Міністерство освіти і науки України

Харківський національний університет імені В.Н.Каразіна

Факультет комп’ютерних наук

Кафедра безпеки інформаційних систем і технологій

Курсова робота

З дисципліни: «Захист інформації в інформаційно-комунікаційних системах»

На тему: «Дослідження алгоритмів забезпечення аутентифікації та конфіденційності передачі даних в локальних мережах масштабу офісу»

Виконав:

студент гр. КБ-41

Кравченко Є. М.

Перевірив:

Доцент

Сватовський І.І.

Харків – 2021 р.

**ЗМІСТ**

[**ВСТУП** 3](#_Toc69698925)

[**ВИСНОВКИ** 4](#_Toc69698926)

[**ПЕРЕЛЬК ДЖЕРЕЛ ПОСИЛАНЬ** 5](#_Toc69698927)

# **ВСТУП**

Овіоирм

# **ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА УПРАВЛІННЯ ДОСТУПОМ**

Аутентифікація стосовно до обчислювальних системи – це доказ достовірності різних елементів цієї системи при їх взаємодії. Користувач при вході в систему повинен пред’явити системі докази, що він саме той користувач, ідентифікатор якого він вводить.

Таким доказом може бути пароль. Документ, отриманий користувачем по електронній пошті, повинен супроводжуватися додатковою інформацією, переконливою користувача, що документ не був змінений при передачі і що автором цього документа є саме та людина, від імені якого цей лист було надіслано. Тут доказом може служити електронний підпис. Пристрої, які взаємодіють з мережею, повинні довести один одному, що жодне з них не підмінено зловмисником з метою відгалуження або прослуховування трафіку. Для цього в протоколі взаємодії цих пристроїв повинна бути передбачена процедура взаємної аутентифікації. Взаємна аутентифікація потрібна і для організації безпечного сеансу користувача і сервера. Аутентифікація може проводитися по відношенню не тільки до окремого користувачева, але і до групи користувачів. Методи аутентифікації розрізняються залежно від того, що служить аутентифікатором, а також від того, яким чином організований обмін аутентифікаційних даними між аутентіфікатором і аутентифікуючим елементами системи.

Абсолютно надійна аутентифікація людини являє собою теоретично неможливе завдання. Немає такого аутентифікатора, який зі стовідсотковою надійністю доводив би автентичність людини. Пароль можна перехопити, електронний ключ вкрасти, відбиток пальця підробити, райдужну оболочку ока підмінити якісним зображенням. Більш того, не існує наукового доказу неможливості збігу у різних людей відбитків пальців або райдужних оболочок ока. навіть збіг результатів аналізу ДНК при сучасному рівні розвитку техніки не може служити абсолютним доказом автентичності людини.

Однак на практиці при аутентифікації користувачів в обчислювальних системах обмежуються деяким не стовідсотковим, хоча і досить високим рівнем достовірності доказу автентичності людини. Аутентифікатори, які використовуються при цьому, поділяють на три класи:

* «щось, що знаю» ­ до цього типу належать багаторазові й одноразові паролі, правила перетворення інформації;
* «щось, що маю» ­ різні мініатюрні пристрої, які називаються апаратними аутентифікаторами/ключами;
* «щось, чим є» – різні біометричні показники того кого аутентифікують.

Клас аутентифікаторів називають фактором. Якщо в процедурі аутентифікації передбачається пред’явлення декількох аутентифікаторів, що відносяться до різних класів, то таку аутентифікацію називають багатофакторною. Найбільше поширення в сьогодні отримала двухфакторна аутентифікація, при якій користувач пред’являє багаторазовий пароль ( «щось, що знаю») і апаратний ключ ( «щось, що маю»). Слід зауважити, що в деяких випадках термін «Багатофакторна аутентифікація» служить для позначення процедур багатоступеневої аутентифікації, побудованих на використанні декількох аутентифікаторів, що відносяться до одного і того ж класу. Прикладом такої процедури є аутентифікація власника банківського рахунку при його дзвінку в банк: спочатку його просять назвати кілька букв з його пароля, а потім задають кілька запитань із заздалегідь узгоджених і зафіксованих в базі даних організації відповідями, наприклад про пам’ятне для клієнта географічне місце, дівоче прізвище матері і т. п.

