არის მრავალფაქტორული ავტორიზაცია (MFA), რომელიც პაროლის გარდა დამატებით ავთენტიფიკაციის მეთოდებს იყენებს. ასევე მნიშვნელოვანია პაროლების სირთულის გაზრდა — გრძელი, უნიკალური და შემთხვევითი სიმბოლოებით დაკომპლექტებული პაროლები. ბრენდებმა და ორგანიზაციებმა უნდა გამოიყენონ AI-სთვის წინააღმდეგობის გაწევის სპეციალური ხელსაწყოები, როგორიცაა ანომალიების გამოვლენის სისტემები, რომლებიც ამჩნევენ გაუგებარ აქტივობას და დროულად პასუხობენ მას.

4. მომავლის პერსპექტივები

ხელოვნური ინტელექტი მუდმივად ვითარდება, რაც ნიშნავს, რომ პაროლებზე შეტევებიც უფრო დახვეწილი გახდება. ამიტომ, პაროლების დაცვის სტრატეგიებიც უნდა განვითარდეს და გაუმჯობესდეს. ბიომეტრიული მონაცემების, ქცევითი ანალიზისა და AI-დამყარებული უსაფრთხოების სისტემების კომბინაცია შეიძლება გახდეს მომავალი სტანდარტი, რომელიც მნიშვნელოვნად შეამცირებს პაროლებზე დაფუძნებული თავდასხმების რისკს. პაროლებზე შეტევა ხელოვნური ინტელექტის გამოყენებით უკვე რეალობაა და ეს გამოწვევა საჭიროებს როგორც ინდივიდების, ისე ორგანიზაციების მხრიდან მეტი ყურადღების მიქცევას უსაფრთხოების საკითხებზე. ძლიერი პაროლების შექმნა, მრავალფაქტორული ავტორიზაცია და AI-გაკონტროლებული დაცვა ერთად შეიძლება დაგვეხმაროს დაიცვათ ჩვენი ციფრული პირადი სივრცე ამ ახალ გამოწვევებთან ბრძოლის დროს.

დადასტურება

აღნიშნული ნაშრომი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის მხარდაჭერით - SPG-24-307.

ბიბლიოგრაფია

1. Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2017). პასსგანზე გვესაუბრება თუ როგორ მუშაობს
2. IBM Research. (2018). DeepLocker
3. Melicher, W., Ur, B., Segreti, S. M., Komanduri, S., Bauer, L., Christin, N., & Cranor, L. F. (2016).
4. Sharma, A., Sahay, S. K., & Kapoor, R. (2020). *Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Research Directions*. Journal of Network and Computer Applications, 167, 102738.
5. Anderson, R., & Moore, T. (2021). Information Security: Principles and Practice. Wiley.
6. Ur, B., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2015). *Measuring Real-World Accuracies and Biases in Modeling Password Guessability*