Calculated winning ratio. This coefficient shows the efficiency of using low-pass filters. Graphs of the envelope voltage at the output of an ideal bandpass filter when a rectangular pulse of different duration is applied to the input– a signal that can be a signal of covert information acquisition means. Modeling of the filtering process with different correlation coefficients was carried out. The simulation results confirmed the possibility of identifying the signal of means of covert information acquisition by the method of determining the two-dimensional probability density of the interference signal against the background of the general signal. The process of improving the immunity of the system as a whole is being studied. The improvement of the signal detection method was carried out due to the use of low-frequency narrow-band filters in the process of signal processing, which allows to achieve a 23% increase in the immunity of the system for identifying and recognizing signals of digital means of covert information acquisition.

Key words: means of tacit information acquisition, random signal, interference resistance, filter, useful signal, impulse.

Лаптев Олександр Анатолійович, доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, м. Київ.

Oleksandr Laptiev, Doctor of Technical Science, Senior Researcher. Associate Professor the Department of Cyber Security and Information Protection, Faculty of Information Technology, Taras Shevchenko National University of Kyiv
E-mail: olaptiev@knu.ua.
Orcid ID: 0000-0002-4194-402X.

Савченко Віталій Анатолійович, доктор технічних наук, професор, директор навчально-наукового інституту захисту інформації Державного університету телекомунікацій, м. Київ.

Vitalii Savchenko, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine.
E-mail: savitan@ukr.net.
Orcid ID: 0000-0002-3014-131X.

Копитко Сергій Богданович, кандидат економічних наук, старший викладач кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку, м. Одеса, Україна.

Serhii Kopytko, candidate of economic sciences, senior lecturer at the Department of cyber security and technical information protection, State University of Intellectual Technologies and Communication, Odesa, Ukraine.
E-mail: KopytkoSB@gmail.com.
Orcid ID: 0000-0001-7353-0422.

Пономаренко Віталій Валерійович, аспірант навчально-наукового інституту захисту інформації Державного університету телекомунікацій, м. Київ.

Vitaliy Ponomarenko, postgraduate student of the Educational and Scientific Institute of Information Protection of the State University of Telecommunications, Kyiv.
E-mail: Ur_suviato@ukr.net.
Orcid ID: 0000-0002-6567-4247.

Пархоменко Іван Іванович, кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, м. Київ.

Ivan Parkhomenko, PhD, Associate Professor at the Departament of Cybersecurity and Information Protection faculty of Information Technology, Taras Shevchenko National University of Kyiv
E-mail: ivan.parkhomenko@knu.ua.
Orcid ID: 0000-0001-6889-9284.

DOI: 10.18372/2410-7840.24.17265
УДК 004.681.3

ВІДДАЛЕНІ АТАКИ В РОЗПОДІЛЕНИХ КОМП`ЮТЕРНИХ МЕРЕЖАХ ТА INTERNET

Володимир Хорошко, Микола Браіловський, Марія Капустян, Юлія Хохлачова

В даній статті детально розглянуто типові віддалені атаки та механізми їх реалізації, а також проаналізовано мережевий трафік, що дозволяє дослідити логіку праці розподіленої комп'ютерної мережі, тобто отримати взаємооднозначну відповідність подій, що відбуваються в системі, та команд, які передаються між об'єктами системи, в момент появи цих подій. Ґрунтуючись на дослідженнях безпеки мережі та аналізі доступності інформації, описано ті можливі віддалені інформаційні руйнівні впливи (віддалені атаки), які в будь-який момент можуть з'явитися в якості небажаних впливів. Також детально розглянуто види модифікації інформації та інформаційного коду. Визначено, що хоча захист інформації в розподілених комп'ютерних мережах та Internet є широкою та різноплановою темою, очевидно, що Internet-технології є рушійною силою розвитку в цьому секторі. Дослідження цієї проблеми дуже складний процес та отримання певних

рішень дуже важливі для безпеки інформації. Сучасним атакам та, в першу чергу, віддаленим, практично не можливо запобігти, тому маючи інформацію про типи та дії віддалених атак в розподілених мережах, можливо забезпечити боротьбу з ними або хоча б зменшити їх вплив на інформацію в розподілених комп'ютерних мережах та Internet.

