УДК 004

В.Плужник, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО МЕРЕЖЕВИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті розроблено програмне забезпечення, яке призначено для системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Метою розробки є дослідження та принципи побудови системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Об'єктом дослідження є процес управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Предметом дослідження є методи управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Методи дослідження базуються на методах захисту інформації, методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

управління ідентифікацією та доступом, мережеві інформаційні ресурси

Постановка проблеми. Інструменти мережевої безпеки спрямовані на запобігання несанкціонованому доступу до даних, крадіжці особистих даних та кіберзагрозам до пристроїв, технологій та процесів.

Мережева безпека запобігає несанкціонованому доступу до інформації або зловживанню мережею організації. Вона включає апаратні та програмні технології, розроблені для захисту безпеки та надійності мережі та даних.

Інструменти мережевої безпеки є важливими для захисту мережі вашої організації та запобігання кільком загрозам, які можуть пошкодити систему та мережу. Вони допомагають контролювати мережу та запобігати витокам даних.

Інструмент мережевої безпеки може аналізувати весь трафік у мережі. Моніторинг трафіку допомагає організації проактивно виявляти проблеми та загрози, перш ніж вони завдадуть їй значної шкоди. Інструменти мережевої безпеки надсилають сповіщення в режимі реального часу про будь-яку незвичайну поведінку, щоб запобігти будь-яким порушенням.

Деякі переваги інструментів мережевої безпеки:

– Інструменти мережевої безпеки мінімізують бізнес- та фінансовий вплив будь-якого порушення, оскільки вони допомагають вам дотримуватися правил та запобігати порушенням.

– Мережева безпека допомагає вашому бізнесу дотримуватися вимог і забезпечує кілька рівнів безпеки, щоб розширити масштаби вашого бізнесу та запропонувати краще робоче місце для ваших співробітників.

– Це забезпечує захист будь-якої конфіденційної інформації та даних, що передаються по мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

– Дослідження системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

– Програмна реалізація системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Об'єктом дослідження є процес управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Предметом дослідження є методи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Методи дослідження базуються на методах захисту інформації, методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Автентифікація – це процес перевірки особи користувача або системи. Повернімося до нашого прикладу зі спортзалом. Адміністратор у спортзалі приймає лише передплатників. Як це досягається в аналоговому світі? Вони можуть попросити вас надати вашу картку члена спортзалу (якщо припустити, що спортзал надає її кожному передплатнику). У вас повинна бути картка члена спортзалу з вашою фотографією та відповідними даними про передплату. Адміністратор може підтвердити вашу особу, перевіривши вашу картку; проблема автентифікації вирішена (якщо хтось не знайде спосіб підробити картку, але це вже інша проблема).

Автентифікація та ідентифікація є основними компонентами будь-якої інформаційної системи та мережі. Важливо розуміти різницю між автентифікацією та ідентифікацією.

Під час ідентифікації користувач (або система чи процес) заявляє про певну (унікальну) особу у відповідних налаштуваннях. Автентифікація – це підтвердження особи користувача (або системи чи процесу). Цей процес зазвичай здійснюється одним із таких способів:

– Щось тобі відомо.

– Щось у тебе є.

– Щось, що ти є.

Використовуються ще два методи, хоча й у меншій мірі:

– Десь ви знаходитесь (логічне/фізичне місцезнаходження).

– Щось, що ви робите (поведінка).

Опишемо кожен із трьох основних механізмів автентифікації.

Щось, що ти знаєш

«Щось, що ви знаєте», стосується чогось, що ви знаєте або запам'ятали. Приклади включають наступне:

– Паролі, такі як 4SNoPawKkdFiCdnmi%WAdWi-;4,mxRMQB.

– Парольні фрази, такі як «Judge Battle Advise Pain 9» та «Baggage Protection Dissatisfy Barrel 8».

– PIN-код (персональний ідентифікаційний номер), такий як 25063та6285.

Більшість мобільних телефонів автоматично блокуються протягом кількох хвилин бездіяльності. Залежно від початкової конфігурації, користувач може розблокувати їх, ввівши правильний PIN-код, пароль або графічний ключ. Хоча графічний ключ і намальований, він нічим не відрізняється від PIN-коду, тобто чогось, що запам'ятовується.

