МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2020 р.

На правах рукопису
УДК 003.26:004.056.55

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Програмний модуль аналізу паролів для захисту від соціотехнічних атак.

Автор: Р.Р. Краснокутський
Науковий керівник: к.т.н., доц. к.т.н., доц. А.В. Ільєнко
Нормоконтролер: к.т.н., доц. к.т.н., доц. А.В. Ільєнко

Київ 2020

ВСТУП

Швидкість впровадження інформаційних технологій у всі сфери діяльності суспільства зумовлює виникнення ризиків порушення конфіденційності персональних даних користувачів, що призводить до необхідності вирішення проблем пов’язаних з інформаційною безпекою. Станом на сьогодні, існує розвинена система засобів захисту інформації від технічних та програмних атак, та розроблена нормативно-правова база, що забезпечує порядок використання інформаційних ресурсів та контроль конфіденційності персональних даних. Загалом усі існуючі засоби захисту інформації направлені на вирішення фізичних, логічних та соціальних питань у сфері інформаційної безпеки.

Захист від фізичних загроз являє собою систему забезпечення безпеки інформації від механічних пошкоджень.

Логічна безпека гарантується системою захисту від несанкціонованого доступу, контролем за діями користувачів.

Система захисту від соціальних загроз складається з юридичних, адміністративних, організаційних та економічних засобів захисту, що підвищують рівень підготовки кадрів.

Нажаль, увесь цей комплекс заходів в більшості покладається на програмні та апаратні засоби захисту. Специфіка соціотехнічних атак унеможливлює використання існуючих програмних засобів захисту інформації, оскільки направлена на вразливість не самої системи, а її користувачів. Відповідно, надійність інформаційної системи в даному випадку залежить в більшості від рівня орієнтованості користувачів у загальних правилах інформаційної безпеки.

Мета роботи – реалізація програмного модулю аналізу паролів для захисту від соціотехнічних атак.

Об'єкт дослідження – процедура реалізації захисту від соціотехнічної атаки з використання персональних даних, що знаходяться у відкритому доступі.

Предмет дослідження – методи реалізації соціотехнічних атак, методи

захисту, правила генерації паролів, алгоритм аналізу паролів для попередження соціотехнічних атак.

Методи досліджень. Проведені дослідження в даній роботі базуються на сучасних методах побудови захищених інформаційних мереж та методах захисту від соціотехнічних атак.

Виходячи з мети, завданням даної дипломної роботи є:

дослідження соціотехнічних атак за ознаковим принципом для подальшого застосування при розробці програмного модуля; дослідження методів захисту від атак на паролі; побудова програмного модуля аналізу паролів для захисту від соціотехнічних атак мовою програмування Rust; тестування програмного модуля.

Практична цінність роботи полягає у створенні авторського програмного модулю аналізу паролів для захисту від соціотехнічних атак мовою програмування Rust, що дає змогу проаналізувати пароль користувача на етапі цього створення та попередити його про недостатню надійність.

Наукова новизна. Удосконалено програмний модуль аналізу паролів для захисту від соціотехнічних атак, за рахунок розширення критеріїв для проведення аналізу паролів для захисту та впровадження алгоритму реалізації пошуку паролів по регулярним виразам, що надало змогу уточнювати необхідні параметри для пошуку відповідностей та забезпечити захист від соціотехнічних атак.

Апробація:

Краснокутський Р.Р. Метод защиты от социотехнических атак / Р.Р. Краснокутський // Динамикатана съвременната наука-2020: XVI международна научно-практическа конференция : тезисы докл. – София (Болгария), 2020.

Краснокутський Р.Р. Програмний модуль аналізу паролів для захисту від соціотехнічних атак / Р.Р. Краснокутський // Nauka i inowacja – 2020: XVI miesdzynarodowej naukowi-praktycznej konferencji: abstracts. – Przemysl (Polska), 2020.

РОЗДІЛ 1. СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАГРОЗА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Дослідження социальної інженерії та соціотехнічних атак

У сучасному світі, в якому ключову роль відіграє інформація, як ознака людського розвитку, його життєдіяльності, інтелектуального розвитку, як засіб досягнення тих чи інших цілей, як інструмент впливу, значущості, управління і влади, значну роль відіграють методи, засоби, механізми отримання інформації і як наслідок - механізми захисту цієї інформації.

Сучасний рівень технологій, інтенсивний розвиток науково-технічної бази, регулярне виділення ряду напрямків в нові науки, поява абсолютно нових теорій і підходів, сучасний соціальний, економічний і політичний розвиток суспільства, посилена коммерціоналізація, ведуть до появи перевиробництва, жорсткої ринкової конкуренції (в державному і приватному секторі), постійного пошуку нових ринків збуту з метою отримання максимального прибутку і вигоди для себе. Це може бути, як бажання багаторазово повернути витрати на нові технології, розробки і самі дослідження, що передують цим розробкам, так і створення монополій на ті чи інші види товарів і послуг. У будь-якому випадку, сьогодні небагато компаній займаються власним виробництвом, ведуть «чесні правила» ринкової гри та використовують в своїй діяльності «білі» схеми ведення фінансового обліку, тобто недобросовісна конкуренція, отримала новий виток свого розвитку. З'явилося чимало компаній, а також незалежних фахівців, які в своїй роботі використовують методи і засоби комерційної розвідки, займаються самі або замовляють «на стороні» інформацію, що отримується шляхом комерційного або промислового шпигунства. Всі ці та багато інших чинників, сприяють удосконаленню методів отримання, накопичення, обробки, передачі та зберігання інформації, як і її утилізацію.

Соціальна інженерія складна в сприйнятті і розумінні, в силу складності коректності встановлення зв'язків, «що може випливати з чого». Це сприйняття і розуміння до всього іншого в нас притупляється, як штучно, так і в силу соціального середовища в якій кожен з нас живе. Самі того не бажаючи, з методами соціальної інженерії ми стикається кожен день, починаючи з дому (це реклама по ТБ і маса передач соціополітичного характеру), продовжуючи в магазині і транспорті, і завершуючи на роботі. Обов'язково, виховувати мислення кожного із співробітників компанії. Таким чином, без збалансованості організації і механізмів управління в компанії, мотивованості кожного із співробітників компанії, як на власний інтерес працювати в компанії, так і на отримання загального результату і досягнення цілей компанії, починаючи від окремо взятого підрозділу і фактичним результатом компанії в цілому, ймовірність зменшення ризику соціальної інженерії мала. Це обумовлено тим, що недостатньо враховувати тільки технологічні загрози інформаційній безпеці і прикладні навички, які можуть використовувати в своїй повсякденній роботі стратегічні підрозділи - IT-служба, підрозділ або група захисту інформації, служба безпеки.

У міжнародній практиці, існує поширена думка, що соціальна інженерія, як осмислений усталений термін з'явився в 60-і роки в американській соціології, і відповідно США з'явилися родоначальниками його. Чи так це насправді?

У 20-30-і роки XX століття розгорнувся потужний рух за наукову організацію праці та управління виробництвом, в якому важливу роль зіграли прикладні розробки соціальної інженерії [1].

Вперше в науковий обіг поняття соціальної інженерії ввів Олексій Гастев - керівник Центрального інституту праці (ЦІТ) в Москві. Вчений поставив питання про комплексну, абсолютно нову науку про працю та управління - прикладна "соціальна інженерія". Ця наука була покликана доповнити колишню теоретичну соціологію і вирішити проблему синтезу найважливіших аспектів організації трудової та управлінської діяльності: технічного,

психофізіологічного, економічного. Гастев А.К. розглядав соціальну інженерію, як відносно самостійну галузь досліджень.

Відповідно до концепції Гастева А.К., стає зрозумілим призначення соціальної інженерії. Виникає уявлення про її наповнення, хто такий соціальний інженер і якими навичками він повинен володіти. Тепер звернемося до сучасних довідників, щоб побачити, наскільки розкритий цей термін нашими сучасниками і що вони вкладають в це поняття.

Має сенс спочатку звернутися до соціологічних словників, враховуючи коріння походження терміна.

1. Соціальна інженерія - (англ. Engineering, social; ньому. Ingenieurwesen, soziales.) Сукупність підходів в прикладних соціальних науках, орієнтованих:

- на зміну поведінки і установок людей;
- на вирішення соціальних проблем;
- на адаптацію соціальних інститутів до умов, що змінюються;
- на збереження соціальної активності.

2. Соціальна інженерія - спеціально організована діяльність, спрямована на трансформацію соціальної реальності (реконструкцію старої або конструювання нової) за допомогою соціальних технологій.

3. Соціальна інженерія - теоретична і практична діяльність, спрямована на створення і використання набору засобів впливу на поведінку людей з метою вирішення соціальних проблем, адаптації організаційних структур суспільства до постійно змінюваних умов і профілактики соціальних конфліктів.

4. Соціальна інженерія - специфічна галузь прикладної соціології, що представляє сукупність прикладних соціальних методів і практичної діяльності, пов'язаної з використанням знань, отриманих в загальній соціологічної теорії, прикладні дослідження, а також в практиці виробничої та іншої діяльності, для вирішення повсякденних і перспективних завдань вдосконалення управління соціальними об'єктами.

Орієнтуючись на область захисту інформації, наведу кілька визначень, які використовують фахівці з питань захисту інформації в своїх роботах.

5. Соціальна інженерія (англ. Social engineering) - сукупність підходів прикладних соціальних наук, або прикладної соціології, орієнтованої на цілеспрямована зміна організаційних структур, що визначають людську поведінку і забезпечують контроль за ним.

6. Соціальна інженерія - це один з розділів соціальної психології, спрямований на те, щоб впроваджувати в їх свідомість деяку модель поведінки і тим самим маніпулювати їхніми вчинками.

7. Соціальна інженерія - це метод (атак) несанкціонованого доступу до інформації або системам зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкостей людського фактора і вважається дуже руйнівним.

8. Соціальна інженерія - це набір прикладних психологічних і аналітичних прийомів, які зловмисники застосовують для прихованої мотивації користувачів публічної або корпоративної мережі до порушень усталених правил і політик в області інформаційної безпеки.

Спочатку в понятті «соціальна інженерія» був відсутній чіткий відтінок зловмисності. Воно застосовувалося для позначення комплексу специфічних знань, які дозволяють управляти процесом створення, модернізації та відтворення якоїсь штучно створеної реальності, використовуваної в винахідницької діяльності.

Зіставляючи наведені раніше визначення і повертаючись до самої концепції соціальної інженерії, в основі підходів лежить системність, підкріплена методологією і аналізом, яка і дозволяє поєднувати технологічну інноваційність, інженерну точність розрахунків з соціально-психологічним моделюванням. Майстерне володіння цими інструментами є запорукою успішного вибудовування поведінкової моделі людей, «добровільно» і «самостійно» діючих в потрібному соціальному інженеру напрямку.

У соціальній інженерії розрізняють два протилежні підходи. Перший підхід, це пряма соціальна інженерія, або просто соціальна інженерія. Другий підхід, це зворотна соціальна інженерія. Другий підхід став продовженням

першого, і методи, які використовуються в прямій соціальній інженерії, часто використовуються в зворотній соціальній інженерії. Розглянемо докладніше кожен з підходів.

Основну схему впливу соціального інженера при прямій соціальної інженерії можна описати спрощеною схемою Шейнова [2]. У загальному вигляді вона приведена в книзі білоруського психолога і соціолога В.П. Шейнова «Приховане управління людиною: психологія маніпулювання», котрий довгий час займався психологією шахрайства.

Під «об'єктом» тут і далі будить матися на увазі жертва, на яку націлена Соціоінженерна атака.

Спочатку, завжди формується мета впливу на той чи інший об'єкт [3]. Потім збирається інформація про об'єкт, з метою виявлення найбільш зручних мішеней впливу. Після цього настає етап, названий психологами атракцією. Атракція (від лат. Attrahere - залучати, притягати) - створення необхідних умов для впливу соціоінженера на об'єкт. Примус до потрібного для соціонженера дії, тобто нав'язування дій, коли об'єкт сприймає такі дії як свої «власні» і в подальшому, «самостійно» приймає рішення виконати необхідні соціоінженеру дії, що відбуваються за фактом настання атракції.

Соціоінженери сьогодні віддають більше переваг зворотного соціальної інженерії (ОСІ - reverse social engineering). Вона дозволяє максимально приховати зловмисний характер своїх дій і фактично дає 98% результат, але вимагає більш ретельної підготовки. Суть ОСІ полягає в тому, що соціоінженер безпосередньо ні до чого не примушує, а створюєте такі умови, що жертва сама звернеться за допомогою до соціоінженеру без будь-якого підозри. Об'єкт впливу вважає соціоінженера людиною, якій можна довіряти, тому не бачить причин не давати йому необхідну інформацію. Навіть якщо об'єкт впливу виявиться досвідченою людиною, інформовану про методи соціальної інженерії, і не тільки про них, далеко не завжди він зможе ці методи розпізнати. З огляду на той факт, що в цей відрізок часу його голова буде зайнята проблемою, яка потребує термінового вирішення. При успішному вирішенні (створеної)

соціоінженером «проблеми», об'єкт може неодноразово звертатися до соціоінженеру, як за допомогою, так і для підтримки дружніх відносини. Це бажаний результат будь-якого соціоінженера!

Диверсія - це перший етап OCI, на якому інженер створює проблему в системі, таку, щоб об'єкт не міг з нею працювати. Це може бути зміна будь-якого параметра (установки монітора, принтера, параметрів файлу і навіть перемикання регістрів клавіатури), створення апаратних неполадок, запуск шкідливих програм і програм-імітаторів. При цьому неполадки повинні бути легко усунути, оскільки інженеру треба буде розв'язати «прикру проблему» «в одну мить».

Реклама - це другий етап OCI, на якому соціоінженер повинен донести до об'єкта інформацію про власну здатності вирішити проблему «в будь-який час доби. Об'єкт сам повинен знайти інформацію про соціоінженере в доступному місці. Тоді у нього виникне ілюзія вільного вибору.

Допомога - спілкування інженера з об'єктом, при якому останній отримує рішення проблеми, а перший - необхідну йому інформацію.

Слід зазначити, що даний метод набув широкого поширення серед порушників, званими «інсайдерами». Причому, ним може виступати, як фахівець з професійними навичками володіння інформаційними технологіями, так і співробітник компанії, який увійшов у змову з замовником інформації за винагороду зі сторони. Причому замовлення на інформацію може бути різним, від клієнтських баз до регулярних звітів про діяльність компанії і її окремих посадових осіб. Що активно використовується в комерційному шпигунстві.

1.2 Найбільш поширені області застосування соціальної інженерії.

В основі будь-якої операції, задуманої соціоінженером або групою, завжди ретельно вивчається об'єкт впливу і використовується «людська вразливість» яка

виражається в бажаннях, рисах характеру, звичках та інших якостях людини яка потрапила в зону пильної уваги атакуючого [4].

Фінансові махінації в організації

Кріс Касперський, відомий автор наводив у своїй статті факти при яких, за отриманням гонорару в видавництво може прийти хто завгодно і назватися в бухгалтерії тим автором, який знаходиться в листі-реєстрі, отримання гонорару. Причому, деякі нахабні товариші, можуть прийти двічі. Послався на те, що за нього хтось інший приходив і отримав гроші, а він перший раз прийшов і така безглузда ситуація. Картина схожа в різних видавництвах, тому що знати всіх авторів в обличчя неможливо. Чимале їх число проживає в інших містах. Проте, чимало фінансових питань вирішується через електронну пошту, по телефону або онлайн-пейджери, що неприпустимо. Введення політики укладення авторських договорів, здатне було б розв'язати це питання на користь видавництва.

Чимало відомо випадків, коли таким же чином приходять отримувати зарплату ряд операторів, що продають якісь послуги і товари, що працюють за угодою з компанією у себе вдома.

Безкоштовне придбання програмних продуктів. Припустимо, зловмисникові потрібно певний програмний пакет і / або технічна консультація. Зламати демо версію або атакувати локальну мережу фірми розробника, сьогодні не виправданий захід. Краще, представившись журналістом, попросити один екземпляр програми в обмін на обіцянку розрекламувати її в деякому популярному журналі. Яка фірма не клюне на таку привабливу перспективу? До того ж разом з продуктом зловмисник отримає і кваліфіковану технічну підтримку безпосередньо від самих розробників, а не дівчат операторів, які обслуговують пересічних клієнтів.

Зловмиснику доведеться складніше, якщо необхідний йому продукт настільки специфічний, що взагалі відсутня на ринку. Розробка "під ключ" зазвичай коштує дорого, але якщо проявити трішки метикує, можливо все. На

сайті work.ua з'являється оголошення про високооплачувану роботу через Інтернет. Прийом співробітників, природно, відбувається на конкурсній основі і кожному кандидату дається тестове завдання, за результатами виконання якого і судять про його, кандидата, професіоналізмі. Ви не пройшли тест? Не турбуйтеся! Підучити, а потім спробуйте свої сили знову, якщо, звичайно, до той час не зрозумієте, хто залишився з носом, а хто - з готовим продуктом. Найсумніше, що пред'являти зловмисникові цивільний позов безглуздо, оскільки склад злочину відсутній.

Захистити себе від подібних обманів дуже важко, оскільки, аналогічна схема набору співробітників широко використовується і легальними фірмами.

Безкоштовний наймання робочої сили. Поширена практика найму «безкоштовної» робочої сили для виконання або якогось замовлення на розробку, або написання власної системи для компанії. Як зазначалося в попередньому пункті, це може бути безпосередньо пошук роботи з будь-якого сайту, компанія висилає по інтернету на позначений нею термін замовлення на розробку якогось модуля або іншого програмного засобу. Або вже розпочату розробку, і здобувачеві потрібно в зазначений термін розробити / доопрацювати якийсь програмний продукт. При цьому, не укладаються ніякі угоди, у вигляді договору на разову роботу.

Або інший механізм, коли компанія запрошує на розробку кваліфіковані кадри. Часто говорять, що виплата зарплати проводиться по закінченню двох місяців роботи і за один місяць, а не два розроблених. По закінченню двох місяців з Вами буде укладено трудовий контракт, якщо підійдете.

Зрозуміло, по закінченню двох місяців виплачується зарплата за місяць, можливо не та обіцяна сума, ніж була позначена на співбесіді і відповідь співробітника відділу кадрів «Вибачте, ви нам не підходите». Або через місяць людину просто просять піти.