Ключові слова: *комп'ютерна мережа, розподілені комп'ютерні мережі, віддалена атака, Internet, мережевий трафік.*

ВСТУП

В теперішній час комп'ютерна техніка використовується практично в усіх сферах людської діяльності. В сучасних комп'ютерних системах зберігаються та обробляються велика кількість інформації різного ступеня відкритості. Існуючі комп'ютерні мережі (КМ) є досить зручним способом отримання та передачі інформації.

Разом з тим зростаючий рівень складності мережевих архітектур, підвищення ступеню відкритості мереж та все більш тісна їх прив'язка до Internet роблять актуальним питання безпеки інформації. Використання Internet в якості глобальної мережі означає для засобів безпеки різноманітних структур не тільки різке збільшення кількості зовнішніх користувачів, але і різноманіття типів комунікаційних зв'язків, і співіснування з новими мережевими та інформаційними технологіями. Тому інформаційні ресурси та засоби здійснення електронних мережевих транзакцій (сервери, маршрутизатори, сервери віддаленого доступу, канали зв'язку, операційні системи, бази даних та застосунки) потрібно захищати особливо надійно та якісно [1, 2, 3].

Слід зазначити, що засоби злому та вторгнення до комп'ютерних мереж і розкрадання інформації розрізняються так само швидко, як і всі високотехнологічні комп'ютерні галузі. В цих умовах забезпечення інформаційної безпеки комп'ютерних мереж є пріоритетною задачею, оскільки від зберігання конфіденційності, цілісності та доступності інформаційних ресурсів в більшості залежить якість та оперативність прийняття стратегічних рішень та ефективність їх реалізацій.

Потрібно враховувати, що Internet – це багатогранна структура, що розвивається, живе своїм життя, і в той же час є невід'ємною інформаційним середовищем. Середовище, в якому існують методи та засоби, що є застосованими спеціалістами, дозволяють вирішувати задачі захисту інформації в цьому середовищі [1, 4].

Internet, як інформаційне досягнення людства, окрім очевидних досягнень, має ряд суттєвих недоліків у системі забезпечення безпеки, яка склалася.

Ґрунтуючись на дослідженнях безпеки мережі та аналізі доступності інформації, спробуємо як найточніше описати ті можливі віддалені інформаційні руйнівні впливи (віддалені атаки), які в будь-який момент можуть з'явитися в якості небажаних впливів. Для того, щоб забезпечити протидію їм, необхідно знати основні типи можливих атак і розуміти механізми їх реалізації.

ОСНОВНА ЧАСТИНА

Розглянемо типові віддалені атаки та механізми їх реалізації, до яких відносяться [1, 4, 5]:

-аналіз мережевого трафіку;

-підміна довіреного об'єкту або суб'єкту розподіленої КМ;

-хибний об'єкт розподіленої КМ;

-використання хибного об'єкту для організації віддаленої атаки на розподілену КМ;

-селекція потоку інформації та збереження її на хибному об'єкті КМ;

-модифікація інформації;

-відмова в обслуговуванні.

Більш детально розглянемо кожну з атак.

Аналіз мережевого трафіку. Головною особливістю розподіленої комп'ютерної мережі (КМ) є те, що її об'єкти розподілені у просторі та зв'язок між ними здійснюється за допомогою мережевих з'єднань та механізмів повідомлень. При цьому керуючі повідомлення та дані, які пересилаються між об'єктами розподіленої КМ, передаються за допомогою мережевих з'єднань у вигляді пакетів обміну. Ця особливість призвела до появи специфічного для розподіленої КМ типового віддаленого впливу, що полягає у собі прослуховування каналу мережі. Це типове віддалення впливу є аналізом мережевого трафіку [1, 3, 4, 5].

По-перше, аналіз мережевого трафіку дозволяє дослідити логіку праці розподіленої КМ, тобто отримати взаємооднозначну відповідність подій, що відбуваються в системі, та команд, які передаються між об'єктами системи, в момент появи цих подій (якщо проводити подальшу аналогію з інструментарієм хакера, то аналіз трафіку в цьому випадку замінює та траєсерувальник). Це досягається шляхом перехвату та аналізу пакетів обміну на канальному рівні. Знання логіки, роботи розподіленої КМ дозволяє на практиці моделювати та здійснювати типові віддалені атаки, які розглянуті у наступних пунктах на прикладі конкретних розподілених КМ [4].

По-друге, аналіз мережевого трафіку дозволяє перехопити потік даних, якими забезпечуються об'єкти розподіленої КМ. Таким чином, віддалена атака даного типу полягає в отриманні на віддаленому об'єкті несанкціонованого доступу до інформації, якою обмінюються мережеві абоненти. Відзначимо, що при цьому аналіз можливий тільки всередині одного сегменту мережі [4].

