НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу»

Виконав:
студентка IV курсу, групи ТС-61
Полікарпова Юлія Геннадіїна _____

Керівник:
доц. каф. ТС
к.т.н., доц. Григоренко Олена Григорівна _____

Рецензент:

----- _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Полікарпової Юлії Геннадіївни

1. Тема роботи «Забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу», керівник роботи Григоренко Олена Григорівна, к. т. н., доцент, затверджені наказом по університету від «30» березня 2020 р. № 924-с.
2. Термін подання студентом роботи: 12 червня 2020 р.
3. Вихідні дані до роботи: контроль доступу, авторизація, аутентифікація, NAC.
4. Зміст роботи: розглянути контроль доступу, зокрема дві фази контролю доступу – аутентифікацію та авторизацію, також слід вирішити наступні задачі: розглянути типи загроз і способи їх подолання, використовуючи контроль доступу, а також розглянути соціальну інженерію, як окрему ланку загроз телекомунікаційній мереж та провести дослідження мережевих систем контролю доступу та описати їх принцип роботи.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

1. Тема, мета та завдання бакалаврської дипломної роботи.
2. Обґрунтування необхідності забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу.
3. Методи протидії атакам, які є значними загрозами для телекомунікаційної мережі, за допомогою контролю доступу.
4. Принцип роботи мережевих систем контролю доступу.
5. Безпечна мережева система контролю доступу.
6. Висновки та рекомендації.

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Опрацювання першого розділу та написання висновків до нього: 1) пояснити поняття інформаційної безпеки та її мети, а також, назвати суб'єкти, які потребують захисту (п. 1.1); 2) завдання контролю доступу та аналіз основних аспектів аутентифікації та авторизації, як складових контролю доступу (п. 1.2); 3) розглянути проблеми збереження конфіденційності даних у бездротових телекомунікаційних мережах (п. 1.3); 4) вказати цілі та постановку проблеми забезпечення конфіденційності даних в телекомунікаційних мережах (п. 1.4).	13.04.20 – 19.04.20	Виконала
2	Опрацювання другого розділу та написання висновків до нього: 1) описати атаки, які являються небезпечними для телекомунікаційних мереж (п. 2.1); 2) зазначити методи протидії атакам, які є значними загрозами для телекомунікаційних мереж, за допомогою контролю доступу (п. 2.2); 3) соціальна інженерія як ризик, який є одним із методів	20.04.20 – 26.04.20	Виконала

	порушення конфіденційності даних (2.3).		
3	Опрацювання третього розділу та написання висновків до нього: 1) пояснити принцип роботи мережевих систем контролю доступу (п. 3.1); 2) провести порівняння моделей мережевих систем контролю доступу (п. 3.2); 3) описати безпечну мережеву систему контролю доступу (п. 3.3).	27.04.20 – 03.05.20	Виконала
4	Оформлення дипломної роботи: 1) написання вступу та загального висновку до дипломної роботи; 2) оформлення роботи (нумерація рисунків, абзаци тощо), переліку скорочень та літератури.	04.05.20 – 10.05.20	Виконала

Студент Юлія ПОЛІКАРПОВА

Керівник роботи Олена ГРИГОРЕНКО

РЕФЕРАТ

Текстова частина дипломної роботи: 83 с., 17 рис.., 30 джерел.

Робота присвячена забезпеченню конфіденційності даних користувачів у телекомунікаційних системах, але використання телекомунікаційних мереж не завжди безпечно, тому адміністратори повинні забезпечувати безпеку мережі за допомогою контролю доступу.

Мета роботи – розгляд основних положень контролю доступу та його складових, а також аналіз методів забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу.

У даній роботі розглядаються потреби споживачів у забезпеченні конфіденційності їх даних у телекомунікаційних системах за допомогою контролю доступу. Тому надається рекомендована технологія управління мережевим доступом для пом'якшення дії загроз та наслідків атак.

ІНФОРМАЦІЙНА БЕЗПЕКА, КОНФІДЕНЦІЙНІСТЬ, ЗАГРОЗА, КОНТРОЛЬ ДОСТУПУ, БРАНДМАУЕР, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, УПРАВЛІННЯ МЕРЕЖЕВИМ ДОСТУПОМ

ABSTRACT

Text part of the thesis: 83 p., 17 fig., 30 sources.

The work is dedicated to ensuring the confidentiality of user data in telecommunications systems, but the use of telecommunications networks is not always secure, so administrators must ensure network security through access control.

The goal of the work is to consider the main provisions of access control and its components, as well as the analysis of methods for ensuring the confidentiality of data in telecommunications networks through access control.

This paper examines the needs of consumers to ensure the confidentiality of their data in telecommunications systems through access control. Therefore, the recommended network access control technology is provided to mitigate the threats and consequences of attacks.

INFORMATION SECURITY, CONFIDENTIALITY, THREAT, ACCESS CONTROL, FIREWORK, AUTHENTICATION, AUTHORIZATION, NETWORK MANAGEMENT

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ACL	Access Control List — список контролю доступу
IEEE	Institute of Electrical and Electronics Engineers – інститут інженерів електротехніки та електроніки
DoS	Denial of Service — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні
MAC	Media Access Control — управління доступом до середовища
КЦД	тріада про конфіденційність, цілісність та доступність (КЦД)
VPN	Virtual Private Network
CAPTCHA	Completely Automated Public Turing Test To Tell Computers And Humans Apart – Повністю автоматизований тест Тьюрінга показника відповідності комп'ютерів та людей
ARP	Address Resolution Protocol – протокол визначення адреси
IP	Internet Protocol – міжмережевий протокол
DNS	Domain Name System
NAC	Network Access Control – управління мережевим доступом
RADIUS	Remote Authentication Dial In User Service – служба обслуговування користувачів
IEEE	Institute of Electrical and Electronics Engineers – інститут інженерів електротехніки та електроніки

ВСТУП

Сучасні мережі не є недоступними об'єктами з чітко визначеними параметрами безпеки. Користувачі віддаленого доступу підключаються з будинків та громадських місць. Відвідувачі, співробітники та партнери можуть потребувати фізичного доступу до внутрішньої мережі, щоб виконати свою роботу. Але навіть працівники піддаються загрозам через доступ до Інтернету, використання електронної пошти та обмін миттєвими повідомленнями. Тому розуміння такого поняття, як «контроль доступу» є важливим у сьогоденні.

Метою роботи є представлення системи, яка буде спрямована на захист конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу.

Актуальність даної роботи полягає у використанні контролю доступу, як функції безпеки, яка контролює доступ до систем та ресурсів у мережі. Його метою є захист інформації від втрат, викрадення, видалення або модифікації навмисно чи випадково тими, хто не має права доступу до неї. Контроль доступу вважається найважливішою складовою інформаційної безпеки та є вагомою опорою інформаційної безпеки. Контроль доступу може здійснюватися різними способами залежно від середовища. Це може спричинити блокування комп'ютерної системи, обмеження доступу до системи за допомогою логіну та паролю, захист даних за допомогою шифрування, шифрування мережевих комунікацій або перевірку цифрового підпису перед наданням доступу до запитуваних даних/файлів.

Завдання програм безпеки полягає у тому, щоб сторонні користувачі не мали змоги змінити чи видалити дані. Хоча програми безпеки не можуть покращити якість даних, вони, безумовно, можуть допомогти у захисті даних, застосовуючи засоби контролю доступу, щоб гарантувати, що будь-які зміни в даних призначені та застосовані правильно. Програми безпеки є дуже важливою вимогою як для комерційних, так і для державних організацій,

щоб запобігти шахрайству та помилкам. Жоден користувач не може змінювати дані таким чином, що робить їх недостовірними, неповними або робити їх ненадійними для прийняття відповідних рішень. Прикладами державних систем є система соціального забезпечення, податкова інформація, спадковий реєстр, реєстр міграційної служби. Приклади комерційних систем включають медичну документацію, особисту інформацію працівника, кредитну/фінансову звітність, систему оплати праці, інформацію про податки та прибутки, реквізити клієнта.

Прикладами контролю доступу можуть слугувати: вхід у серверну кімнату чи центр обробки даних (ЦОД) за допомогою аутентичності фізичного ключа або відбитку пальця, або введення паролю доступу; запитування у користувача/віддаленого користувача вказати ім'я користувача (логін) та пароль під час спроби отримати доступ до компютерних ресурсів; користувач відмовив у доступі під час спроби отримати доступ до конфіденційних документів, пов’язаних із підприємством або клієнтом; користувач заборонив доступ під час спроби отримати доступ до інформації, пов’язаної з персоналом.

Цілісність даних може бути захищена шляхом надання доступу до ресурсів на основі необхідних знань та потреб: різним типам користувачів потрібен різний рівень доступу. Наприклад, внутрішнім користувачам може знадобитися повний доступ, тоді як зовнішнім користувачам може знадобитися доступ лише для читання або перегляду інформації. Користувачам слід надавати доступ на основі посади, обов'язків та функцій роботи, які вони виконують. Ресурси також повинні мати різні рівні класифікації. Наприклад, документи слід класифікувати лише як конфіденційні, приватні, публічні чи внутрішнього використання. Необхідно вести детальний електронний журнал операцій, щоб у разі будь-якого шахрайства або втрати даних, журнали можна було переглянути, щоб з’ясувати першопричину та винуватця.

У першому розділі проаналізовані дві фази контролю доступу – аутентифікація та авторизація. Аутентифікація – це підтвердження особи користувача або хоста, який здійснює доступ до системного або мережевого ресурсу. Авторизація дозволяє чи обмежує доступ до інформації залежно від типу користувачів та їх ролей (співробітник, адміністратор чи менеджер). Також розглянуті поняття інформаційної безпеки та суб’єкти, які потребують захисту.

Об'єктом дослідження є заходи забезпечення конфіденційності даних в телекомунікаційних мережах, а предметом дослідження є методи контролю доступу для забезпечення конфіденційності.

Необхідно вирішити наступні задачі: розглянути типи загроз і способи їх подолання, використовуючи контроль доступу, а також розглянути соціальну інженерію, як окрему ланку загроз телекомунікаційній мереж – у другому розділі, і дослідити мережеві системи контролю доступу та описати їх принцип роботи – у третьому розділі.

1 ОБГРУНТУВАННЯ НЕОБХІДНОСТІ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ КОНТРОЛЮ ДОСТУПУ

1.1 Розуміння поняття інформаційної безпеки та її мета, суб’єкти, які потребують захисту

Інформаційна безпека визначається як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» згідно із законодавством України [8]. Загалом, це захист даних та системних активів від тих, хто хотів би їх неправомірно використати. Це може означати захист від зловмисників, які нападають на мережі, вірусів/хробаків, стихійних лих, несприятливих екологічних умов, нестачі живлення, крадіжок, вандалізму чи інших небажаних явищ.

У сьогоднішньому обчислювальному середовищі виявляється, що логічні активи є принаймні такими ж цінними, як фізичні активи, якщо не більше. Крім того, необхідно також захищати дані кваліфікованих співробітників, які беруть участь у колективних операціях. Файли, робочий інвентар кваліфікованих співробітників – найцінніші активи, тому що без них взагалі не можливо вести бізнес. Копіюючи фізичні та логічні активи, зберігаючи резервні копії в іншому місці варто, але без кваліфікованих людей, які б керували та підтримували цілісність даних, можна легко втратити все.

Намагаючись зберегти активи, потрібно враховувати наслідки методів безпеки, які вирішено застосувати. Є добре відомі слова: «Єдина надійно захищена система – це вимкнений, викинутий у бетонний блок і запечатаний у приміщенні, оздобленому свинцем, з озброєною охороною – і навіть тоді

можна сумніватися». Хоча, звичайно, більшість буде впевнена, що систему у такому стані можна вважати розумно безпечною, вона не придатна для використання та не є достатньо продуктивною. При підвищенні рівня безпеки – знижується рівень продуктивності. Метою забезпечення безпеки є знаходження балансу між захистом, зручністю використання та вартістю.

Крім того, захищаючи актив, систему чи оточення, потрібно зважати на рівень безпеки пов'язаний із вартістю предмета, що підлягає захисту. Можна, знизивши продуктивність, застосувати дуже високий рівень безпеки до кожного активу. У будь-якому середовищі, де планується досягнення підвищеного рівня безпеки, також потрібно враховувати кошторис, який дорівнює вартості активів, для того, щоб переконатися в обґрунтованості рівня захисту їх вартості. Ціна безпеки ніколи не повинна перевищувати значення того, що вона захищає.

Визначення точної точки, у якій дані можуть вважатися захищеними, представляє певну загрозу, якщо ці системи/програми з питань безпеки контролюються певними органами чи структурами.

Адже, якщо вони є зафіксованими у якійсь базі даних, то якимось чином хтось може отримати доступ до них, а, відповідно, і до інформації, яка там зберігається. Тому завжди виникатимуть нові атаки, до яких технології вразливі. Якщо використовуються міцні паролі, з'являться інші підходи, які зловмисник може використовувати. Наприклад, в момент роз’єднання системи безпеки та Інтернету – програма може бути фізично доступною, а відповідно, зламаною.

Визначення того, яким чином можна прийти в небезпечний стан, є набагато простішим завданням. Факторами цього є процеси, наведені нижче:

– невчасне оновлення ПЗ;

– використання легких паролів, таких як «пароль» або «12345678»;

– завантаження заражених програм з Інтернету;

– відкриття небезпечних вкладень електронної пошти від невідомих відправників;

– використання бездротових мереж без шифрування, які може контролювати будь-хто і т. ін [30].

Насправді, створити досконало захищену систему досить складно. Можна вказати на ті сфери, які треба контролювати та підтримувати, щоб вживати заходи для збереження даних.

Три основні поняття інформаційної безпеки – конфіденційність, цілісність та доступність, загальновідомі як тріада про конфіденційність, цілісність та доступність (КЦД), як показано на рисунку 1.1. Тріада КЦД дає нам модель, яка є основною в обговоренні концепції безпеки, і, як правило, орієнтується на безпеку, що стосується даних [8, 18].

Рисунок 1.1 – Тріада КЦД

Конфіденційність – це поняття, подібне до приватності, але це не є те саме. Конфіденційність – це необхідний компонент приватності, який посилається на здатність захищати дані від тих, хто не має права їх переглядати; це концепція, яка, можливо, реалізується на багатьох рівнях процесу.

Наприклад, розглянемо випадок, коли особа знімає гроші з банкомату. Відповідна особа, імовірно, прагне зберегти конфіденційність персонального ідентифікаційного номера/коду (ІН), який дозволяє в поєднанні з карткою

банку отримувати кошти з банкомату. Крім того, власник банкомату сподівається зберегти конфіденційність номера рахунку, балансу та будь-якої іншої інформації, необхідної для повідомлення банку, з якого надходять кошти. Банк буде зберігати конфіденційність транзакцій з банкоматами та зміну балансу на рахунку після зняття коштів. Якщо в будь-який момент трансакції буде порушено конфіденційність, результати можуть бути невтішними для особи, власника банкомату та банку, а це може призвести до того, що в полі захисту інформації є несправності.

Конфіденційність може бути порушена через втрату ноутбука, що містить дані; людину, яка дивиться через наше плече, поки ми вводимо пароль; вкладення електронної пошти, надіслане не тій особі; зловмисника, що проникає в нашу системи, або подібні проблеми.

Цілісність – здатність запобігати зміні даних несанкціонованим або небажаним способом. Це може означати несанкціоновану зміну чи видалення даних або частини даних, або це може означати дозволену, але небажану зміну чи видалення даних. Для збереження цілісності не тільки потрібно мати засіб, щоб запобігти несанкціонованим змінам даних, але також потрібна можливість скасування змінених даних, які були деформовані несанкціонованим способом [19].

Такі ОС, як Windows та Linux для запобігання несанкціонованим змінам часто реалізують дозволи/права доступу, що обмежують дії, які несанкціонований користувач може виконувати над заданим файлом. Крім того, деякі подібні системи та безліч додатків, таких як бази даних, можуть дозволяти скасування чи відміну змін, які є небажаними.

Цілісність особливо важлива, при обговоренні даних, що служать основою для рішення інших задач. Якщо зловмисник змінив дані, що містять результати медичних тестів, буде призначено хибне лікування, яке може призвести до смерті пацієнта.

Останньою фазою тріади КЦД є доступність. Доступність стосується можливості доступу до даних, коли це потрібно. Втрата доступності може

статися у будь-якій точці ланцюга, який дозволяє отримати доступ до даних. Такі проблеми можуть виникнути внаслідок втрати електроенергії, несправностей в ОС або додатках, мережевих атак і т. ін. Коли такі проблеми спричинені стороннім чинником, наприклад, зловмисником, їх зазвичай називають атакою типу DoS (з англ. Denial of Service – «відмова в обслуговуванні»).

1.2 Завдання контролю доступу та основні аспекти аутентифікації та авторизації, як складових контролю доступу

Контроль доступу має виконувати чотири основні завдання: дозволяти доступ, забороняти доступ, обмежувати доступ та скасовувати/відкликати доступ. Майже всі ці дії підлягають логічному описанню [15].

Дозвіл доступу – надання певній стороні чи сторонам доступу до заданого ресурсу. Наприклад, якщо потрібно надати конкретному користувачеві або певній групі людей доступ до файлу або до всіх файлів у базі даних. Також можна надавати доступ у фізичному сенсі, надаючи працівникам доступ до конкретного архіву за допомогою ключа або ідентифікаційної картки.