Пароль – це послідовність символів що зберігається в секреті, обрана користувачем, або згенерувана програмним або апаратним засобом, або ж призначена адміністратором. Паролі відносяться до аутентифікаторів класу «щось, що знаю». Паролі бувають одноразовими і багаторазовими. Багаторазові паролі, як видно з їх назви, можуть використовуватися як доказ автентичності багаторазово. У процедурах аутентифікації, заснованих на одноразових паролях, той кого аутентифікують повинен кожен раз пред’являти нове значення пароля. Зазвичай для генерації одноразових паролів застосовуються спеціальні програми або апаратні пристрої.

Механізми аутентифікації на основі багаторазових паролів, володіючи простотою і логічною ясністю, традиційно є найпопулярнішим засобом аутентифікації. Однак їм властиві відомі слабкості. Це, по-перше, можливість розкриття і розгадування паролів, по-друге, можливість «підслуховування» пароля при його передачі по мережі шляхом аналізу мережевого трафіку. По-третє, власники паролів можуть стати жертвами соціального інжинірингу.

Для зниження рівня загрози розкриття паролів адміністратори мережі, як правило, застосовують вбудовані програмні засоби, що служать для формування політики призначення і використання паролів: задання максимального і мінімального термінів дії пароля, зберігання списку вже використаних паролів, управління поведінкою системи після кількох невдалих спроб логічного входу і т. п.

Багато користувачів нехтують загрозами, які несуть в собі легко вгадуються паролі. Так, черв’як Mumu, який вразив комп’ютерні мережі в 2003 році, шукав свої жертви, підбираючи паролі з дуже короткого списку: password, passwd, admin, pass, 123,1234,12345, 123456 і порожній рядок. Така напрочуд примітивна стратегія дала прекрасні (з точки зору атакуючої сторони) результати – безліч комп’ютерів було зламано.

У списку найбільш популярних паролів, що застосовуються користувачами Інтернету при доступі до веб-серверів, опублікованому в серпні 2013 року компанією Google, місця в першій десятці займають імена і дати народження членів сім’ї і близьких друзів, назви місць народження, дати весілля, клички домашніх тварин, що-небудь, пов'язане з улюбленою футбольною командою, і слово «password». Як видно з наведеного списку, для зацікавленої людини не складе великих труднощів підібрати ці паролі.

Але навіть при виборі менш передбачуваного пароля користувач все ж ризикуєте, що він буде розгаданий простим перебором всіх можливих символів, такий метод називають брутфорс-атакою. Час підбору напряму залежить від різноманітності набору символів, з якого формується пароль, і довжини пароля. Після проведення експерименту визначено, що час підбору пароля сильно зростає при збільшенні його довжини всього лише на два знаки. Так, при використанні тільки букв латинського алфавіту (малих і великих) час підбору пароля з 8 знаків в 3000 разів більше, ніж з 6 знаків.

Серйозною проблемою використання багаторазових паролів є їх ручна синхронізація. У звичайному житті нам потрібно не один, а кілька паролів: для входу в комп’ютерну мережу підприємства, в якому ми працюємо, отримати доступ до «особистого кабінету» провайдера мобільного зв’язку, для доступу до банківського рахунку і ще для доступу до інтернет-сайтів. Часто трапляється, що у всіх цих випадках застосовується один і той же пароль (можливо, з невеликими варіаціями), тому що у нас немає часу придумувати і, головне, запам’ятовувати новий пароль для доступу до нового ресурсу. Таке явище називають ручною синхронізацією паролів. Виконавши реєстрацію на підозрілому сайті, користувач повідомляєте свій пароль його власникам, який тепер може бути використаний для доступу до інших облікових даних, які можуть мати критичне значення.