За характером взаємодії, аналіз мережевого трафіку є пасивним впливом. Здійснення даної атаки без зворотного зв'язку веде до порушення конфіденційності інформації всередині одного сегменту мережі на канальному рівні. При цьому, здійснення атаки, безумовно, по відношенню до її цілі.

Підміна довіреного об'єкту чи суб'єкту розподіленої КМ. Одною з проблем безпеки розподіленої КМ є недостатня ідентифікація та аутентифікація її віддалених об'єктів. Основна складність полягає в здійсненні однозначної ідентифікації повідомлень, що передаються між суб'єктами та об'єктами взаємодії. Зазвичай, в розподілених КМ ця проблема вирішується таким чином: в процесі створення віртуального каналу, об'єкти розподіленого КМ обмінюються певною інформацією, яка ідентифікує даний канал. Такий обмін, зазвичай, називають «рукостисканням».

Зазначимо, що не завжди для зв'язку двох віддалених об'єктів розподіленої КМ створюється віртуальний канал. Практика демонструє, що найчастіше для службових повідомлень (наприклад, від маршрутизаторів) використовується передача поодиноких повідомлень, які не потребують підтверджень [1, 5].

Як відомо, для адресації повідомлень в розподілених КМ використовується мережева адреса, що є унікальною для кожного об'єкту системи на канальному рівні моделі OSI – це апаратний адрес мережевого адаптера на мережевому рівні – адреса визначається в залежності від протоколу мережевого рівня, що використовується (наприклад, IP-адреса). Мережева адреса також може використовуватись для ідентифікації об'єктів розподіленої КМ. Але мережева адреса достатньо просто підробляється, тому використовувати її в якості єдиного засобу ідентифікації об'єкта неприпустимо.

В цьому випадку, коли розподілена КМ використовує нестійкі алгоритми ідентифікації віддалених об'єктів, опиняється можливою типова віддалена атака, яка полягає в передачі по каналам зв'язку повідомлень від імені довільного об'єкта або суб'єкта розподіленої КМ. При цьому існує два різновиди даної типової віддаленої атаки [6]:

-атака при встановленому віртуальному каналі;

-атака без встановленому віртуальному каналі.

У випадку встановленого віртуального з'єднання атака буде полягати в присвоєнні прав довіреного суб'єкта взаємодії, який детально підключився до об'єкту системи, що дозволяє атакуючому вести сеанс роботи з атакуючим об'єктом розподіленої системи від імені довіреного об'єкту. Реалізація віддалених атак даного типу зазвичай складається з передачі пакетів обміну з об'єкту, що атакується на ціль атаки від імені довіреного суб'єкту взаємодії (при цьому передані повідомлення будуть сприйматися системою як коректні). Для здійснення атаки даного типу необхідно здолати систему ідентифікації та аутентифікації повідомлень, яка, в принципі, може використовувати контрольну суму, яка обчислена за допомогою відкритого ключа, що динамічно виробляється при встановленні каналу, випадкові багатобітові лічильники каналів та мережеві адреси об'єктів. Однак, на практиці [16], для класифікації пакетів обміну використовується два 8-бітові лічильники – номер каналу та номер пакету; в протоколах інших типів для ідентифікації використовуються зазвичай два 32-бітових лічильника.

Як було зазначено раніше, для службових повідомлень у розподілених КМ часто використовується передача поодиноких повідомлень, які не потребуються підтвердження, тобто не потрібно створювати віртуальне з'єднання. Атака без встановленого віртуального з'єднання полягає в передачі службових повідомлень від імені мережевих управляючих пристроїв, наприклад від імені маршрутизаторів.

Очевидно, що в цьому випадку, для ідентифікації пакетів можливо лише використання статичних ключів, які визначені заздалегідь, що дуже не зручно і потребує складної системи управління ключами. Однак, при відмові від такої системи ідентифікація пакетів без встановленого віртуального каналу буде можлива лише за мережевим адресом відправника, який легко підробити [15].

Посилка хибних управляючих повідомлень може привести до серйозних порушень роботи розподіленої КМ. Розглянута типова віддалена атака, що використовує нав'язування хибного маршруту, базується на описаній ідеї.