Відхилення/заборона доступу – це протилежна дія дозволу доступу. Під час відхилення доступу, відбувається заборона доступу заданої сторони до відповідного ресурсу. Більшість систем управління доступом повинні бути налаштовані таким чином, щоб забороняти доступ за замовчуванням, при цьому авторизовані користувачі можуть користуватися ресурсами в тій мірі, яка була установлена.

Обмеження доступу – доступ до ресурсу, але лише до певного моменту. Особливо важливим обмеження доступу є при використанні додатків, які, можливо, піддаються впливу схильних до атаки програмних середовищ. У фізичному сенсі обмеження контролю доступу можна пояснити за допомогою замка у будівлі: допустимо, що є три ключі: перший відчиняє

всі двері, другий – лише кілька дверей, а третій – тільки одну, тобто відбувається обмеження.

Якщо розглядати обмеження доступу для програмного забезпечення, часто виникатиме термін «пісочниця» (з англ. sandbox). Він використовується для опису обмежень, які встановлюються. Пісочниця – набір ресурсів, присвячених програмі, процесу чи подібній сутності, за межами якої суб'єкт не може працювати. Пісочниці можуть бути дуже корисними для зберігання речей, яким не можна довіряти, наприклад, код із загальнодоступних веб-сайтів. Прикладом пісочниці може слугувати її використання у віртуальній машині Java (з англ. JVM – Java Virtual Machine), під якою запускаються програми, написані мовою програмування Java. JVM спеціально розроблена для захисту користувачів від потенційно шкідливого ПЗ, яке вони можуть завантажувати.

Відкликання доступу є дуже важливим пунктом у контролі доступу. Важливо, щоб при наданні доступу користувачу до ресурсу, можна було анулювати права на доступ до даних. Наприклад, після звільнення співробітника, варто відкликати його змогу доступу до будь-яких файлів установи, де він працював: до його робочого облікового запису електронної пошти, заборонити підключатися до віртуальної приватної мережі (з англ. VPN – Virtual Private Network) організації, дезактивувати ідентифікаційну картку, а також скасувати інші доступні можливості.

Для цього використовуються два основні методи: списки контролю доступу (з англ. ACLs – Access Control Lists) та списки можливостей (з англ. Capability List or Capabilities). Кожен із них має позитивні та негативні аспекти, і способи виконання чотирьох основних завдань, які було розглянуто раніше, будуть відрізнятися залежно від обраного методу для здійснення контролю доступу.

ACLs є дуже поширеним вибором реалізації контролю доступу та зазвичай використовуються для контролю доступу файлових систем, на яких працюють ОС, і для контролю потоку трафіку в мережах, до яких приєднані

системи. ACLs найчастіше обговорюються в контексті брандмауерів і маршрутизаторів. ACLs будуються спеціально для окремої системи. Їх структура містить ідентифікатори усіх процесів (активних одиниць), яким дозволений доступ до відповідного ресурсу, і перелік операцій для кожного процесу, які йому дозволено здійснювати по відношенню до ресурсу (рис. 1.2).

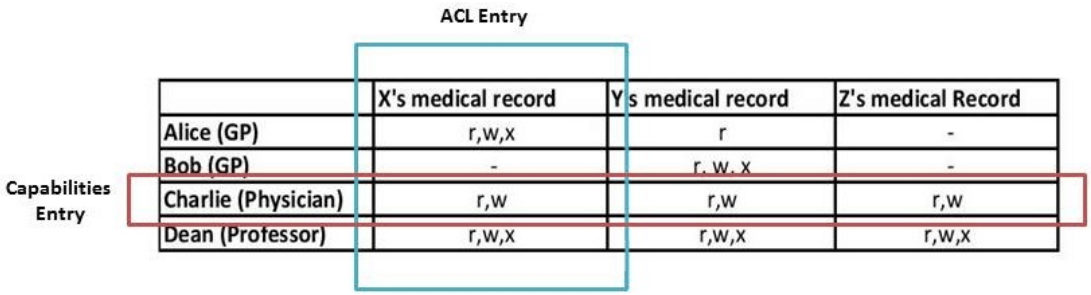

Рисунок 1.2 – Структура ACLs та списків можливостей

Списки можливостей надають альтернативне рішення контролю доступу, яке використовує іншу структуру, ніж те, що використовується в ACLs. У списку можливостей перераховані процеси, до яких дозволений доступ та у кожного ресурсу є список операцій, які цьому процесу можна здійснювати (рис. 1.2). На відміну від списків можливостей, ACLs вимагають авторизацію, а списки можливостей використовують маркер, який можна передавати тому чи іншому користувачу [10].

Що стосується мережевих ACL, спостерігається доступ, контрольований ідентифікаторами, які використовуються для мережевих транзакцій, такими як IP адреси, Media Access Control (MAC) адреси та порти. ACL під час роботи наявні у складових мережевої інфраструктури, таких як, маршрутизатори, комутатори, брандмауери пристроїв, а також у брандмауерах ПЗ, Facebook, Google, електронна пошта чи інші форми програмного забезпечення.

Права доступу/дозволи в мережевих ACL, як правило, мають бінарний характер, тобто складаються з дозволу та заборони. Під час налаштування ACL, використовується вибраний ідентифікатор або ідентифікатори для того, щоб указати, до якого трафіку ми звертаємось, і повідомити, дозволений трафік чи ні.

Однією з найпростіших форм мережево-орієнтованих ACL є фільтрація MAC-адрес. MAC-адреси теоретично є унікальними ідентифікаторами, приєднаними до кожного мережевого інтерфейсу в системі. Кожний мережевий інтерфейс має жорстко кодовану MAC-адресу, видану при його створенні. Зазвичай можуть бути впроваджені, як бездротові точки доступу.

Використаємо термін «контроль доступу», як парасольку для будь-яких проблем із безпекою для доступу до системних ресурсів. У рамках цього широкого визначення є дві області первинного інтересу, а саме аутентифікація та авторизація.

Аутентифікація – це процес визначення, чи повинен користувач (або інший об'єкт) мати доступ до системи. Проблема аутентифікації виникає, коли інформація про аутентифікацію повинна пройти через мережу. Коли задіяні мережі, аутентифікація майже повністю є проблемою безпеки протоколів.

За визначенням, аутентифікованим користувачам дозволяється доступ до системних ресурсів. Однак, аутентифікованому користувачеві зазвичай не надається глобальний доступ до всіх системних ресурсів. Наприклад, можна дозволити лише привілейованому користувачеві (наприклад, адміністратору) встановлювати програмне забезпечення в системі. Тоді доведеться обмежувати дії аутентифікованих користувачів, а це є поле авторизації, яке буде розглянуто нижче в цьому ж підпункті. Зауважимо, що аутентифікація – це двійкове рішення – доступ надається або його немає – в той час, як авторизація стосується більш тонкого набору обмежень доступу до різних системних ресурсів.

Термін «контроль доступу» часто використовується як синонім авторизації. Однак, це не так. Контроль доступу включає в себе і аутентифікацію, і авторизацію. У свою чергу відповідають на такі питання:

– Перевірка аутентичності: «Чи є Ви тим, ким представляєтесь?»

– Авторизація: «Чи дозволено робити запропоновану дію?».

Ідеальний пароль – це те, що ви знаєте; те, що комп’ютер може перевірити, що ви знаєте; і те, що ніхто інший не здогадається, навіть з доступом до необмежених обчислювальних ресурсів. Тобто, практично важко навіть наблизитися до цього ідеалу.

1.3 Ключові поняття про методи контролю доступу та їх застосування для збереження конфіденційності даних

Безперечно, кожен знайомий із паролями. Сьогодні користуватися комп’ютером практично неможливо без накопичення значної кількості паролів. Навіть для входу у комп’ютер, ввівши ім'я користувача, наступним кроком вводимо пароль, щоб отримати доступ саме до потрібного облікового запису, якщо цим комп’ютером користується ще хтось. Крім того, багато інших речей, які в буденності не називають «паролем», виконують роль паролів. Наприклад, PIN-код, який використовується для картки банкоматів, фактично є паролем. А якщо так сталося і пароль був втраченим або забутим, то веб-сайт, орієнтований на користувача, може підтвердити аутентифікацію на основі номера соціального страхування, дівочого імені матері або дати народження. Проблема з такими паролями полягає у тому, що вони часто не є секретними.

Якщо їх залишати на власних пристроях (а користувачі, як правило, вибирають легкі паролі, тобто доступні дані про себе), то злом пароля буде напрочуд легким. Тому до вибору паролю слід ставитися відповідально, тому що досягти безпеки за допомогою паролів вірогідно. Із точки зору безпеки, найкраще вирішенням проблеми з паролем – використання випадково

згенерованих криптографічних ключів. Проблема такого підходу полягає в тому, що люди повинні запам'ятати свої паролі, а випадково вибрані біти запам’ятати складніше. Не слід забувати і про економічний фактор. Паролі безкоштовні, а за смарт-картки та біометричні пристрої треба платити. Крім того, вони зручніші у використанні: перевантаженому системному адміністратору зручніше скинути пароль, ніж надати нову смарт-картку або видати користувачеві новий великий палець.

Уже було сказано, що криптографічні ключі вирішать проблему з паролями. Щоб зрозуміти, чому це так, потрібно порівняти ключі з паролями. З одного боку, припустимо, є зловмисник, який стикається з 64-бітовим криптографічним ключем. Тоді є 2^{64} можливих ключа, і, якщо ключ був обраний випадковим чином, то зловмисник повинен в середньому випробувати 2^{63} ключів, перш ніж він знайде правильний.

З іншого боку, припустимо, що зловмисник стикається з паролем, і йому відомо, що пароль має вісім символів, і 256 можливих варіантів для кожного символу. Тоді є $256^8 = 2^{64}$ можливих паролів. На перший погляд, злам таких паролів може здатися неймовірним. На жаль, користувачі не вибирають паролі випадково, оскільки повинні запам'ятати свої паролі. Як результат, користувач набагато частіше вибирає словник із 8 символів, наприклад:

«password» або «12345678»,

ніж, наприклад,

«mp@$U!a[».

Отже, у цьому випадку зловмисник може зробити набагато менше, ніж 2^{63} спроб і мати високу ймовірність успішного злому паролю. Наприклад, ретельно підібраний словник з $2^{20} \approx 1\ 000\ 000$ паролів, можливо, дасть зловмиснику обґрунтовану ймовірність зламати заданий пароль. Суть полягає в тому, що невипадковість вибору пароля лежить в основі проблем із паролями.

Не всі паролі створюються однаково. Наприклад, можна погодитись, що такі паролі слабкі:

«Руслан»,

«Шевченко»,

«08081994»,

«AntonBorsch»,

особливо якщо іменем користувача є Руслан, Антон Борщ, або день народження 08.08.1994.

Безпека часто базується на паролях, а отже, у користувачів повинні бути паролі, які важко здогадатися. Однак користувачі повинні мати можливість запам'ятати свої паролі. Зважаючи на це, перевіримо чи є наступні паролі кращими, ніж слабкі паролі вище:

«jfIej(43j-EmmL+y»,

«09864376537263»,

«P0kem0N»,

«FSa7Yago».

Перший пароль «jfIej(43j-EmmL+y» зловмиснику, безумовно, буде важко розгадати, але користувачу було б також важко запам'ятати. Такий пароль, імовірно, користувач занотує та закріпить аркуш з паролем неподалік від комп’ютера. Це може зробити роботу зловмисника набагато простішою, ніж якби користувач обрав більш легший пароль.

Другий пароль «09864376537263» також, мабуть, занадто громіздкий, щоб запам’ятали більшість користувачів. Навіть висококваліфікованому військовослужбовцю США, відповідальному за запуск ядерних ракет, потрібно пам'ятати лише 12-значні кодекси стрільби [2].

Пароль «P0kem0N» може бути важко здогадатися, оскільки це не стандартне словникове слово, тому що присутні цифри та великі літери. Однак, якщо користувач, як відомо, був шанувальником мультфільму «Pokémon», цей пароль може стати відносно легкою здобиччю.

І останній пароль, «FSa7Yago», може виявитися таким, що важко здогадатися, але занадто складно запам'ятати. Однак є хитрість, яка допоможе користувачеві запам'ятати його – він заснований на парольній фразі. Тобто «FSa7Yago» походить від фрази «Four Score and seven Years ago». Отже, цей пароль повинен бути порівняно легким для запам'ятовування користувачем, а зловмиснику зламати його буде порівняно важко.

Цікавий експеримент із паролем описаний у [2]. Користувачів розділили на три групи та дали наступні поради щодо вибору пароля:

– Група А – Вибрати паролі, що містять щонайменше шість символів, з щонайменше однією великою літерою. Це досить типова порада щодо вибору пароля.

– Група В – Вибрати паролі на основі парольних фраз.

– Група С – Вибрати паролі, що складаються з восьми випадково вибраних символів.

Експериментатори намагалися зламати отримані паролі кожної з цих трьох групи. Результати були такими:

– Група А – Близько 30% паролів було легко зламати. Користувачі цієї групи легко запам’ятали свої паролі.

– Група В – Близько 15% паролів було зламано, і, як і у користувачів групи А, користувачі цієї групи легко запам'ятали свої паролі.

– Група С – близько 10% паролів було зламано. Не дивно, що користувачам цієї групи було важко запам'ятати свої паролі.

Ці результати чітко вказують на те, що парольні фрази є найкращим варіантом для вибору пароля, оскільки отримані паролі порівняно важко зламати, але їх легко запам'ятати.

Цей експеримент із паролями також продемонстрував, що відповідальності користувачів важко досягти. У кожній із груп А, В і С приблизно третина користувачів не дотримувались інструкцій. Якщо припустити, що невідповідні користувачі прагнуть вибирати паролі, подібні до групи А, приблизно третину цих паролів було б легко зламати. Суть

полягає в тому, що майже 10% паролів, імовірно, будуть легко ламатися, незалежно від наданих порад [9, 16].

У деяких ситуаціях має сенс призначати паролі, і якщо це так, недотримання політики щодо паролів не є проблемою. Тут ідеться про те, що користувачі, імовірно, будуть довше та важче запам’ятовувати призначені паролі, порівняно з паролями, які вони вибирають самі.

Знову ж таки, якщо користувачам дозволяється вибирати паролі, то найкраща порада – це вибирати паролі на основі парольних фраз. Крім того, системні адміністратори повинні використовувати інструмент для розбиття паролів для перевірки на слабкі паролі, оскільки зловмисники, безумовно, будуть.

Також часто пропонуються періодичні зміни пароля. Однак, користувачі можуть просто сповістити, що «змінили» пароль, не змінюючи його. У відповідь на таких користувачів система створила протидію, яка могла запам'ятати, наприклад, п'ять попередніх паролів. Але розумний користувач незабаром дізнається, що він може пройти п'ять змін пароля, а потім відновити свій пароль до початкового значення. Або якщо користувачу потрібно щомісяця вибирати новий пароль, він може вибрати: «admin01» у січні, «admin02» у лютому тощо. Примушувати неохочих користувачів вибирати досить надійні паролі не так просто, як може здатися.

Біометрика являє собою метод аутентифікації «це хтось є». Існує багато різних видів біометрії, включаючи такі давно встановлені методи, як відбитки пальців. Останнім часом були розроблені біометричні показники, засновані на розпізнаванні мови, розпізнаванні ходи і навіть цифровому собаці (розпізнаванні запаху). Біометрика на даний момент є дуже активною темою для досліджень [2, 27].

На арені інформаційної безпеки біометричні дані розглядаються як більш безпечна альтернатива паролям. Щоб біометричні дані були практичною заміною паролів, потрібні дешеві та надійні системи. Сьогодні існують корисні біометричні системи, включаючи ноутбуки, що

використовують аутентифікацію відбитків пальців, системи друку долонь для безпечного входу в обмежені об'єкти, використання відбитків пальців для розблокування дверей автомобіля тощо. Але зважаючи на потенціал біометричних даних – і загальновідомі слабкі сторони аутентифікації на основі пароля – можливо, дивно, що біометрика не використовується широко.

Ідеальна біометрія задовольняла б усім наступним:

– Універсальність – Біометрія повинна застосовуватися практично до всіх. Насправді жодна біометрія не стосується всіх. Наприклад, невеликий відсоток людей не має читабельних відбитків пальців.

– Відмінність – Біометрію слід відрізняти від віртуальною реальності. Насправді ми не можемо бути впевненими на 100%, хоча, теоретично, деякі методи можна виділити з дуже низькими показниками помилок.

– Постійність – в ідеалі фізична характеристика, яка ніколи не повинна змінюватися. На практиці достатньо, якщо характеристика залишається стабільною протягом досить тривалого періоду часу.

– Надійність та зручність для користувачів – це лише деякі з додаткових реальних міркувань для практичної системи біометрії. Деякі біометричні показники, які виявилися перспективними в лабораторних умовах, згодом не змогли досягти подібних показників на практиці.

Біометрика також застосовується при різних проблемах ідентифікації. У проблемі ідентифікації ми намагаємось відповісти на запитання «Хто це?» Тобто при ідентифікації мета полягає в тому, щоб визначити суб'єкта зі списку багатьох можливих предметів. Це відбувається, наприклад, коли підозрілий відбиток пальців із місця злочину надсилається до бази даних відбитків пальців у лабораторію правоохоронних органів для порівняння з усіма мільйонами записів відбитків пальців, які наявні в той момент у базі даних.