Крадіжка клієнтських баз. Статистика таких крадіжок невелика. Але це не означає, що таких випадків мало. Навпаки, з метою приховування таких прецедентів компанії намагаються замовчувати факт розкрадання клієнтських

баз, тому що це значно позначиться на репутації організації в цілому. Попит на бази даних завжди був і залишається найбільш значним.

У своїй основі лежить недбале ставлення співробітників компанії. Дуже часто рахунку фактури, інші фінансово-платіжні документи лежать стопками на столах співробітників, які мають звичку виходити на 10-30 хвилин з кабінету, не блокуючи свою робочу станцію. Сміттєві корзини в організаціях часто заповнені тими документами, які повинні знищуватися тільки за допомогою шредера або спалюватися за рахунок спеціально-організованих виїздів для утилізації фінансових документів, магнітних носіїв і т.д. У ряді магазинів (меблеві, де продажем техніки та інших) не рідкісні випадки, коли продавець, дуже довго оформляє покупку через слабкі навичок роботи з системою. На прохання, чи може допомогти ввести в 1С дані або інше програмне засіб, що веде власну базу даних, відгукуються, і дозволяють сісти за робоче місце оператора. При цьому можуть відлучитися від робочого місця на кілька хвилин, персонал магазину не особливо турбується, що на робочому місці сидить стороння людина.

Не рідко, під виглядом обслуговуючої фірми (представника 1С наприклад) або технічної служби на підприємство проникають сторонні, уточнюючи якими базами зараз користуються співробітники і як би бажаючи оновити бази, доповнити новими. Можна подружитися з системним адміністратором і підмінити його, коли тому потрібно у справах в робочий час вирішувати інші питання (організувати виклик йому в військкомат, в домоуправління і т.д. підкинувши в пошту повістку). І при перевірці, зателефонувавши системногму адміністратору він підтвердить легальність свого товариша.

Інша поширена схема, це працевлаштування менеджером зі збуту на 1-2 місяці (на випробувальний термін), після отримання копії бази, не чекаючи строку закінчення піти з організації, обґрунтувавши тим, що така робота не підходить, буду пробувати на іншій посаді.

Найпоширеніший випадок, це звільнення провідного менеджера або групи менеджерів разом з базою клієнтів. Причому, досить швидко з'явитися нова фірма, що працює з тими ж клієнтами, що і на попередньому місці. З огляду на

прихильність багатьох компаній до конкретного менеджера, що веде їх фірму, і бажає працювати тільки з ним (можливо, були якісь усні домовленості, що влаштовують дві сторони) ведуть до прямих фінансових втрат і вироблення негативного ставлення на ринку самої організації, яку покинув цей менеджер або група менеджерів з продажу.

1.3 Класифікація видів та методів атак з використанням соціальної інженерії

Корпорація Microsoft все загрози пов'язані з використанням методів соціотехніки для спрощення сприйняття, виділяє в п'ять основних напрямків проведення атак. Вважаю її досить вдалою класифікацією і тому візьмемо її в якості загальної структури.

Напрямки атак:

1. Мережеві атаки.
2. Телефонні атаки.
3. Пошук інформації в смітті.
4. Персональні (особистісні) підходи.
5. Зворотній соціальна інженерія (або інсайд).

Як згадувалося раніше, головною метою атак зловмисників є так звана чутлива інформація: персональна інформація користувачів (імена, паролі, акаунти, ідентифікаційні номери, банківські реквізити тощо) та дані про корпоративних мережах. За допомогою такого роду відомостей можливий обхід багаторівневих систем захисту від вторгнень [5]. Зловмисниками рухають людські потреби - отримання грошей, отримання соціального статусу і підняття власної самооцінки. Як було з'ясовано, найдорожчими і тому, найнебезпечнішими є неправомірні дії співробітників, тобто внутрішні загрози.

Фахівці із захисту інформації, вважають, що основними причинами витоку конфіденційних відомостей є:

1. Відкритий доступ співробітників до великого обсягу інформації, часто не необхідних для виконання їхніх службових обов'язків.
2. Несвоєчасна деактивация електронних акаунтів співробітників, звільнених з компанії.
3. Непряма, але важлива причина - наявність (або дозвіл) в компанії засобів комунікації, небезпечних для використання. До таких засобів належать, наприклад, інтернет-пейджери і безкоштовні поштові сервіси (mail.ru, rambler.ru і т.п.).
4. Електронна пошта та Інтернет, якщо їх використання не регламентується відповідними політиками і не контролюється спеціальними засобами.

Мережеві загрози. У шахраїв є цілий арсенал відпрацьованих засобів і напрацьованого досвіду, який постійно поповнюється і навіть професіоналу часто складно оцінити ситуацію, щоб не попастися на чергову хитрість. В силу того, що сьогодні основна маса інформації будь-якої компанії обробляється в електронному вигляді і передається, як по внутрішнім, так і зовнішнім телекомунікаційним каналам зв'язку, розглянемо найбільш небезпечні загрози, які використовують найбільш популярні сьогодні в будь-якій компанії канали - електронну пошту, Інтернет, служби миттєвого обміну повідомленнями.

Загрози пов'язані з електронною поштою. Електронна пошта стала повсякденним інструментом будь-якого співробітника в компанії. Щодня багато з нас отримують через корпоративні та приватні поштові системи десятки і навіть сотні електронних листів. При такому потоці кореспонденції неможливо приділити належну увагу кожного листа, та й не рідко, просто притупляється пильність або виникає цікавість, а хто нам написав, або лист за змістом виявляється переконливим, щоб натиснути на посилання всередині нього або вислати певні дані за вказаною адресою.

Шкідливі програми. Шкідливі програми включають в себе віруси, черв'яки, троянські програми, а також різні скрипти і виконані програми.

Поштові черв'яки - це шкідливі програми, які поширюються по каналах електронної пошти у вкладеннях до поштових повідомлень [6]. Вони запускаються при відкритті користувачами вкладених файлів і використовують уразливості в поштових клієнтах. Поштові черв'яки забезпечені механізмами саморозмноження і використовують для поширення списки розсилки поштових клієнтів.

Потенційно небезпечні програми. Досить новий вид погроз, який виник на увазі зміненого останнім часом портрета порушника. Це досить потужний і дуже часто потрібний клас програмних засобів, що поставляється з операційною системою і засобами адміністрування та розробки легально безпосереднім розробником або третіми розробниками. Такі програми прийнято відносити до класу «riskware» або «greyware» («потенційно небезпечні програми»). Хоча це легітимне ПО і створені на благо, але в руках зловмисників можуть завдати значної шкоди інформаційній системі. У зв'язку з чим, фахівці з ІБ віднесли такі кошти до погроз.

Програми-шпигуни. Серед потенційно небезпечних програм, особливо виділяються програми-шпигуни (spyware). Дане ПО дозволяє збирати відомості про окремого користувача або цілої організації приховано.

Першими такими програмами були мережеві сніфери, віднесені до класу програм-bags, яка стежить за діями користувача і протоколюється все, що бачить. Набір таких програм представлений в Мережі в багатому асортименті дозволяє відстежувати і протоколювати будь-який доступний канал.

Рекламні коди або adware. Рекламні коди (adware) - це програмне забезпечення, яке проникає на комп'ютер в рекламних цілях. Дане ПО відноситься до розряду потенційно небезпечних. Формально adware- програми є легальними, що дозволяє виробникам відкрито їх розробляти, а рекламним компаніям - вільно поширювати. З'явившись кілька років тому у вигляді найпростіших скриптів, автоматично відкривали безліч додаткових вікон в

браузері, зараз вони остаточно переступили грань між небажаним, але все-таки легальним, софтом і шкідливими програмами.

Деякі сучасні adware-програми використовують вірусні технології для проникнення і приховування себе в системі [7]. Все більше виявляються програм даного класу містять риси троянців. Це відбивається в способі інсталяції в систему (наприклад, за допомогою вразливостей в браузерах) або в поведінці на комп'ютері користувача.

Спам. Істотна частка спам-повідомлень розсилається через «ботнети». Як правило, окремий інфікований комп'ютер використовується для посилки невеликої частки повідомлень, при цьому в розсилці беруть участь сотні і тисячі призначених для користувача машин. Спамерам вдалося налагодити наскрізний моніторинг доставки повідомлень, в результаті лист, відкинуте при спробі доставки з однієї IP-адреси, відправляється заново тільки з іншого IP. Це робить відображення (reject) пошти по DNSBL-списками DNSBL_DNS Black lists - чорні списки доменних імен Інтернету. Містять базу адрес, найбільш часто використовуваних спамерами. неефективним - спроби доставити Ваше повідомлення повторяться з інших IP-адрес.

Інтернет-пейджери або служба миттєвого обміну повідомленнями. Інтернет-пейджери (в англійській термінології Instant messaging, далі скорочено - IM) - це кошти діалогового обміну повідомленнями.

Двома основними видами атак, заснованих на використанні служби миттєвого обміну повідомленнями, є вказівка в тексті листа посилання на шкідливу програму і доставка самої програми, а також один із способів запиту і передачі конфіденційної інформації.

Телефонні атаки. Дані тип атак є класичним типом, які в силу обмеженості поширення в 70-х - 80-х роках персональних комп'ютерів був найпопулярніший.

Дана загроза забезпечує шахраям унікальні можливості для проведення социотехнических атак. Це звичне і в той же час знеособлене засіб спілкування,

оскільки жертва не може бачити зловмисника. Комунікаційні функції, підтримувані більшістю комп'ютерних систем, можуть також зробити привабливою мішенню корпоративні телефонні станції.

Сьогодні дані атаки стали складніше і більш безпечними для шахрая, тому що з'явилися кошти підробляють голос як свій, так і наприклад співробітника компанії, з яким вже відбулася зустріч і його голос був записаний на диктофон (як варіант). Ці ж розробки дозволяють створювати необхідний фон (наприклад, галасливого офісу call-центру), що створює довіру в говорить на іншому кінці. Більш того, технічні засоби дозволяють підробляти номера і якщо на іншому кінці включений АОН, а шахрай виставить себе на лінії номер, свідомо завжди зайнятий (це нескладно вирахувати), тоді шанси перевірити дзвонить ускладнені або наближаються до нуля [8].

На кінцевого користувача. Ще одним видом атак є крадіжка PIN-кодів кредитних і телефонних карток через телефонні будки або внутрішнім порушником в компанії. Найчастіше при цьому крадеться особиста інформація конкретних людей, але іноді зловмисникам вдається роздобути таким способом PIN-коди корпоративних кредитних карт, що дає необмежені можливості для використання телефонної мережі для дзвінків по всьому світу за рахунок компанії.

Більшість людей досить обережні при введенні PIN-кодів в банкомати, але при користуванні громадськими телефонами багато з них ведуть себе більш безтурботно.

З використанням технології VoIP. Зростаюча популярність засобів для передачі звукової інформації між комп'ютерами (званих також Voice over IP (VoIP)) змушує вживати заходів до контролю передачі такої інформації. Є різні реалізації для дзвінків з комп'ютера на комп'ютер і / або на звичайні телефони.

Існують стандартизовані протоколи для обміну такою інформацією, сюди можна віднести Session Instatiation Protocol (SIP), прийнятий IETF і H.323,

розроблений ITU [9]. Ці протоколи є відкритими, що робить можливим їх обробку.

На мобільного користувача. Варіанти "стільникового" шахрайства, відносно нова загроза. На мобільні телефони приходять СМС з повідомленням того, що мовляв ви підключені до нової послуги і якщо ви бажаєте відписатися, наберіть 4-х значний номер вказаний на екрані. Зрозуміло, при наборі цього номера на віртуальний рахунок шахрая з балансу мобільного користувача знімається сума.

Пошук інформації в смітті. Несанкціонований аналіз сміття - або, як це ще називають, «пірнання в сміттєві контейнери» - часто дозволяє зловмисникам отримати цінну інформацію. Паперові відходи компанії можуть містити відомості, які зловмисник може використовувати безпосередньо (наприклад, номери облікових записів і ідентифікатори користувачів) або які полегшують йому проведення подальших атак (списки телефонів, схеми структури організації і т. Д.). Для зловмисника, котрий використовує соціотехніки, відомості другого типу особливо цінні, тому що вони допомагають йому проводити атаки, не викликаючи підозри. Наприклад, знаючи імена та прізвища людей, що працюють в певному підрозділі компанії, зловмисник має набагато більше шансів при пошуку підходу до її співробітникам, більшості з яких буде легко повірити, що людина, так багато знає про компанію, є їхнім колегою.

Персональні (особистісні) підходи. Мабуть, це найбільш дешевий і простий метод з одного боку, тому що необхідну інформацію зловмисник на пряму запитує у об'єкта впливу, з іншого боку в зв'язку з неможливістю вивчити людини і передбачити його до кінця, він є найскладнішим.

Зловмисник використовує найчастіше такі чотири стратегії:

- Залякування. Зловмисники, які обрали цю стратегію, часто змушують жертву виконати запит, видаючи себе за осіб, наділених владою.
- Переконання. Найпопулярніші форми переконання - лестощі і посилання на відомих людей.

- Виклик довіри. Цей підхід зазвичай вимагає досить тривалого часу і пов'язаний з формуванням довірчих відносин з колегою або начальником заради отримання у нього в кінцевому підсумку потрібної інформації, стандартна стратегія моделі OCI.
- Пояснення. Зловмисник, який вибрав цей підхід, пропонує співробітникові компанії допомогу, для надання якої нібито потрібна особиста інформація співробітника. Отримавши цю інформацію, зловмисник краде ідентифікаційні дані жертви.

В контексті соціотехніки цікавий той факт, що більшість людей, визнаючи, що самі іноді брешуть, виходять з того, що інші завжди говорять їм правду. Беззастережне довір'я - одна з цілей зловмисника, котрий використовує методи соціотехніки.

При персональному підході використовується весь арсенал погроз і засобів, який розглядався до цього. Починаючи від віртуальних методів і банальної переписки по електронній пошті або інтернет-пейджера з об'єктом, і завершуючи фізичним контактом з об'єктом впливу. Фізичним доступом в службові приміщення за допомогою співробітників компанії. Фізичний доступ до інформаційної системи, видаючи себе за фахівця сервісної служби або фахівця виробляє оновлення бази даних інформаційної системи (наприклад, правовий інформаційної системи «Консультант Плюс») [10]. Спроба фізичного виявлення наявності бездротової мережі в будинку і подальше підключення до неї. Фізична компрометація співробітників працюють вдома і підключаються до ресурсів корпоративної мережі з їх допомогою, або видаючи себе за одного співробітника який перебуває у відрядженні. А також, спроба підглянути за набором користувача логіна і пароля з-за спини або збоку. Попросити його самого дати свої параметри для входу в мережу з метою щось поліпшити або терміново надрукувати один документ. Безпосередня крадіжка мобільного пристрою, що здійснює вхід в корпоративну мережу.

Зворотня соціальна інженерія. Як було відзначено раніше, це улюблена техніка соціоінженера, яка діє напевно. Особи, що мають авторитет в технічній

або соціальній сфері, часто отримують ідентифікатори і паролі користувачів і іншу важливу особисту інформацію просто тому, що ніхто не сумнівається в їх порядності. Наприклад, співробітники служби підтримки ніколи не запитують у користувачів ідентифікатор або пароль, їм не потрібна ця інформація для вирішення проблем. Проте багато користувачів заради якнайшвидшого усунення проблем добровільно повідомляють ці конфіденційні відомості. Зловмиснику навіть не треба питати про це.

Інсайд. Говорячи про інсайдерстве (маючи на увазі кожного співробітника компанії) доречно говорити про лояльність співробітника до компанії. Чим вище цей рівень, тим менший ризик. Для цього потрібне проведення значної психологічної роботи та прищеплення корпоративної культури в компанії. Потрібно розуміти, що групи можуть значно видозмінюватися, і в залежності від цього, в них можуть з'являтися мені-Дідеріх, що частіше здатне «видавлювання» з групи співробітників (відділ, департамент і інші організаційні одиниці) - ентузіастів прийшли працювати, а не «байдики бити », тому що їм ніколи займатися інтригами, шантажем і саботажем. Що провокує подальшу ситуацію зміни груп, коли ризик витоку інформації стає максимальним [11]. З цієї причини поєднання роботи з персоналом та технічних заходів, здатне мати якусь дію. З урахуванням дефіциту кваліфікованих фахівців, не доводиться думати, що вся група людей в рамках кожного підрозділу за короткий термін можна підібрати якісну за складом і кваліфікації. Це дорогий і вирощування всередині компанії кадрів, може коштувати дешевше і безпечніше.

Ключовими внутрішніми загрозами є:

- загроза витоку конфіденційної інформації;
- крадіжка конфіденційних даних через необережність;
- порушення авторських прав на інформацію;
- нецільове використання інформаційних ресурсів компанії;
- саботаж IT-інфраструктури.

Безліч загроз, яке було розглянуто вище, актуальні і тут. Розглянемо в загальному перераховані загрози.

Загроза витоку конфіденційної інформації. Розголошення/ неправомірне розголошення корпоративних конфіденційних і для службового користування даних, коли інформація залишає корпоративний периметр і потрапляє до осіб неправомірно їх використовують. Клас такої інформації цінний, як правило - це комерційні та промислові секрети фірми, інтелектуальна власність, персональні дані службовців, клієнтів і партнерів. Для реалізації цієї загроз використовуються всілякі підручні засоби і доступні канали, розглянуті вище - це мережеві канали передачі даних (корпоративна пошта, веб-пошта, Інтернет (чат, форум і т. Д.), Інтернет-пейджерів (ICQ, MSN, Yahoo! , Miranda, AOL Messenger), P2P-мережі, VoIP-програми та ін.)

Інший канал - мобільні пристрої (USB-пристрої, пам'ять мобільного телефону або фотоапарата, MP3-плеєра). Проблема актуальна і складна, і часто не карається (див. 5.2.). Для захисту можуть знадобитися організаційно-технічні заходи, це і тематична фільтрацію трафіку (пошти, Інтернету, інтернет-пейджери), контроль на рівні робочої станції (принтер, USB- пристрою), архівування корпоративної кореспонденції (для ефективного розслідування інцидентів внутрішньої IT-безпеки), адміністративні обмеження (блокування P2P-мереж, IM-агентів, WEB-mail і будь-яких інших відкритих каналів на рівні брандмауера).