Підміна довіреного об'єкту розподіленої КМ (РКМ) є активним впливом, що здійснюється з метою порушення конфіденційності та цілісності інформації по наступу на об'єкті певної події, який атакується. Дана віддалена атака може бути як

внутрішньо сегментною, так і меж сегментною, як із зворотнім зв'язком, так і без зворотного зв'язку з об'єктом, що атакується та здійснюється на мережевому та транспортному рівнях.

Хибний об'єкт розподіленої КМ. В тому випадку, якщо в РКМ недостатньо надійно вирішені проблеми ідентифікації мережевих управляючих пристроїв, що виникають при взаємодії останніх з об'єктами системи, то подібна розподілена система може піддаватися типовій віддаленій атаці, яка пов'язана із зміною маршрутизації та впровадженням в систему хибного об'єкту. В тому випадку, якщо структура мережі така, що для взаємодії об'єктів необхідно використання алгоритмів віддаленого пошуку, то це також дозволяє впровадити в систему хибний об'єкт. Тож, існує дів принципово різні причини, що обумовлюють появу типової віддаленої атаки «Хибний об'єкт РКМ»[6, 7].

Впровадження в РКМ хибного об'єкту нав'язування хибного маршрутизатору. Сучасні глобальні мережі являють собою сукупність сегментів мережі, що пов'язані між собою через мережеві вузли. При цьому маршрутом називається послідовність вузлів мережі, за допомогою якої дані передаються від джерела до отримувача. Кожен маршрутизатор має спеціальну таблицю, яка називається таблицею маршрутизації, в якій для кожної адреси вказується оптимальний маршрут. Відмітимо, що таблиці маршрутизації існують не тільки у маршрутизаторів, а і у будь-яких хостів у глобальній мережі. Для забезпечення активної та оптимальної маршрутизації в РКМ застосовуються спеціальні керуючи протоколи, які дозволяють маршрутизаторам обмінюватися інформацією один з одним, повідомляти хостам про новий маршрут, віддалено керувати маршрутизаторами. Важливо відмітити, що всі описані вище протоколи, дозволяють віддалено змінювати маршрутизацію в мережі Internet, тобто є протоколами керування мережею [4, 5].

Тому, абсолютно очевидно, що маршрутизація в глобальних мережах відіграє важливу роль та, як наслідок цього, може піддаватися атаці. Основна мета атаки, яка пов'язана з нав'язуванням хибного маршруту, полягає в тому, щоб новий маршрут проходив через хибний об'єкт – хост атакуючого [7].

Реалізація даної типової віддаленої атаки полягає в несанкціонованому використанні протоколів керування мережею для зміни вихідних таблиць маршрутизації.

Для зміни маршрутизації атакуючому необхідно надіслати по мережі певні дані протоколами керування мережею спеціальні службові повідомлення від імені мережевих керуючих пристроїв. В результаті успішної зміни маршруту, атакуюча сторона отримає повний контроль над потоком інформації, якою обмінюються два об'єкти РКМ, та атака передає в другу стадію, що пов'язана з прийомом, аналізом та передачею повідомлень, які отримуються від дезінформованих об'єктів РКМ.

Нав'язування об'єкту РКМ хибного маршруту – активний вплив, що здійснюється по відношенню до будь-яких з цілей атаки. Дана типова віддалена атака може здійснюватися як в одному сегменті, так і міжсегментно, як із зворотнім зв'язком, так і без нього з об'єктом, який атакується, на транспортному та прикладному рівнях [6, 7].

Впровадження в розподілену мережу хибного об'єкту здійснюється шляхом використання недоліків алгоритму віддаленого каналу.

В РКМ часто виявляється, що її віддалені об'єкти з самого початку не мають достатньо інформації, необхідної для адресації повідомлень. Звичайною такою інформацією є апаратні (адреса мережевого адаптера) та логічні (IP-адреса) адреси об'єктів РКМ. Для отримання подібної інформації в розподілених мережах використовуються різні алгоритми віддаленого пошуку, які полягають в передачі по мережам спеціального виду пошукових запитів, та в очікуванні відповідей на запит з інформацією, яку шукають. Після отримання відповіді на запит, суб'єкт РКМ , який зробив запит, має всі необхідні дані для адресації. Керуючись отриманими з відповіді даними про об'єкт, який шукають, суб'єкт розподіленої мережі, який зробив запит, починає адресацію до нього.