Проблемою ідентифікації є порівняння одного відбитку з багатьма, тоді як для аутентифікації такої проблеми немає, тому що якийсь заданий відбиток порівнюється лише з одним. Наприклад, якщо зловмисник бажає отримати доступ до комп’ютера користувача і при цьому використовує біометричну мишу, то захоплене зображення відбитків пальців зловмисника порівнюється лише зі збереженим відбитком пальців користувача. Проблема ідентифікації за своєю суттю є складнішою та підлягає значно більшій кількості помилок через більшу кількість порівнянь, які необхідно здійснити. Тобто, кожне порівняння несе в собі ймовірність помилки, тому чим більше потрібно порівнянь, тим вищий показник помилок.

Існує дві фази до біометричної системи. По-перше, відбувається етап реєстрації, коли суб'єкти збирають свою біометричну інформацію та вводять до бази даних. Зазвичай під час цієї фази потрібне дуже ретельне вимірювання відповідної фізичної інформації. Оскільки це разова робота, прийнятно, якщо процес повільний і потрібні кілька вимірювань. У деяких польових системах реєстрацію відмічено як слабкий момент, оскільки може бути важко отримати результати, порівнянні з результатами, отриманими в лабораторних умовах.

Друга фаза в біометричній системі – це фаза розпізнавання. Відбувається, коли система виявлення біометрії використовується на практиці для визначення того, чи потрібно (для проблеми аутентифікації) аутентифікувати користувача чи ні. Ця фаза повинна бути швидкою, простою та точною.

Припустимо, що суб'єкти співпрацюють, тобто вони готові надати відповідні фізичні характеристики. Це є обґрунтованим припущенням у випадку аутентифікації, оскільки аутентифікація, як правило, потрібна для доступу до певних інформаційних ресурсів або для входу в іншу область із обмеженням.

Проблемою ідентифікації часто є те, що суб'єкти не співпрацюють. Наприклад, розглянемо систему розпізнавання обличчя, яка

використовується для ідентифікації. Казино в Лас-Вегасі використовують такі системи для виявлення відомих шахраїв під час спроби входу в казино [5]. Ще одна фантастична пропозиція використання розпізнавання обличчя – це виявлення терористів в аеропортах. Жоден зловмисник не бажає бути спійманим, тому намагатиметься максимально уникати контакту з біометричною системою.

Існує два типи помилок, які можуть виникнути при розпізнаванні біометрії. Припустимо, зловмисник представляється користувачем, і система помилково аутентифікує його, як користувача. Швидкість, з якою відбувається така помилкова аутентифікація, – це фродова швидкість (з англ. fraud – шахрайство). Тепер припустимо, що користувач намагається пройти аутентифікацію, але система не зможе її засвідчити. Швидкість, з якою виникає цей тип помилок, – це інсалтова швидкість (з англ. insult – збиток) [2].

Для будь-якої біометрії можна знизити рівень фродової швидкості або інсалтової за рахунок іншої. Наприклад, якщо потрібна 99-відсоткова відповідність голосового відбитка, можна отримати низький рівень фродової швидкості, але інсалтова швидкість буде високою, оскільки голос оратора, природно, час від часу трохи змінюватиметься. З іншого боку, якщо встановити поріг у 30% голосовому відбитку, фродова швидкість, імовірно, буде високою, але система матиме низький рівень інсалтової швидкості.

Будь-який метод аутентифікації, який вимагає підтвердження особи двома різними способами, відомий як двофакторна аутентифікація. Прикладом двофакторної аутентифікації може слугувати картка банкомату, де користувач повинен мати картку та знати PIN-код. Інші приклади двофакторної аутентифікації включають кредитну карту разом з підписом, систему відбитків пальців біометрії, яка також потребує пароль, і мобільний телефон, для якого потрібен PIN-код.

Авторизація – це частина контролю доступу, що стосується обмеження дій аутентифікованих користувачів. На жаль, деякі автори використовують термін «контроль доступу», як синонім авторизації.

Вище було обговорено аутентифікацію, де проблема полягає у встановленні ідентичності. У своїй найпростішій формі авторизація стосується ситуації, коли аутентичність користувача вже підтверджена, і потрібно застосувати обмеження щодо того, що аутентифікованому користувачу дозволяється робити. Зауважимо, що аутентифікація є двійковою (або користувач має аутентифікацію, або ні), а авторизація може бути набагато різноманітнішим процесом із більшою кількістю варіантів подій.

Далі буде описано поняття CAPTCHA, які призначені для обмеження доступу людей (на відміну від комп'ютерів), і розглянуто брандмауери, які можна використовувати, як форму контролю доступу до мереж.

Тест Тьюрінга був запропонований Аланом Тьюрінгом у 1950 році. У тесті люди задавали питання людині та комп'ютеру. Той, хто запитував (лаборант), не бачив ні людини, ні комп'ютера, та мав змогу запитувати лише набиравши питання на клавіатурі, а відповіді отримував на екрані комп’ютера. Лаборант не знав де відповідь комп’ютера, а де – людини. Метою було: відрізнити людину від комп’ютера, виходячи виключно з питань і відповідей, які виводилися на екран, тобто зрозуміти чи може машина мислити як людина. Якщо лаборант не міг знайти різницю між комп’ютером та людиною конструктивно, а покладався лише на інтуїцію – комп'ютер проходив тест Тьюрінга. Цей тест є золотим стандартом штучного інтелекту, і жоден комп'ютер ще не пройшов тест Тьюрінга, але іноді деякі заявляють, що вони наближаються.

«Completely Automated Public Turing Test To Tell Computers And Humans Apart – Повністю автоматизований тест Тьюрінга показника відповідності комп'ютерів та людей», або CAPTCHA (також ще називають HIP – human interactive proofs) – це тест, який людина може пройти, але

комп'ютер не може пройти з вірогідністю вищою, ніж здогадки [6]. Урахувати слід те, що тест генерується комп'ютерною програмою та оцінюється комп'ютерною програмою, проте жоден комп'ютер не може пройти тест, навіть якщо цей комп'ютер має доступ до вихідного коду, який використовується для створення тесту. Іншими словами, «CAPTCHA – це програма, яка може генерувати та оцінювати тести, які вона сама не може пройти» [6].

Спочатку це здається парадоксальною, що комп’ютер може створити і скласти тест, який він не може пройти. Однак це стає менш парадоксальним, під час уважнішого вивчення деталей процесу.

Оскільки CAPTCHAs призначені для запобігання людям доступу до ресурсів, CAPTCHA може розглядатися як форма контролю доступу. Згідно з першоджералми, початковою мотивацією виникнення CAPTCHAs було Інтернет-опитування, у якому просили користувачів проголосувати за кращу випускницю з інформатики. Інтернет-форму легко заповнити, скориставшись послугами автоматизованих «ботів», щоб сфальсифікувати результати голосування [7]. Тому, щоб таких випадків не виникало, було створено CAPTCHA. Сьогодні CAPTCHAs використовуються в широкому спектрі різноманітних додатків. Наприклад, безкоштовні сервіси електронної пошти використовують CAPTCHAs, щоб запобігти автоматичному підпису спамерів на велику кількість облікових записів електронної пошти.

Вимоги до CAPTCHA повідомляють, що для більшості людей тест повинен бути легким, а для машин – завдання повинні бути важкими або неможливими, навіть якщо машина має доступ до програмного забезпечення CAPTCHA. З точки зору зловмисника, єдиною невідомою є деяка випадковість, яка використовується для генерації конкретної CAPTCHA. Також бажано мати різні типи CAPTCHA, якщо хтось не може передати один конкретний тип. Наприклад, багато веб-сайтів дозволяють користувачам вибирати аудіо CAPTCHA, як альтернативу звичайній візуальній CAPTCHA.

Приклад CAPTCHA показаний на рисунку 1.3 [7]. У цьому випадку людину можуть попросити знайти три слова, які проілюстровані на зображенні. Це порівняно просте завдання для людини, і сьогодні це також досить просте завдання для комп'ютерів, тому вже існують більш складні CAPTCHA.

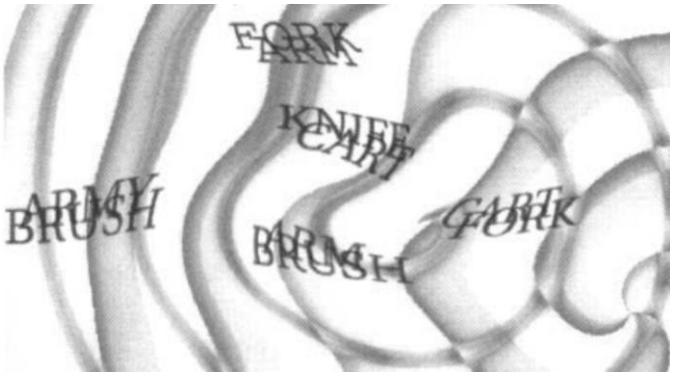

Рисунок 1.3 – Візуальна CAPTCHA

Є твердження, що комп’ютери насправді кращі за людину у вирішенні всіх основних візуальних завдань CAPTCHA, за винятком – так званої проблеми сегментації, тобто проблеми відокремлення літер одна від одної. Отже, складні CAPTCHAs мають тенденцію виглядати більше як на рисунку 1.4, ніж як на рисунку 1.3.

Рисунок 1.4 – Складні CAPTCHAs

Щодо словесної візуальної CAPTCHA, можна припустити, що зловмисник знатиме набір можливих слів, які можуть з’явитися, і він знає загальний формат зображення, а також типи спотворень, які можна застосувати. З точки зору зловмисника, єдине невідоме – випадкове число,

яке використовується для вибору слова чи слів та спотворення отриманого зображення.

Існує кілька типів візуальних CAPTCHAs, рисунок 1.3 та рисунок 1.4 є репрезентативними прикладами. Існують також аудіо CAPTCHAs, у яких звук певним чином спотворений. Людське вухо дуже добре відрізнити звук від подібних спотворень, тоді як машини з цим завданням не впораються. Наразі, текстові CAPTCHAs масштабні підприємства не використовують.

Проблеми з обчисленнями, які необхідно вирішити, щоб зламати CAPTCHAs, можна розглядати як важкі проблеми вобласті штучного інтелекту або AI (artificial intelligence).

Наприклад, автоматичне розпізнавання спотвореного тексту є проблемою AI, і це саме стосується проблем, пов'язаних із спотвореним звуком. Якщо зловмисники здатні зламати такі CAPTCHAs, вони фактично вирішили важку проблему з AI. У результаті, зусилля зловмисника не були марними.

Зловмисники не надають переваг грі за правилами – тому можуть на різних веб-сторінках, в коментарях чи інших полях, розповсюджувати інформацію, наприклад, що, якщо людина вирішить дану CAPTCHA, то отримає безкоштовний доступ, наприклад, до сайту, який вимагає платну підписку. І тоді випадкові користувачі інтернету вирішуватимуть зловмисникам CAPTCHAs. Тобто, зловмисник отримує рішення багатьох завдань за мінімальних втрат [8].

Перейдемо до поняття «брандмауер». Припустимо ситуацію, що співробітник бажає зустрічі з директором. По-перше, співробітнику, мабуть, потрібно буде звернутися до секретаря директора. Якщо секретар вважає, що зустріч є доречною, він планує її; інакше він відмовляє співробітнику в зустрічі. Таким чином, секретар відфільтровує багато запитів, які в іншому випадку займуть певний час.

Брандмауер дуже схожий на секретаря. Брандмауер вивчає запити доступу до мережі і вирішує, чи являються вони аргументованими. Якщо це так, запити дозволяються, а якщо ні – здійснюється відмова [13].

Якщо співробітник побажає зустрітися з директором, секретар зробить певний рівень фільтрації; однак, якщо співробітник забажає зустрітися з Президентом, то секретар Президента виконає набагато вищий рівень фільтрації. Це дещо аналогічно брандмауерам, коли деякі прості брандмауери фільтрують лише очевидні чіткі запити, а інші види брандмауерів докладають набагато більших зусиль для фільтрації всього підозрілого.

Мережевий брандмауер, як показано на рис.1.5, розміщений між внутрішньою мережею, яка може вважатися відносно безпечною, і зовнішньою мережею (Інтернет), яка, як відомо, небезпечна. Завдання брандмауера – визначити, що пропускати та що виводити із внутрішньої мережі. Таким чином, брандмауер забезпечує контроль доступу до мережі.

Як і у більшості понять інформаційної безпеки, для брандмауерів немає стандартної термінології. Але існує декілька типів брандмауерів один і них – мережевий, як показано на рисунку 1.5. Кожен тип брандмауера фільтрує пакети, вивчаючи дані до певного рівня стеку мережевого протоколу.

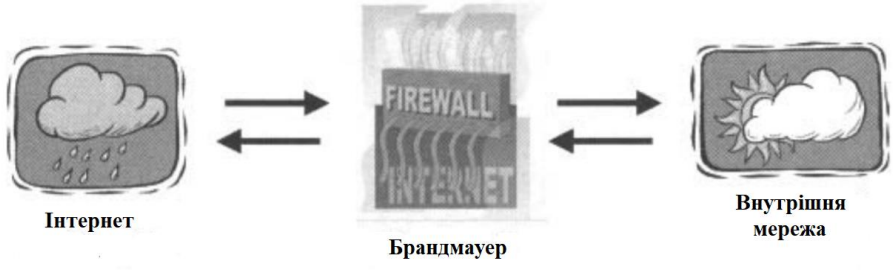

Рисунок 1.5 – Мережевий брандмауер

Класифікації брандмауерів:

– Фільтр пакетів – це брандмауер, який працює на мережевому рівні.

– Постійний фільтр пакетів – це брандмауер, який працює на транспортному рівні.

– Проксі-сервер програми – це брандмауер, який працює на рівні програми, де він працює, як проксі.

1.4 Цілі та постановка проблеми забезпечення конфіденційності даних в телекомунікаційних мережах

Метою роботи являється розгляд основних положень контролю доступу та його складових, а також розгляд методів забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу.

Згідно мети роботи, основними задачами є:

1. Визначення завдання контролю доступу.
2. Функціональний опис складових контролю доступу: аутентифікації та авторизації.
3. Розгляд загроз, які являються небезпечними для телекомунікаційної мережі.
4. Знаходження оптимальних методів, які забезпечують конфіденційність даних.
5. Надання економічної оцінки телекомунікаційній системі, найменшим чином схильної до атак.

Об’єктом дослідження являється конфіденційність даних і заходи її забезпечення в телекомунікаційних системах за допомогою контролю доступу.

Предметом дослідження являються методи забезпечення конфіденційності даних у телекомунікаційних мережах за допомогою контролю доступу.

У даній дипломній роботі буде розглядатися важливість конфіденційності даних у телекомунікаційних мережах та способи/методи забезпечення конфіденційності даних у телекомунікаційних мережах за допомогою контролю доступу, а також будуть проаналізовані загрози, які являються небезпечними для телекомунікаційних мереж.

Основними складовими контролю доступу являються аутентифікація та авторизація, тому будуть розглянуті ці питання більш детально та надані рекомендації щодо їх продуктивного використання.

Підсумковою частиною роботи повинні виступати рекомендації щодо покращення конфіденційності даних та описана найбільш захищена телекомунікаційна система.

1.5 Висновки з розділу 1

1. Розглянуто більш детально поняття інформаційної безпеки, метою якої є захист даних та системних активів від тих, хто хотів би їх неправомірно використати, а її суб’єктами являються фізичні та логічні активи. Надано опис фундаменту інформаційної безпеки - тріади КЦД (конфіденційність, цілісність, доступність) .
2. Проаналізовано головні завдання контролю доступу, якими є дозволяти доступ, забороняти доступ, обмежувати доступ та скасовувати/відкликати доступ.
3. Проведено порівняння списків контролю доступу та списків можливостей. Їх спільною метою є обмеження доступу неавторизованим користувачам.
4. Описано різницю між аутентифікацією та авторизацією, яка полягає у тому, що аутентифікація – це розпізнавання користувача, а

авторизація – це надання користувачу прав; обґрунтовано важливість використання складних паролів методом асоціативного запам’ятовування паролів, який полягає у використанні зашифрованих фраз. Описано CAPTCHAs, як спосіб авторизації: є графічні та слухові; слухові CAPTCHAs ефективніші, тому що складніше сприймаються комп’ютерною системою.

5. Опрацьовано поняття біометрії, як засобу ідентифікації користувача і вказано, що головним недоліком системи біометрії є значна можливість помилки, оскільки процедуру цієї системи можна уникнути.

6. Метою роботи являється розгляд основних положень контролю доступу та його складових, а також розгляд методів забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу.