Слабкістю паролів є також процедура реакції на неправильно введений пароль. На перший погляд очевидним прийомом, спрямованим на протидію підбору паролів, здається блокування облікового запису, з якого було проведено кілька (зазвичай три) невдалих спроби входу. Однак в деяких ситуаціях такий підхід дає зловмиснику прекрасну можливість швидко заблокувати роботу підприємства. Дійсно, ідентифікатори користувачів є менш захищеною інформацією, ніж паролі, до того ж вони часто легко вгадуються (ADMIN, STUDENT, IVANOV, Natasha і т.д.) І їх легше підглянути, так як вони виводяться на екран. Тому зловмисник може легко підібрати імена, виконати по три невдалих спроби аутентифікації для кожного облікового запису, викликати їх блокування і привести таким чином систему в заблокований стан. Зняття блокування з облікових записів може стати серйозною проблемою, якщо таких записів дуже багато.

Поряд з паролями існує інший варіант використання аутентифікатора з класу «щось, що знаю». Адміністратор заздалегідь безпечним чином повідомляє користувачеві деяке правило, наприклад правило перетворення послідовності чисел в інші символи. Під час процедури аутентифікації система виводить на екран випадкову послідовність чисел. Користувач відповідно до відомим тільки йому і системі правилом перетворює їх в іншу послідовність символів, яку вводить в якості пароля. Оскільки система також «знає» правило перетворення, вона може перевірити правильність введеного пароля. Тобто спочатку в даному випадку секретом що розділяється виступає правило перетворення.

**Сувора аутентифікація в комп’ютерній мережі на основі багаторазових паролів**

Як правило, аутентифікація користувачів в комп’ютерних мережах будується на основі централізованої схеми. На одному з серверів мережі підтримується база даних, в якій зберігаються облікові дані про всіх користувачів мережі. Облікові дані зберігаються поряд з іншою інформацією про ідентифікатори та паролі користувачів. Коли користувач здійснює логічний вхід в мережу, він набирає на клавіатурі свого комп’ютера свої ідентифікатор і пароль. За ідентифікатором користувача в централізованій базі даних, що зберігається на сервері, знаходиться відповідний запис, з неї витягується пароль і порівнюється з тим, який ввів користувач. Якщо вони збігаються, то аутентифікація вважається успішною, користувач отримує легальний статус і права, які визначені для нього системою авторизації.

Однак така спрощена схема має великий недолік: а саме - при передачі пароля з клієнтського комп’ютера на сервер, що виконує процедуру аутентифікації, цей пароль може бути перехоплений зловмисником. Тому в різних системах аутентифікації застосовуються різні прийоми, щоб уникнути передачі пароля по мережі в незахищеному вигляді.

Аутентифікація, в процесі якої використовуються методи шифрування, а аутентифікатор не передається по мережі, називається суворою аутентифікацією. Розглянемо приклад суворої аутентифікації користувачів, що реалізується засобами ОС. Нехай аутентифікація користувачів мережі виконується на основі їх паролів, що зберігаються в зашифрованому вигляді в централізованій базі SAM (Security Accounts Manager). Паролі зашифровуються за допомогою односторонньої функції шифрування при занесенні їх в базу даних під час процедури створення облікового запису для нового користувача. Введемо позначення для цієї односторонньої функції – ОФШ. Таким чином, пароль Р зберігається в базі даних SAM у вигляді дайджесту d(P). (Знання дайджесту не дозволяє відновити початковий текст).

При логічному вході користувач локально вводить в свій комп’ютер ім’я-ідентифікатор (ID) і пароль Р. Клієнтська частина підсистеми аутентифікації, отримавши ці дані, передає запит по мережі на сервер, який зберігає базу SAM. У цьому запиті у відкритому вигляді міститься ідентифікатор користувача, але пароль в мережу ні в якому вигляді не передається. До паролю на клієнтській стороні застосовується та ж одностороння функція ОФШ1, яка була використана під час запису пароля в базу даних SAM, тобто динамічно обчислюється дайджест пароля d(P).

У відповідь на запит, що надійшов від клієнта, серверна частина служби аутентифікації генерує випадкове число S випадкової довжини, так зване слово-виклик (challenge). Це слово передається по мережі з сервера на клієнтську машину користувача. До слова-виклика на клієнтській стороні застосовується одностороння функція шифрування ОФШ2. На відміну від функції ОФШ1, функція ОФШ 2 є параметричною та отримує в якості параметра дайджест пароля d (P). Отримана в результаті відповідь d(S) передається по мережі на сервер бази SAM.