Крадіжка конфіденційних даних через необережність. Чимало співробітників неуважні, як до свого робочого столу, так і до ряду дій які вони роблять на протязі дня на своєму робочому місці, піддаючи тим самим корпоративні секрети ризику ненавмисно, і часто через необережність або незнання. Наприклад, вони можуть випадково викласти секретні документи на веб-сайт, перенести дані в ноутбук або кишеньковий комп'ютер, який згодом буде вкрадений або загублений, а також відіслати конфіденційні відомості по невірному поштовою адресою. Технічні засоби захисту і в цьому випадку використовуються одні й ті ж (фільтрація трафіку і контроль операцій на рівні робочих станцій) плюс шифрування даних на мобільних пристроях. Часто,

зіткнувшись з проблемою, співробітник запитує у колег, чому мовляв, не можу викласти документ на сайт або в папку на файл-сервері, які зможуть роз'яснити неправомірність виконуваних дій [12]. Саме цим, згідно екосистемі внутрішніх порушників, недбалі і маніпульовані інсайдери відрізняються від скривджених і нелояльних.

Нецільове використання інформаційних ресурсів компанії. Або зловживання мережевими ресурсами, проблема 98% компаній. Тут актуальні всі ті загрози, що завжди підстерігає серфінгіста по Інтернету. А також використання робочого часу в своїх цілях, що може грати на швидкості і якості виконання робочих завдань, а також захопленість ряду романтичних натур може дозволити третім особам використовувати цей факт для крадіжки конфіденційної інформації. Погоня за «халявою» як мультимедійних файлів, програм, інших інформаційних ресурсів здатне занести в корпоративну мережу чимало троянських програм, завантажувачів, вірусів і т.д.

Саботаж IT-інфраструктури. Один з найнебезпечніших видів інсайдерів - «скривджені», або «саботажники», тому що вони прагнуть завдати шкоди з особистих, найчастіше безкорисливим, мотивами. Це люди, яким не важливо чого варто інформація якої вони здатні завдати шкоди або знищити. Ображені співробітники в своєму арсеналі здатні використовувати будь-який сценарій описаний вище, включаючи диверсію - скопіювати вкрай важливу для компанії інформацію на свій мобільний носій, а потім знищити її на всіх серверах фірми і в резервних копіях на матеріальних носіях. В руках саботажника виявляється сильний маніпулятивний механізм. Чи не рідкісний випадок видалення всієї інформації взагалі (при звільненні або перед оголошенням про звільнення). Тому моніторинг робочої атмосфери і корпоративних конфліктів важливий, в сумі з технічними обмеженнями дій кожного співробітника.

1.4 Інсуючі методи захисту від соціальної інженерії

Фішинг

Основою захисту від фішинг-атак є, «навчання» користувачів. Своєчасне і повне інформування співробітників про дану загрозу і про необхідність ретельної перевірки джерела запиту конфіденційних або персональних даних усуне основну умову існування фішинг-атак. Тобто виховання у співробітників компанії скептичного ставлення до будь-яких несподіваних входять листів. З цією метою в компаніях вводиться спеціальна політика, яка регламентує дії користувачів, які отримують подібні листи і використовують конкретні принципи використання електронної пошти з обов'язковими прикладами атак, що використовують ці принципи:

- вкладення в документи
- гіперпосилання в документах.
- запити особистої або корпоративної інформації, які виходять із середини компанії.
- запити особистої або корпоративної інформації, які виходять із-за меж компанії.

При виникненні нових різновидів фішингу, необхідно допрацьовувати документ і з доробками знайомити користувачів.

Шкідливі програм. Політика безпеки є необхідним атрибутом будь-якої продуманої стратегії захисту від черв'яків. Простий заборона на відкриття вкладених файлів з електронних листів знижує ризик зараження поштовими хробаками практично до нуля.

Спам. У політиці ІБ необхідно чітко прописати дії користувачів, якщо до них приходить електронне повідомлення від невідомого адресата. Тут підходить все, що зазначено в загрозі «фішинг» [13]. Проте, повторю, потрібно вказати механізм і порядок дії для користувача, зробити приклади для наочності. У самих правилах жорстко вказати наступні моменти:

- якщо назва теми говорить сама за себе, адресат не відомий, навіть не відкриваючи визначати в кошик;
- якщо адресат відомий, але тема не відноситься до робочого процесу і викликає підозру, тим більше якщо видно, що лист прибуло з вкладеннями, видалити лист або довести до відома службу підтримки;
- ніколи не відкривати вкладення в листі від невідомого адресата, незалежно від розширення вкладення (офісні документи, архіви, додатки, фотографії);
- ніколи не натискати на посилання в тілі листа і клацати на картинки, навіть якщо адресат відомий;
- уважно придивлятися до назви вкладення і розширенню від відомого адресата;
- ні в якій мірі не висилати ніякі свої паролі і облікові записи, ні за яку вимогу, будь-то безпосередній керівник або директор компанії, або співробітник служби ІБ і адміністратор;
- якщо запитувана інформація від «легального» користувача викликає недовіру, що це потрібно написати або переслати, краще передзвонити і повідомити про це безпосереднього своєму керівнику, а також до служби ІБ або ІТ (при відсутності служби ІБ).

Додатки класу peer-to-peer. Основу захисту від загроз, пов'язаних з використанням P2P_піложеній, є введення в організації відповідної політики безпеки. Дана політика повинна передбачати:

- заборона використання неавторизованого програмного забезпечення в корпоративній мережі;
- заборона з'єднання через певні порти, характерні для деяких P2P-додатків;
- застосування спеціалізованих засобів для забезпечення моніторингу використання інтернет-ресурсів, а також сканування корпоративних

мережевих ресурсів і робочих станцій на наявність і використання неавторизованого ПО і матеріалів.

Телефонія. У політиці ІБ необхідно жорстко прописати:

- заборонити називати прямі міські корпоративні і мобільні номери і внутрішні номери як конкретних осіб, так і підрозділів;
- заборонити на фразу «Мені потрібно поговорити з вашим администратором» або «Мені б головного бухгалтера почути» здійснювати переклад дзвінка. Завжди уточнити питання і після безпосередньої розмови з даним співробітником або відділом відмовити або перевести дзвінок, якщо він очікуваний;
- заборонити називати ПІБ співробітників, особливо керівників, і відповідальних за ту чи іншу ділянку роботи;
- жорстко прописати, що тільки наші спеціалісти можуть надавати допомогу по телефону.

Зберігання та утилізація сміття. Співробітники компанії повинні розуміти всі наслідки, до яких може привести викидання паперових документів або електронних носіїв інформації в сміттєву корзину. Як тільки сміття залишає територію компанії, її права можуть більше на нього не поширюватися.

У політиці ІБ повинні бути прописані чіткі правила по роботі з документами і магнітними накопичувачами, які з тих чи інших причин вже не потрібні. Паперове сміття завжди слід подрібнювати в паперорізальних машинах, а електронний - знищувати фізично або прати записані на ньому дані за допомогою спеціальних технічних засобів. Якщо будь-які документи (наприклад телефонний довідник) через розміри або жорсткості неможливо подрібнити в паперорізальної машині або у користувача немає технічної можливості це зробити, потрібно визначити спеціальну процедуру позбавлення від них [14]. Сміттєві контейнери слід розміщувати в захищеній області периметра компанії потрапляє в область прямої видимості служби безпеки, недоступний стороннім особам.

Соціальний або особистісний канал. Захиститися від атак, заснованих на залякуванні, можна, сприяючи формуванню корпоративної культури, яка виключає страх. Якщо співробітники компанії завжди поводяться чемно і поштиво, залякування не дозволить зловмиснику домогтися бажаного, тому що піддався атаці співробітник швидше за все повідомить про це начальству. Доброзичливе ставлення до співробітників з боку керівництва і нагляд за процедурою вирішення проблем і прийняття рішень - найгірше, з чим може зіткнутися зловмисник, який використовує методи соціотехніки.

1.4 Висновки до розділу

Сьогодні, навіть найбільш розрізнена інформація про підприємство і її співробітників, окремої взятої особистості, або проєктах, вміло зібрана в одному місці «на вимогу», може виявитися досить значною за своїм змістом. Як наслідок, збільшується вартість і значимість інформації. Інформаційні технології перестали жити відокремлено своїм життям, разом з IT-підрозділами та окремо взятими фахівцями, і стали більшою мірою брати участь в бізнес-процесах кожної компанії, підвищуючи ефективність роботи компанії і використовуваних засобів виробництва, збільшуючи її активи. У свою чергу, це не могло не відбитися на вимогах, критеріях та підході до захисту інформації. Нові вимоги диктуються міжнародними організаціями, співтовариствами, державою, стандартами та сертифікатами, окремо взятими фахівцями із захисту інформації, IT-фахівцями, керівництвом підприємств і найбільш нагальною необхідністю. Найчастіше кіберзлочинці вкрай винахідливі в своєму використанні соціальної інженерії. Ознайомившись з їх методами, можна зробити висновок, що різні психологічні трюки дуже допомагають зловмисникам домагатися поставлених цілей [15]. Виходячи їх цього, варто звертати увагу на будь-яку дрібницю, яка може мимоволі видати шахрая, перевіряти і перевіряти ще раз інформацію про

зв'язуються з вами людей, особливо якщо обговорюється конфіденційна інформація. Розглянувши головни методи соціальної інженерії, ми визначили найбільш імовирні сценарії перебігу атак. Дослідивши основні методі протидії даним атакам, ми визначили основні критерії, котрих необхідно дотримуватись при розробці захисту від соціотехнічних атак.

РОЗДІЛ 2. СУЧАСНІ МЕТОДИ ЗАХИСТУ ВІД СОЦІОТЕХНІЧНИХ АТАК НА ПАРОЛІ

2.1 Дослідження видів атак на паролі

Криптографічні методи, зокрема шифрування, добре забезпечують захист інформації (конфіденційності, цілісності, автентичності та т. Д.) Від зовнішнього порушника. Такий порушник, можливо, може перехоплювати повідомлення, що передаються по каналу зв'язку, а в деяких випадках модифікувати їх і навіть вставляти в сеанс зв'язку власні повідомлення (найчастіше намагаючись видати їх за повідомлення іншого джерела). Однак інформація в каналі зв'язку попередньо піддається криптографічним перетворенням і передається відповідно до криптографічними протоколами, спеціально розробленими для того, щоб перешкодити порушнику реалізувати загрози безпеки. Для того щоб порушити безпеку інформації, що циркулює в системі, йому необхідно знайти вразливість в системі захисту, або в використаних в ній криптографічних алгоритмах [16]. Аналогічні труднощі постають перед порушником, який отримав доступ до захищеної автоматизованої ІС в якості користувача, який не володіє привілеями, необхідними для доступу до цікавлять його даними.

Однак ситуація змінюється, якщо порушник отримує доступ до системи від імені користувача, уповноваженого виконувати операції з важливими його

даними (наприклад, копіювання конфіденційних файлів, знищення критично важливих даних і т. Д.). У цьому випадку вся криптографічний захист не буде корисною. Таким чином - найвразливіше місце автоматизованої інформаційної системи - точки доступу до неї. Ці точки доступу захищаються протоколами аутентифікації (перевірки справжності користувача). А найзручніша для користувача і найбільш використовувана форма аутентифікації - парольний захист.

Існує ряд стандартних прийомів, які застосовуються зловмисниками з метою обійти парольний захист. Для кожного з цих прийомів вироблений механізм протидії.

За результатами опитування, проведеного в квітні 2006 р компанією Sophos, 41% користувачів використовують один і той же пароль у всіх випадках, з них 75% використовують не тільки один і той же пароль у всіх випадках але він є простим, легко вгадуваним. Отже, 31% користувачів (75% від 41%) не мають обліковими записами з надійно захищеними паролями доступу.

Надійний пароль повинен задовольняти цілий ряд вимог.

1. Пароль має бути секретним:
   - недопустимо відображення пароля на екрані;
   - записаний пароль не можна зберігати в місцях, доступних неавторизованих особам, наприклад, на листочках, що приклеюються до моніторал;
   - файл паролів повинен мати надійну криптографічний захист;
   - пароль не рекомендується зберігати в комп'ютері навіть в спеціальних захищених файлах - для більшої безпеки пароль слід зберігати записаним на зовнішній носій, який повинен бути надійно захищений від несанкціонованого доступу [17];
   - можливості операційної системи та інших програм по збереженню пароля повинні ігноруватися, на пропозицію програм запам'ятати пароль потрібно завжди відповідати відмовою.

2. Пароль повинен бути довгим. Пароль повинен складатися не менше ніж з 8 символів, інакше він легко може бути зламаний програмами прямого перебору.
3. пароль повинен бути важко вгадуваним. Неприпустимо збіг пароля з логіном, використання в якості пароля імені, прізвища, дати народження, номерів телефонів користувача або його родичів, кличок улюблених домашніх тварин, назв спортивних клубів, географічних назв, наприклад, улюблених місць відпочинку і т.п.
4. Пароль не повинен являти собою поширені слова, імена, назви для захисту від атаки зі словником.
5. Пароль повинен бути складним. Пароль повинен являти собою випадкову комбінацію різних символів для захисту від атаки методом прямого перебору: пароль повинен містити не тільки літери, як прописні, так і малі, цифри, а також різні не буквено-цифрові символи (`~! @ # $% ^ & * () _ + - = {} | [] \: "; '<>?,. /), які можуть бути введені з клавіатури, тобто при введенні пароля має виконуватися перемикання верхнього і нижнього регістрів клавіатури, а, якщо можливо, то і перемикання розкладки клавіатури; кращими паролями є паролі, згенеровані як випадкові послідовності [18].
6. Він має містити регулярно змінюватися. Бажано, щоб зміни пароля здійснювалися не рідше одного разу в 60-90 днів і не за графіком, а випадковим чином.
7. Пароль повинен мати відчутні відмінності від паролів, що використовувалися раніше.
8. Кожен пароль повинен використовуватися унікально. Тільки одним користувачем і для отримання доступу тільки до однієї з систем або програм, т. Е. Не можна використовувати один і той же пароль для доступу, наприклад, до сеансу роботи з комп'ютером і для доступу до електронної поштової скриньки.

9. Підказки до паролів не повинні використовуватися. Слід завжди ігнорувати передбачені на випадок, якщо пароль буде забутий пропозиції операційної системи або інших програм ввести при завданні пароля підказку, вказати додаткові відомості або відповідь на контрольне запитання (наприклад, про вашому зростанні, улюблене блюдо, дівочого прізвища матері, номер паспорта і т.п.), - зловмиснику може виявитися значно легше впізнати (підібрати) відповідь на підказку, ніж дізнатися пароль.
10. Пароль не повинен передаватися по недостатньо надійно захищеними каналами зв’язку:
11. наприклад, пересилатися по електронній пошті, передаватися по телефону, факсу.
12. Пароль повинен негайно замінюватися, якщо є підозри, що він міг бути розкритий.

Найбільш ефективно протидіяти несанкціонованому доступу можна, поєднуючи парольний захист з іншими методами обмеження доступу, наприклад, використовують біометричні технології ідентифікацію, наприклад, за відбитками пальців, райдужну оболонку ока або іншим індивідуальних характеристик [19].

Якщо необхідно забезпечити надійний захист, пароль обов'язково повинен задовольняти вимогам складності і досить великої довжини. У таблиці 1 наведені кількість варіантів, які необхідно перебрати в разі «лобове» атаки методом прямого перебору, якщо пароль складається з 6-ти символів. Також в таблиці дані значення довжини пароля, такі щоб число варіантів при його переборі дорівнювало числу варіантів перебору випадкового криптографічного ключа довжиною 56 і 256 біт - такі довжини ключів передбачені в старому, але ще дуже поширеному стандарті шифрування DES (США) і діючих стандартах AES (США) і ГОСТ 28147-89 [20].

У більшості систем користувачі мають можливість самостійно вибирати паролі або отримують їх від системних адміністраторів. При цьому для

зменшення деструктивного впливу людського фактора необхідно реалізувати ряд вимог до вибору і використання паролів.

Встановлення мінімальної довжини пароля ускладнює завдання зловмисника при спробі підглянути пароль або підібрати пароль методом "повного перебору".

Використання в паролі різних груп символів ускладнює завдання зловмисника при спробі підібрати пароль методом "повного перебору» перевірка і відбраковування пароля за словником ускладнює завдання зловмисника при спробі підібрати пароль за словником.

Встановлення максимального терміну дії пароля ускладнює завдання зловмисника по підбору паролів методом тотального випробування, в тому числі без безпосереднього звернення до системи захисту (режим off - line) [21].

Встановлення мінімального терміну дії пароля перешкоджає спробам користувача замінити пароль на старий після його зміни за попереднім вимогу

Ведення журналу історії паролів забезпечує додатковий ступінь захисту за попереднім вимогу.

Застосування евристичного алгоритму, відкидаючого паролі на підставі даних журналу історії ускладнює завдання зловмисника при спробі підібрати пароль за словником або з використанням евристичного алгоритму

Обмеження кількості спроб введення пароля перешкоджає інтерактивному підбору паролів зловмисником.

Підтримка режиму примусової зміни пароля користувача забезпечує ефективність вимоги, що обмежує максимальний термін дії пароля.

Використання затримки при введенні неправильного пароля перешкоджає інтерактивного підбору паролів зловмисником.

Заборона на вибір пароля самим користувачем і автоматична генерація паролів виключає можливість підібрати пароль за словником [22]. Якщо алгоритм генерації паролів не відомий зловмисникові, останній може підбирати паролі тільки методом "повного перебору".

Примусова зміна пароля при першій реєстрації користувача в системі захищає від неправомірних дій системного адміністратора, що має доступ до паролю в момент створення облікового запису.

Немає кращого способу протестувати надійність парольного захисту комп'ютерної системи, ніж спроба її злому. Сьогодні будь-який бажаючий, може легко знайти будь-яку найдетальнішу інформацію про сучасні технології подолання парольного захисту. Найголовніше - знання методів злому паролів і аналіз цих методів є основою для того, щоб сформулювати правила пральний захисту, що забезпечують максимально надійне протидія спробам несанкціонованого доступу до інформації.

Для злому парольного захисту використовуються наступні методи.