2 ОПИСАННЯ АТАК І МЕТОДИ ЇХ УСУНЕННЯ ЗА ДОПОМОГОЮ КОНТРОЛЮ ДОСТУПУ ТА РОЛЬ ЗАСОБІВ ПРОТИДІЇ ЗАГРОЗАМ У ЗАБЕЗБЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ДАНИХ

2.1 Визначення атак, які являються небезпечними для телекомунікаційних мереж

У сьогоденні все ще відбувається перетинання користувачів із випробуваним, десятилітнім арсеналом традиційних засобів комп’ютерних атак, включаючи атаки відмови в обслуговуванні (DoS), зломщиків паролів, сканерів портів, Sniffers та RootKits. Проте, багато з цих основних інструментів та прийомів за останні кілька років пережили ренесанс, із новими можливостями та основними архітектурами, які роблять їх більш потужними, ніж будь-коли [5, 17]. Зловмисники ґрунтовно заглиблюються в широко використовувані протоколи та самі ядра ОС. Окрім зростаючих можливостей, інструменти комп’ютерних атак стають все більш простими у використанні. Навіть тоді, коли користувачі думають, що все вже винайдено та побачено, публічно виходять нові та прості у використанні інструменти для нападу з функцією, яка знімає «шкарпетки» (з англ. Socks – мережеві протоколи прозорої відправки пакетів від клієнта до сервера через проксі-сервер). Завдяки постійному зростанню досконалості та простоти використання засобів нападів, а також широкому розміщенню слабких цілей в Інтернеті, суспільство живе в золоту епоху загроз.

Основною метою даного розділу являється описання останніх подій у цій еволюції засобів комп'ютерних атак. Щоб створити найкращі засоби захисту для телекомунікаційних мереж, потрібне розуміння можливостей та тактик противників. Для досягнення цієї мети проаналізовано кілька активних областей просування серед інструментів атак, включаючи розподілені атаки, активний Sniffing і RootKits на рівні ядра, а також захисні методи для кожного типу атаки.

Розподілені атаки (з англ. Distributed attacks). Однією з головних тенденцій еволюції засобів комп'ютерної атаки є рух до розподілених архітектурних атак. По суті, зловмисники застосовують розподілену потужність самого Інтернету, щоб поліпшити свої можливості атакувати. Тут стратегія є досить простою, можливо, оманливою, тому враховуючи силу деяких з цих розповсюджених атак. Зловмисник використовує звичайну комп’ютерну атаку і розподіляє роботу серед багатьох систем. Коли в атаці співпрацює все більше систем, шанси зловмисника збільшуються. Ці розподілені атаки пропонують хакерам ряд переваг, зокрема:

– Атака може складніше проявлятися.

– Зазвичай атаки ускладнюють ідентифікацію нападника.

– Атаки можуть прискорити зловмисне діяння, скорочуючи час, необхідний для досягнення заданого результату.

– Атаки дозволяють зловмиснику отримати більше цільових ресурсів.

На жаль, в Інтернеті доступна величезна кількість дуже слабких систем. Адміністратори та власники таких систем не застосовують автоматичну корекцію безпеки від постачальників, а також не конфігурують свої системи надійно, часто просто використовуючи конфігурацію за замовчуванням прямо з поля. Недостатньо захищені комп’ютери в університетах, компаніях будь-яких розмірів, урядових установах, будинках із постійним підключенням до Інтернету та інших місцях – легка здобич для зловмисника. Навіть низько кваліфіковані зловмисники можуть легко захопити сотні чи тисячі систем по всьому світу. Ці зловмисники використовують автоматизовані засоби сканування вразливості, включаючи доморощені сценарії та безкоштовні інструменти, такі як сканер незахищеності Nessus, серед багатьох інших, для сканування великих частот Інтернету. Вони без розбору сканують, день у день, шукаючи, щоб перейняти вразливі системи. Після взяття підходящої кількості систем, зловмисники будуть використовувати ці системи жертв, як частину розподіленої атаки

проти іншої цілі. Зловмисники адаптували багато класичних засобів комп'ютерної атаки до розповсюдженої парадигми.

Розподілена атака на відмову в обслуговуванні (з англ. DDoS – Distributed Denial of Service). Однією з найпопулярніших і широко застосовуваних методів розподіленої атаки є атака розподіленої відмови в обслуговуванні. Під час DDoS-атаки зловмисник переймає велику кількість систем і встановлює на кожну систему дистанційно керовану програму, яку називають зомбі. Зомбі мовчки бігають на задньому плані, очікуючи команд. Зловмисник контролює ці системи зомбі за допомогою спеціалізованої клієнтської програми, що працює на одній машині. Зловмисник використовує одну клієнтську машину для передачі команд безлічі зомбі, кажучи їм одночасно провести певні дії [1]. У DDoS-атаці найпоширенішою дією є затоплення жертви пакетами, коли всі зомбі одночасно запускають групи пакетів, машина жертви раптово виявиться заваленою псевдотрафіком. Після вичерпання всіх можливостей комунікаційного зв’язку жертви, жоден законний трафік користувача не зможе дістатися до системи, що призводить до відмови в обслуговуванні.

Розподілений злом пароля (з англ. Distributed Password Cracking). Злом паролів – ще одна методика, яка існує вже багато років, і зараз вона використовується в розповсюджених атаках. Метод заснований на тому, що більшість сучасних обчислювальних систем (наприклад, UNIX та Windows) мають базу даних, що містить зашифровані паролі, що використовуються для аутентифікації. У Windows паролі зберігаються в базі даних SAM. У системах UNIX паролі знаходяться у файлах / etc / passwd або / etc / shadow. Коли користувач входить у систему, машина запитує у користувача пароль, зашифровує введене користувачем значення і порівнює зашифровану версію того, що користувач ввів із збереженим зашифрованим паролем. Якщо вони ідентичні, користувачеві дозволяється входити в систему.

Ідея злому пароля проста: вкрасти зашифрований файл пароля, вгадати пароль, зашифрувати здогад і порівняти результат зі значенням у вкраденому

зашифрованому файлі пароля. Якщо зашифрований здогад відповідає шифрованому паролю, зловмисник визначив пароль. Якщо два значення не збігаються, зловмисник робить іншу здогадку. Оскільки паролі користувачів часто є передбачуваними комбінаціями ідентифікаторів користувачів, словникових слів та інших символів, ця методика дуже успішно визначає паролі.

Розподілене сканування портів (з англ. Distributed Port Scanning). Ще одна техніка атаки, яка добре піддається розподіленому підходу, – сканування портів. Порт є важливою концепцією протоколу управління передачею (з англ. TCP – Transmission Control Protocol) та протоколу користувальницьких пакетів (з англ. UDP – User Datagram Protocol), двох протоколів, якими користується переважна більшість Інтернет-служб. Кожен сервер, який отримує трафік TCP або UDP з мережі, прослуховує один або кілька портів. Ці порти – це як маленькі віртуальні двері на машині, куди пакети можуть зайти або вийти. Номери портів служать адресами в системі, куди слід спрямовувати пакети. Хоча адміністратор може налаштувати мережевий сервіс для прослуховування на будь-якому порті, найпоширеніші сервіси прослуховують на відомих портах, щоб клієнтське ПЗ знало, куди надсилати пакети. Веб-сервери зазвичай прослуховують порт TCP 80, а сервери електронної пошти – порт TCP 25. Сервери доменних імен (з англ. DNS – Domein Name Servers) слухають запити на порт UDP 53. Сотні інших портів призначені іншим різним служба.

Сканування портів – це процес надсилання пакетів до різних портів цільової системи, щоб визначити, які порти мають послуги прослуховування. Це схоже на стукіт у двері цільової системи, щоб побачити, які з них відкриті. Знаючи, які порти відкриті в цільовій системі, зловмисник має гарне уявлення про сервіси, що працюють на машині [25]. Потім зловмисник може сфокусувати атаку на службах, пов'язаних із цими відкритими портами. Крім того, кожен відкритий порт цільової системи вказує можливу точку входу для зловмисника. Зловмисник може сканувати апарат і визначити, що порт 25

TCP та порт 53 UDP відкриті. Цей результат повідомляє зловмиснику, що машина, імовірно, поштовий сервер і DNS-сервер. Хоча існує велика кількість традиційних інструментів сканування портів, одним з найпотужніших (на сьогоднішній день) є інструмент Nmap.

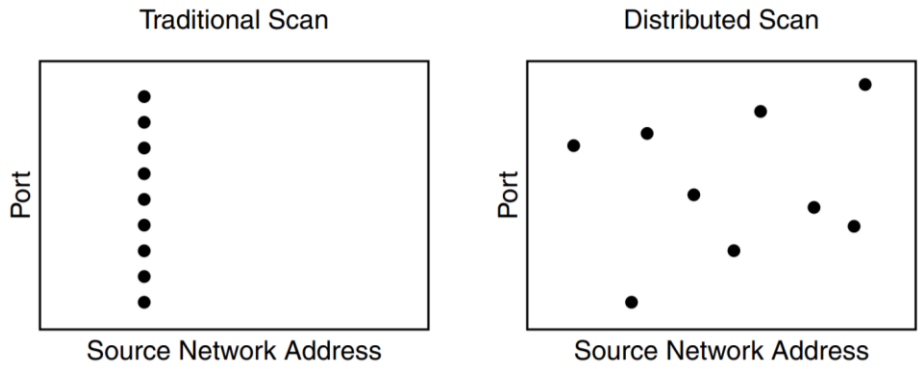

Рисунок 2.1 – Традиційне сканування (а) та розподілене сканування (б)

Оскільки сканування портів часто є попередником більш глибокої атаки, співробітники служби безпеки часто використовують інструменти IDS для виявлення сканування портів як показника раннього попередження. Більшість IDS включають конкретні можливості розпізнавання сканування портів. Якщо пакет надходить з даного джерела, який переходить до одного порту, а потім інший пакет з того ж джерела, який переходить до іншого порту, а потім ще один пакет для іншого порту, IDS може швидко віднести ці пакети до виявлення сканування. Ця схема трафіку показана на лівій частині рисунка 2.1 (а), де номери портів побудовані відповідно до мережевої адреси джерела. IDSs можуть легко помітити таке сканування, та сповістити адміністратора.

Атаки повторного відтворення (з англ. Relay Attacks). Кінцева методика такої атаки передбачає передачу інформації від одного обладнання до іншого через Інтернет, щоб приховати істинне джерело нападу. Встановлюючи додаткові оманливі шляхи між зловмисником та ціллю, нападник може уникнути затримання. Припустимо, зловмисник може взяти під контроль

шість машин, які мають доступ до Інтернету, розташованих по всьому світу, і хоче атакувати нову систему. Зловмисник може налаштувати програми перенаправлення пакетів на шість систем. Перша машина буде пересилати будь-які пакети, отримані на даному порту, до другої системи. Потім друга система пересилатиме їх до третьої системи і т.д., для досягнення нової мети. Кожна система виступає етапом у ланцюзі ретрансляції для руху трафіку. Якщо, і коли буде виявлено напад, адміністраторам доведеться простежити атаку назад через кожну точку ланцюга ретрансляції, перш ніж знайти зловмисника.

Зловмисники часто встановлюють ланцюги ретрансляції, що складаються з численних систем по всьому світу. Крім того, для подальшого приховування своїх адрес, зловмисники часто намагаються переконатися, що між країнами, де містяться їх канали передачі даних, наявні значні розбіжності людської мови та геополітичних відносин. Наприклад, перша ретрансляція може бути у США, а друга – у Китаї, третя може бути в Індії, а четверта – у Пакистані. Нарешті, ланцюг закінчується в Ірані для нападу на систему, а потім по тій же схемі прямує назад у США вже з результатом. На кожному етапі ланцюга ретрансляції адміністраторам з безпеки доведеться боротися з різкими змінами в людській мові, менш дружніми відносинами між країнами та величезними питаннями правоохоронної юрисдикції.

Атаки повторного відтворення часто реалізуються за допомогою дуже гнучкого інструменту під назвою Netcat, який доступний для UNIX та Windows. Іншим популярним інструментом являється Redir.

Активний сніфінг (з англ. Sniffing – нюхати). Сніфінг – це ще одна не нова техніка, яка швидко удосконалюється новими можливостями. Традиційні сніфери – прості інструменти, які збирають (перехоплюють) і аналізують мережевий трафік. Користувач встановлює програму Sniffer на комп'ютер, яка фіксує всі дані, що проходять через мережевий інтерфейс комп'ютера, незалежно від того, призначений він для цієї машини чи іншої системи [29, 30]. При використанні мережевими адміністраторами – сніфери

можуть захоплювати помилкові пакети, щоб допомогти усунути несправності в мережі. Якщо вони використовуються зловмисниками, сніфери можуть захоплювати конфіденційні дані з мережі, наприклад паролі, файли, дані електронної пошти чи будь-що інше, що передається мережею.

Традиційний сніфінг. Традиційні засоби сніфінгу пасивні; вони терпляче чекають, поки трафік пройде в мережу та збирають дані, коли він надходить. Ця пасивна методика добре працює для деяких типів мереж. Традиційний Ethernet – популярна технологія, що використовується для створення великої кількості локальних мереж (з англ. LAN – local area networks) – це широкосмугове середовище. Ethernet-концентратори – це пристрої, що використовуються для створення традиційних локальних мереж Ethernet. Увесь трафік, відправлений до будь-якої однієї системи в локальній мережі, транслюється на всі машини в локальній мережі. Традиційний сніфер може обробляти будь-які дані, що надходять між іншими системами в тій самій локальній мережі. У традиційній сніфер-атаці зловмисник переймає одну систему в локальній мережі, встановлює сніфер і збирає трафік, призначений для інших машин у тій самій локальній мережі. Одні з найкращих традиційних сніферів включають програми Snort та Snffit.

Активний сніфінг. Хоча засоби захисту від пасивних сніферів ефективні та практичні у використанні, зловмисники розробили різноманітні методики їх уникання. Тому були створені методи, відомі як активний сніфінг, які передбачають введення трафіку в мережу, щоб зловмисник міг захопити дані, які в іншому випадку повинні бути нерозбірливими. Однією з найдієвіших програм активного сніфінгу є Dsniff. Можна вивчити різні методи Dsniff для сніфінгу, вводячи трафік в мережу, включаючи перевантаження MAC-адреси, псевдотрафік ARP, фейкові відповіді DNS та атаки «людина по середині» (person-in-the-middle) на SSL.

Перевантаження MAC-адреси. Комутатор Ethernet визначає, куди надсилати трафік по локальній мережі на основі адреси управління доступом (з англ. MAC – Media Access Control). MAC-адреса – це унікальне 48-бітове

число, присвоєне кожній комунікаційній платі у світі. MAC-адреса вказує на унікальне обладнання мережевого інтерфейсу для кожної системи, підключеної до локальної мережі. Комутатор Ethernet відстежує трафік в локальній мережі, щоб дізнатися, які роз’єми на комутаторі пов'язані з якими MAC-адресами. Наприклад, комутатор побачить трафік, що надходить з MAC-адреси AA:BB:CC:DD:EE:FF на роз’єм номер один. Комутатор запам'ятає цю інформацію та надсилатиме дані, призначені для цієї MAC-адреси лише до першого роз’єму на комутаторі. Аналогічно, комутатор автоматично визначатиме MAC-адреси, пов'язані з іншими мережевими інтерфейсами в локальній мережі, і надсилає їм відповідні дані.

Один з найпростіших, активних методів сніфінгу полягає в перевантаженні локальної мережі трафіком, який має помилкові MAC-адреси. Зловмисник використовує програму, яка встановлена на машині в локальній мережі для генерації пакетів з випадковими MAC-адресами та подачі їх у комутатор. Комутатор намагатиметься запам'ятати всі MAC-адреси під час їх надходження. Урешті-решт, ємність пам'яті комутатора буде вичерпана хибними MAC-адресами. Коли їх пам'ять заповнюється, деякі комутатори переходять у режим, коли трафік направляється на всі машини, підключені до локальної мережі. Таким чином, використовуючи перевантаження MAC-адресами, зловмисник може бомбардувати комутатор, щоб комутатор передавав увесь трафік на всі машини в локальній мережі. Потім зловмисник може використовувати традиційний сніфінг, щоб захопити дані з локальної мережі.

Псевдотрафік ARP (з англ. Address Resolution Protocol – протокол визначення адреси). Хоча деякі комутатори виходять з ладу під потоком MAC-адрес в режимі, коли вони пересилають увесь трафік до всіх систем в локальній мережі, інші комутатори цього не роблять. Під час перевантаження ці комутатори запам'ятовують початковий набір MAC-адрес, які були автоматично виявлені в локальній мережі, і використовують ці адреси протягом усієї тривалості перевантаження. Зловмисник не може запустити

перевантаження MAC-адресами, щоб перекрити комутатор. Однак, зловмисник все ще може підірвати таку локальну мережу, вводячи інший тип трафіку на основі протоколу визначення адреси (ARP).

ARP використовується для співставлення IP адрес (Internet Protocol) з MAC-адресами в локальній мережі. Коли одна машина має дані для передачі в іншу систему в локальній мережі, вона формує пакет з IP-адресою призначення; однак IP-адреса – це лише налаштування конфігурації на машині призначення. Машина, що відправляє пакет, визначає, до якого апаратного пристрою в локальній мережі надсилати пакет за допомогою ARP. Припустимо, машина в локальній мережі має пакет, призначений для IP-адреси 10.1.2.3. Машина з пакетом відправить запит ARP по локальній мережі, запитуючи, який мережевий інтерфейс пов'язаний з IP-адресою 10.1.2.3. Машина з цією IP-адресою передасть відповідь ARP, кажучи, по суті, «IP-адреса 10.1.2.3 пов'язана з MAC-адресою AA:BB:CC:DD:EE:FF». Коли система отримує відповідь ARP, вона зберігає відображення IP-адреси на MAC-адресу в локальній таблиці, так званій таблиці ARP, для подальшого використання. Потім пакет буде доставлений до мережевого інтерфейсу з цією MAC-адресою. Таким чином, ARP використовується для перетворення IP-адрес у MAC-адреси, щоб пакети могли бути доставлені у відповідний мережевий інтерфейс в локальній мережі. Результати зберігаються в таблиці ARP системи, щоб мінімізувати потребу в додатковому ARP-трафіку в локальній мережі.