Розглянемо випадок, коли ви входите в TryHackMe. Ви повинні ідентифікувати себе за допомогою імені користувача або електронної пошти та автентифікувати свою особу за допомогою пароля. (Якщо ви входите в TryHackMe через Google, ви надаєте свої облікові

дані для входу Google, і Google підтвердить вашу особу TryHackMe.) Ім'я користувача та електронна пошта є унікальними для вас; отже, ідентифікація може бути здійснена без жодної двозначності. Вважається, що пароль відомий лише вам, що доводить, що ви є власником облікового запису.

Щось у тебе є

«Щось, що у вас є» стосується об’єкта, зазвичай фізичного, який у вас є. Це може бути як телефон, так і ключ безпеки.

Наприклад, коли ви хочете зареєструватися в деяких додатках для обміну миттєвими повідомленнями, вас просять надати номер телефону, зазвичай номер мобільного телефону. Цей номер телефону є вашою ідентифікатором у цьому додатку. Як ви можете довести, що це справді ваш номер телефону? Один із способів – надіслати вам код через SMS або зателефонувати вам на цей номер і повідомити код. Прочитання SMS протягом кількох хвилин або отримання дзвінка на цей номер доведе, що у вас є цей номер телефону. У випадку номера мобільного телефону, цього буде достатньо, щоб підтвердити, що у вас є SIM-картка (або eSIM).

Апаратний ключ безпеки достатньо малий, щоб його можна було носити на зв'язці ключів або в гаманці. Ви можете використовувати ключ безпеки для автентифікації, підключивши його до порту USB або USB C або піднісши його до зчитувача NFC (Near-Field Communication). Прикладами апаратних ключів безпеки є, наприклад, Yubico, Titan Security Key, Nitrokey та Thetis.

Щось, що ти є

«Щось, чим ви є», стосується біометричних зчитувачів. Прикладами є зчитувачі відбитків пальців, сканери розпізнавання обличчя, сканери сітківки ока та розпізнавання голосу.

Ви, найімовірніше, стикалися з автентифікацією за допомогою зчитувача відбитків пальців під час спроби розблокувати телефон. Багато сучасних мобільних телефонів дозволяють користувачеві автентифікуватися за допомогою відбитка пальця, зберігаючи пароль/PIN-код/графічний ключ як резервний варіант на випадок, якщо автентифікація за відбитком пальця не вдасться.

Розпізнавання облич також стає популярним у сучасних смартфонах. З роками біометричні зчитувачі та сканери стають не тільки надійнішими, але й доступнішими. Ця технологія вигідна як компаніям, які вимагають високого рівня безпеки, так і споживачам.

Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація (MFA) означає використання двох або більше з перерахованих вище механізмів (щось, що ви знаєте/маєте/є). Мета полягає в тому, щоб забезпечити додатковий захист у разі порушення одного з механізмів автентифікації.

Якщо ви хочете скористатися банкоматом банку, вставте свою кредитну/дебетову картку та введіть свій PIN-код. Ця процедура є одним із найперших прикладів двофакторної автентифікації (2FA). Очевидна корисність полягає в тому, що зловмиснику недостатньо просто отримати вашу картку, оскільки йому також потрібно знати ваш PIN-код.

Багато домашніх сейфів, доступних сьогодні, використовують 2FA, не обов'язково рекламуючи це. Вони вимагають від власника вставити ключ і ввести правильний PIN-код, щоб сейф відкрився. Вам потрібно знати PIN-код і мати ключ, щоб його відкрити. Отже, якщо комусь іншому вдасться отримати ключ від сейфа, він все одно не зможе відкрити сейф, не знаючи PIN-коду.

У другому випадку двофакторна автентифікація (2FA) вимагає двох механізмів автентифікації та підпадає під більш загальну багатофакторну автентифікацію (MFA), яка вимагає двох або більше факторів автентифікації. Ця вимога може значно покращити безпеку та захистити від різних атак, таких як ті, що використовують слабкі паролі.

Після автентифікації користувачеві має бути надано належний рівень доступу. Авторизація визначає, до чого має бути дозволено автентифікованому користувачеві отримувати доступ та що робити. Повертаючись до нашого прикладу зі спортзалом, ми

очікуємо, що платний учасник спортзалу матиме право доступу до будь-якого тренувального обладнання протягом встановленого робочого часу. Абонент не може позичати та брати бігову доріжку додому протягом місяця. Спортзал – це не бібліотека! Механізми контролю доступу забезпечать належне виконання авторизації. Якщо в спортзалі є належний механізм контролю доступу, хтось помітить, як ви намагаєтеся перенести та винести бігову доріжку.