Розпізнавання пароля. Часто користувачі записують паролі на листках, в блокнотах, зошитах, доступних неавторизованих особам. Доступність записаних паролів, їх несекретних, є однією з важливих «дірок» в пральний захисту. Часто паролі доступу можуть бути отримані шляхом їх вивідування, зазвичай з використанням тих чи інших методів психології або соціальної інженерії. Різновидом цього методу є вивідування інформації, яка могла бути використана користувачем в підказках, іноді передбачаються на випадок, якщо пароль забутий. Такі підказки пропонуються, наприклад, поштовими серверами при реєстрації електронної поштової скриньки і, звичайно, представляються пропозицією відповісти на деякий контрольне запитання, такий як «Ваш зріст», «Ваша улюблена страва», «номер Вашого паспорту», «дівоче прізвище матері» і т. п. Для бажає отримати доступ до захищеного паролем ресурсу, як правило, значно легше дізнатися інформацію, необхідну для правильної відповіді на подібні питання, ніж сам пароль [23].

Соціальний інжиніринг. Соціальний інжиніринг - маніпулювання людьми з метою проникнення в захищені системи користувача або організації. Якщо підібрати або вкрасти пароль не вдається, можна спробувати обманом змусити користувача віддати пароль самому. Класична тактика соціального інжинірингу - телефонний дзвінок жертві від імені того, хто має право знати

запитувану інформацію. Наприклад, зловмисник може представитися системним адміністратором і попросити повідомити пароль (або інші відомості) під переконливим приводом. Схиляння користувача до відкриття посилання або вкладення, які відкривати не слід або заманювання його на підставний сайт також відносять до методів соціального інжинірингу. Необхідно пам'ятати правило: повідомляти пароль стороннім особам ні в якому разі не можна. Навіть якщо ці особи мають право його знати. Єдиним винятком може бути вимога суду або правоохоронних органів видати пароль під загрозою відповідальності за відмову від дачі показань. Але і в цьому випадку необхідно переконатися, що співробітники правоохоронних органів - саме ті, за кого вони себе видають.

Вгадування пароля. У багатьох випадках в якості пароля використовуються імена, прізвища, номери телефонів та інші особисті дані користувача або його родичів і друзів. Така інформація може бути відома зловмисникам, що дозволяє використовувати її для вгадування і підбору пароля. У найбільш примітивному випадку пароль вибирається користувачем таким же як облікове ім'я (логін).

Фішинг. Процедура «вивудження» паролів випадкових користувачів Інтернету. Зазвичай полягає в створенні «підставних» сайтів, які обманом змушують користувача ввести свій пароль.

Наприклад, щоб отримати пароль до банківського рахунку, може бути створений сайт з дизайном, ідентичним сайту деякого банку. Адреса цього сайту, природно, буде іншим, але найчастіше зловмисник реєструє доменне ім'я, яке відрізняється від банківського на один символ. В результаті користувач, зробивши помилку, потрапить на підставний сайт і не помітить своєї помилки. Для заманювання користувачів клієнтам банку можуть також розсилатися електронні листи з вмістом типу «перевірте свій рахунок» або «ознайомтеся з новими акціями», причому в листі міститься посилання, що веде на підставний сайт.

Коли клієнти банку потрапляють на сайт зловмисника, їм (як і на справжньому сайті) пропонується ввести логін і пароль для доступу до рахунку.

Ця інформація зберігається в базі даних зловмисника, після чого клієнт перенаправляється на головну сторінку цього сайту [24]. Користувач бачить, що введення пароля «не спрацював» і думає, що зробив помилку або сайт просто «глючить». Він пробує ввести пароль заново і на цей раз успішно входить в систему. Це розсіює його підозри. Тим часом витік пароля вже сталася.

Інший різновид фішингу заснована на тому факті, що багато користувачів використовують один і той же пароль для різних ресурсів. В результаті, провівши успішну атаку на менш захищений ресурс, можна отримати доступ до більш захищеним.

Наприклад, створюється сайт, потенційно цікавий решті користувачів. Якщо мета атаки - конкретна людина, то попередньо вивчаються його інтереси і захоплення. Інформація про цей сайт доноситься до потенційних жертв.

Користувачеві, що зайшов на сайт, пропонується зареєструватися, зокрема придумати собі пароль. Тепер залишається тільки подивитися, чи не підходить введений пароль до інших ресурсів цього користувача (наприклад, до електронної пошти, адреса якої була вказана при реєстрації).

Щоб протистояти загрозі фішингу, необхідно уважно перевіряти адресу сайту, перш ніж вводити важливий пароль. Найкраще помістити цю адресу в закладки браузера і користуватися виключно цими закладками, ні в якому разі не переходячи по посиланнях з електронних листів [25]. Слід користуватися різними паролями для доступу до різних сервісів.

Дотримання всіх семи перерахованих вище рекомендацій досить складно. Важко запам'ятати кілька надійних (довгих і безглуздих) паролів, а ймовірність забути пароль вище ймовірності піддатися злому. Однак існує ряд засобів, що полегшують це завдання, зокрема програми для зберігання паролів.

У програмі KeePass Portable всі паролі зберігаються в зашифрованому файлі, для доступу до якого необхідно ввести пароль (єдиний, який доведеться по-справжньому запам'ятати). При цьому програма не відображує ці паролі на екрані в явному вигляді. Щоб ввести пароль для доступу до ресурсу (наприклад, певного сайту або електронною поштою), необхідно вибрати ресурс зі списку і

вибрати в контекстному меню команду Copy Password To Clipboard. Пароль буде поміщений в буфер обміну. Навіть уважно відстежуючи дії користувача, противник не побачить пароля, який не набирається на клавіатурі і не з'являється в явному вигляді на екрані. Далі необхідно просто перейти в вікно програми, що вимагає пароль, і помістити його з буфера обміну в поле для введення (натисканням Ctrl + V або командою Вставити контекстного меню). Пароль відразу буде відображатися у вигляді зірочок. Через кілька секунд він буде автоматично видалений з буфера. Програма дозволяє також генерувати випадкові паролі заданої довжини, причому користувач може навіть не знати, який пароль створила йому програма - важливо, щоб вона надавала цей пароль кожного разу, коли необхідно авторизуватись. Нарешті, KeePass Portable не вимагає установки в системі: програма може переноситися на флешносітеле і запускатися безпосередньо з нього.

Словникова атака. Найбільш поширеним варіантом при виборі пароля є завдання в якості пароля деякого слова, що, в першу чергу, обумовлено легкістю запам'ятовування такого пароля. В цьому випадку пароль може бути виявлений за допомогою спеціальних програм-зломщиків паролів, що реалізують, так звану, словникову атаку, що складається в послідовному переборі всіх слів, що містяться в електронному словнику, що підключається до такої програми.

В даний час для визначення пароля розроблений ряд спеціальних словників, опублікованих або розміщених в Інтернеті. Такі словники містять сотні тисяч слів, імен, назв, найбільш часто вживаних як паролі, в тому числі географічних, назв корпорацій, торгових марок, назв кінофільмів, спортивних клубів і т.п. Словниковий перебір здійснюється дуже швидко, особливо, якщо словник складений як частотний, в якому слова розташовані з урахуванням частоти їх використання в якості паролів. Словники можуть підключатися до програм злому паролів [26].

Парольні зломщики можуть не тільки перевіряти всі слова зі словника, але і формувати безліч додаткових варіантів, застосовуючи певні правила видозміни слів для генерації можливих паролів. Наприклад, проводиться почергове зміна

літерного регістра, в якому набрано слово; змінюється на зворотний порядок проходження букв в слові; в початок і в кінець кожного слова приписується цифра 1; деякі букви замінюються на близькі по зображенню цифри (в результаті, наприклад, з слова password виходить pa55w0rd) і т.д. Наприклад, у відомому парольного зломщиків LC4, поряд з можливістю установки ряду параметрів злому, що підвищують ефективність роботи програми, в числі інших налаштувань передбачено завдання наступних параметрів атаки по словнику:

- звичайне використання словника;
- записані двічі слова;
- зворотній порядок символів слів;
- урізання до заданої кількості символів слова;
- слова без голосних, за винятком великої;
- транслітерація кирилиці латинськими літерами по заданій таблиці транслітерації;
- заміна розкладки локалізації латинською розкладкою клавіатури;
- заміна латинської розкладки клавіатури розкладкою локалізації.

Алгоритми формування безлічі варіантів слів можуть бути різні. Деякі парольні зломщики по черзі перевіряють кожне слово зі словника і формують на його основі безліч варіантів, інші програми-вломщікі спочатку обробляють весь словник за допомогою заданих правил, генеруючи, по-суті, новий великий варіативний словник, який використовується для підбору пароля.

Метод прямого перебору (brute-force attack - метод грубої сили, «лобова атака»). Цей метод передбачає прямий перебір всіх можливих комбінацій всіх допустимих в паролі символів. Перебір символів здійснюється до тих пір, поки не буде знайдена потрібна комбінація.

Описані вище способи подолання парольного захисту шляхом впізнавання або вгадування пароля з перебором обмеженої кількості сполучень букв, цифр і символів, що вводяться з клавіатури, може привести до успіху лише в тому випадку, коли користувач ігнорує елементарні правила вибору пароля. Словникова атака ефективна лише при ігноруванні користувачем одного з

основних правил вибору пароля - не використовувати в якості пароля семантично певне слово [27]. У разі вибору нетривіальний і досить довгий пароль, його успішний підбір можливий тільки методом прямого перебору з використанням спеціальних програм-зломщиків. Програмна реалізація методу автоматичного перебору дозволяє зламати будь-який пароль, але для складних паролів може знадобитися чимало часу, особливо з огляду на можливе перемикання верхнього і нижнього регістрів і розкладки клавіатури.

Проведене дослідження стійкості паролів до злому з використанням програми SAMInside, призначеної для злому паролів Windows NT / 2000 / XP, на комп'ютері AMD 2400 XP + зі словником обсягом 9 мегабайт при швидкості перебору 5310986 паролів / сек показало наступне:

- час злому пароля, що складається зі слів англійського мови становить до 2 хвилин;
- час злому пароля довжиною 8 символів, що складається з цифр становить 18 секунд;
- час злому пароля довжиною 8 символів, що складається з цифр і букв англійського алфавіту становить до 6 діб;
- час злому пароля довжиною 8 символів, що складається з цифр, букв і символів досягає 61 діб.

Програми злому парольного захисту часто передбачають можливість зменшення числа перебраних комбінацій символів, і як наслідок, істотне прискорення роботи. Для цього в настройках програм пральних зломщиків передбачається можливість використання апріорної інформації про зламувати паролі (якщо така є), а саме, інформації про довжину пароля (числі символів), типі символів (наприклад, якщо відомо, що пароль складається тільки з букв, або з букв і цифр, не без включення інших символів). Якщо частина використовуваних в паролі символів відома, то як правило, можливий їх облік і програма прямого перебору використовує їх як «маску» (brute force with mask), що еквівалентно зменшенню довжини пароля [28]. Для запобігання таких атак

не можна допускати можливість підглядання за введенням пароля сторонніми особами.

В сучасних операційних системах паролі закриваються за допомогою досить надійних криптографічних алгоритмів, що не дозволяє розраховувати на їх швидку дешифрацию. В цьому випадку парольні зломщики просто шифрують всі підбираються або автоматично генеруються паролі з використанням того ж самого криптографічного алгоритму, який застосовується для засекречування паролів в атакується операційній системі, і порівнюють результати шифрування із записами в системному файлі, де зберігаються шифровані паролі користувачів цієї системи.

Прийняті в більшості операційних систем заходи захисту від підбору пароля передбачають обмеження числа неправильних спроб введення пароля, аудит спроб входу в систему, можливість завдання правил, що визначають політику безпеки пральний захисту.

Використання програмних закладок. Для добування паролів, що зберігаються в пам'яті комп'ютера, в тому числі, системних паролів можуть використовуватися спеціальні програми - програмні закладки, таємно встановлюються в атакується комп'ютер з метою отримання інформації про користувача паролі.

Програмна закладка - це програма або фрагмент програми, таємно впроваджується в захищену систему і дозволяє зловмиснику, впровадити його, здійснювати несанкціонований доступ до тих чи інших ресурсів захищеної системи.

До найбільш поширеною різновиди програмних закладок - перехоплювачів паролів відносяться програми, які будучи запровадженими в операційну систему, отримують доступ до паролів, що вводяться користувачами, перехоплюють їх, записують в спеціальний файл або в інше місце, доступне зловмисникові, впроваджуючи закладку в систему [29].

До найбільш небезпечних видів таких шкідливих програм відносяться, зокрема, трояни-клавіатурні монітори, що записують натискання клавіш

клавіатури і записуючі їх в лог-файл з подальшою передачею цієї інформації по мережі, наприклад, на запрограмований в них адресу електронної пошти. Деякі види троянів-клавіатурних моніторів здатні виділяти і зберігати інформацію тільки про запровадження паролі. Спеціально для добування зберігаються в пам'яті комп'ютера паролів призначені троянські програми-парольні злодії. Слід зазначити, що троянські програми є найпоширенішими з усіх видів шкідливих комп'ютерних програм (зазвичай званих комп'ютерними вірусами) і все більш часто використовуються для добування пральний інформації. Згідно з недавнім звітом компанії McAfee кількість Троянів, призначених для крадіжки паролів в інтернеті за 2008 рік зросла на 400%.

Віддалений доступ до комп'ютера. Отримання пральний інформації зловмисником можливо при успішному проведенні мережевих атак і отриманні можливості віддаленого управління комп'ютером. Очевидно, що в цьому випадку, забезпечується можливість отримання будь-якої, в тому числі, пральний інформації, що зберігається в комп'ютері.

Безпосередній доступ до комп'ютера. Якщо безпосередній доступ зловмисника до захищеного комп'ютера, то їм може бути отримана інформація, записана в комп'ютері, включаючи дані про паролі, включаючи користувацькі облікові записи та системні паролі.

Такі атаки можливі, якщо в політиці безпеки або при адмініструванні комп'ютерної системи допущені помилки, зокрема не перекрита можливість завантаження операційної системи з зовнішніх носіїв (дискет, CD, DVD). У цьому випадку будь-яка інформація з атакованого комп'ютера може бути скопійована і піддана аналізу. Зокрема, стає можливим підбір пароля, навіть якщо він зберігався в комп'ютері в зашифрованому вигляді.

У разі, коли не закритий фізичний доступ до комп'ютера, може виявитися можливим розкрити корпус комп'ютера і отримати повний доступ до інформації, записаної на жорсткому диску, або шляхом завантаження з зовнішнього жорсткого диска, або шляхом підключення жорсткого диска атакується комп'ютера до іншого комп'ютера.

Перехоплення паролів з використанням технічних засобів. Використання технічних каналів витоку для отримання конфіденційної, в тому числі пральний, інформації є досить непростим, але розв'язуваної завданням. В переважній більшості випадків використовуються електромагнітний і електричний канали витоку, рідше - оптичний канал, який передбачає можливість візуального спостереження за процесом введення інформації. Таке спостереження може здійснюватися з використанням оптичних приладів або відеокамер.

Один з можливих варіантів використання електромагнітного каналу витоку інформації заснований на реєстрації електромагнітних полів кабельних ліній за якими передається інформація. Наприклад, якщо комп'ютер підключений через модем до телефонної лінії, то навіть при безконтактному підключенні до лінії, найчастіше здійснюваному за допомогою індуктивних датчиків, ставати можливим перехоплення трафіку, в тому числі, паролів (наприклад, паролів до електронної поштової скриньки).

Вкрай небезпечними слід вважати пристрої, призначені для перехоплення сигналів клавіатури - апаратно реалізовані клавіатурні монітори. Такий пристрій може бути приховано встановлено на провід клавіатури або як «перехідник» між системним блоком і роз'ємом клавіатури, або всередині системного блоку. У цьому випадку вся набирається на клавіатурі інформація перехоплюється і передається, як правило, по радіоканалу.

Для збереження секретності вводиться пароля, він, як правило, не відображається на екрані, а представляється в рядку введення пароля у вигляді «зірочок», «крапочок» або, рідше, інших символів. При такому відображенні пароля, іноді зірочки тільки приховують вміст цього поля, при тому, що інформація, що відноситься до поля введення вже знаходиться в пам'яті комп'ютера. У цих випадках пароль, відображений рядком зірочок, може бути визначений за допомогою спеціальних програм.

2.2 Методи захисту від атак на паролі

Знання принципів роботи протоколів аутентифікації і методів розгадування паролів корисно. Тепер необхідно вжити заходів для захисту мережі. Виконавши 10 рекомендацій, наведених в даній статті, можна надійно захистити комп'ютери від атак зі зломом пароля. Рекомендації розташовані в порядку убування важливості [30].

Відключення хешу пароля LM. Більшість програм злому паролів працює виключно з хешем паролів LM. Блокувати зберігання хешів пароля LM можна за допомогою трьох методів.

- використовувати паролі довжиною не менше 15 символів. Якщо довжина пароля більше 14 символів, система не може генерувати хеш паролів LM;
- відключити зберігання хешу паролів LM в масштабах всієї системи з використанням Group Policy або Local Security Policy. Слід перейти в розділ Computer Configuration \ Windows Settings \ Security Settings \ Local Policies, вибрати Security Options і двічі клацнути на пункті Network Security: Do not store LAN Manager hash value on next password change. Клацніть на кнопці Enabled, а потім на кнопці OK. Або ж можна відредагувати реєстр. Слід відкрити редактор реєстру (наприклад, Regedt32.exe) і перейти в розділ HKEY_LOCAL_ MACHINE \ SYTEM \ CurrentControlSet \ Control \ Lsa. У меню Edit потрібно вибрати пункт Add Key і ввести з клавіатури NoLMHash. Потім необхідно натиснути клавішу Enter, вийти з редактора реєстру і перезавантажити комп'ютер. Для активізації параметра потрібно змінити пароль;
- вставити в пароль спеціальний символ Unicode. Певні символи Unicode блокують генерацію хешу пароля LM. Список символів Unicode, що мають таку дію, наведено в табл. 1 глави 3 керівництва "Microsoft Windows 2000, Security Hardening Guide" site: microsoft.com).