ARP включає підтримку можливості, яка називається «безоплатний ARP». За допомогою безоплатного ARP машина може надсилати відповідь ARP, хоча жодна машина не надсилає запит ARP. Більшість систем потребують записів ARP у своїх таблицях ARP, щоб покращити продуктивність в локальній мережі. У іншій формі активного сніфінгу зловмисник використовує підроблені безкоштовні ARP-повідомлення для перенаправлення трафіку для сніфінгу комутаторів локальної мережі, як

показано на рисунку 2.2. Для більшої візуалізації машина нападника в локальній мережі позначається чорною шапочкою.

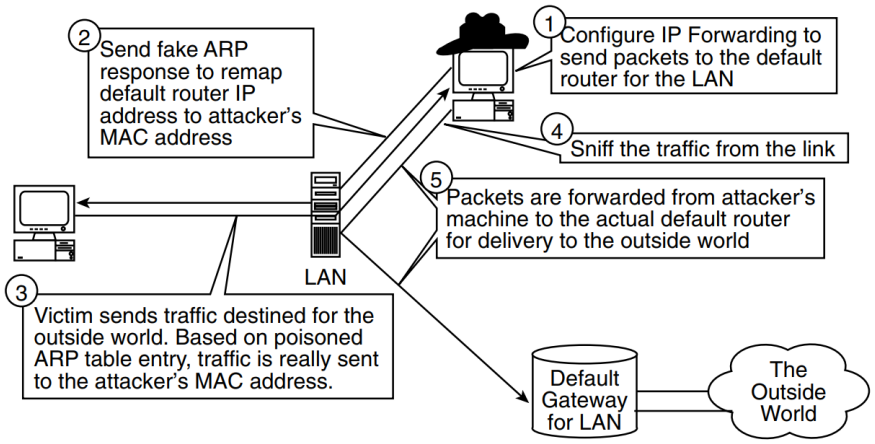

Рисунок 2.2 – Активний сніфінг у комутованому середовищі за допомогою безкоштовних ARP-повідомлень

Етапами атаки, показаної на рисунку 2.2 являються:

1. Зловмисник активує переадресацію IP-адреси на машині зловмисника в локальній мережі. Будь-які пакети, спрямовані комутатором на машину з чорною шапкою, будуть перенаправлені на маршрутизатор за замовчуванням для локальної мережі.

2. Зловмисник відправляє безоплатно ARP-повідомлення на цільову машину. Зловмисник хоче сніфінгувати трафік, відправлений з цієї машини у зовнішню мережу. Безкоштовне повідомлення ARP відобразить IP-адресу маршрутизатора за замовчуванням для локальної мережі на MAC-адресу власної машини зловмисника. Цільова машина приймає це помилкове ARP-повідомлення і вводить його в свою таблицю ARP. У таблиці ARP мішені з'являється помилковий запис.

3. Цільова машина відправляє трафік, призначений для зовнішньої мережі. Він звертається до таблиці ARP, щоб визначити MAC-адресу, пов'язану з маршрутизатором за замовчуванням для локальної мережі. MAC-

адреса, яку він знаходить у таблиці ARP, є адресою зловмисника. Усі дані про зовнішню мережу надсилаються на машину зловмисника.

4. Зловмисник сніфінгує трафік лінії зв’язку.

5. Переадресація IP, активована на кроці 1, переспрямовує весь трафік з машини зловмисника до маршрутизатора за замовчуванням для локальної мережі. Маршрутизатор за замовчуванням пересилає трафік у зовнішню мережу. Таким чином, жертва зможе направляти трафік у навколишню мережу, але він пройде через машину зловмисника, щоб її проаналізували на виході.

Ця послідовність кроків дозволяє зловмиснику переглядати весь трафік до зовнішньої мережі для цільової системи (мішень). Зауважимо, що для цієї методики зловмисник зовсім не модифікує комутатор. Зловмисник здатний аналізувати комутовану локальну мережу, маніпулюючи таблицею ARP жертви. Оскільки трафік ARP та пов’язана з ним MAC-адреса передаються лише через локальну мережу, ця методика працює лише в тому випадку, якщо зловмисник керує машиною в тій самій локальній мережі, що і цільова система.

Фейкові відповіді DNS. Методика введення пакетів у мережу для сніфінгу трафіку за межами локальної мережі включає маніпулювання системою доменних імен (з англ. DNS – Domain Name System). У той час, як ARP використовується в локальній мережі для зіставлення IP-адрес на MAC-адреси в локальній мережі, DNS використовується в мережі для зіставлення доменних імен та IP-адреси. Коли користувач вводить доменне ім’я в якесь ПЗ клієнта, наприклад, введення www.skoudisstuff.com у веб-браузер, система користувача надсилає запит на DNS сервер.DNS сервер зазвичай розташований по всій мережі в іншій локальній мережі. Після отримання запиту DNS сервер шукає відповідну інформацію у своїх конфігураційних файлах та надсилає відповідь DNS на машину користувача, що включає IP-адресу, наприклад, 10.22.12.41. DNS сервер відображає ім'я домену IP-адреси для користувача.

Зловмисники можуть перенаправляти трафік, надсилаючи клієнту хибні відповіді DNS. Зловмисник, який сидить у будь-якій мережі між цільовою системою та сервером DNS, може аналізувати запити DNS по лінії зв’язку. Побачивши запит DNS від клієнта, зловмисник може надіслати клієнту підроблену відповідь DNS, що містить IP-адресу машини зловмисника. Клієнтське ПЗ на машині користувача надсилатиме пакети на цю IP-адресу, думаючи, що вона спілкується з потрібним сервером. Натомість, інформація надсилається на машину зловмисника. Зловмисник може переглядати інформацію, використовуючи традиційний сніфер, і перенаправляти трафік за призначенням.

Атака «людина по середині» (з англ. Person-in-the-Middle) на SSL. Введення підроблених DNS відповідей у мережу є особливо потужною технікою, коли вона використовується для налаштування атаки «людина по середині» на криптографічні протоколи, такі як SSL, які зазвичай використовується для безпечного доступу до Інтернету. По суті, зловмисник відправляє фейкову відповідь DNS на мішень, щоб через якийсь період часу машини зловмисника встановлювали нову сесію SSL. Як зазначено на рис. 2.3, зловмисник використовує спеціалізований інструмент ретрансляції для встановлення двох криптографічних сесій: одну між клієнтом та зловмисником, а іншу між зловмисником та сервером. Поки дані переміщуються між цими сесіями, зловмисник може переглядати їх чітким текстом.

Етапи, показані на рисунку 2.3, включають:

1. Зловмисник активує програму для відмови Dsniff – інструмент, який надсилає фейкові відповіді DNS. Крім того, зловмисник активує інший інструмент Dsniff під назвою webmitm, скорочення для Web Monkey-in-Middle. Цей інструмент реалізує спеціалізоване відтворення SSL.

2. Зловмисник спостерігає за запитом DNS з машини жертви та надсилає помилкову відповідь DNS. Підроблена відповідь DNS містить IP-адресу машини зловмисника.

3. Користувач отримує відповідь DNS і встановлює сесію SSL з IP-адресою, включеною у відповіді.

4. Інструмент webmitm, що працює на машині зловмисника, встановив сесію SSL з машиною користувача та ще один сеанс SSL з фактичним веб-сервером, до якого клієнт хоче отримати доступ.

5. Користувач надсилає дані через з'єднання SSL. Інструмент webmitm розшифровує трафік із з'єднання SSL з жертвою, відображає його для зловмисника та шифрує трафік для транзиту на зовнішній веб-сервер. Зовнішній веб-сервер отримує трафік, не усвідомлюючи, що відбувається атака «людина по середині».

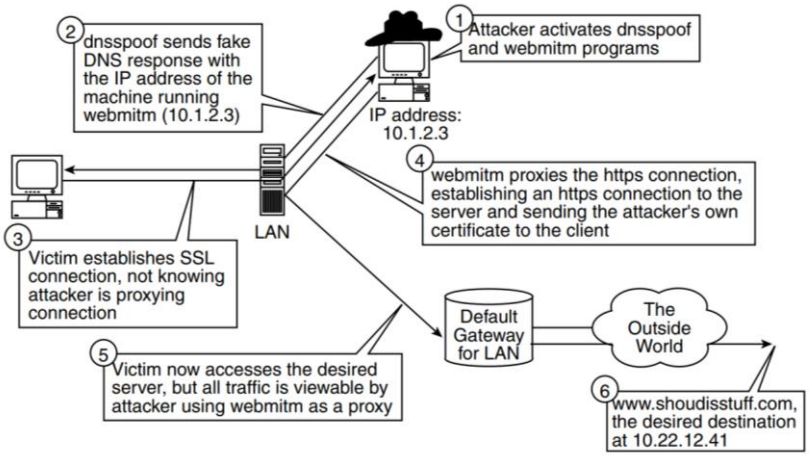

Рисунок 2.3 – Введення відповідей DNS для переадресації та захоплення трафіку SSL

RootKits на рівні ядра (з англ. Kernel-Level RootKits). Подібно до того, як зловмисники націлюються на ключові протоколи, такі як ARP та DNS, на дуже фундаментальному рівні, вони також експлуатують ядра операційних систем. Зокрема, велика розробка ведеться на рівні ядра RootKits. Щоб краще зрозуміти RootKits на рівні ядра, спершу слід проаналізувати їх еволюційних предків, традиційних RootKits.

Традиційні RootKits. Традиційний RootKit – це набір інструментів, який дозволяє зловмиснику підтримувати суперкористувацький доступ

(обліковий записв ОС, який дозволяє користувачу виконувати всі операції, без обмежень) до системи. Як тільки зловмисник отримує контроль на кореневому рівні машини, RootKit дозволяє зловмиснику підтримувати цей доступ. Традиційні RootKits, як правило, вимикають інструменти системи захисту, створюючи «чорний хід», щоб зловмисник мав доступ до системи, минаючи звичайні засоби безпеки. Вони також включають різні програми, щоб зловмисник ховався в системі, щоб приховати сліди активності зловмисника або інших загроз. Одні з найбільш повнофункціональних традиційних RootKits включають Linux RootKit 5 (lrk5), який працює на Solaris та Linux.

Традиційні RootKits реалізують через «чорний хід» та приховують механізми, замінюючи критично важливі програми, що входять до операційної системи. Наприклад, більшість традиційних RootKits включає заміну програми /bin/login, яка використовується для аутентифікації користувачів, які входять у систему UNIX. Версія RootKits /bin/login, як правило, включає в себе зворотний пароль, відомий зловмиснику, який може бути використаний для доступу до кореневого рівня (каталогу) машини. Зловмисник запише нову версію /bin/login, змінить часові позначки та розмір файлу відповідно до попередньої версії.

Так само, як програма /bin/login замінена на реалізацію «чорного ходу», більшість RootKits включає програми заміни троянських коней для інших UNIX інструментів, які використовуються системними адміністраторами для аналізу системи. Багато традиційних RootKits включають в себе замінники троянських коней для команди «Is» (яка зазвичай показує вміст каталогу). Змінені версії «Is» приховують інструменти зловмисника, ніколи не показуючи їх присутності. Аналогічно, зловмисники замінять netstat – інструмент, який показує, які порти TCP та UDP використовуються, з модифікованою версією, що лежить через порти, які використовує зловмисник. Так само буде замінено багато інших системних програм, включаючи ifconfig, du та ps. Усі ці програми діють як очі та вуха системного

адміністратора. Зловмисник використовує традиційний RootKit для заміни цих очей та вух новими версіями, які приховують присутність зловмисника в системі.

Щоб виявити традиційні RootKits, багато системних адміністраторів використовують засоби перевірки цілісності файлової системи, такі як програма Tripwire. Ці інструменти обчислюють криптографічно сильні хеші критично важливих системних файлів (таких як /bin/login, ls, netstat, ifconfig, du та ps) і зберігають ці цифрові ідентифікатори файлів на безпечному носії, наприклад, на флешці, дискеті. Потім, періодично (зазвичай щодня або щотижня), інструмент перевірки цілісності перераховує хеші виконуваних файлів у системі та порівнює їх із збереженими значеннями. Якщо є зміни, тобто програма була змінена, то системний адміністратор оповіщений.

RootKits на рівні ядра. У той час, як традиційні RootKits замінюють важливі виконуючі програми або файли, зловмисники пішли ще далі, впровадивши RootKits на рівні ядра. Ядро є серцем більшості операційних систем, що контролює доступ до всіх ресурсів, таких як жорсткий диск, системний процесор та пам'ять. RootKits рівня ядра змінюють саме ядро, а не маніпулюють програмами на рівні додатків, як традиційні RootKits. Як показано на лівій частині рис. 2.4, традиційний RootKit можна виявити, оскільки інструмент цілісності файлової системи, такий як Tripwire, може розраховувати на ядро, щоб воно могло перевірити цілісність прикладних програм. Коли програми модифікуються, «правдива програма» Tripwire використовує «правдиве ядро» для виявлення програм заміни троянських коней.

RootKit на рівні ядра показано на правій частині рисунка 2.4. Незважаючи на те, що всі прикладні програми недоторкані, саме ядро пошкоджено, полегшуючи зловмиснику доступ до всієї системи, тим самим даючи адміністратору хибні твердження про присутність зловмисника в системі.

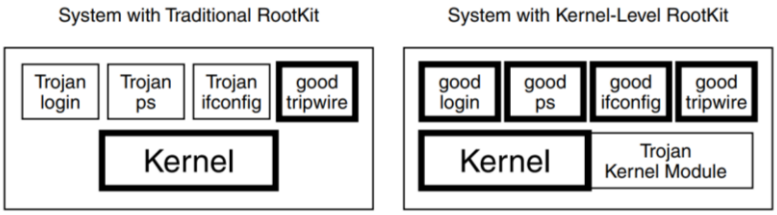

Рисунок 2.4 – Традиційний RootKit та RootKit на рівні ядра

Хоча було випущено велику кількість RootKits на рівні ядра з різноманітними функціями, найпопулярніші можливості цих інструментів включають:

1. Перенаправлення на виконання. Ця можливість перехоплює виклик для запуску певної програми/додатку або файла, які вимагають запустити іншу програму, яку обирає зловмисник. Розглянемо сценарій, що включає UNIX /bin /логін. Зловмисник встановить RootKit на рівні ядра і залишить файл /bin /login без змін. Усі запити на виконання /bin/login (які виникають, коли хтось увійде в систему) буде відображено у прихованому файлі /bin/backdoorlogin. Коли користувач намагається увійти в систему, буде виконана програма /bin/ backdoorlogin, що містить пароль «backdoor», який дозволяє отримати доступ до кореневого рівня системи. Однак, коли системний адміністратор запускає перевірку цілісності файлів, наприклад Tripwire, аналізується стандартна процедура /bin/login. Перенаправляється лише виконання; можна переглянути оригінальний файл /bin/login та перевірити його цілісність. Цей оригінальний файла не змінюється, тому хеш Tripwire залишиться тим самим.

2. Приховування файлів. Багато RootKits рівня ядра дозволяють зловмиснику приховати будь-який файл у файловій системі. Якщо будь-який користувач або додаток шукає файл, ядро дасть хибну відповідь і відповість, що файл відсутній на машині. Звичайно, файл все ще знаходиться в системі, і зловмисник може отримати доступ до нього за потреби.

3. Приховування процесів. Крім приховування файлів, зловмисник може використовувати RootKit на рівні ядра, щоб приховати запущений процес на машині.

Кожна з цих можливостей досить потужна сама по собі. У сукупності вони пропонують зловмиснику можливість повністю трансформувати машину/обладнання/пристрій на ті запити, які бажані для нападника. Системний адміністратор матиме вигляд системи, створеної зловмисником, і все виглядатиме недоторканим. Але насправді система буде неправдивою та хибною в цілому. Крім того, виявити RootKits на рівні ядра часто досить важко, оскільки весь доступ до системи покладається на змінене зловмисником ядро.

2.2 Методи протидії атакам, які є значними загрозами для телекомунікаційних мереж, за допомогою контролю доступу

Гонка озброєнь між безпекою телекомунікаційного середовища та комп'ютерними зловмисниками набирає обертів. Оскільки зловмисники розробляють методи для широко розповсюджених атак та заглиблюються в протоколи та операційні системи, потрібно старанно працювати над захистом систем. Адже ретельно проектуючи та підтримуючи системи, можна підтримувати безпечну інфраструктуру.

Захист проти розподілених атак на відмову в обслуговуванні. Для захисту від будь-якого надлишкового трафіку пакетів, включаючи DDoS-атаки, необхідно забезпечити, щоб критичні мережеві з'єднання мали достатню пропускну здатність і надлишковість для усунення простих атак. Якщо підключення до мережі є критично важливим, слід мати принаймні резервне з’єднання, оскільки зловмисник може легко заповнити всі нижчі швидкості з'єднання [12].