Розглянемо ще один нетехнічний приклад: Віка забронювала номер у готелі на один тиждень. Завдяки цьому бронюванню Віка повинна мати право доступу до свого готельного номера, серед інших громадських приміщень, протягом усього перебування. Хоча їй дозволено доступ до призначеного їй номера, їй не дозволено, наприклад, доступ до інших номерів. Як це можна забезпечити? Знову ж таки, авторизація забезпечується механізмами контролю доступу.

У прикладі з готелем Віці надають ключ, який надає їй доступ до призначеного їй номера. Відповідно, контроль доступу здійснюється за допомогою замків та ключів. Більш вишуканий готель може використовувати смарт-картки та електронні зчитувачі карток для відмикання дверей номера. У будь-якому випадку існує механізм, який би забезпечив авторизацію.

Розглянемо технічний приклад. Як частина команди з продажу, Ігор повинен мати доступ до всіх файлів, пов'язаних із продажами, які необхідні для ефективного та результативного виконання його роботи. Наприклад, команді з продажу не потрібно мати доступ до документів, що стосуються, наприклад, управління персоналом та бухгалтерського обліку. У цьому випадку контроль доступу можна забезпечити, встановивши відповідні дозволи доступу до файлів та бази знань компанії.

Коротко кажучи, авторизація визначає, до чого користувач повинен мати доступ, тоді як контроль доступу забезпечує дотримання встановленої політики. Наприклад, після входу до свого облікового запису електронної пошти ви повинні мати можливість читати свої електронні листи та надсилати нові. Однак за замовчуванням ви не повинні мати доступу до поштової скриньки жодного зі своїх колег. Поштовий сервер має бути розроблений таким чином, щоб дозволяти користувачеві доступ до своєї поштової скриньки та забороняти йому доступ до поштових скриньок інших користувачів.

Авторизація проти контролю доступу

– Авторизація – етап прийняття рішення – визначає, який доступ слід надавати кому, на основі ролей або політик.

Вирішення, що секретар може надсилати електронні листи від імені менеджера.

– Контроль доступу – механізм забезпечення дотримання правил – реалізує правила, визначені на етапі авторизації.

Запобігання зміненню документа користувачами шляхом забезпечення доступу лише для читання.

Підзвітність та ведення журналу

Підзвітність гарантує, що користувачі несуть відповідальність за дії, які вони виконують у системі. Іншими словами, після автентифікації своєї особи та отримання дозволу на доступ до системи вони можуть нести відповідальність за свої дії. Підзвітність можлива, якщо у нас є можливості аудиту, які зазвичай вимагають належного функціонування журналювання.

Почнемо з нетехнічного прикладу: спортзал. У вас є абонемент у спортзал, і ви відвідуєте його тричі на тиждень. Тепер, коли ви стали його постійним клієнтом, адміністратор впізнає вас і не просить пред'являти вашу картку члена. Це ніби ви завжди «залогінені» в спортзалі! Ви помічаєте, що всі, хто має «доступ» до спортзалу, дотримуються певних правил. Наприклад, ніхто не розбиває настінне дзеркало, якщо незадоволений швидкістю свого прогресу. Якщо вони це зроблять, їхнє членство буде анульовано, і вони сплатять усі збитки. Іншими словами, кожен несе *відповідальність* за свої дії. Ця модель забезпечує зручність для всіх для безпечних тренувань.

Розглянемо більш технічний приклад, наприклад, касира банку. Такий працівник може переглядати та проводити різні операції на рахунку клієнта. Як ми можемо гарантувати, що недобросовісний працівник не зловживатиме такими повноваженнями? Нам потрібно безпечно реєструвати всі транзакції та відповідні деталі. Ми повинні мати можливість перевіряти всі проведені транзакції та перевіряти, хто що зробив. Без такої можливості ми не можемо ні покладатися на таку систему, ні довіряти їй.

Ведення журналу

Критичним аспектом підзвітності є ведення журналу. Ведення журналу – це процес запису подій, що відбуваються в системі. Цей процес включає дії користувачів, системні події та помилки. Реєструючи дії користувачів, організація може вести облік того, хто і коли отримував доступ до якої інформації. Цей запис життєво важливий для дотримання нормативних вимог, реагування на інциденти та судово-медичних розслідувань.