Застосування довгих, складних паролів. Паролі повинні мати довжину не менше 15 символів і принаймні деякі елементи якої складності. За замовчуванням в комп'ютерах з Windows XP і новішими операційними системами активізовані складні паролі (питання про те, наскільки високий рівень складності паролів Microsoft, залишається відкритим). При використанні пароля довжиною більше 14 символів створення кешу паролів LM блокується, і більшість інструментів розгадування паролів, в тому числі більшість розрахункових таблиць, виявляються марними. А для розгадування складного пароля неефективними будуть більшість таблиць, які не дозволяють розкрити складні хеші паролів NT за прийнятний період часу. Ситуація може змінитися в міру вдосконалення методів злому паролів.

Відключення аутентифікації LAN Manager і NTLM. Більшість аналізаторів паролів успішно діють тільки проти процедур аутентифікації LAN Manager і NTLM. Після вичерпного тестування, що дозволяє переконатися, що такий захід не порушить виробниче середовище, слід заборонити використання протоколів аутентифікації LAN Manager і NTLM. Зробити це можна за допомогою редактора реєстру або об'єкта Group Policy Object (GPO). Необхідно перейти до Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options \ Network Security: LAN Manager Authentication level і активізувати режим Send NTLMv2 response only / refuse LM & NTLM.

Блокування облікових записів. Блокування облікових записів зупинить або принаймні істотно сповільнить більшість атак з розгадуванням пароля. Рекомендується встановити блокування з наступними параметрами:

- поріг блокування облікового запису слід встановити таким чином, щоб число невдалих спроб введення пароля не перевищувало п'яти;
- скидати лічильник блокування (параметр Reset account lockout counter after) через 1 хвилину (мінімальне можливе значення);
- встановити тривалість блокування (параметр Account lockout duration) рівним 1 хвилині.

Побоювання викликає комп'ютерний "хробак", що викликає відмови в обслуговуванні (DoS), але якщо «хробак» розгадує паролі, використовуючи імена входу всіх користувачів, то краще блокувати навіть законних користувачів, поки «хробак» не зупинено. Після того як загроза «хробака» буде усунена, всі облікові записи користувачів активізуються протягом 60 секунд.

Примусова заміна паролів з розумною частотою. З Group Policy або Local Security Policy слід перейти в Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Password Policy і привласнити параметру Maximum password age значення, що перевищує 90 днів. Витративши досить часу, можна розкрити будь-який пароль за допомогою будь-якої програми розгадування, злому або розрахункової таблиці. Але якщо пароль складний і має довжину не менше 15 символів, то для його злому більшості хакерів потрібно більше 90 днів. Підійде будь-який інтервал зміни пароля, але не слід міняти паролі занадто часто, щоб користувачі не почали записувати свої паролі на папері.

Захист процесу завантаження. Для захисту від фізичної атаки слід використовувати параметри BIOS, заборонивши завантаження з будь-якого пристрою, крім первинного жорсткого диска, а потім захистити BIOS за допомогою пароля. Цей прийом запобіжить (або, принаймні, затримає) локальні, фізичні атаки з розгадуванням пароля, в тому числі скидання паролів і витяг хешів паролів.

Перейменування облікових записів з широкими повноваженнями. Корисно перейменувати облікові записи з широкими повноваженнями, такі як Administrator, присвоївши їм імена, відмінні від обираних за замовчуванням. Зміна добре відомих імен облікових записів з великими повноваженнями - ефективний захист від багатьох програм автоматизованого відгадування паролів.

Додатковий захист облікових записів з широкими повноваженнями. Паролі облікових записів з найбільшими повноваженнями повинні бути найдовшими і складними на підприємстві, з мінімальним інтервалом зміни.

Активізація попереджувальних повідомлень на екрані регістрації. Активізація попереджувальних повідомлень на екрані реєстрації запобігає багато спроб розгадування паролів методом грубої сили, оскільки такі автоматизовані програми, як TSGrinder, не очікують попереджувального повідомлення. Активізувати екранні попередження можна за допомогою Group Policy, перемістившись з консольного дереву в Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options і двічі клацнувши на Interactive logon: Message text for users attempting to log on (і пов'язаної з нею функції Interactive logon: Message title for users attempting to log on).

Регулярний аудит паролів. І нарешті, слід регулярно проводити перевірки, намагаючись зламати паролі своєї організації з використанням деяких інструментів, перерахованих в урізанні «Типи атак на пароль». Зробити це потрібно раніше зломщиків. Результати можна використовувати в якості тесту відповідності, щоб допомогти кінцевим користувачам, що не дотримуються правил, виправити свої помилки (Табл.2.1.).

Таблиця 2.1.

МЕТОДИ ЗАХИСТУ ПАРОЛЯ

Метод захисту	**Опис**
Відключення хешу пароля LM	Рекомендується: - використовувати паролі довжиною не менше 15 символів; - відключити зберігання хешу паролів LM в масштабах всієї системи з використанням Group Policy або Local Security Policy; - вставити в пароль спеціальний символ Unicode.

Продовження Таблиці 2.1.

Застосування довгих, складних паролів.	Паролі повинні мати довжину не менше 15 символів і принаймні деякі елементи якої складності.
Відключення аутентифікації LAN Manager і NTLM.	Після вичерпного тестування, що дозволяє переконатися, що такий захід не порушить виробниче середовище, слід заборонити використання протоколів аутентифікації LAN Manager і NTLM.
Блокування облікових записів.	Рекомендується встановити блокування з наступними параметрами: - поріг блокування облікового запису після п’ти спроб введення пароля; - скидати лічильник блокування (параметр Reset account lockout counter after) через 1 хвилину; - встановити тривалість блокування (параметр Account lockout duration) рівним 1 хвилині.
Примусова заміна паролів з розумною частотою.	З Group Policy або Local Security Policy слід перейти в Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Password Policy і привласнити параметру Maximum password age значення, що перевищує 90 днів.
Захист процесу завантаження.	Слід використовувати параметри BIOS, заборонивши завантаження з будь-якого пристрою, крім первинного жорсткого диска, а потім захистити BIOS за допомогою пароля.

Продовження Таблиці 2.1.

Перейменування облікових записів з широкими повноваженнями.	Перейменувати облікові записи з широкими повноваженнями, присвоївши їм імена, відмінні від обираних за замовчуванням.
Додатковий захист облікових записів з широкими полномочіямі.	Паролі облікових записів з найбільшими повноваженнями повинні бути найдовшими і складними на підприємстві, з мінімальним інтервалом зміни.
Активізація попереджувальних повідомлень на екрані регістрації.	Активізувати екранні попередження можна за допомогою Group Policy, перемістившись з консольного дереву в Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options.
Регулярний аудит паролів.	Слід регулярно проводити перевірки, намагаючись зламати паролі своєї організації.

2.3 Актуальність удосконалення програмного модуля аналізу паролів

Аутентифікація користувачів, тобто підтвердження їх достовірності, забезпечується в першу чергу шляхом використання парольного захисту.

Слабкий парольний захист є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу. У 2019 році 80%

комп'ютерних зломів були реалізовані внаслідок недосконалості парольного захисту

Не зважаючи на існуючі методи генерування та зберігання паролів, більшість користувачів використовують звичайні слова та числові комбінації. А враховуючи об’єми персональної інформації, що люди публікують у соц-мережах, досить імовірно, що скадові паролю можуть опинитись у вільному доступі. Звичайно не у вигляді парольних комбінацій, але як імовірні складові.

Оскільки, повністю захищених систем не існує, виникає необхідність постійного удосконалення програмних засобів захисту. Будь-яка захищена система вразлива до повного перебору усіх можливих комбінацій паролю. Оскільки більшість систем не дають змогу здійснити атаки шляхом повного перебору, зловмисникам необхідно комбінувати методи атаки на паролі. Найбільш вразливою є атака з використанням персонального словника, складеного на основі доступної у мережі інформації про жертву.

Пипустимо атака базується на використанні персонального словника, сформованого на основі публічно-доступної інформації про ціль зловмисника, яку можливо отримати із соціальних мереж, відкритих інформаційних ресурсів, з використанням соціальної інженерії. Дієвим захистом від подібної атаки, є проведення навчання користувачів або працівників організацій, у яких використовують захищені інформаційні ресурси, впровадження для широкого використання програмні засоби створення надійних паролів шляхом випадкових комбінацій символів, використанням багатофакторної аутентифікації, або біометричних ідентифікаторів. Існуючі програмні засоби захисту від подібних атак, виконують більш загальну функцію, і їх ефективність не може бути точно оцінена.

Зважаючи на це, зростає потреба покращення існуючої системи захисту інформації, та розробки нових методів захисту від найбільш актуальних загроз, зокрема від атак з використанням соціальної інженерії.

Розглянутий програмний модуль аналізу пароля, після удосконалення може унеможливити проведення атак за персональним словником, або

соціотехнічних атак, шляхом попередження створення ненадійних паролів, що містять персональні даня користувача, або легко вгадуваня слова та числа. Такий програмний модуль може застосовуватись у будь-яких інформаційних системах, де використовується парольна аутентифікація, незалежно від того, чи є у самій системі відкрита для аналізу інформація про даного користувача.

Широке використання такого програмного модуля, може значно знизити ризик соціотехнічних атак на персонал, та виступати надійним методом перевірки вразливості паролів до подібних атак у майбутньому. Не зважаючи на те що даний модуль лише зменшує імовірність підбору пароля за персональним словником, це суттєво впливає на імовірність проведення соціотехнічної атаки в цілому, адже унеможливлює прихований доступ зловмисника до персональних даних користувача, і використання особистості користувача для реалізації наступних етапів більш складних атак.

2.4 Висновки до розділу

Раніше основним інструментом для злому облікових записів був «брутфорс» - перебір всіх можливих комбінацій, що вимагало багато часу і потужного комп'ютера. Однак знання того, що вибирають користувачі, змінило способи отримання паролів. Тепер «брутфорс» - це останній спосіб. Метод «брутфорса» є універсальним засобом для злому, але займає багато часу. Все через те, що зловмисник послідовно перебирає кожну можливу комбінацію, число яких зростає в геометричній прогресії з кожним додатковим символом в паролі. Наприклад, для пін-коду з 4 цифр максимальне число варіантів становить 10 тисяч. А для 5 цифр це вже 30,2 тис можливих комбінацій. Сьогодні зловмисники вже не кидаються в атаку на акаунти користувачів, озброївшись одним лише «брутфорсом». Вони попередньо підвищують свою освіченість, збираючи відомості про жертву з соціальних мереж і форумів. Там можна знайти

важливі для неї слова, імена і дати. Це знання дозволяє швидше підібрати пароль. Однак користувачі можуть протистояти кіберзлочинцям. Для цього потрібно використовувати складні комбінації фраз для пароля, уникати персональних даних в паролі і регулярно їх міняти. Також не варто використовувати паролі від важливих сервісів на зразок онлайн-банкінгу на різних сумнівних сайтах. Найкраще для подібних служб мати свої унікальні облікові дані, які більше ніде не використовуються. У випадку коли користувач все ж намагається створити ненадийний пароль, він повинен бути попереджений про його ненадийність, саме це обумовлює необхиднисть створення програмних засобів аналіху пароля.

РОЗДІЛ 3. УДОСКОНАЛЕНИЙ ПРОГРАМНИЙ МОДУЛЬ АНАЛІЗУ ПАРОЛІВ

3.1 Опис середовища розробки ПЗ

При виборі мови програмування, для програмного модуля аналізу паролів було обрано мову Rust.

Rust - нова експериментальна мову програмування, що розробляється Mozilla. Мова компільована і мультипарадигмальна, позиціонується як альтернатива C / C ++, що вже само по собі цікаво, так як навіть претендентів на конкуренцію не так вже й багато. Можна згадати D Вальтера Брайта або Go від Google.

У Rust підтримуються функіцональние, паралельне, процедурне і об'єктно-орієнтоване програмування, тобто майже весь спектр реально використовуваних в прикладному програмуванні парадигм.

Rust намагається зайняти проміжне положення між низькорівневими мовами типу C / C ++ і високорівневими Java / C # / Python / Ruby ... Чим ближче

мова перебуває до заліза, тим більше контролю, легше передбачити як код буде виконуватися. На противагу C / C ++ з'явилися Python / Java і всі інші. У них немає необхідності замислюватися про очищення пам'яті. Найстрашніша біда - це NPE, витоку не таке вже часте явище. Але щоб це все працювало необхідний, як мінімум, garbage collector, який в свою чергу починає жити своїм життям, паралельно з призначеним для користувача кодом, зменшуючи його передбачуваність. Віртуальна машина ще дає платформонезавісимость, але на скільки це необхідно - спірне питання, чи не буду його зараз піднімати.

Rust є низькорівневим мовою, на виході компілятор видає бінарник, для роботи якого не потрібні додаткові хитрощі. Вся логіка з видалення непотрібних об'єктів інтегрується в код в момент компіляції, тобто збирача сміття під час виконання теж немає. У Rust так само немає порожніх посилань і типи є безпечними, що робить його навіть більш надійним ніж Java.

В основі управління пам'яттю лежить ідея володіння посиланням на об'єкт і позичання. Якщо кожним об'єктом володіє тільки одна змінна, то як тільки закінчується термін її життя в кінці блоку, все на що вона вказувала можна рекурсивно очистити. Також посилання можна позичати для читання або запису. Тут працює принцип один письменник і багато читачів.

Незважаючи на синтаксис, схожий на C, головну особливість програм на Rust розробники взяли з Haskell, і звучить вона так:

Якщо програма на Rust скомпілювати і не впала під час запуску, то вона буде працювати до тих пір, поки ви самі її не зупините.

Це означає, що програми на Rust майже так само надійні, як програми на Haskell. Майже - тому що якщо програміст використовує «небезпечний» блок unsafe, який дає йому прямий доступ до пам'яті, то в теорії це іноді може привести до збоїв. Але навіть з такими блоками Rust намагається справлятися сам і падає тільки в безнадійних випадках.

Коли мова поєднує в собі кілька різних підходів з інших мов, він отримує більшість переваг кожного з них:

- висока швидкість роботи програм;

- можливість написати код в ООП-стилі: з класами і об'єктами (але є обмеження);
- стабільність в роботі і при компіляції;
- компілятор сам пропонує варіанти виправлення помилок в коді;
- крос-платформний компілятор;
- підтримка багатопоточності;
- підтримка «небезпечних» блоків для прямої роботи з пам'яттю;
- можна вставляти код на C і C ++.

Мінуси в основному пов'язані зі швидкістю розвитку мови. Так як Rust розвивається дуже швидко, то часто буває так, що код зі старої версії не працює в новій версії. Ще до мінусів можна додати:

- надлишкову документацію, яка іноді суперечить сама собі;
- мінливий від версії до версії синтаксис;
- неповну підтримку ООП і складну роботу з об'єктами і спадкуванням.

Особливості Rust:

- мова є кросплатформним, підтримуються Windows (> = 7, на даний момент тільки x86), а також Linux і MacOS (x86 і amd64);
- компілятор Rust написаний на Rust і використовує LLVM;
- багато що було запозичено з миру ФП - лямбда, замикання, кортежі, алгебраїчні типи даних, патерн матчінг, fold, map, filter, змінні за замовчуванням незмінні;
- використовується сувора статична типізація з автоматичним виведенням типів;
- у мові є метапрограмування (типізоване);
- є генерики, успадкування як такого немає, тільки тайпкласси;
- немає неявного перетворення типів, розмір примітивних типів як правило не залежить від платформи, немає ніякого null;
- мова підтримує Unicode, все рядки зберігаються в UTF-8 (подібно до того, як це зроблено в Vala) разом з довжиною і можуть містити в собі нульові символи;

- у стандартній бібліотеці є легковагі потоки (upd: випиляли) і типізовані канали для взаємодії між ними, а також футуро;
- у мови немає повноцінного GC, дані розміщуються або в стеку, або в купі, але пам'ять звільняється при виході з Скоуп, або використовуються лічильники посилань (для сміливих є і звичайні посилання);
- компілятор дуже жорстко стежить за тим, як ви працюєте з пам'яттю, наприклад, якщо він запідозрить можливість стану гонки, програма не скомпілюється;
- при дуже сильному бажанні ці перевірки можна обійти, що особливо зручно, наприклад, якщо ви хочете слінковаться з кодом на Сі;
- Rust має деякий рантайм, але на мові також можна писати і без Рантайм, що дозволяє використовувати Rust в задачах типу розробки ядра ОС.

3.2 Опис алгоритму аналізу паролів для попередження соціотехнічних атак

Сьогодні, використання пароль ного захисту інформаційних ресурсів є досить розповсюдженим і використовується майже усіма користувачами. Це обумовлює необхідність покращення систем генерації та перевірки паролів, для збільшення надійності інформаційних ресурсів та захищеності персональних даних. Сьогоднішні інформаційні системи використовують цілий комплекс заходів та методів що попереджують вгадування паролюб такі як: затримки між спробами вводу пароля, обмежена кількість спроб вводу, двухфакторна автентифікація, та інші.

Нажаль, найбільша кількість хакера ким атак сьогодні, все ще успішно використовує злам пароль ного захисту. Але програмні засоби генерації надійних паролів, та рекомендації для користувачів не є достатньо надійними, тому

виникає необхідність постійного покращення систем перевірки паролів на етапі його створення та подальшого вводу у информаційні системи.

Для розробки нових методів захисту пароля, необхідно визначити основні критерії надійності пароля, та обрати напрямок, котрий потенційно є найбільше вразливим. Складність пароля є мірою ефективності, з якою пароль здатний протистояти його вгадування або методу повного перебору. У своїй звичайній формі складність пароля є оцінкою того, як багато спроб в середньому потрібно зломщикові, без прямого доступу до паролю, для його вгадування. Інше визначення терміна - функція від довжини пароля, а також його заплутаності і непередбачуваності. Тому, розглядаючи надійність пароля, потрібно зважати на два основних критерії, а саме:

- легкість перевірки вгадуваності пароля
- кількість спроб, необхідних для підбору пароля.

Перший критерій залежить від способу зберігання та сфери використання пароля. Існує кілька варіантів надійного зберігання паролів:

В хмарі. Доступ до онлайн-сховища можна отримати з будь-якого пристрою при наявності підключення до інтернету. Паролі як правило зберігаються в текстовому файлі. Якщо ноутбук і смартфон вкрадуть або зламається, то відновити дані буде дуже просто. Як правило, всі дані в хмарному сховищі шифруються. Досить буде запам'ятати один пароль від аккаунта хмари або від файлу, якщо він додатково зашифрований, або обидва пароля.