Хоча ця базова смуга пропускної здатності усуває найнижчі рівні зловмисників, але слід бути готовим до того, що не вдасться придбати

достатню пропускну здатність, щоб не відставати від зловмисників, які встановили зомбі на сто чи тисячі систем і вказали на вашу систему, як цільову. Якщо доступність системи в Інтернеті є критично важливою для бізнесу, потрібно використовувати додаткові методи для обробки DDoS-атак. З технологічної точки зору, можливо, варто розглянути інструменти для формування трафіку, які допоможуть керувати кількістю вхідних сеансів, щоб сервери не перевантажувались. Звичайно, достатньо великий кадр зомбі, що переповнює зв'язок, може навіть пригнічувати формувачів трафіка. Тому слід використовувати системи виявлення вторгнень (з англ. IDSs - Intrusion Detection Systems), щоб визначити, коли відбувається напад. Ці ідентифікатори виконують функцію мережевої сигналізації про взломи, аналізуючи мережу для руху трафіку, який відповідає загальним принципам атак, що зберігаються в базі даних IDSs. З процедурної точки зору, для таких сигналів від IDSs, слід очікувати, що команда реагує на інциденти. Для критичних підключень до Інтернету необхідно мати номер мобільного телефону для власної команди реагування на інциденти. Коли запускається DDoS-атака, команда реагування на інциденти повинна бути в змозі швидко та ефективно розмежувати сили команди реагування на інциденти провайдера. Після оповіщення, провайдер може розгорнути фільтри у своїй мережі для блокування активної DDoS-атаки.

Захист від розподіленого злому пароля. Захист від розподіленого злому паролів насправді такий же, як і для традиційного злому пароля: усування слабких паролів із систем. Оскільки розподілений злом паролів прискорює процес злому, паролі повинні бути навіть складніші для здогадок. Потрібно розпочати з політики, яка зобов'язує користувачів встановлювати паролі, не менші за мінімальну довжину (наприклад, більше дев'яти символів) і включати цифри, літери та спеціальні символи у кожен пароль. Користувачі повинні знати про політику; таким чином, ключовою є програма обізнаності, що підкреслює важливість того, що чим важчий пароль, тим складніше його здогадатися. Крім того, щоб допомогти застосувати політику паролів,

можливо, потрібно розгорнути інструменти фільтрації паролів на серверах аутентифікації. Коли користувач встановлює новий пароль, ці інструменти перевіряють пароль, щоб переконатися, що він відповідає політиці щодо паролів. Якщо пароль занадто короткий або не включає цифри, літери та спеціальні символи, користувачеві буде запропоновано вибрати інший пароль [11]. Програма passfilt.dll, що входить у комплект ресурсів Windows NT, та програма passwd+ в системах UNIX реалізують цей тип функцій, як і кілька сторонніх додаткових продуктів аутентифікації. Можна також розглянути питання про видалення стандартних паролів із дуже чутливих середовищ, використовуючи технології доступу на основі токена (генератор одноразових паролів в системах аутентифікації).

Нарешті, адміністратори служби безпеки повинні періодично застосовувати інструмент для розбиття паролів проти паролів власних користувачів, щоб ідентифікувати слабкі, перш ніж це зробить зловмисник. Коли виявляються слабкі паролі, повинен бути визначений і затверджений процес інформування користувачів про те, що вони повинні вибрати кращий пароль. Обов'язково потрібно отримати відповідні дозволи перед тим, як проводити внутрішні проекти розподілу паролів, щоб гарантувати, що керівництво розуміє та підтримує цю важливу програму безпеки. Якщо не отримати схвалення керівництва, це може негативно вплинути на кар’єру.

Захист від розподіленого сканування. Найкращий захист від розподіленого сканування портів – це вимкнення всіх непотрібних служб у своїх системах. Якщо єдиною метою обладнання є запуск веб-сервера, який обмінюється даними через HTTP і HTTPS, у системі повинні бути відкриті лише порт 80 TCP і порт 443 TCP. Якщо не потрібен поштовий сервер, який працює на тому ж пристрої, що і веб-сервер, слід налаштувати систему так, щоб поштовий сервер було вимкнено. Якщо система Windows на машині не потрібна, вимкніть її. Слід розробити захищений конфігураційний документ, який забезпечує покроковий процес для всіх системних адміністраторів організації зі створення захищених серверів [9].

Крім того, необхідно забезпечити постійне оновлення IDS зондів. Більшість постачальників IDS регулярно поширюють нові ознаки атак – зазвичай раз на місяць. Коли є новий набір ідентифікаторів атаки, слід швидко перевірити його та розгорнути його на зондах IDS, щоб вони могли виявити останню групу атак.

Захист від атак повторного відтворення. Оскільки основна частина дій в даній атаці відбувається поза власною мережею організації, мало що можна зробити, щоб запобігти подібним атакам. Насправді не можна зупинити зловмисників від переспрямування своїх пакетів через купу машин перед атакою. Найкращою тактикою для забезпення безпеки систем являється автоматичне застосування резервних з'єднань безпеки та вимкнення всіх непотрібних сервісів. Крім того, важливо співпрацювати з представниками правоохоронних органів у розслідуванні таких нападів.

Одним з часто використовуваних засобів захисту від традиційних сніферів є комутаційна локальна мережа. На відміну від концентратора Ethernet, який виконує функцію трансляції, комутатор Ethernet передає дані лише за призначенням у локальній мережі. Жодна інша система в локальній мережі не може бачити дані, оскільки комутатор Ethernet надсилає дані до відповідного місця призначення і нікуди більше. Ще однією широко застосовуваною технікою, щоб завадити традиційним сніферам являється шифрування даних у момент передачі. Якщо у зловмисників немає ключів шифрування, вони не зможуть визначити вміст даних, які дістали з мережі. Два найпопулярніші протоколи шифрування – це рівень захищених сокетів (з англ. SSL – Secure Sockets Layer), який найчастіше використовується для захисту веб-трафіку, і захисна оболонка (з англ. SSH - Secure Shell), це протокол, який найчастіше використовується для захисту доступу до інших мережевих протоколів [24].

Захист від методів активного сніфінгу. Побачивши, як зловмисник може захопити всіляку корисну інформацію з мережі за допомогою аналізуючих інструментів, як можна захищатись від цих атак? По-перше,

коли це можливо, потрібно шифрувати дані, які передаються через мережу та використовувати захищені протоколи, такі як SSL для веб-трафіку, SSH для зашифрованих сесій входу та передачі файлів. Користувачі повинні мати можливість застосовувати ці засоби для захисту конфіденційної інформації, як з точки зору технології, так і з точки зору обізнаності.

Особливо важливо, щоб системні адміністратори, менеджери мережі та персонал безпеки розуміли та використовували захищені протоколи для ведення своїх робочих дій. Не надсилайте будь-яку конфіденційну інформацію через мережу, використовуючи сесію SSL, створену з ненадійним сертифікатом. Якщо SSH-клієнт попереджає, що загальнодоступний ключ сервера таємничо змінився, потрібно перевірити.

Крім того, слід дійсно розглянути можливість позбутися від концентраторів, оскільки їх просто занадто легко пронюхати. Хоча вартість може бути вищою за концентратори, комутатори не тільки покращують безпеку, але й покращують продуктивність. Якщо повна міграція в комутовану мережу неможлива, принаймні, слід розглянути можливість використання комутованої Ethernet.

А для мереж, що містять дуже чутливі системи та дані, слід увімкнути захист на портах комутаторів на рівні порту, конфігурувавши кожен порт комутатора з конкретною MAC-адресою машини, використовуючи цей порт, щоб запобігти проблемам із перевантаженням MAC та фейковими повідомленнями ARP. Крім того, для надзвичайно чутливих мереж потрібно використовувати статичні таблиці ARP на кінцевих машинах, жорстко кодуючи MAC-адреси для всіх систем в локальній мережі. Захист порту на комутаторах і жорстко кодованих таблицях ARP може бути дуже важким для управління, оскільки для заміни компонентів або навіть комутуючих плат Ethernet потрібно оновити MAC-адреси, що зберігаються в декількох системах. Для дуже чутливих мереж цей рівень безпеки необхідний і повинен бути реалізований.

Захист від RootKit на рівні ядра. Щоб зупинити установку RootKits на рівні ядра (або традиційних RootKits) потрібно перешкоджати зловмисникам отримувати доступ до суперкористувацького режиму в своїх системах. Без доступу суперкористувача зловмисник не може встановити RootKit на рівні ядра. Потрібно надійно налаштувати системи, вимкнувши всі непотрібні служби та застосувавши всі резервні (тимчасові) засоби безпеки. Системи підсилення безпеки та збереження резервних засобів безпеки – найкращий запобіжний засіб для роботи з RootKits на рівні ядра.

Інший вихід включає використання ядер, які не підтримують завантажувані модулі ядра (з англ. LKMs – loadable kernel modules), особливість деяких операційних систем, яка дозволяє ядру динамічно змінюватися.

2.3 Соціальна інженерія як ризик, який є одним із методів порушення конфіденційності даних

Успіх атак соціальної інженерії зумовлений насамперед двома факторами: людською природою та бізнес середовищем.

Людська природа. Люди здебільшого довіряють та співпрацюють за своєю природою. У галузі соціальної психології вивчалася взаємодія людини, як у групах, так і індивідуально. Ці дослідження дійшли висновку, що майже будь-хто, хто мав би справу з кваліфікованим спеціалістом, який може впливати на те, щоб людина поводилася певним чином чи розголошувала інформацію, яку вона зазвичай не робила б за інших обставин. Ці дослідження також встановили, що люди, які перебувають мають владу, можуть легко залякати інших людей.

Здебільшого, соціальна інженерія має справу з індивідуальною динамікою на відміну від групової динаміки, оскільки основними цілями є служба підтримки та адміністративна чи технічна підтримка людей, та взаємодія зазвичай один на один, але не обов'язково віч-на-віч (тобто

стосунки зазвичай мають віртуальну природу, тобто або по телефону, або в Інтернеті). Зловмисники, як правило, шукають осіб, які виявляють ознаки сприйнятливості до цього психологічного нападу.

Бізнес середовище. У поєднанні з людською природою, поточна тенденція розвитку виробництва/бізнесу, їх об'єднань та поглинань, швидкий технологічний прогрес та розповсюдження мереж широкої сфери зробили бізнес середовище сприятливим для соціальної інженерії. У сьогоднішньому світі бізнесу рідкість ніколи не зустрічатися з людьми, з колегами/співробітниками спілкуються регулярно, у тому числі з власних організацій, не кажучи вже про постачальників, продавців та замовників. Взаємодія людини віч-на-віч стає все більш рідкісною із широким впровадженням телекомунікаційних технологій для працівників. На сьогоднішньому ринку можна працювати в організації та, крім кількох винятків, зрідка з’являтися в офісі. Незважаючи на цей рівень спілкування, який наявний із людьми в робочому середовищі, основна довіра до людей, у тому числі до тих, кого ніколи насправді не зустрічали, в основному, залишається неушкодженою, якщо співробітник впевнений, що спілкується з колегою.

Підприємства та організації сьогодні стали більш орієнтованими на обслуговування, ніж будь-коли раніше. Співробітників часто оцінюють, наскільки вони сприяють «командному» середовищу та рівню обслуговування, який вони надають клієнтам та іншим відділам.

Напрямки соціальної інженерії. Атаки в соціальній інженерії, як правило, дотримуються поетапного підходу, і в більшості випадків напади дуже схожі на чіткий план, який призведе до конкретної мети. Для простоти етапи можна класифікувати як [22, 23]:

– збір інформації;
– вибір цілі;
– напад.

Збір інформації. Однією із запорук успішної атаки соціальної інженерії є інформація. Напрочуд легко зібрати достатню інформацію про організацію та її персонал для того, щоб звучати як працівник компанії, представник продавця або, в деяких випадках, член регуляторного чи правоохоронного органу. Організації, як правило, розміщують надто багато інформації на своїх веб-сайтах, як частину своїх маркетингових стратегій. Ця інформація часто описує або дає підказки щодо постачальників, з якими вони мають справу, перераховує телефонні та електронні довідники та вказує, чи є філії та, якщо так, де вони знаходяться. Деякі організації навіть переглядають цілі організаційні схеми на своїх веб-сторінках. Уся ця інформація може бути приємною для потенційних інвесторів, але вона також може бути використана для того, щоб закласти основу для атаки соціальної інженерії.

Недостатньо продумані веб-сайти – не єдині джерела відкритого доступу до інформації. Те, що викидають організації, також може бути джерелом важливої інформації. Перебираючи сміття організації (відома атака під назвою «дайвінг у смітник» – з англ. dumpster diving), можна виявити рахунки-фактури, кореспонденцію, посібники тощо, які можуть допомогти зловмиснику отримати важливу інформацію. Кілька засуджених комп'ютерних злочинців зізналися у дайвінгу, щоб зібрати інформацію про свої цілі. Мета нападника на цьому етапі – дізнатися якомога більше інформації для того, щоб оперувати поняттями як законний співробітник, підрядник, продавець чи стратегічний партнер або, в деяких випадках, як офіційний правоохоронний орган.

Вибір цілі. Після того, як буде зібрано відповідний обсяг інформації, зловмисник шукає помітні недоліки у персоналі організації. Найпоширенішою ціллю є персонал служби технічної допомоги, системні та мережеві адміністратори, оскільки ці фахівці проходять підготовку для надання допомоги і зазвичай можуть змінювати паролі, створювати акаунти, повторно активувати акаунти тощо. У деяких організаціях функція служби підтримки передається третій стороні без реального зв'язку з фактичною

організацією. Це збільшує шанси на успіх, оскільки співробітник служби довідки зазвичай не знає жодного з працівників організації. Мета більшості зловмисників – або зібрати конфіденційну інформацію, або закріпитися в системі. Зловмисники розуміють, що як тільки вони мають доступ, навіть на рівні гостей, порівняно легко збільшити свої привілеї, запустити більш руйнівні атаки та приховати свої сліди.

Наступні найпоширеніші жертви – адміністративні помічники. Це багато в чому пов’язано з тим, що ці особи мають доступ до великої кількості конфіденційної інформації, яка зазвичай зберігає дані членів керівництва. Помічники адміністративних служб можуть використовуватися як точки нападу, або для збору додаткової інформації щодо імен впливових людей в організації. Також більшість адміністративних помічників знають паролі своїх керівників. Деякі з цих помічників регулярно виконують завдання для своїх керівників, які вимагають привілеїв керуючого облікового запису (наприклад, оновлення електронної таблиці, бронювання зустрічей в електронних календарях тощо).

Атаки. Фактично вони поділяються на три категорії: (1) атаки, які апелюють до самолюбства або егоїзму жертви (его-атаки), (2) атаки, які використовують переваги почуття симпатії чи співпереживання, (3) атаки, що ґрунтуються на залякуванні.

Его-атаки. При першому типі нападу – атака его – зловмисник звертається до деяких найбільш основних характеристик людини. Усім людям подобається, коли їх хвалять, кажуть, наскільки вони розумні і що вони дійсно знають як керувати підприємством. Зловмисники використовуватимуть це для отримання інформації від своїх жертв, оскільки зловмисник є сприйнятливою аудиторією для жертв, щоб показати, скільки знань вони мають. Зловмисник, як правило, вибирає жертву, яка відчуває себе недостатньо оціненою і працює на посаді, яка є нижчою за її здібності. Зловмисник зазвичай може це відчути лише після короткої розмови з особою. Часто зловмисники, які використовують цей тип нападу, дзвонять декільком

різним працівникам, поки вони не знайдуть потрібного. На жаль, у більшості випадків потерпілий не здогадується про те, що він чи вона зробила щось не так.

Атаки симпатії або співпереживання. У другій категорії нападів зловмисник, як правило, видає себе за співробітника (зазвичай нового співробітника), підрядника, нового продавця або стратегічного партнера, який потребує допомоги. Важливість інформаційної фази стає очевидною, оскільки зловмисникам доведеться створити певний рівень довіри у жертви, щоб жертва була впевненою, що має справу з тим, ким представився зловмисник. Це робиться шляхом назви імені жертви, використання відповідної лексики або демонстрації знань організації. Зловмисник робить вигляд, що він або вона поспішає і повинен виконати якесь завдання, яке вимагає доступу, але не може згадати логін або пароль облікового запису тощо. Почуття терміновості зазвичай є частиною сценарію, оскільки це є приводом для обходу необхідних процедур, які можуть бути застосовані для відновлення доступу, якщо зловмисник був справді особою, якою представився. Людська природа співчувати або співпереживати тому, хто потрапив у скрутне положення є успіхом для зловмисника; таким чином, у більшості випадків атаки задовольняються. Якщо зловмисник не зможе отримати доступ або інформацію від одного працівника, він вибере іншу жертву.

Атаки залякування. У третій категорії зловмисники прикидаються діячами влади, або впливовою особою в організації, або, в деяких задокументованих випадках, правоохоронними органами. Зловмисники обирають жертву на кілька рівнів в організації нижче рівня особи, якою вони прикидаються. Зловмисник створює правдоподібну причину для того, щоб зробити якийсь тип запиту про скидання пароля, зміну облікового запису, доступ до систем або конфіденційної інформації (у випадках, коли зловмисник представляються службовцем правоохоронного органу, сценарій,

як правило, обертається навколо якогось розслідування або питання національної безпеки, і працівник не повинен обговорювати інцидент).