Одночасно при цьому на сервері слово-виклик S аналогічно шифрується за допомогою тієї ж односторонньої функції ОФШ2 і дайджесту пароля користувача d(P), витягнутого з бази SAM, а потім порівнюється з відповіддю, переданою клієнтською стороною. При співпадінні результатів вважається, що аутентифікація пройшла успішно. Таким чином, аутентифікація проходить без передачі пароля по каналах зв’язку. Зауважимо, що при кожному запиті на аутентифікацію генерується нове слово-виклик, так що перехоплення відповіді d(S) клієнтського комп’ютера не може бути використана в ході іншої процедури аутентифікації.

**Сувора аутентифікація в протоколі CHAP**

Іншим прикладом суворої аутентифікації може служити аутентифікація по квитуванню виклику (Challenge Handshake Authentication Protocol, CHAP), що застосовується в протоколі РРР Протокол РРР передбачає два режими аутентифікації: аутентифікація по протоколу РАР, коли пароль передається по лінії зв’язку у відкритому вигляді, і аутентифікація по протоколу CHAP, при якій пароль по лінії зв’язку не передається, отже, забезпечується більш високий рівень безпеки.

Розглянемо застосування протоколу CHAP при аутентифікації віддалених користувачів, підключених до Інтернету по комутованого каналу. Тут аутентифікуючою стороною є сервер провайдера, а стороною що аутентифікується – клієнтський комп’ютер. При укладанні договору клієнт отримує від провайдера пароль (нехай, наприклад, це буде слово «parol»). Він зберігається в базі даних провайдера у вигляді дайджесту Z = d (parol), отриманого шляхом застосування до паролю односторонньої хеш-функції MD5.

У протоколі CHAP передбачено чотири типи повідомлень: Success (успіх), Challenge (Виклик), Response (відповідь), Failure (помилка).

Аутентифікація виконується в наступній послідовності:

1. Користувач-клієнт активізує певну програму віддаленого доступу до сервера провайдера, вводячи призначені йому ім’я і пароль. Ім’я передається по мережі провайдеру в складі запиту на з’єднання, але пароль не передається в мережу ні в якому вигляді.

2. Сервер провайдера, отримавши запит від клієнта, генерує псевдовипадкове слово виклик (нехай це буде слово «challenge») і передає його клієнту разом зі значенням, ідентифікуючим повідомлення в рамках даного сеансу (ID), і власним ім’ям. Це повідомлення типу Challenge. Для захисту від перехоплення відповіді аутентифікатор повинен використовувати різні значення слова-виклику при кожній процедурі аутентифікації.

3. Програма клієнта, отримавши цей пакет, витягує з нього слово-виклик, додає до нього ідентифікатор і обчислений локально дайджест Z = d(parol), а потім обчислює за допомогою все тієї ж функції MD5 дайджест Y = d {(ІD, challenge, d(раго1)} від всіх цих трьох значень. Результат клієнт посилає серверу провайдера в пакеті Response.

4. Сервер провайдера порівнює отриманий по мережі дайджест Y з тим значенням, яке він отримав, локально застосувавши ту ж хеш-функцію до набору аналогічних компонентів, що зберігаються в його пам’яті.

5. Якщо результати збігаються, то аутентифікація вважається успішною і аутентифікатор посилає партнеру пакет Success.

Спосіб аутентифікації, при якому багаторазові паролі користувачів зберігаються в базі даних сервера у вигляді дайджестів, здається цілком безпечним, адже навіть якщо зловмисник зможе отримати до них доступ, він навіть теоретично не зможе відновити вихідне значення паролів по дайджесту. Однак творець першого хробака Роберт Морріс вирішив цю проблему. Він розробив досить просту програму, яка генерувала можливі варіанти паролів, використовуючи слова зі словника і послідовним перебором символів. Для кожного згенерованого слова обчислювався дайджест і порівнювався з дайджестами з файлу паролів. Така стратегія виявилася дуже ефективною, і хакеру вдалося заволодіти кількома паролями.

# **ВИСНОВКИ**

В курсовій роботі було розглянуто

# **ПЕРЕЛЬК ДЖЕРЕЛ ПОСИЛАНЬ**

1. Архамович В. М. Комп'ютерні мережі / В. М. Архамович. – Київ, 2010. – 246 с.