У браузері. В цьому випадку всі комбінації запам'ятали логінів і паролів будуть вводитися автоматично. Ось тільки збережуться вони до першої невдалої переустановлення браузера, а після цього відновити їх буде неможливо. Тому це не найоптимальніший варіант.

На зовнішньому носії. Флешка зручна тим, що її можна носити з собою. Але вона може зламатися або потрапити в руки до третіх осіб. Щоб паролі були моментально лічені, інформацію в текстовому файлі можна зашифрувати за допомогою спеціальної програми або вбудованої функції редактора Microsoft Word. Все, що потрібно запам'ятати в даному випадку, - єдиний майстер-пароль.

За допомогою спеціального додатку-сховища. У цього способу є безліч переваг: до нього можна отримати доступ з будь-якого пристрою, досить запам'ятати єдиний пароль і дані профілю.

Другий критерій залежить від необхідної потужності для перебору паролів відповідної довжини та необхідного набору символів що можуть в ньому використовуватись. Час злому пароля пов'язанмй з бітовою міцністю (міцність пароля), яка є мірою інформаційної ентропії пароля. Більшість методів злому пароля вимагають комп'ютерно зробити багато пробних паролів, кожен з яких повинен бути перевірений. Одним з прикладів є метод грубої сили (brute-force), при якому комп'ютер підбирає усілякі ключі або паролі, поки один з них не підійде. Більш поширені методи злому паролів, такі, як атака словником, перевірка за шаблоном, заміна списку слів і т. д. намагаються зменшити кількість необхідних спроб і, як правило, застосовуються до методу грубої сили. З підвищенням міцності паролю експоненціально збільшується кількість можливих паролів для перебору при відновленні пароля і зменшується ймовірність того, що пароль буде знайдений в якомусь словнику для злому.

Можливість злому паролів з використанням комп'ютерних програм також залежить від кількості перевірених паролів в секунду. Якщо хеш цільового пароля відомий атакуючому, це число може бути досить великим. Якщо ні, швидкість залежить від того, чи встановлений ліміт швидкості автентифікації (як часто може вводитися пароль), або від тимчасових затримок, капчі, або примусового блокування після деякого числа невдалих спроб. Інша ситуація, коли можливо швидке вгадування, — якщо пароль використовується для формування криптографічного ключа. У таких випадках зловмисник може швидко перевірити, чи успішно пароль, який перевіряється декодує зашифровані дані. Наприклад, один комерційний продукт може перевірити 103,000 WPA-PSK паролів в секунду.

Індивідуальні настільні комп'ютери можуть перевірити більше ста мільйонів паролів в секунду, використовуючи утиліти для злому паролів, запущених на CPU і мільярди паролів в секунду при використанні утиліт, які

використовують GPU. Розглянемо утиліту John the Ripper. Вибраний користувачем пароль з восьми знаків з числами, у змішаному регістрі, і з символами, за оцінками, досягає 30-бітної надійності, згідно з NIST. 2^30 — це один мільярд перестановок і потрібно в середньому 16 хвилин, щоб зламати його. Коли звичайні настільні комп'ютери об'єднуються для злому, як це може бути зроблено при ботнетах, можливості злому пароля значно розширюються. В 2002 році distributed.net успішно підібрало 64-бітний ключ RC5 за 4 роки, використовуючи більш 300000 різних комп'ютерів в різний час, і генеруючи в середньому понад 12 мільярдів ключів в секунду. Графічні процесори можуть прискорити злом паролів на коефіцієнт з 50 до 100 і більше для комп'ютерів загального призначення. З 2011-го комерційні продукти мають можливість тестування до 2,800,000,000 паролів в секунду на стандартному настільному комп'ютері з використанням потужного графічного процесора. Такий пристрій може зламати 10-символьний пароль в одному регістрі за один день. Слід зазначити, що робота може бути розподілена на кілька комп'ютерів для додаткового прискорення пропорційно числа доступних комп'ютерів з порівнянними GPU. Незважаючи на свої можливості, настільні процесори повільніше в зломі паролів, ніж спеціально побудовані машини, призначені для злому пароля. Грунтуючись на цій інформації хакери розробляють нові алгоритми брутфорса.

В заглазному можна визначити, що паролі завдовжки до шести символів включно, складені з 95 ASCII-символів (26 букв латинського алфавіту в обох регістрах, 10 цифр і 33 службових символів), зламуються методом повного перебору («грубої сили») на звичайному персональному комп'ютері за допомогою сучасної відеокарти буквально за лічені хвилини. Але додавання навіть одного-двох символів вже серйозно ускладнює завдання, подовжуючи час перебору до декількох днів і навіть місяців. Однак довжина - нехай і головний, але далеко не єдиний критерій оцінки стійкості пароля. Принципове значення має відсутність якогось передбачуваного шаблону в самому наборі і невипадковість в послідовності символів пароля.

Складність пароля в комп'ютерній індустрії зазвичай оцінюють в термінах інформаційної ентропії. Ця величина, що розраховується в бітах ентропії, дозволяє зі значним ступенем точності оцінити складність пароля. Так, ентропія на один символ для пароля з усіх ASCII-символів складе близько 6,56 біт; таким чином, складність 6-символьного пароля буде складати 39,36 біта ентропії, 7-символьного - вже 45,95 біт, а 8-символьного - 52,48 біт.

Щоб зламати пароль 52-бітної складності методом перебору, потрібно кількість спроб, що дорівнює 2 в 52-й ступеня. При використанні пари сучасних відеокарт класу GeForce GTX 570, здатних підбирати по 1,5 мільярда паролів в секунду, перебір всіх можливих комбінацій займе приблизно пару місяців безперервної роботи, що, загалом, і дає уявлення про стійкість такого пароля.

Однак це стосується виключно паролів, що не містять якихось передбачуваних шаблонів, тобто згенерованих машинно, з теоретично максимальною ентропією. Для поведінки самої людини типова передбачуваність, тому при складанні пароля він підсвідомо буде використовувати якісь знайомі поєднання і комбінації цифр, символів і букв. Мимоволі пригадуються пам'ятні дати, дні народження, імена дорогих людей, назви знайомих місць і предметів.

На ділі це означає значно більшу вразливість, оскільки метод «грубого підбору» завжди застосовується в комбінації з іншими способами злому, зокрема зі словниковим підбором. При цьому використання відомих масок і шаблонів значно спрощує завдання. Крім звичайних словників і словників реальних користувальницьких паролів зі зламаних сайтів, широко відомі маски на підстановку окремих букв або додавання чисел, популярні числові послідовності - шаблони дат, телефонів, індексів, номерів соціального страхування, а також багато інших прийоми, марно здаються їх авторам надзвичайно оригінальними.

За оцінками Національного інституту стандартів і технологій США (NIST), ентропія першого символу з букв нижнього регістру і цифр в паролі, придуманих людиною, становить 4 біта, наступних семи - 2 біти, а застосування верхнього регістру і службових символів додає ще 6 бітів, що в сумі дає всього 24 біта,

тобто в два з гаком рази менше в порівнянні з теоретичним максимумом для заданого набору символів і довжини. Тобто час підбору такого пароля навіть методом «грубої сили» зменшується вдвічі, в реальності ж «гібридна» атака дозволить зловмисникові домогтися успіху набагато швидше.

І тут ми знову повертаємося до довжини: складність пароля довжиною 14 символів теоретично складе 91,84 біта, а довжиною 20 символів - вже 131,2 біта, і на злом таких паролів тільки методом перебору при існуючих обчислювальних потужностях піде кілька десятків, а то і сотень років. Гібридні методики, зрозуміло, значно знижують стійкість подібних кодів, а «людський фактор» робить їх ще вразливішою. Проте довжина робить свою справу: для звичайного користувача пароля, навіть якщо в ньому є не дуже явні шаблони, рекомендована кількість символів на сьогодні має бути не менше 14. Такий пароль буде набагато безпечніше, ніж «суперстійкі» колись паролі з 6 -8 символів.

Отже для покращення парольного захисту інформаційних систем необхідно розглянути процес створення та вводу пароля. Уже дев’ять років поспіль експерти компанії SplashData складають список 100 найгірших паролів року. Так вони сподіваються привернути увагу до проблеми, вважаючи, що подібна статистика змусить користувачів задуматися про безпеку і усвідомити, що комбінації на кшталт «123456» - це зовсім небезпечні паролі. Але навіть після численних витоків даних, зломів, атак шифрувальників та інших інцидентів, список очолюють все ті ж «password» і «123456».

Як і в минулі роки, аналітики вивчили більше 5 000 000 паролів, «витекли» в широкий доступ під час різних інцидентів. На жаль, в порівнянні з минулими роками список змінився мало, користувачі як і раніше охоче використовують найпростіші комбінації на кшталт «qwerty» і «password», а також імена знаменитостей (наприклад, в цьому році в топ-25 з'явилося слово «donald»), попокультурние терміни, різні бренди тощо.

За підрахунками SplashData, близько 10% користувачів застосовують хоча б один з паролів, які увійшли в список найгірших у цьому році (Табл.3.1.). Ще 3% користувачів застосовують найгірший пароль, тобто «123456».

У підсумку список 25 найгірших паролів 2019 року виглядають наступним чином:

Таблиця.3.1.

НАЙПОПУЛЯРНІШІ НЕНАДІЙНІ ПАРОЛІ 2019 РОКУ

1	12345
2	123456
3	123456789
4	test1
5	Password
6	12345678
7	Zinch
8	g_czechout
9	Asdf
10	Qwerty
11	1234567890

Продовження Таблиці 3.1.

12	1234567
13	Aa123456
14	Iloveyou
15	1234
16	abc123
17	111111
18	123123
19	Dubsmash
20	Test
21	Princess
22	Qwertyuiop
23	Sunshine
24	BvtTest123
25	11111

Інша команда SafetyDetectives зібрала інформацію про понад 18 мільйонів паролів і вибрали з них 20 найбільш використовуваних, найбільш передбачуваних, і, як результат, найбільш зламуваних паролів у світі.

Слово "пароль" є найпопулярнішим серед користувачів по всьому світу, а також серед користувачів домену .edu і користувачів з США. Варіації даного пароля в інших мовах, наприклад "passwort" (Німеччина) або "motdepasse" (Франція), також представлені у відповідних списках даних країн.

Крім цього, в окремих країнах і в усьому світі популярні слова "ангел", "дракон", "супермен" і інші слова, що знаходять відображення в культурі широкої категорії користувачів.

Більшість європейських користувачів (зокрема з Іспанії та Італії) вважають за краще використовувати в якості паролів імена.

Згідно з нашим дослідженням, українські користувачі відрізняються від користувачів з інших країн. Замість смислових слів вони вважають за краще використовувати комбінації клавіш, навіть в разі використання в якості паролів буквено-цифрових комбінацій.

Імена часто використовуються в паролі, особливо це стосується імен, зазначених в адресах електронної пошти - такий пароль використовують 4.19% користувачів по всьому світу. Частіше за інших користувачів подібні прості для злому паролі використовують італійці (4.13%), і німці (2.51%).

Комбінація "123", додана до або після імені з адреси електронної пошти, зустрічається в 0.03% паролів користувачів з усього світу. Додавання випадкових цифрових комбінацій до паролю - хороший спосіб ускладнити пароль, проте подібна проста комбінація надто популярна, тому хакерам не важко зламати такий пароль.

Крім цього, широко використовуються загальновживані слова і фрази ("letmein", "iloveyou", "princess", "superman" і т.д.).

Також залишаються популярними певні комбінації клавіш - 25% з 30 найпопулярніших паролів є комбінаціями клавіш. "Qwerty" є найпопулярнішою

комбінацією, при цьому також широко представлені діагональні комбінації, такі як "1q2w3e4r" і «zaq12wsx".

У всіх країнах одним з найпопулярніших паролів є слово "привіт" (на відповідній мові), яке присутнє практично у всіх списках 20 найпопулярніших паролів по країнам.

У десятку найбільш популярних паролів в країнах-любителів футболу - Іспанії та Італії - входять назви відомих футбольних команд. Користувачі з Німеччини та Іспанії віддають перевагу числовим комбінаціям.

Дана статистика є досить корисною для інформування користувачів про необхідність створення надійного пароля, котрий відповідає усім критеріям. Також дану статистику можна використати для створення алгоритму аналізу паролів. Саме такий алгоритм буде лежати в основі програмного модуля аналізу паролів.

Розроблений алгоритм є достатньо простим у своїй ідеї, але при достатньо професійному рівні програмної реалізації та постійному покращенні, може суттєво зменшити відсоток хакерськ атак з використанням зламу паролю.

Перша частина алгоритму аналізу паролів, буде обробляти існуючі відкриті бази паролів, для виявлення закономірностей та створення правил/шаблонів, по яким люди найчастіше створюють паролі. Для початку було проаналізовано. Яку саме довжину пароля, користувачі вважають достатньо надійною.

З графіку слідує, що найбільш розповсюдженим є пароль довжиною 6 символів (Рис.3.1.). Це суперечить більшості рекомендацій, у яких мінімальною довжиною є 8 символів.

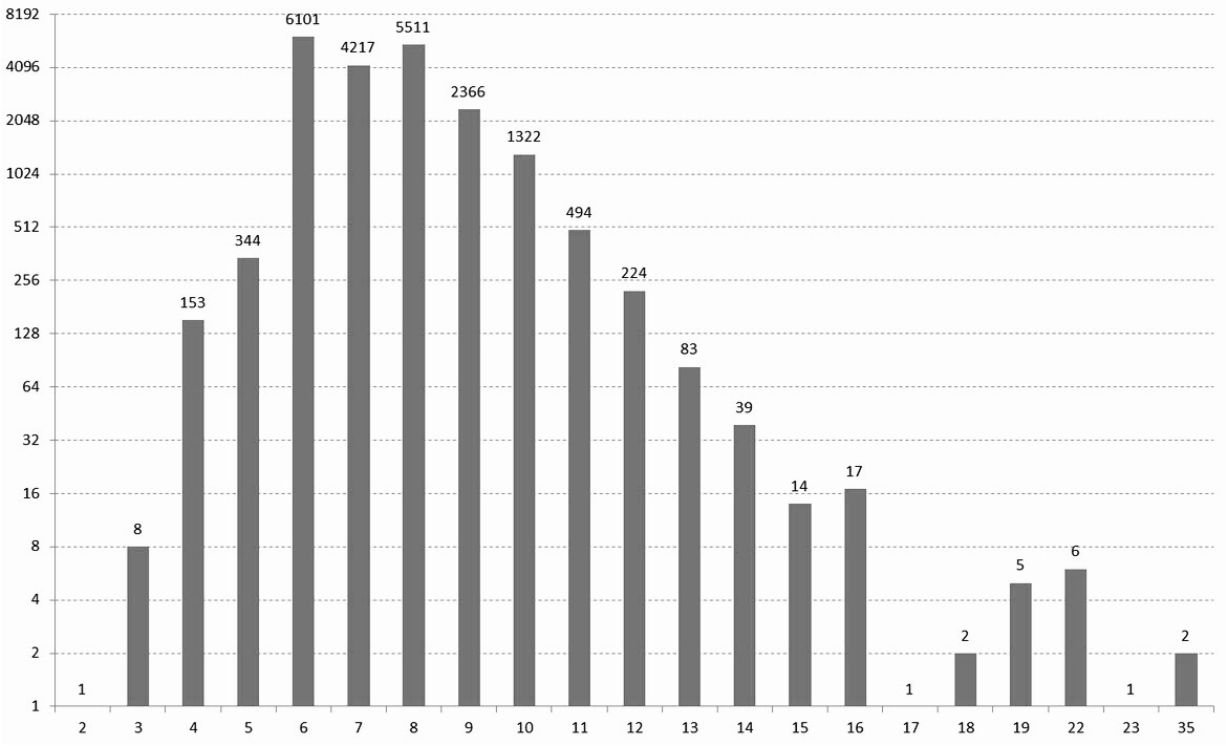
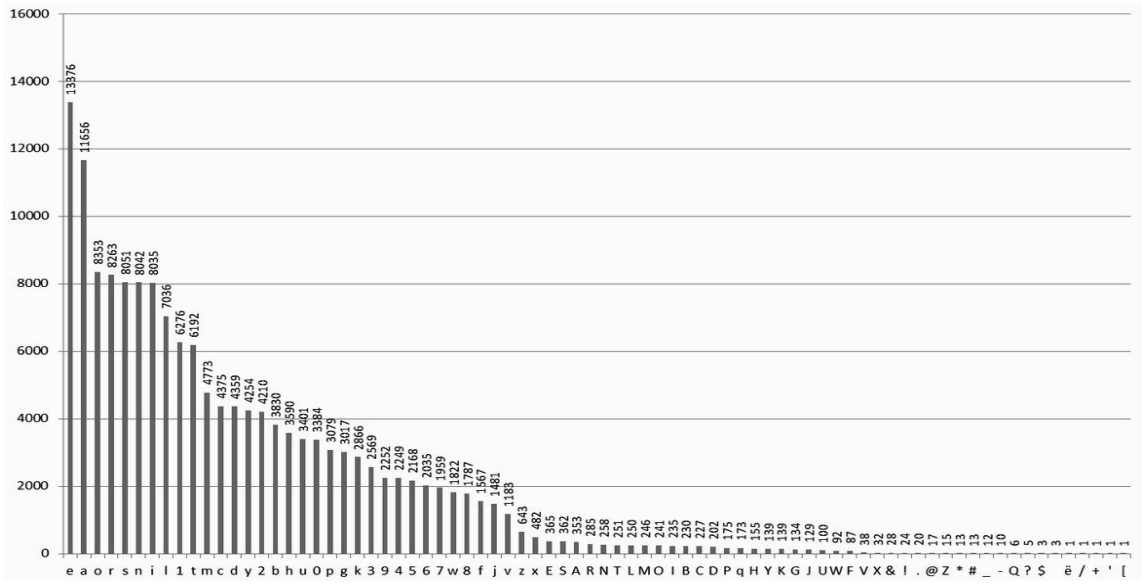


Рис.3.1. Графік розподілу кількості символів відносно популярності паролів.