Завдяки комплексній системі реєстрації, організація може відстежувати дії будь-якого користувача, виявляти будь-які аномалії або несанкціонований доступ і вживати відповідних заходів. Наприклад, якщо неавторизований користувач намагається отримати доступ до конфіденційних даних, система реєстрації може генерувати сповіщення для сповіщення персоналу служби безпеки.

Ведення журналів також може допомогти організаціям виявляти інциденти безпеки та реагувати на них. Аналізуючи дані журналів, команди безпеки можуть виявляти закономірності підозрілої активності, такі як повторні невдалі спроби входу або незвичайні моделі доступу. Цю інформацію потім можна використовувати для розслідування потенційних загроз безпеці та реагування на них.

Оскільки підзвітність є ключовим компонентом будь-якої безпечної інфраструктури, слід належним чином подбати про те, щоб ведення журналу відбувалося належним чином та безпечно. Крім того, залежно від вимог безпеки, журнали повинні бути захищеними від несанкціонованого доступу. Причина полягає в тому, що ви не хочете, щоб зловмисник видаляв або змінював журнали та приховував свої дії в мережі. Ось чому гарною практикою є налаштування окремого сервера журналювання з одним завданням: безпечне отримання та зберігання журналів. Звідси й переадресація журналів.

Пересилання журналів – це процес надсилання даних журналів з однієї системи до іншої. Цей процес часто об’єднує дані журналів з кількох джерел у централізоване місце для кращого аналізу та керування. Пересилання журналів також може використовуватися для надсилання даних журналів до хмарного сервісу для зберігання та аналізу.

Пересилання журналів має кілька переваг. Централізуючи дані журналів, організації можуть легше аналізувати та співвідносити події журналів з різних систем для виявлення потенційних загроз безпеці. Це підводить нас до управління інформацією та подіями безпеки (SIEM).

Ведення журналу та SIEM

Управління інформацією та подіями безпеки (SIEM) – це технологія, яка об’єднує дані журналів з кількох джерел та аналізує їх на наявність ознак загроз безпеці. Рішення SIEM можуть допомогти організаціям виявляти аномалії, потенційні інциденти безпеки та надавати сповіщення командам безпеки.

Інтегруючи логування та SIEM, організації можуть краще розуміти активність своїх систем та мереж, а також контролювати потенційні загрози. Ця інтеграція дозволяє організаціям ефективніше виявляти загрози безпеці та реагувати на них.

Крім того, інтеграція ведення журналу та SIEM забезпечує додаткові переваги, такі як звітність про відповідність вимогам та судово-медичні розслідування. Звітність про відповідність вимогам є важливою частиною системи безпеки будь-якої організації, а ведення журналу допомагає організаціям виконувати вимоги до звітності, збираючи дані, необхідні для аудитів. Судово-медичні розслідування мають вирішальне значення для визначення джерела та причини інциденту безпеки. Рішення для ведення журналу та SIEM

дозволяють організаціям проводити судово-медичні розслідування, надаючи детальну історію активності системи та мережі.

Управління ідентифікацією

Керування ідентифікацією (IdM) включає всі необхідні політики та технології для ідентифікації, автентифікації та авторизації. IdM має на меті забезпечити, щоб уповноважені особи мали доступ до активів та ресурсів, необхідних для їхньої роботи, тоді як неавторизованим особам доступ заборонено. IdM вимагає, щоб кожному користувачеві або пристрою було призначено цифрову ідентифікацію.

IdM допомагає організаціям захищати конфіденційні дані та підтримувати дотримання нормативних вимог. Це також дозволяє організаціям оптимізувати процеси доступу користувачів, зменшувати витрати, пов'язані з управлінням ідентифікацією, та покращувати взаємодію з користувачами. Впроваджуючи ефективну стратегію IdM, організації можуть гарантувати, що їхні користувачі автентифіковані та авторизовані для безпечного доступу до необхідних їм ресурсів.

Деякі джерела використовують IdM та керування ідентифікацією та доступом (IAM) як взаємозамінні. Інші джерела вважають, що IdM більше зосереджений на питаннях безпеки, пов'язаних з ідентифікацією користувача, таких як автентифікація та дозволи. Вони стверджують, що IdM займається управлінням атрибутами та дозволами користувачів, пристроїв та груп, тоді як IAM більше займається оцінкою атрибутів та дозволів і наданням або забороною доступу відповідно до політики компанії. У цьому завданні ми представляємо їх як різні, хоча межа між ними, як правило, розпливчаста.