Захист від соціальної інженерії. Щоб захистити себе від загрози соціальної інженерії, повинно бути базове розуміння інформаційної безпеки. Загалом, інформаційна безпека позначає стан, який компанія досягає, коли її дані та інформація, системи та послуги є належним чином захищеними від будь-якого типу загрози. Інформаційна безпека захищає інформацію від широкого спектру загроз, щоб забезпечити безперервність бізнесу, мінімізувати збитки для бізнесу та максимально повернути інвестиції та бізнес-можливості. Інформаційна безпека – це захист активів, іміджу та репутації бізнесу – а можливо, і саме його існування. Механізми/рівні захисту зазвичай поділяються на три категорії, і важливо зазначити, що для дієвого захисту активів інформаційної безпеки організації незалежно від типу загрози, включаючи атаки соціальної інженерії, потрібна комбінація всіх трьох [23, 25]. Цими рівнями захисту є:

– фізична безпека
– логічна (технічна) безпека
– адміністративна безпека

Фізична безпека. Компоненти фізичної безпеки – найпростіші для розуміння і, мабуть, найпростіші для реалізації. Більшість людей подумають про ключі, замки, тривогу та охорону, коли думають про фізичну безпеку. Хоча це аж ніяк не єдині запобіжні заходи, які потрібно враховувати під час захисту інформації, але вони є логічним початком. Фізична безпека, поряд з двома іншими (логічними та адміністративними), є життєво важливою складовою та основою для більшості рішень щодо інформаційної безпеки. Фізична безпека стосується захисту активів від крадіжок, вандалізму, катастроф, стихійних лих, навмисних чи випадкових пошкоджень, а також нестабільних умов навколишнього середовища, таких як електричні, температурні та інші подібні екологічні проблеми. Стійка фізична безпека вимагає ефективного будівництва будівель та споруд, готовності до

аварійних ситуацій, надійного електропостачання, надійного та прийнятного кліматичного контролю та ефективного захисту від внутрішніх і зовнішніх зловмисників.

Логічна (технічна) безпека. Логічні заходи безпеки – це ті, що використовують технічне рішення для захисту інформаційного активу. Наприклад, системи брандмауера, системи контролю доступу, системи паролів та системи виявлення вторгнень. Ці елементи управління можуть бути дуже ефективними, але, як правило, покладаються на людський фактор або взаємодію для успішної роботи. Як вже було сказано, саме цей людський фактор можна експлуатувати досить легко.

Адміністративна безпека. Контроль адміністративної безпеки зазвичай включає політику, процедури, рекомендації тощо. Приклади адміністративної безпеки включають політику інформаційної безпеки, програми обізнаності та попередню перевірку нових співробітників. Ці приклади мають адміністративний характер, не потребують логічного чи технічного рішення для реалізації, але всі вони стосуються питання захисту інформації.

2.4 Висновки з розділу 2

1. Проаналізовано загрози, які являються небезпечними для телекомунікаційної мережі, зокрема це: атаки відмови в обслуговуванні (DoS), зломщики паролів, сканери портів, Sniffers та RootKits, і визначено, що їх спільною метою є отримання або зміна даних користувачів чи всієї організації шляхом перевантаження мережі надлишковим трафіком, аналізуванням мережі, підбором паролів.

2. Описано методи протидії атакам, найкращими із них є використання локальної мережі, яка має надсилати дані лише до одного місця призначення; використання шифрування даних; використання систем виявлення вторгнень.

3. Зазначено декілька рекомендацій для того, щоб не стати жертвою зловмисників: потрібно використовувати оновлене програмне забезпечення, оскільки ідентифікатори шкідливого ПЗ постійно змінюються, також потрібно захищати обладнання телекомунікаційної мережі, тобто вмикати захист на портах комутаторів, а також слід мати хоча б одне резервне з’єднання.

4. Висвітлено проблему соціальної інженерії, як методу для отримання зловмисниками конфіденційних даним або злому телекомунікаційної мережі шляхом збору доступної інформації, а потім використання її для того, щоб отримати вищий рівень доступу до даних.

3 АНАЛІЗ ТА ТЕХНОЛОГІЧНЕ РІШЕННЯ МЕРЕЖЕВИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

3.1 Принцип роботи мережевих систем контролю доступу

Управління мережевим доступом (з англ. Network Access Control – NAC) забезпечує безпеку мережі, обмежуючи доступність мережевих ресурсів до пристроїв кінцевих точок на основі визначеної політики безпеки.

Процес NAC. Загальне рішення NAC спочатку виявляє пристрій кінцевої точки, підключений до мережі. Після виявлення пристрою сервер NAC ініціює процес аутентифікації та оцінки безпеки. Це може бути виконано або безпосередньо програмним агентом (управляюча система в моделі клієнт-сервер – частина системи, яка виконує підготовку інформації і її обмін між клієнтською та серверною частинами), встановленим на пристрої кінцевих точок, або опосередковано шляхом тестування відповідей пристрою кінцевої точки зовнішнім мережевим механізмом сканування. Якщо пристрій кінцевої точки відповідає визначеній політиці безпеки захищеної мережі, доступ пристрою кінцевої точки буде наданий відповідно до його призначення або ідентичності [14, 16].

Небезпечні пристрої кінцевих точок будуть виділені в карантинній зоні до моменту повторного введення в мережу та оцінки їх відповідності вимогам безпеки. Усунення порушень політики збереження конфіденційних даних в інформаційних системах може бути запропоновано рішенням NAC пристрою кінцевої точки, залежно від ризику зловмисної спроби доступу до мережі.

3.2 Порівняння моделей мережевих систем контролю доступу

Залежно від потрібного мережевого середовища, існує два типи (моделі) NAC-рішень, які засновані на агентах і без агентів, для здійснення управління мережевим доступом.

Модель NAC на основі агентів. Рішення NAC на основі агентів розгортає агент NAC на пристрої кінцевої точки. Агент NAC безпосередньо виконує перевірку безпеки та аутентифікацію на пристроях кінцевих точок та надає інформацію і результати оцінки серверу NAC для аутентифікації.

Приклад NAC на основі агентів – протокол 802.1X. Це протокол, визначений IEEE (з англ. Institute of Electrical and Electronics Engineers), для запобігання підключенню елементів до мережі до того, як їм буде призначена IP-адреса. Усі пристрої кінцевих точок, мережеві пристрої та застаріле обладнання повинні бути налаштовані на використання 802.1X.

Мережі 802.1X для роботи потрібні наступні три компоненти:

– Агент NAC – виступає стороною клієнта. Він завантажується на пристрій користувача та використовується для запиту доступу до мережі.

– Мережевий пристрій NAC – мережева інфраструктура, яка використовується для аутентифікації, наприклад, мережеві комутатори або точки бездротового доступу.

– Сервер NAC – отримує віддалений код аутентифікації в службі обслуговування користувачів (з англ. Remote Authentication Dial In User Service – RADIUS) і використовує його для перевірки облікових даних аутентифікації в базі даних.

Агент NAC на пристрої кінцевої точки представляє мережевий обліковий запис мережевого пристрою, сумісному з NAC. Мережевий пристрій передасть його серверу NAC, а сервер перевірить і підтвердить мережевий обліковий запис. Після перевірки, мережевий порт на мережевому пристрої, сумісному з NAC, буде відкритий та наданий користувачеві доступ до мережі.

Модель NAC без агентів. Інший тип рішення NAC не потребує встановлення постійного програмного агента на пристрої кінцевої точки. Інформація про пристрій кінцевої точки збирається за допомогою оцінки вразливості мережі або тимчасового програмного забезпечення, встановленого на пристрої кінцевої точки:

– мережевий NAC (використовуючи інструмент оцінки вразливості, такий як сканер вразливості, оцінку на пристрої кінцевої точки можна здійснити шляхом збору інформації, такої як відповіді пристрою кінцевої точки. Ця модель застосовується до традиційних кінцевих систем типу ПК, але особливо корисна для підтримки більш різноманітних середовищ кінцевих систем, де немає кінцевих систем, що базуються на користувачі, та кінцевих систем з нетрадиційними операційними системами).

– NAC на основі прикладних програм. Цей тип NAC схожий на рішення на основі агентів NAC. Замість постійного програмного агента, встановленого на пристрої кінцевої точки, на пристрій користувача кінцевої точки завантажується прикладна програма Java або роз'ємний програмний агент, під час доступу до веб-сторінки із захищеної мережі. Місцеве оцінювання проводиться тимчасовим агентом на пристрої кінцевої точки).

NAC дозволяє адміністраторам мережі автоматизувати виконання політики. Замість того, щоб вимагати, щоб користувачі забезпечували відповідність своїх пристроїв політиці проти зловмисного ПЗ, адміністратори можуть просто дозволити мережі виконувати цю роботу замість них. NAC пропонує чудовий спосіб контролю доступу до мережі за допомогою автоматизованого виконання політики та управління мережевою безпекою без великих адміністративних витрат.

Простіше кажучи, NAC дозволяє визначити комплексну політику безпеки для конкретної мережі, впровадити цю політику на централізованому сервері та змусити мережу автоматично застосовувати цю політику для всіх користувачів мережі. NAC – це набагато більше, ніж просто аутентифікація

користувача – він також розроблений для захисту мережі від користувачів та пристроїв, які можуть бути дозволені, але все ще створюють загрозу.

Найдоречніше місце для нього розташоване на кінцях мережі, запобігаючи загрозам безпеки, перш ніж вони отримають будь-яку форму доступу. Рішення NAC, що включає комутатори (switch), які виконують роль точок примусового виконання політики безпеки, забезпечує проактивний підхід до безпеки мережі.

3.3 Розгляд безпечної мережевої системи контролю доступу

Сьогодні доступ до мережі для декількох типів пристроїв або тимчасових користувачів – це очікування, а не помилка. Сучасні вимоги мережі включають:

– заданий рівень доступу, незалежно від того, «хто» чи «де» він знаходиться;

– доступ для гостей, таких як клієнти, партнери, віддалені працівники;

– контроль доступу для нового діапазону підключених пристроїв, наприклад смартфонів, планшетів та цифрових камер.

Локальні комутатори мають відповідати цим вимогам, повинні включати всебічні функції NAC та комплектацію: використання разом із відповідними програмними засобами на сторонах сервера та клієнта, забезпечення чудового рівня контролю за станом безпеки пристроїв, які підключаються до відповідної мережі. Реалізація NAC повинна бути заснована на стандартах довіреної обчислювальної групи, щоб гарантувати сумісність з основними сторонніми постачальниками програмного забезпечення NAC, наприклад, такими як Microsoft та Symantec. Це надаватиме клієнтам впевненість у створенні комплексного рішення NAC від надійних постачальників.

В основі використання NAC для безпечної мережі лежать три ключові елементи (рис. 3.1):

– відсутність (або обмеженість) доступу без авторизації;

– карантин та відновлення (виправлення) непідтримуваних пристроїв;

– встановлення рівня доступу до мережевих ресурсів на основі авторизованого пристрою.

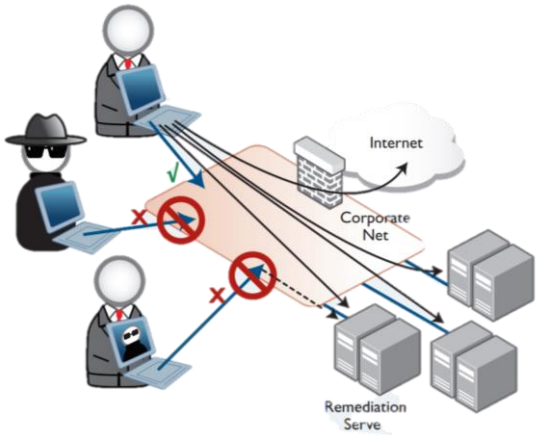

Рисунок 3.1 – Принцип реалізації NAC

Практично це означає, що кожен пристрій повинен ідентифікувати себе, коли він підключається, і, якщо це доречно, потім перевіряється його відповідність політиці безпеки організації. У типовій мережі пристрої, які:

– не можуть надати дійсну особу: повністю заборонені в мережі (або, можливо, обмежені в доступі);

– успішно пройшли аутентифікацію, але провалити тест на дотримання політики: надається доступ до процесу виправлення та відновлення;

– успішно ідентифікуються та вважаються дотриманими політики безпеки: надається доступ до мережевих ресурсів, які відповідають даним особам.

Таким чином, впровадження політики безпеки та контроль доступу до ресурсів здійснює сама мережа, використовуючи NAC. Зловмисне ПЗ не може завдати шкоди мережі, оскільки йому не надається доступ до мережі. Зловмисники не можуть скоїти крадіжку або спричинити вихід з ладу мережі, оскільки вони або заблоковані, або дуже жорстко обмежені.

Щоб забезпечити прогрес у мережевій безпеці, важливими елементами, що входять до функцій комутатора повинні бути: трьохступенева аутентифікація, аутентифікація в роумінгу, двохфакторна аутентифікація та інтеграція з інфраструктурою NAC.

Трьохступенева аутентифікація. Трьохступенева аутентифікація дозволяє мережі ідентифікувати всі пристрої, що підключаються до неї. Може використовуватися як частина комплексного рішення NAC; або самостійно, коли забезпечує низький рівень непродуктивних витрат реалізації безпеки доступу до мережі.

Аутентифікація в роумінгу. Користувачі мобільних пристроїв переходять від однієї точки вкладення (наприклад, в електронній пошті) до іншої. Після того, як користувач отримав доступ, аутентифікація в роумінгу повинна гарантувати, що йому буде зручно користуватися і не виникатиме потреба повторної аутентифікації під час роумінгу.

Двохфакторна аутентифікація. Пристрої та користувачі можуть бути аутентифіковані окремо, щоб уникнути складних спроб обійти безпеку.

Інтеграція з інфраструктурою NAC. Обладнання повинно інтегруватися як ключовий компонент у будь-яке рішення NAC.

Трьохступенева аутентифікація та її різновиди: 802.1X, веб-аутентифікація, аутентифікація MAC. 802.1X – це дуже безпечний протокол аутентифікації, який дозволяє зашифровувати обмін паролем та перевірку сертифікатів. Користувачеві пропонується ввести ім'я та пароль, і це перевіряється відповідно до бази даних користувачів, перш ніж вони зможуть отримати доступ до мережі. Це безпечно і конфігурується, але вимагає вбудованого програмного забезпечення 802.1X та налаштування його на

клієнтському пристрої. Не всі пристрої, що підключаються до мережі, мають це ПЗ вбудоване або попередньо налаштоване – це особливо стосується користувачів, які є тимчасовими відвідувачами.

Веб-аутентифікація надається для обслуговування комп'ютерів, на яких 802.1X відсутній або не налаштований. Комутатор виявляє активність веб-браузера з персонального комп'ютера користувача та представляє екран аутентифікації у веб-браузері. Користувач не може рухатися далі, поки не підтвердить дійсну особу за допомогою вікна аутентифікації. Ця аутентифікація може бути виконана звичайним текстом, використовуючи протокол HTTP, або виконана в зашифрованому вигляді за допомогою протоколу HTTPS.

Аутентифікація MAC – це резервний варіант, який можна використовувати для неінтерактивних пристроїв, таких як принтери або веб-камери. MAC-адреса пристрою надає унікальність, яку можна використовувати для аутентифікації пристрою. Забезпечивши ці три параметри аутентифікації, комутатори дозволяють побудувати мережу, у якій можна аутентифікувати всі пристрої, що підключаються до мережі (рис. 3.2).

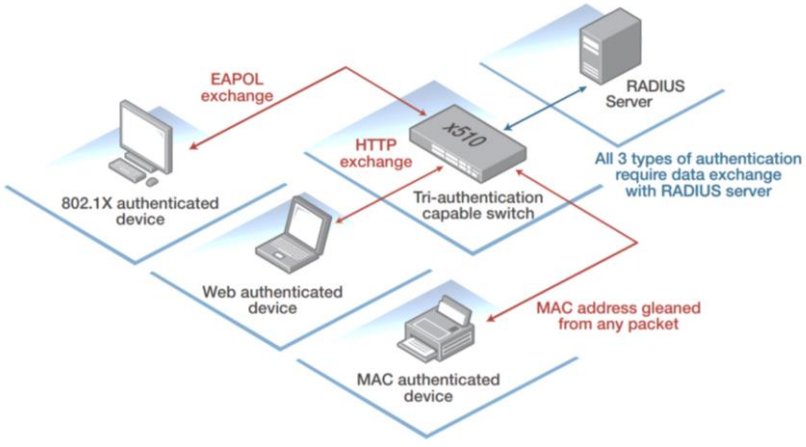

Рисунок 3.2 – Принцип роботи мережі з трьохступеневою аутентифікацією

Аутентифікація в роумінгу. Користувачі бездротової мережі Ethernet мобільні та можуть переходити з однієї точки доступу до іншої. Користувач

може бути аутентифікований комутатором, за точками доступу. За замовчуванням аутентифікований сеанс асоціюється з певним портом комутатора, що може зробити користування незручним для повторної ідентифікації під час переміщення між точками доступу, приєднаними до різних портів. Щоб вирішити цю проблему, комутатори повинні дозволяти переходити до статусу аутентифікації разом із користувачем. Ця можливість називається «аутентифікацією в роумінгу». Під час аутентифікації в роумінгу, коли користувач переходить з одного порту на інший, інформація про аутентифікацію користувача переноситься з вихідного порту на новий. Тому користувачеві не потрібно повторно аутентифікуватись (рис. 3.3).