Враховуючи це, можна припустити. Зо зловмисник буде підбирати комбінації довжиною від 4 до 14 символів. Цей діапазон покриваю найбільшу



кількість паролів користувачів у світі.

Рис.3.2. Графік розподілу частоти вживаності символів у паролі.

Наступним етапом є аналіз символів що найчастіше використовуються у паролях. Відповідно до графіка, можемо бачити, що найчастіше зустрічаються голосні літери латинського алфавіту, а саме «e», «a», «o» (Рис.3.2.). Також досить розповсюдженими є літери «r», «s», «n».

Ця інформація допоможе у створенні правил та підборі найбільш імовірних слів для створення пароля.

Алгоритм також аналізує доступні паролі, та шукає шаблони ха якими люди комбінують відомі їм слова та числові комбінації. Серез розлянутих групп слів, було проаналізовано імовірність використання назв міст, та шаблони номерів телефонів. Як результат, програма сама генерує правила на основі реальних словників паролів, що були скомпрометовані за минулі роки.

Розглянемо план дій зловмисника, котрий намагається отримати доступ до інформаційного ресурсу шляхом зламу пароля користувача. Відповідно до правил соціальної інженерії, зловмиснику необхідно зібрати усю корисну інформацію про користувача, після чого поєднати зібрану інформацію використовуючи найбільш популярні шаблони для створення паролів. Алгоритм аналізу паролів використовує такий же план дій.

Програмна реалізація алгоритму отримує від користувача необхідні дані, введені у формі реєстрації облікового запису у соцмережі, а саме: ім’я та дата народження, місто у якому проживаю користувач, номер телефону, та інше. Більш досконала програмна реалізація може сканувати необхідну информацію із посилання на обліковий запис користувача з будь-якої іншої соцмережі.

Визначення віку користувача також може стати корисним, оскільки, люди старше 55 років вибирають вдвічі складнішт паролі, ніж молодь: в середньому, 7,5 бітів ентропії проти 6,3 бітів. Такими є результати найбільшого в історії дослідження безпеки паролів, проведеного фахівцями з Кембриджського університету на анонімній основі з майже 70 мільйонів акаунтів Yahoo.

Кембриджські дослідники розрахували середню силу паролів в бітах для різних демографічних груп. Виявилося, що найсильніші паролі у німців і корейців, а найслабші - у жителів Індонезії.

З'ясувалося також, що люди, схильні періодично міняти паролі до свого облікового запису, вибирають більш сильні комбінації символів. Це теж цілком логічно, тому що обидві цих звички властиві просунутим користувачам.

Після визначення ключових слів та чисел, програма використовує згенеровані правила, створені на основі попередньо досліджених закономірностей, для генерування найбільш імовірних паролів користувача, котрі він може вигадати у процесі реєстрації.

Після генерації варіантів пароля, кожен з них порівнюється з введеним паролем користувача, і у разі високого відсотка відповідності, повідомляє про необхідність зміни пароля (Рис.3.3.).

Рис.3.3. Блок схема розробленого алгоритма.

Програмний модуль, в даному випадку використовує для аналізу словник паролів, що знаходився у вільному доступі. Даний словник був опублікований на сторінці wordbook.xyz, де зібрані оприлюднені словники паролів по категоріям їх джерел та датам витоків. Обраний нами словник містить у собі 100000 пароів, опублікованих 17 грудня 2020 року, а отже є достатньо актуальним для використання у програмній реалізації запропонованого алгоритму.

Для поривняння було використано словник найрозповсюдженіших імен що використовуються як нікнейм у соціальних мережах, таких як Facebook, Twitter, LinkedIn, Instagramm, Behance. У даному словнику відібрано 4 945 найпопулярніших імен.

Далі було використано словник із найвідомішими назвами міст, усіх країн світу, що налічує 3 275 назв.

Пошук по датам, було реалізовано в межах від 1940 до 2019 року, оскільки саме у цей період імовірно народились цільові користувачі.

Для пошуку по датам в межах 1940-2019 років у словнику паролів,було використано регулярні вирази:

"(?:19[4-9][0-9]|20[01][0-9])" - для пошуку по рокам.

"(?:[015-9][0-9])" - для пошуку по рокам, у скороченому записі.

"(?:0[1-9]|1[0-2])" - для пошуку по місяцям.

"(?:0[1-9]|[12][0-9]|3[01])" – для пошуку по дням.

«?(9[976]\d|8[987530]\d|6[987]\d|5[90]\d|42\d|3[875]\d|2[98654321]\d|9[8543210]|8[6421]|6[6543210]|5[87654321]|4[987654310]|3[9643210]|2[70]|7|1)\d{9}" – для пошуку за номерами телефону.

Надалі, саме ці регулярні вирази, та їх комбінації будуть лежати у основі пошуку, та підрахунку статистики, на основі якої будуть побудовані правила.

Дані регулярні вирази можна налаштувати під пошук у конкретному часовому проміжку, що дасть змогу будувати правила для певної вікової групи людей.

Також було розроблено регулярний вираз для порівняння із шаблоном номерів телефонів. Для початку він розпізнає початкові індекси країн, та порівнює кількість наступних чисел на відповідність шаблонам телефонних

номерів. Усі розроблені правила зберігаються у файлі конфігурацій (Рис.3.4.).

```
# passwords = "data/Ashley_Madison.txt"
passwords = "data/10-million-password-list-top-1000000.txt"
# passwords = "data/xsplit.txt"
# passwords = "data/Top304Thousand-probable-v2.txt"

# Try to match these patterns AND every word from filtered 'words' list on every password
try_patterns = ["ddmmyy", "yymmdd", "yyyy", "mmdd", "ddmm", "dd", "phone"]

check_words_at_begin = true
check_words_at_mid = true
check_words_at_end = true

num_generated_passwords = 20

[group]
[group.name]
words_filename = "data/first-names.txt"
words_filter = ".{4,}"

[group.city]
words_filename = "data/usa-cities-and-states.txt"
words_filter = ".{4,}"

[patterns]
# Regex, years 1940-2019
yyyy = "(?:19[4-9][0-9]|20[01][0-9])"
yy = "(?:[015-9][0-9])"
# Regex, months 01-12
mm = "(?:0[1-9]|1[0-2])"
# Regex, days 01-31
dd = "(?:0[1-9]|[12][0-9]|3[01])"

# Concat pattern for 'dd' + 'mm' + 'yyyy' to create 'ddmmyyyy'
ddmmyyyy = ["dd", "mm", "yyyy"]

ddmm = ["dd", "mm"]
mmdd = ["mm", "dd"]
ddmmyy = ["dd", "mm", "yy"]
yymmdd = ["yy", "mm", "dd"]

not_a_number = '(\b|[^\d])'

# Taken "Generic International Phone Number" from https://phoneregex.com/ and changed slightly
generic_phone = '\+?(9[976]\d|8[987530]\d|6[987]\d|5[90]\d|42\d|3[875]\d|2[98654321]\d|9[8543210]|8[6421]|6[6543210]|5[87654321]|4[987654310]|3[9643210]|2[70]|7|1)\d{9}

phone = ["not_a_number", "generic_phone", "not_a_number"]
```

Рис.3.4. Файл конфігурацій.

Під час попереднього дослідження в процесі написання програмного коду, було визначено, що найчастіше користувачі використовують комбінації дня з місяцем, або місяця з роком. В той час як комбінація дня з роком, дала результат менше 1% від загальної кількості знайдених паролів з використанням дати. Як результат, така комбінація ігноруватиметься в побудованих правилах, відповідно до низької імовірності співпадінь.

Програмний модуль порівнює усі словники, та знаходить збіги у паролях, іменах, містах, датах та номерах телефонів, після чого визначає де саме знаходяться необхідні символи відносно інших символів. Після декількох тестів з різними словникам, було визначено, що 9.6% усіх паролів починаються з шуканого імені, і далі мають ще декілька додаткових символів. Також 4.2% паролів містять додаткові символи до та після імені, а 2.4% - закінчуються іменем

(Рис.3.5.).

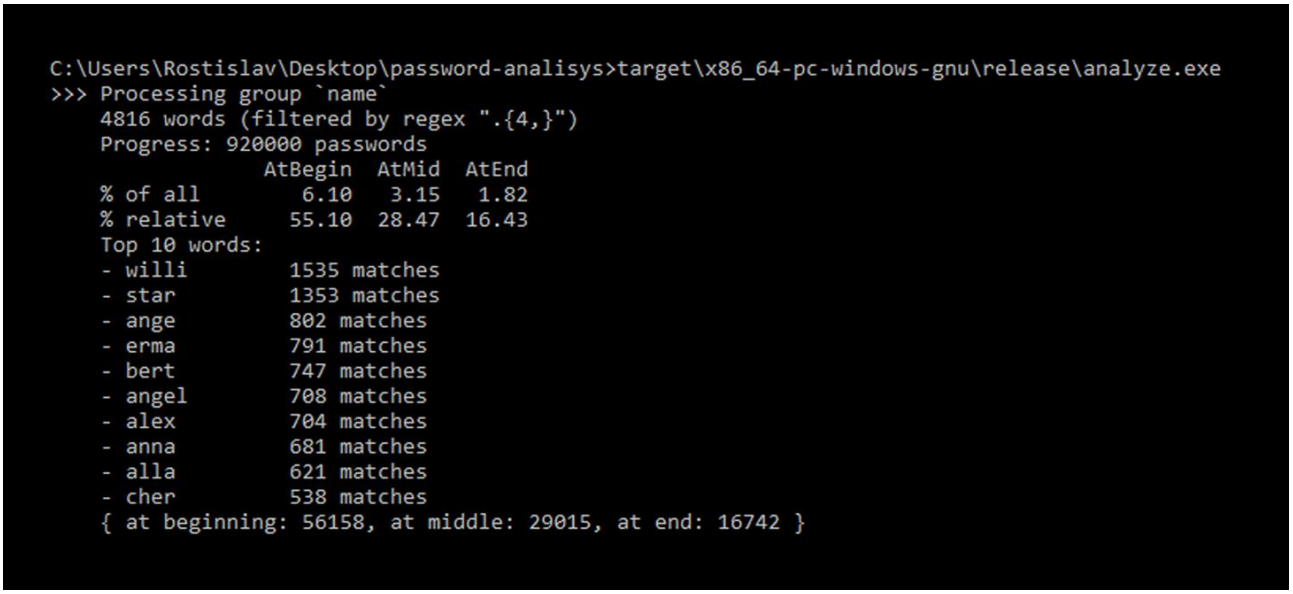


Рис.3.5. Проміжний результат обрахунків.

Також після аналізу було визначено що значна кількість паролів містять назву міста в певному вигляді. 1,26% усіх паролів починаються з назви міста, і далі мають ще декілька додаткових символів, 0.27% паролів містять додаткові символи до та після назви, а 0.21% - закінчуються назвою міста (Рис.3.6.).

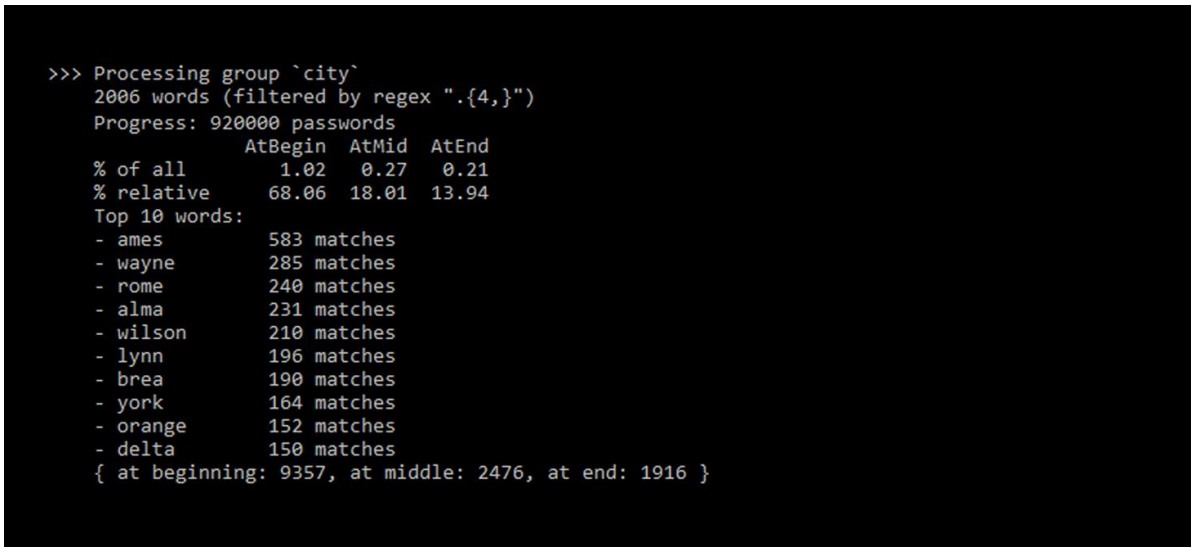


Рис.3.6. Проміжний результат обрахунків.

Виходячи з даних результатів, можемо підрахувати, що існує імовірність 16.2%, що зловмисник зможе підібрати значну частину символів пароля

перебравши декілька імен пов’язаних з користувачем.

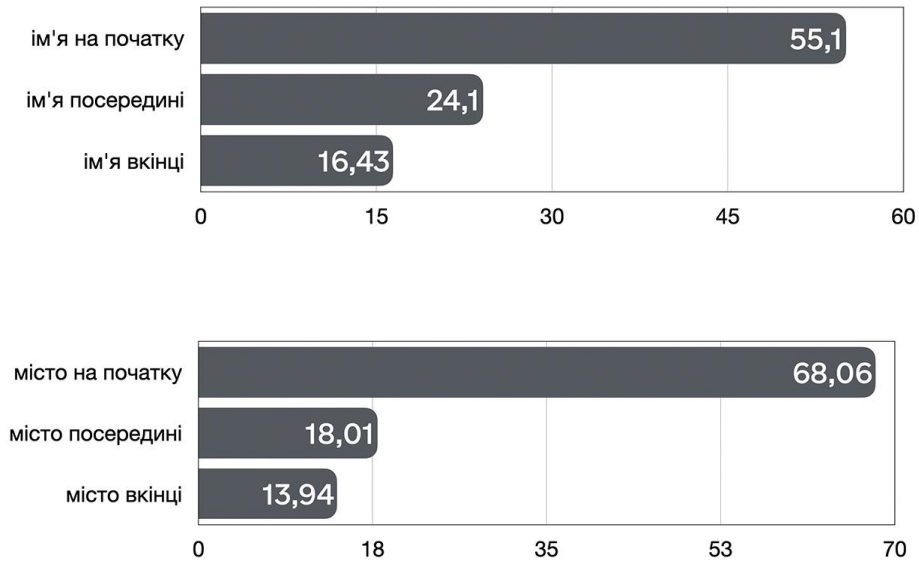


Рис.3.7. Відсотковий розподіл місця слова в паролі.

Загалом, серед усіх знайдених паролів що місять у собі ім’я, відсотковий розподіл положення імені відносно додаткових символів виглядає так: 55,1-68,06% - на початку, 18,01-28.47% - між символами, 16,43-13,94% - у кінці (Рис.3.7.).

Далі програма за допомогою вказаних регулярних виразів проводить пошук дат (Рис.3.8.).

```
>>> Processing 7 patterns
    Pattern stats:
      ddmmyy        64809 times (  0.070% of total)
      yymmdd        34000 times (  0.037% of total)
      yyyy          73079 times (  0.079% of total)
      mmdd          84810 times (  0.092% of total)
      ddmm          99089 times (  0.108% of total)
      dd           327766 times (  0.356% of total)
      phone          1257 times (  0.001% of total)

>>> 920871 passwords checked in total
>>> Calculated stats were stored in `stats.toml`
```

Рис.3.8. Проміжний результат обрахунків (регулярні вирази)

Визначивши усі імовірні форми запису дати та встановивши діапазон пошуку в межах від 1940 до 2019 років, та виконавши пошук по всьому словнику паролів, отримаємо наступну статистику: 0.07% паролів містить дату у формі запису «день-місяць-рік», 0,037% паролів також містять повну форму запису дати, але у зворотному порядку, починаючи з року (Рис.3.9.).

Наступні варіанти форми запису є менш точними, оскільки імовірніше можуть містити у собі випадкові символи, але відсоток частоти їх використання у паролях значно вищий. Формат дати «день-місяць» є найпопулярнішим і зустрічається у 0,108% усіх паролів. Також досить популярним є використання формату «рік» у повному записі, а саме: 0,79% від загальної кількості паролів. Слід зазначити що серед паролів також було знайдено значну кількість номерів телефонів, що свідчить про те, що хоча загальний відсоток дуже малий, є достатньо велика кількість людей, що використовують увесь номер телефону в якості пароля, що є дуже ненадійним.

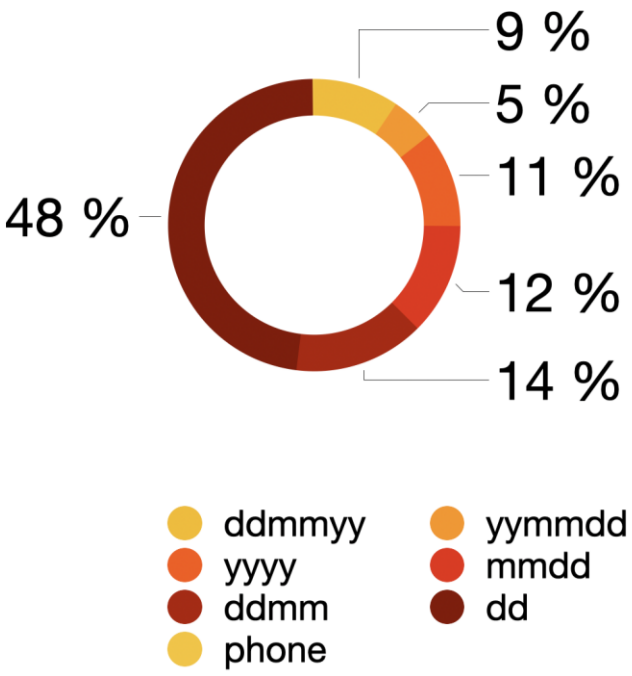


Рис.3.9. Діаграма формату запису дат.