Управління ідентифікацією (IdM)

Управління цифровими ідентифікаторами (IdM) – це важливий компонент кібербезпеки, що стосується процесу управління та контролю цифрових ідентифікацій. Він включає управління ідентифікаторами користувачів, їхню автентифікацію, авторизацію та контроль доступу. Головна мета IdM – забезпечити доступ до певних ресурсів та інформації лише уповноваженим особам. Системи IdM використовуються для керування ідентифікаторами користувачів у мережі організації.

Системи IdM використовують централізовану базу даних для зберігання ідентифікаційних даних користувачів та прав доступу. Вони також надають функціональні можливості для керування та моніторингу доступу користувачів до ресурсів. Системи IdM зазвичай включають такі функції, як надання користувачів, автентифікація та авторизація. Надання користувачів стосується процесу створення та керування обліковими записами користувачів, тоді як автентифікація та авторизація стосуються перевірки особи користувача та надання доступу до певних ресурсів.

Системи IdM є критично важливими в організаціях, де існує кілька систем і програм, що потребують контролю доступу. Вони допомагають спростити управління ідентифікацією користувачів, зменшуючи ризик несанкціонованого доступу до ресурсів. Крім того, системи IdM забезпечують єдину точку відліку для управління ідентифікацією користувачів, що спрощує для організацій управління правами доступу користувачів.

Керування ідентифікацією та доступом (IAM)

IAM – це більш комплексне поняття, ніж IdM. Воно охоплює всі процеси та технології для управління цифровими ідентифікаторами та правами доступу, а також їх захисту. Системи IAM включають різноманітні функції, такі як надання користувачам доступу, контроль доступу, управління ідентифікаторами та управління відповідністю. Системи IAM гарантують, що лише авторизовані користувачі мають доступ до певних ресурсів і даних, а їхній доступ моніториться та контролюється.

Системи IAM пропонують комплексне рішення для керування та захисту доступу до ресурсів в організації. Вони інтегруються з кількома системами та програмами, забезпечуючи централізоване уявлення про ідентифікаційні дані користувачів та права доступу. Системи IAM використовують різні технології для керування доступом, включаючи контроль доступу на основі ролей, багатофакторну автентифікацію та єдиний вхід.

Системи IAM допомагають організаціям дотримуватися нормативних вимог, таких як HIPAA, GDPR та PCI DSS. Вони надають функції для керування життєвим циклом ідентифікації користувачів, включаючи адаптацію, видалення та скасування доступу. Крім того, системи IAM дозволяють організаціям відстежувати та перевіряти активність користувачів, що допомагає запобігти порушенням безпеки та забезпечити дотримання галузевих норм.

IdM та IAM є важливими компонентами кібербезпеки. Вони гарантують, що лише уповноважені особи мають доступ до певних ресурсів та інформації. Системи IdM керують ідентифікаторами користувачів, тоді як системи IAM охоплюють ширші функції для управління та захисту цифрових ідентифікаторів та прав доступу.

Атаки проти автентифікації

Це завдання охоплюватиме приклади атак на наївний протокол автентифікації. Мета полягає в тому, щоб дати уявлення про важливість використання існуючих та перевірених протоколів замість створення протоколу та його використання без ретельного тестування одноранговими користувачами.

Автентифікація в аналоговому світі

Припустимо, ви належите до кінного клубу. Клуб резервує місцевий ресторан для щотижневих зустрічей. Ви можете поспілкуватися про свої пригоди, насолоджуючись улюбленою стравою. Охоронець біля входу знає не всіх членів клубу. Тож ви розробляєте схему автентифікації, щоб охоронець міг вирішити, чи відчиняти двері.

Одна з найпростіших ідей, яка спадає на думку, – це використання загальної секретної фрази. Тож кожен, хто хоче увійти, повинен сказати секретну парольну фразу; нікому не буде дозволено вхід, якщо він не скаже «*сім коней*» на запитання «Скільки?». Цей механізм автентифікації працює чудово, доки зловмисник, що стоїть поруч, не підслухає та не дізнається вашу парольну фразу. Тепер він отримає доступ до вашої приватної зустрічі, ніби він один із вас. Було б корисно, якби у вас було щось складніше.