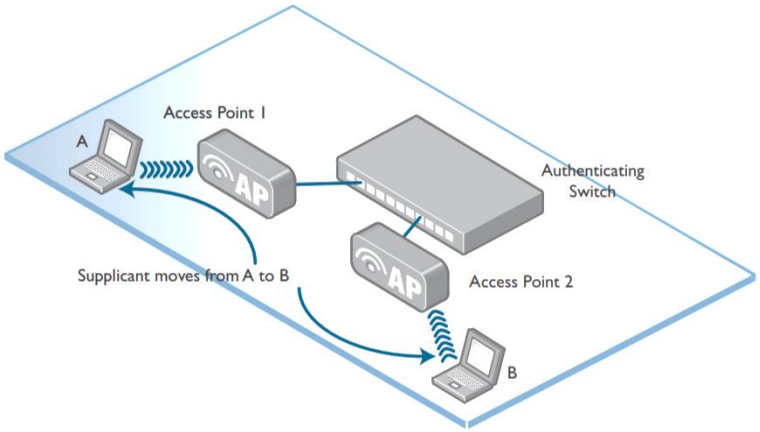

Рисунок 3.3 – Принцип дії аутентифікації в роумінгу

Аутентифікація в роумінгу в бездротових та дротових середовищах. У середовищах, де аутентифікація 802.1X не використовується в точці доступу, альтернативою є використання веб-аутентифікації на комутаторі, який є основою точки доступу (рис. 3.4).

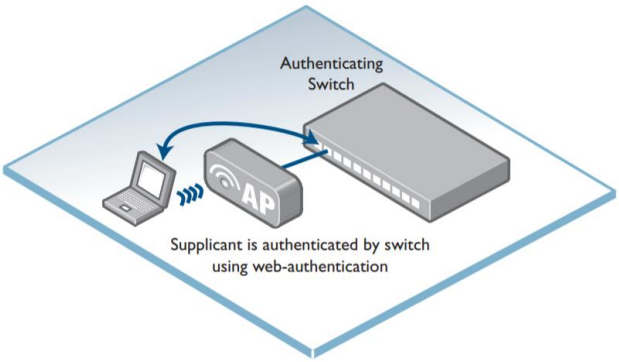

Рисунок 3.4 – Принцип дії аутентифікації в роумінгу у бездротовому середовищі

У цій ситуації найбільш важливою є аутентифікація в роумінгу. У дротовому середовищі, де простий протокол розширюваної аутентифікації (з англ. Extensible Authentication Protocol – EAP) фільтрується, комутатори, використовуються на межі мережі, тоді 802.1X або веб-аутентифікація виконується на комутаторі, здатному до аутентифікації, на рівні агрегації (процес об'єднання елементів в єдину систему) (рис. 3.5).

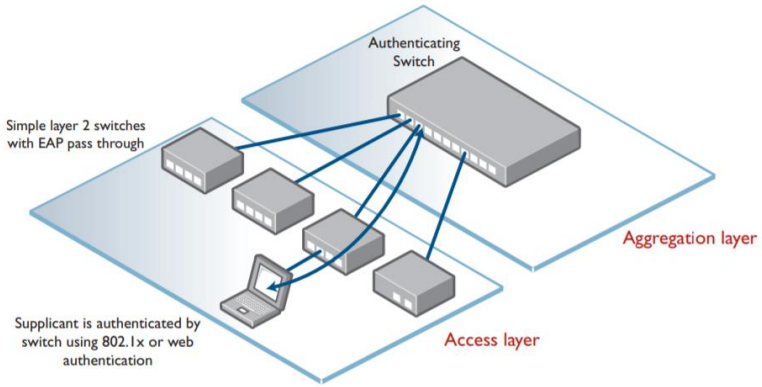

Рисунок 3.5 – Принцип дії аутентифікації в роумінгу у дротовому середовищі

У цьому випадку аутентифікація в роумінгу для веб-аутентифікації дозволяє користувачеві відключитися від одного граничного комутатора та підключитися до іншого, не потребуючи повторної аутентифікації. Аутентифікація в роумінгу може підтримувати випадок, коли користувач

підключений безпосередньо до комутатора аутентифікації. Функція аутентифікації в роумінгу для відключених портів дозволяє користувачеві відключитися від порту на аутентифікаційному комутаторі та підключитися до іншого порту комутатора без необхідності повторної аутентифікації (рис. 3.6).

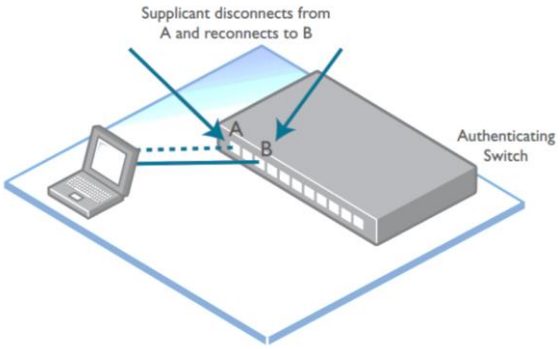

Рисунок 3.6 – Принцип дії аутентифікації в роумінгу при переході від одного порту комутатора до іншого без повторної аутентифікації

Двохфакторна аутентифікація. Традиційно аутентифікація доступу до мережі передбачає лише один метод аутентифікації. Після того, як користувач або пристрій авторизовано за допомогою MAC-аутентифікації, веб-аутентифікації або 802.1X, тоді процес аутентифікації завершено. Цей одноетапний підхід до аутентифікації має потенційні ризики для безпеки:

– несанкціонований користувач може отримати доступ до мережі з авторизованого пристрою, наприклад, викравши пристрій, який підтверджується аутентифікацією MAC;

– авторизований користувач може отримати доступ до мережі з несанкціонованого пристрою. Методи аутентифікації 802.1X та веб-аутентифікація підтверджують особу користувача, а не пристрою, яким вони користуються.

Щоб зменшити загрозу для безпеки від заданих ризиків, потрібна двофакторна аутентифікація. Двофакторна аутентифікація включає аутентифікацію як користувача, так і пристрою. Запитуючий пристрій стане

аутентифікованим лише у тому випадку, якщо обидва ці кроки будуть успішними. Процес, який відбувається при двофакторній аутентифікації, є буквальним – заявник двічі засвідчується аутентифікацію двома різними методами. Для двофакторної аутентифікації підтримуються наступні послідовності аутентифікації:

– Аутентифікація MAC з аутентифікацією 802.1X;
– Аутентифікація MAC з подальшою веб-аутентифікацією;
– 802.1X аутентифікація з подальшою веб-аутентифікацією.

У якості іншого, подальшого рівня безпеки, потрібна підтримка використання різних серверів RADIUS (з англ. Remote Authentication Dial-In User Service — протокол передачі даних, що використовується в комп'ютерних мережах для аутентифікації, авторизації та обліку різноманітних сервісів) для різних методів аутентифікації. Для кожного з трьох методів аутентифікації можна використовувати різні сервери RADIUS. Це дозволяє повністю розділити бази даних RADIUS, які використовуються для методів аутентифікації, які використовуються при двофакторній аутентифікації. Через це розділення бази даних зловмисник не може обійти двофакторну аутентифікацію, використовуючи однакову комбінацію імені користувача/пароля для обох методів. Ім'я користувача/пароль, які існують на одному сервері RADIUS, для аутентифікації одним методом, не повинно бути присутнє на сервері RADIUS, використовуваному другим методом (рис 3.7).

Інтеграція з інфраструктурою NAC. Інтеграція NAC дає можливість комутаторам виконувати роль виконавчих точок в інфраструктурі NAC із сторонніми розробниками ПЗ. Зокрема, це означає, що комутатор:

- транспортує пакети, які формують запит сервера NAC клієнтського пристрою;
- отримує повідомлення про прийняте рішення та виконує його.

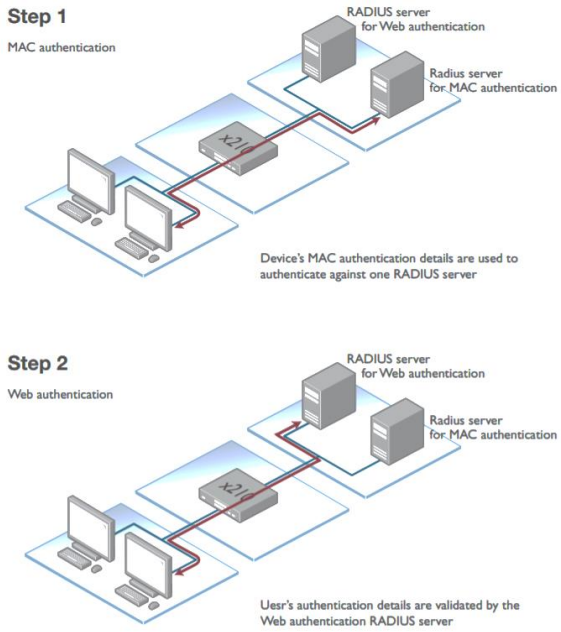

Рисунок 3.7 – Принцип дії двофакторної аутентифікації

На рисунку 3.8 зображена роль комутатора, як точки забезпечення політики безпеки у рішенні NAC. Сервер NAC визначає рівень доступу до мережі, який може мати користувач, або коректуючі дії, необхідні для підведення комп'ютера або іншої кінцевої точки до прийнятного рівня відповідності. Комутатор виконує функції виконавця політики, забезпечуючи постійну безпеку мережі та відповідний доступ до ресурсів.

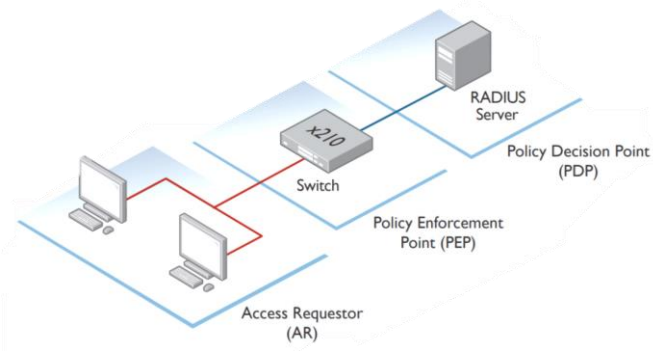

Рисунок 3.8 – Інтеграція з інфраструктурою NAC

3.4 Висновки з розділу 3

1. Описано процес управління мережевим доступом (NAC), основною задачею якого є перевірка аутентифікації кінцевих точок у мережі та надання/заборона доступу до мережі.

2. Проведено порівняння моделей мережевих систем контролю доступу: які засновані на агентах (програма, яка виконує підготовку інформації і її обмін між клієнтською та серверною частинами мережі) і без агентів. Основна відмінність полягає у тому, що модель NAC на основі агентів виконує перевірку безпеки та аутентифікацію на пристроях кінцевих точок, у той час як модель NAC без агентів не потребує встановлення постійного програмного агента на пристрої кінцевої точки, а може замінити агент тимчасовим ПЗ.

3. Проаналізовані основні функції системи, яка забезпечує безпеку мережі за допомогою контролю доступу. Цими функціями є трьохступенева аутентифікація, аутентифікація в роумінгу, двохфакторна аутентифікація та інтеграція з інфраструктурою NAC. Двохфакторна аутентифікація є найдієвішим способом збереження доступу до файлів у мережі, оскільки включає аутентифікацію як користувача, так і пристрою. Тому слід використовувати технологію управління мережевим доступом, яка полягає у налаштуванні комутаторів.

ВИСНОВКИ

Запропонована робота присвячена дослідженню забезпечення конфіденційності даних в телекомунікаційних мережах за допомогою контролю доступу. У ході роботи розроблено рекомендації для захисту мережі з використанням контролю доступу.

У першому розділі обґрунтовувалася необхідність забезпечення збереження конфіденційності даних в телекомунікаційних мережах із використанням контролю доступу. У ході доведення виділено два компоненти контролю доступу: аутентифікацію та авторизацію. І надано їм відповідні визначення: аутентифікація – це перший крок надання доступу користувачеві до ресурсів, тобто це процес ідентифікації користувача та перевірки того чи він має право входити в запитувану мережу та отримувати доступ до ресурсів; а авторизація – це частина контролю доступу, що стосується обмеження дій аутентифікованих користувачів.

У другому розділі описано загрози і визначено, що їх спільною метою є отримання або зміна даних користувачів чи всієї організації, а також описано методи протидії атакам, найкращими із них є використання локальної мережі, яка має надсилати дані лише до одного місця призначення, використання шифрування даних, використання систем виявлення вторгнень.

У третьому розділі описано процес управління мережевим доступом (NAC), основною задачею якого є перевірка аутентифікації кінцевих точок у мережі та надання/заборона доступу до мережі, проведено порівняння моделей мережевих систем контролю доступу: які засновані на агентах і без агентів та надано технологічне рішення мережевих систем контролю доступу з використанням комутаторів, які використовуються як фільтри трафіку, який має циркулювати мережею.

Результатом роботи є рекомендована технологія управління мережевим доступом для пом'якшення дії загроз та наслідків атак, поєднуючи

(інтегруючи) контроль доступу з автоматизованим управлінням пристроями, підключених до мережі, наприклад, налаштованих комутаторів.

ПЕРЕЛІК ПОСИЛАНЬ

1. R. Anderson Security Engineering, Wiley, 2001. – pp. 51 – 67, 258 – 288.

2. A. Jain, L. Hong and S. Pankanti Biometrie Identification. Communications of the ACM, vol. 43, 2000. – pp. 91 – 98.

3. D. Terdiman Vegas gung-ho on gambling tech, Wired, September 2003.

4. L. von Ahn, M. Blum, and J. Langford Telling humans and computers apart automatically. Communications of the ACM, vol. 47, February 2004. – pp. 57-60.

5. M. Kotadia Spammers use free porn to bypass Hotmail protection. ZD Net UK, May 6, 2004.

6. Десятчиков А. А. Метод обработки дистанционной биометрической информации в системах контроля и управления доступом, 2007.

7. Тумоян Е. П. Разработка и исследование метода создания и использования хранилищ ключевой информации на основе распознавания биометрических образов, 2003.

8. Белов Е. Б. Основы информационной безопасности / Е. Б. Белов, В. П. Лось, Мещеряков Р. В., Шелупанов А. А. – М. : "Горячая линия-Телеком", 2006. – 544 с.

9. Герасименко В. А. Основы защиты информации / В.А. Герасименко В. А., А.А. Малюк. М. : МГИФ. 1997. – 537 с.

10. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. – М. : Горячая линия – Телеком, 2010. – 272 с. ил.

11. D. S. Ms. Charjan, P. S. Ms. Bochare and Y. R. Bhuyar An Overview of Secure Sockets Layer, vol. 6, 2013. – pp. 388–393.

12. M. Kozlova Seven luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti, 2017.

13. A. M. Plaskovsky, A. G. Novopashenny, Y. E. Podgurskiy and V. S. Zaborowski Metodyi i sredstva zaschity i kompyuternoy informatsii. Firewall. Access control at the application level, 2012. – pp. 152 – 187, 210 – 239.

14. Технологии защиты информации в компьютерных сетях. – М. : НОУ «Интуит», 2016. – 368 с.

15. Ворона В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – М. : Горячая линия – Телеком, 2010. – 245 с.

16. Волхонский В. В. Системы контроля и управления доступом / В. В. Волхонский. – СПб. : Университет ИТМО, 2015.

17. DDoS, Machine Learning, Measures // Understanding Denial-of-Service Attacks, 2016, ISBN:13:978-1-4987-2965-9. – 12 – 34 с.

18. Леонтьев В. П. Безопасность в сети Интернет: учебное пособие / В.П. Леонтьев. – 3-е изд., и доп. – М. : ОЛМА Медиа Групп, 2008. – 256 с.

19. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша – К.: ВБ «Аванпост-Прим», 2012. – 214 с.

20. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз): монографія / В. М. Бутузов.— К.: КІТ, 2010. – 145 с.

21. Бабок В. П. Інформаційна безпека та сучасні мережені технології: англ.-укр.-рос. словник термінів / В. П. Бабок, В. Г. Корченко.— К. : НАУ, 2003. – 670 с.

22. Корченко О. Г. Класифікація методів соціального інжинірингу / О. Г. Корченко, Є. В. Паціра, Д. А. Пуха // Захист інформації.— К.: НАУ, 2007. – 37 – 45 с.

23. Шудрова К. Социальная инженерия в информационной безопасности / К. Шудрова // Директор по безопасности, 2012. – 13 – 17 с.

24. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк// Безпека інформації, 2013. – 118 – 129 с.

25. Методика информационной безопасности. / [Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А и др.] – М. : Издательство – Экзамен, 2004. – 544 с.

26. Барабанова М. И., Кияев В. И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.– СПб. : Изд-во СПбГУЭФ, 2010. – 267 с.

27. Тихонов И. А. Информативные параметры биометрической аутентификации пользователей информационных систем по инфракрасному изображению сосудистого русла Биомедицинская техника и радиоэлектроника. 2010. – 26 – 32 с.

28. Герасименко В. А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. – кн.1. - М. : Энергоатомиздат, 2004. – 400 с.

29. Григоренко О.Г., Полікарпова Ю.Г. Атаки, які загрожують телекомунікаційній мережі та методи покращення її безпеки [Електронний ресурс] // XIV Міжнародна науково-технічна конференція "Перспективи телекомунікацій 2020". – 2020.

30. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с.