Серед усіх паролів, 41.7% містять число у діапазоні 00-19 та 40-99, що

відповідає короткій формі запису року. Не можна стверджувати напевно, що дані числа є саме скороченим записом року, але імовірність цього досить велика. Уточнити статистику саме по цьому варіанту можна, провівши перехресний пошук паролів що містять у собі імена і дати, але ігноруючи паролі що містять більше двох числових символів. В такому випадку, імовірність того, що два числа, що стоять після, або перед іменем, є саме коротким записом року, дуже велика, і її також можна використовувати при формуванні правил.

Після виконання усіх попередніх підрахунків, програмний модуль записує усі зібрані статистичні дані, та в даному випадку, поєднує статистику пошуку імен, із статистикою пошуку по датам та формує власний список імовірностей.

3.3 Тестування програмного модуля аналізу паролів

Користувачу необхідно ввести своє їм’я, дату народження, місто та паролі які цей користувач використовую у повсякденному житті. Так, наприклад при розподілі імен з імовірністю 55.1% - на початку, 28.47% - між символами, 16.43% - у кінці, програма згенерує 25 варіантів пароля. Далі, відповідно до статистики використання різних форм запису дат, до імен додаватимуться комбінації дати, номеру телефону, назви міста введеної користувачем.

Складним випадком є генерування пароля, якщо ім’я стоїть посередині. В такому випадку, дата може знаходитись або до, або після імені, а в іншій частині містяться додаткові символи, що не відомі програмі, і не розпізнаються. Таким чином, варіанти з іменем у середині є не остаточно вірними, та потребують доповнення. Відсоток їх відповідності введеному користувачем паролю, може становити не більше 66%.

Проведемо тестування програмного модуля. Для початку користувач вводить дату народження у форматі рік-місяць-день, далі вводиться ім’я, назва міста та номер телефону. Після введеня цих даних, користувач вводить свій

пароль, котрий необхідно перевірити (Рис.3.10.)

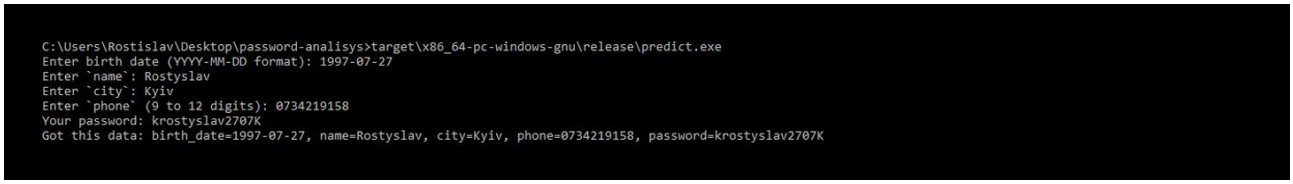


Рис.3.10. Хід тестування

Після запуску, програмний модуль використовує згенерованя в результаті попереднбого аналізу баз паролів правила, та генерує паролі. Утворений список з 25 паролів, містить найбільш вразливі з точки зору соціальної інженерії варіанти паролів для даного користувача.

Цей список порівнюється з введеним користувачем паролем, та обраховується його відповідність кожному із варіантів, після чого програма виводить на екран співпадіння з одним із варіантів. Саме це число і є відсотком ненадійності пароля даного користувача.

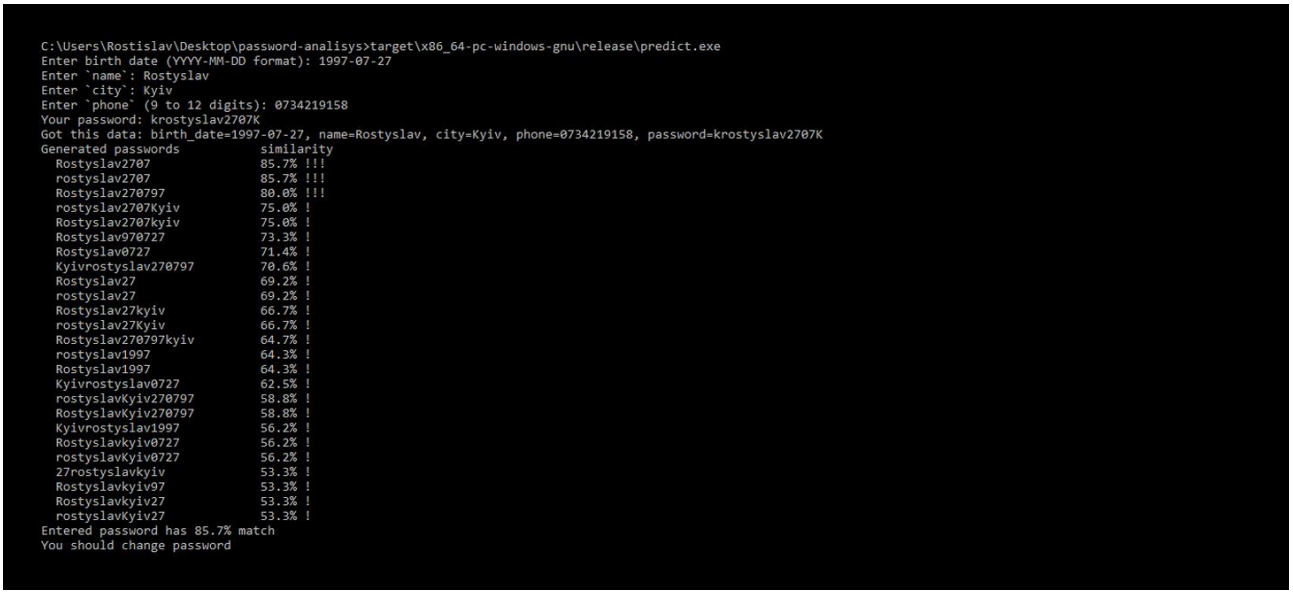


Рис.3.11. Хід тестування

У випадку, якщо цей відсоток перевищує 50%, пароль вважається ненадійним, програма повідомляє користувачу, що йому необхідно змінити пароль, та надає рекомендації щодо цього. Після того як користувач створив

новий пароль, рекомендується повторно перевірити його, щоб підтвердити що новий пароль є достатньо надійним. Рекомендований відсоток надійності в межах від 0 до 30% (Рис.3.11.).

Якщо сайт показує користувачам оцінку складності їх пароля, частка слабких паролів падає з 75 до 35 відсотків. Ще більшого поліпшення паролів можна домогтися, якщо порівнювати їх з паролями інших користувачів або розповідати про те, скільки часу знадобиться зловмисникам на підбір пароля, повідомляється в журналі Computers & Security.

Дослідники під керівництвом Стівена Фёрнелла (Steven Furnell) оцінили ефективність різних способів повідомлення користувача про слабкий паролі. Для цього вони провели два експерименти. У першому брало участь 300 користувачів, яких просили завести аккаунт і придумати пароль для нього. Користувачів розбили на п'ять груп, кожній з яких показували різні варіанти рад біля поля введення пароля:

- прохання не використовувати старі паролі;
- базові поради про довжину пароля, використанні різних типів символів і не використанні особистої інформації;
- стандартна смужка складності пароля з трьома класами (слабкий, середній, сильний);
- емодзі, відповідний класу складності;
- емодзі з радою, наприклад, «Нормально, але ти міг би придумати краще».

З'ясувалося, що серед користувачів, які не отримували майже ніяких підказок (перша група) частка слабких паролів була на рівні 75 відсотків. Серед всіх інших груп частка значно впала: до рівня від 45 відсотків у другої і третьої групи і до 35 відсотків у останньої групи, які бачили емодзі з радою.

Під час другого експерименту 500 інших учасників також просили придумати пароль, але їх розбили на чотири групи з різними підказками про складність:

- проста оцінка складності з трьома класами;

- оцінка складності і часу, необхідного на повний перебір;
- оцінка складності і порівняння з паролями інших користувачів, наприклад, «Слабкий пароль, що входить в 400 найслабших»;
- оцінка складності та ймовірності збігу пароля з паролем іншого користувача.

Другий експеримент показав ще більшу різницю, якщо користувач отримує не просто величину складності, а більш наочний та очевидний приклад, такий як швидкість підбору пароля або порівняння з гіршими паролями. В цьому експерименті найефективнішою виявилася оцінка складності і порівняння з паролями інших користувачів, наприклад, «Слабкий пароль, що входить в 400 найслабших».

Судячи з цих досліджень,досить недооцінену роль у інформаційній безпеці, а саме у пароль носу захисті відіграє те, наскільки завчасно користувач буде попереджений про вразливість його паролів. Саме тому алгоритми аналізу паролів є дуже єфекьивними та вкрай необхідними для покращення попередження атак в майбутньому. Розроблений програмний модуль, дає змогу проаналізувати пароль користувача на є трапі цього створення, та попередити його про недостатню надійність, наряду із порівнянням паролів інших користувачів, або підрахунком часу необхідного на злам шляхом повного перебору.

Також, розроблений програмний модуль може застосовуватись як частина програмного забезпечення існуючої системи інформаційної безпеки організації. Його доцільно використовувати для перевірки рівня компетентності працівників організації у сфері інформаційної безпеки. Під час прийому нового працівника на роботу, при наданні новим працівникам доступу до автоматизованих систем та інформаційних ресурсів, при наданні працівникам власного робочого місця та апаратного забезпечення з можливістю парольної аутентифікації, слід проводити повний інструктаж та при необхідності навчання персоналу та їх перевірку за допомогою даного програмного модуля. Працівнику необхідно ввести у програму усю доступну про нього інформацію (інформацію до якої мають доступ

сторонні особи, таку як власне ім’я, імена близьких, назви улюблених брендів, спортивних команд, міст, та інші назви що можуть використовуватись як пароль, дати народження усіх близьких, значущі дати у житті працівника, номери телефонів, та інші числові комбінації. Після чого працівнику необхідно ввести пароль. Після того як уся необхідна інформація введена, програма обробляє усі введені дані, та видає коефіцієнт надійності пароля працівника. Якщо отриманий коефіцієнт занизький, програма повідомить працівника про необхідність змінити пароль, та надасть рекомендації як правильно сформувати надійний пароль. Аналогічний порядок перевірки рекомендовано проводити на регулярні основі, для перевірки стану надійності усіх аутентифікаційних даних працівників.

За статистикую Facebook, соціальна інженерія це другий найбільш поширений метод злому облікових записів «Facebook». Тому реалізація даного алгоритму у соцмережах може стати надзвичайно дієвим способом запобігання подібних атак.

3.4 Висновок до розділу

У процесі розробки програмного модуля аналізу паролів, було проаналізовано 100000 паролів, та виявлено найбільш вразливі комбінації персональних даних, паролі на базі яких мають найбільший коефіцієнт ненадійності. Можна зробити висновок, що даний програмний модуль та його модифікації можуть суттєво поліпшити надійність парольного захисту, та загалом зменшити імовірність проведення атак з використанням соціальної інженерії.

Якщо змінити звичний нам процес реєстрації у соцмережі, та надати користувачу можливість одразу створити та заповнити майбутню сторінку, а лише потім дати йому форму створення логіну та пароля, тоді запропонований алгоритм може зібрати попередньо введені персональні дані, необхідні

зловмиснику для підбору пароля, та імітуючи атаку, згенерувати словник із найбільш імовірних комбінацій, що є вразливими для подібних атак зі сторони зловмисників у майбутньому. Після порівняння усіх комбінацій із такого словника, із паролем, котрий користувач намагається створити, і у разі хоча б часткового співпадіння, такий пароль буде відхилений. Користувача буде сповіщено про те що його пароль вразливий до атак на основі соціальної інженерії, та запропоновано створити більш надійний пароль, що відповідатиме вимогам, і не буде мати співпадінь із результатами отриманими за допомогою алгоритму.

ВИСНОВКИ

У дипломній роботі була поставлена задача розробки програмного модуля аналізу ненадійних паролів з метою захисту від соціотехнічних атак.

В першому розділі було розглянуто поняття соціальної інженерії. Зокрема було розглянуто основні методи атаки на основі соціальної інденерії. Досліджено методи та заходи направлені на захист від подібних атак, для подальшого застосування при розробці програмного модуля, що дозволило визначити найбільш дієві з них. Актуальні засоби технічного захисту лише імітують реалізацію соціотехнічної атаки, але не створюють передумови для запобігання виникнення вразливостей.

В другому розділі було розглянуто основні види атак на пароль, проаналізовано їх ефективнсть, що допомогло в визначенні тіпу атак, котрий найбільше потребує покращення систем захисту. Також було розглянуто основні способи покращення захищености паролів, зокрема виділено основни критерії для створення надійних паролив.

Було підтверджено актуальність розробки нових програмних засобів захисту, що можуть використовуватись для попередження вразливостей пароля до соціотехнічних атак.

В третьому розділі було розроблено алгоритм аналізу паролів, з метою визначення найрозповсюдженіших правил побудови паролів. Алгоритм було модифіковано можливістю пошуку по регулярним виразам, що надало змогу уточнювати необхідні параметри для пошуку відповідностей. На базі описаного алгоритму, побудовано програмний модуль оцінки ненадійних паролів з метою захисту від соціотехнічних атак мовою програмування Rust.

Досліджено програмний модуль, що дозволило підтвердити його коректність роботи.

Отже, було реалізовано основні завдання дипломної роботи і проілюстровано можливість інтеграції розробленого програмного модуля.

Результати дипломної роботи можуть бути використані для подальшої модифікації розробленого алгоритму з метою збільшення його ефективності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК – Пресс», 2006. – 320с.

2. Ананьин Е. В., Кожевникова И. С., Лысенко А. В., Никишова А. В., Мартынова Л. Е., Назарова К. Е., Попков С. М., Белозёрова А. А. Основные виды атак социальной инженерии // Молодой ученый. — 2017. — №1. — С.

3. “Социальная инженерия и защита от неё в корпоративной среде.” [Електронний ресурс]: http://nauka-rastudent.ru/34/3683/

4. “Возможности защиты от социальной инженерии.” [Електронний ресурс]: https://bugtraq.ru/library/books/attack/chapter02/05.html

5. “Атаки на пароль.” [Електронний ресурс]: https://studopedia.su/16_4323_ataki-na-parol.html

6. Бабак В. П., Корченко О. Г. Інформаційна безпека та сучасні мережеві технології. Англ.-укр.-рос. слов. термінів. - К.: НАУ, 2003. - 670 с.

7. Корченко А. Г. Несанкционированный доступ к компьютерным системам и методы защиты: Учеб. пособие. – К.: КМУГА, 1998. – 116.

8. Robert B. Cialdini. The Science of Persuasion // Scientific American Magazine. – 2001, – №2. – P.76-81Robert B. Cialdini. The Science of Persuasion // Scientific American Magazine. – 2001, – №2. – P.76-81.

9. И. Н. Кузнецов Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе. - М.: ООО Изд. Яуза, 2001.

10. “Парольная защита.” [Електронний ресурс]: https://life-prog.ru/1_2842_sposobi-ataki-na-parol-obespechenie-bezopasnosti-parolya.html

11. “Социальная реальность: SET — лучший набор гениального хакера.” [Електронний ресурс]: https://xakep.ru/2011/01/18/54557/

12. “Как социальная инженерия открывает хакеру двери в вашу

организацию.”

[Електронний ресурс]: https://www.ptsecurity.com/ru-ru/research/analytics/social-engineering/

13. “Социальная инженерия: неуловимый враг в мире кибербезопасности.” [Електронний ресурс]: https://habr.com/ru/company/wirex/blog/423285/

14. “Атаки на информацию с помощью методов социальной инженерии.” [Електронний ресурс]: http://www.jetinfo.ru/jetinfo_arhiv/konsalting-v-ib-kaznit-nelzya-pomilovat/chelovek-cheloveku/2015

15. “Защита пользователей от социальной инженерии.”

[Електронний ресурс]: https://sites.google.com/site/abcsocialnaainzeneria/home/ tehniki-socialnoj-inzenerii/mery-protivodejstvia

16. “Парольная защита.”

[Електронний ресурс]: http://mf.grsu.by/UchProc/livak/b_protect/zd_3.htm

17. “Простой и надежный пароль – коллективное творчество” [Електронний ресурс]: https://habr.com/ru/post/118499/

18. “Недостатки парольной аутентификации.”

[Електронний ресурс]: http://www.azone-it.ru/polzovateli-hotyat-otkazatsya-ot-paroley

19. “Недостатки и достоинства методов аутентификации: пароли.” [Електронний ресурс]: http://www.sws.ru/nedostatki-i-dostoinstva-metodov-autentifikatsii-paroli.html

20. “Защита информации с помощью пароля.”

[Електронний ресурс]: https://studopedia.su/16_4323_ataki-na-parol.html

21. “Способы атаки на пароль. Обеспечение безопасности пароля..” [Електронний ресурс]: https://life-prog.ru/1_2842_sposobi-ataki-na-parol-obespechenie-bezopasnosti-parolya.html

22. “Использование утечек паролей для ускорения атак.” [Електронний ресурс]: https://blog.elcomsoft.com/ru/2017/02/ispolzovanie-utechek-paroley-dlya-uskoreniya-atak/

23. “Как защитить пароль от взлома.”

[Електронний ресурс]: https://hidemyna.me/ru/articles/kak-zawitit-parol-ot-vzloma/

24. “Атака по Расширенной Маске, когда известны структура и символы пароля.”

[Електронний ресурс]:https://passcovery.ru/helpdesk/knowledgebase.

25. “Социальная инженерия: сущность и парадигмальная методология.” [Електронний ресурс]: http://www.dslib.net/soc-filosofia/socialnaja-inzhenerija-suwnost-i-paradigmalnaja-metodologija.html

26. “К вопросу о социальной инженерии.”

[Електронний ресурс]: https://cyberleninka.ru/article/n/k-voprosu-o-sotsialnoy-inzhenerii

27. “Социальная инженерия – технология «взлома» человека.” [Електронний ресурс]: https://medium.com/@Emisare/socialnaya-ingeneria-9f16e0ba7fa5

28. “Рассказывать ли сотрудникам о социальной инженерии?.” [Електронний ресурс]: https://habr.com/ru/post/357412/

29. “Социальные хакеры: 4 причины, почему они легко взломают вашу систему.”

[Електронний ресурс]: https://kontur.ru/articles/2739

30. “Про подбор паролей.”

[Електронний ресурс]: https://pikabu.ru/story/pro_podbor_paroley_1424251