Ви можете спланувати десять запитань з десятьма різними секретними відповідями замість одного запитання та однієї відповіді; однак зловмисник, який перебуває досить близько, зрештою вивчить їх усі. Використання безпечного механізму автентифікації без застосування криптографії може бути практично неможливим. На щастя, у сценарії з охоронцем біля дверей легко помітити будь-яких підозрілих осіб, які бездіяльно гуляють; інакше вся ваша група буде скомпрометована.

Автентифікація в цифровому світі

Ситуацію в мережі ще складніше захистити. Якщо користувач надсилає своє ім'я користувача та пароль у відкритому тексті, будь-хто, хто перехоплює трафік у мережі, може дізнатися це ім'я користувача та пароль. Як ми можемо запобігти отриманню облікових даних для входу?

Сервер і користувач можуть домовитися про фіксований секретний ключ. Замість того, щоб надсилати пароль у відкритому вигляді, користувач шифрує його за допомогою вибраного секретного ключа. Щоразу, коли користувачі хочуть увійти, вони надсилають своє ім'я користувача та пароль у зашифрованому вигляді за допомогою призначеного їм секретного ключа. Тепер зловмисник ніколи не повинен мати змоги дізнатися пароль, чи не так? На жаль, хоча вони не зможуть дізнатися пароль, вони все одно зможуть пройти автентифікацію.

Хоча зловмисник не знає пароля, він все одно може автентифікуватися, відтворивши ту саму відповідь. Ця атака вважається **атакою повторного відтворення**. Чи можемо ми щось зробити, щоб виправити це?

Зробіть відповідь на виклик унікальною

Зашифрований пароль, який завжди має одне й те саме значення, легко обійти. Нам потрібен певний механізм, який гарантуватиме, що відповідь не буде використана повторно. Один із підходів – використовувати поточний час і дату як частину відповіді. Іншими словами, користувач надсилатиме зашифрований поточний час (і дату) разом із паролем.

Хоча це вимагає синхронізації годинників обох сторін, це гарантує, що відповідь буде дійсною лише протягом короткого часу, зазвичай у мілісекундах.

Це завдання має на меті пролити світло на деякі проблеми, пов'язані з автентифікацією та протоколами автентифікації. Багато інших вразливостей можуть потрапити в протоколи автентифікації; однак це виходить за рамки цієї кімнати.

Атака повторного відтворення відбувається , коли зловмисник перехоплює дійсні дані автентифікації (наприклад, зашифрований пароль або токен сеансу) та повторно надсилає (або «відтворює») їх, щоб видати себе за оригінального користувача, навіть не знаючи пароля та не розшифровуючи повідомлення.

– Користувач шифрує свій пароль за допомогою спільного секретного ключа та надсилає його на сервер.

– Зловмисник перехоплює це зашифроване повідомлення під час його передачі мережею.

– Пізніше зловмисник відтворює точне повідомлення на сервері.

– Сервер приймає його як дійсний, оскільки він відповідає очікуванням, навіть якщо реального входу не відбулося.

Система не має можливості визначити, чи:

– Цей запит є свіжим (від легітимного користувача), або

– Це повторне повідомлення з попереднього сеансу.

Чому це трапляється:

– Статична відповідь: Зашифрований пароль виглядає однаково щоразу.

– Відсутність актуальності: Сервер не перевіряє, коли було створено повідомлення.

– Без одноразового номера/позначки часу: Немає унікального значення для кожного сеансу для розрізнення запитів.

Як запобігти атакам повторного відтворення

Щоб уникнути атак повторного відтворення, протоколи автентифікації повинні гарантувати, що кожна спроба автентифікації є унікальною.

– Мітки часу – Включити поточний час у зашифроване повідомлення. Сервер відхиляє старі позначки часу.

– Nonces Використовуйте одноразове випадкове число (nonce) для кожного сеансу або завдання.

– Токени сесії – генерувати унікальні токени сесії після автентифікації.

– Протоколи виклику-відповіді – сервер надсилає виклик; клієнт підписує його своїм секретним ключем. Запобігає повторному використанню.

Сучасні протоколи, що пом'якшують це:

– Kerberos: використовує позначки часу та симетричне шифрування для запобігання атакам повторного відтворення.

– OAuth 2.0: видає короткочасні токени та використовує токени оновлення для тривалих сеансів.

– TLS/SSL: використовує унікальні ключі сеансу та рукостискання з одноразовими числами для забезпечення актуальності повідомлень.

Моделі контролю доступу

Система контролює доступ до різних ресурсів на основі обраної моделі. Деякі з поширених моделей контролю доступу:

– Дискреційний контроль доступу (DAC).

– Контроль доступу на основі ролей (RBAC).

– Обов'язковий контроль доступу (MAC).

Дискреційний контроль доступу

Багато хто вже використовував дискреційний контроль доступу (DAC) під час обміну файлами або папками з друзями та колегами. Під час використання DAC власник ресурсу явно додасть користувачів із відповідними дозволами.

Розглянемо наступний приклад. Ви зберігаєте свої фотографії на одній з онлайн-платформ для зберігання. Щоб поділитися всіма зображеннями, пов'язаними з вашим випускним, з родиною, ви додаєте їхні облікові записи окремо та надаєте їм доступ до відповідного альбому. Зрештою, дозволи альбому відображатимуть кілька облікових записів із правами перегляду.

Весь процес простий і повністю контролюється власником даних. Він дуже добре працює для обміну даними з членами родини або кількома користувачами компанії. Однак це може стати складним, коли ви намагаєтеся масштабувати обмін з багатьма користувачами, особливо якщо роль користувача змінюється з часом. Ця ситуація підводить нас до обміну на основі ролей користувачів.

Контроль доступу на основі ролей

Контроль доступу на основі ролей (RBAC) використовує дуже інтуїтивно зрозумілий підхід. Кожен користувач має одну або кілька ролей або функціональних посад; крім того, вони мають право доступу до різних ресурсів на основі своїх ролей.

Бухгалтеру потрібен доступ до бухгалтерських книг компанії, але не потрібен доступ до дослідницьких та розробницьких лабораторій чи документів. Відповідно, користувачі розподіляються на різні групи залежно від їхніх ролей. Авторизація та доступ надаються залежно від групи, до якої належить користувач.

Класифікація користувачів на основі їхніх ролей має багато переваг. Наприклад, якщо користувачеві призначено нову роль, все, що потрібно, це додати його до відповідної нової групи. Більше того, якщо користувачі відмовилися від певної ролі, нам потрібно лише видалити їх зі старої групи. Такий підхід робить обслуговування більш керованим та ефективним.

Обов'язковий контроль доступу

Операційна система, що використовує обов'язковий контроль доступу (MAC), надасть пріоритет безпеці та значно обмежить можливості користувачів. Такі системи використовуються для певних цілей або для обробки високосекретних даних. Отже, користувачам не потрібно виконувати завдання, що перевищують суворо необхідні. Іншими словами, користувачі не зможуть встановлювати нове програмне забезпечення або змінювати дозволи на доступ до файлів.

AppArmor надає можливість використовувати MAC на дистрибутиві Linux. Він вже постачається з різними дистрибутивами Linux, такими як Debian та Ubuntu.

Проект **SELinux** забезпечує гнучку MAC-адресу для систем Linux. Вона є стандартною для кількох дистрибутивів Linux, таких як Red Hat та Fedora.

Єдиний вхід

Користувачам потрібен доступ до різних джерел для виконання своїх щоденних робочих завдань. Наприклад, їм потрібен доступ до електронної пошти, спільних файлів, принтерів тощо. Доступ до цих ресурсів вимагає від користувача облікових даних для успішної автентифікації. Кількість різних імен користувачів та паролів робить це досить складним, особливо якщо користувачі не мають підстав використовувати один і той самий пароль у кількох системах.

Єдиний вхід (SSO) вирішує цю проблему. Замість того, щоб користувачеві доводилося запам'ятовувати кілька імен користувачів та паролів, йому потрібно запам'ятати лише один набір облікових даних для входу. Він може автентифікувати себе в одній системі, що надає йому доступ до інших систем, необхідних для його роботи.

Традиційно користувач повинен створити кілька паролів, таких як пароль для входу на комп'ютер, ще один пароль для перевірки електронної пошти та третій пароль для доступу до спільного файлового ресурсу. Запам'ятовування такої кількості паролів може бути складним завданням, особливо тому, що, в ідеалі, пароль не слід використовувати повторно. Кращим підходом було б вимагати від користувача одноразового входу в систему та надавати йому доступ до всіх необхідних служб; саме це робить SSO.

SSO дозволяє організаціям автентифікувати користувачів один раз, перш ніж надати їм доступ до ресурсів, необхідних для їхньої роботи. Це може дати нам багато переваг. Ми розглянемо деякі з них.

– Один надійний пароль: очікувати, що користувач запам'ятає один надійний пароль, прийнятніше, ніж просити його запам'ятати десять різних надійних паролів.

– Простіша багатофакторна автентифікація (MFA): додавання MFA до кожної окремої служби є надзвичайно складним завданням для виконання та підтримки. За допомогою єдиного входу (SSO) MFA потрібно вмикати та налаштовувати один раз.

– Простіша підтримка: запити на підтримку, такі як скидання пароля, стали простішими, оскільки тепер вони обмежені одним обліковим записом.

– Ефективність: Користувачеві не потрібно входити в систему щоразу, коли йому потрібен доступ до нової послуги.

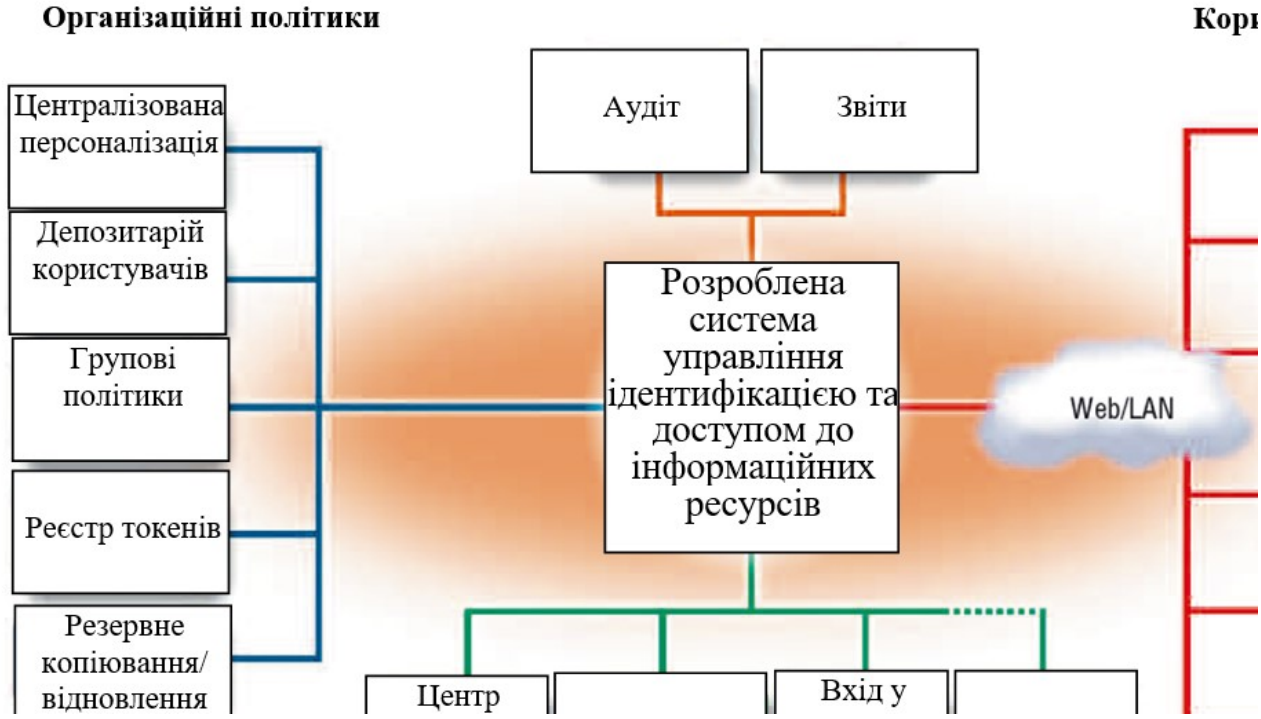

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

– Досліджена система управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

– На основі отриманих результатів досліджень створена програмна реалізація системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Розроблені алгоритми дозволяють успішно вирішувати завдання управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження

технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
5. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
9. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
10. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
14. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
18. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
19. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
20. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи ћозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
21. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. –

Кропивницький: ЦНТУ. – 2023. – С. 26.
22. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
23. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
24. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
25. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
26. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
28. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
29. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
30. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
31. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
32. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.