У випадку використання РКМ механізмів віддаленого пошуку існує можливість на об'єкті, який атакують, перехопити посланий запит та послати на нього хибку відповідь, де вказати дані, використання яких призведе до адресації на хибний об'єкт, який атакує. В подальшому весь потік інформації між суб'єктом та об'єктом впливу буде проходити через хибний об'єкт РКМ.

Інший варіант впровадження в РКМ хибного об'єкта використовую недоліки алгоритму віддаленого пошуку та полягає в періодичній передачі на об'єкт, що атакується, заздалегідь підготовленої хибної відповіді без прийому пошукового запиту. Атакуючому для того, щоб надіслати хибну відповідь, не завжди обов'язково очікувати на прийом запиту (він може, в принципі, не мати подібної можливості у перехваті запиту). При цьому атакуючий може спровокувати об'єкт, який атакують, на

передачу пошукового запиту, і тоді ця хибна відповідь буде мати успіх [6]. Дана типова віддалена атака дуже характерна для глобальних мереж, коли у атакуючого завдяки знаходженню його в іншому сегменті відносно цілі атаки просто немає можливості перехопити пошуковий запит.

Хибний об'єкт РКМ – активний вплив, що здійснюється з метою порушення конфіденційності та цілісності інформації, який може бути атакою за запитом від об'єкту, який атакують, а також безумовною атакою.

Ця віддалена атака є, як внутрішньо сегментною, так і міжсегментною, має зворотній зв'язок з об'єктом, який атакують, та здійснюється на канальному та прикладному рівнях.

Використання хибного об'єкта для організації віддаленої атаки на РКМ. Отримавши контроль над потоком інформації, що проходить між об'єктами, хибний об'єкт РКМ може застосовувати різні методи впливу на перехоплену інформацію. У зв'язку з тим, що впровадження в розподілену систему хибного об'єкта є метою багатьох віддалених атак та представляє серйозну загрозу безпеці РКМ в цілому, у подальшому будуть детально розглянуті методи впливу на інформацію, перехоплену хибним об'єктом [3, 4].

Селекція потоку інформації та збереження її на хибному об'єкті РКМ. Однією з атак, яку може здійснювати хибний об'єкт РКМ, є перехоплення інформації, яка передається між об'єктом і суб'єктом впливу. Важливо відмітити, що факт перехоплення інформації (файлів, пакетів та блоків) можливий тому, що при виконанні деяких операцій над файлами (читання, копіювання, модифікація тощо) вміст цих файлів передається мережею, а значить вступає на хибний об'єкт. Найпростіший спосіб реалізації перехоплення – це збереження у файлі всіх отриманих хибним об'єктом пакетів обміну [6].

Тим не менше, даний спосіб перехоплення інформації виявляється недостатньо інформативним. Це відбувається в наслідку того, що в пакетах обміну окрім полів даних існують службові поля, які не представляють в даному випадку для атакуючого безпосередній інтерес. Відповідно, для того, щоб отримати безпосередньо файл, що передається, необхідно проводити на хибному об'єкті динамічний семантичний аналіз потоку інформації для його селекції.

Модифікація інформації. Однією з особливостей будь-якої системи впливу, яка побудована за принципом хибного об'єкта, є те, що вона здатна модифікувати перехоплену інформацію. Слід особливо відмітити, що це один із способів, що дозволяє програмно модифікувати потік інформації між об'єктами РКМ з іншого об'єкту. Тому що для реалізації перехоплення інформації в мережі необов'язково атакувати розподілену мережу за схемою «хибний об'єкт». Ефективною буде атака, що здійснює аналіз мережевого трафіку, що дозволяє отримати всі пакети, які проходять каналом зв'язку, але на відміну від віддаленої атаки за схемою «Хибний об'єкт» вона не здатна до модифікації інформації [1, 5].

Більш детально розглянемо види модифікації інформації. До них відносять:

- модифікація при даних, що передаються;
- модифікація коду, що передається.

Однією з функцій, якою може володіти система впливу, що побудована за принципом «Хибний об'єкт», є модифікація даних, які передаються. В результаті селекції потоку перехопленої інформації та його аналізу система може розпізнавати типи файлів, що не передаються (виконуючий або текстовий). Відповідно, у випадку виявлення текстового файлу або файлу даних з'являється можливість модифікувати дані, що проходять через хибний об'єкт. Особливу загрозу ця функція представляє для мереж обробки конфіденційної інформації.

Іншим видом модифікації може бути модифікація коду, що передається. Хибний об'єкт при проводження селективного аналізу інформації, що проходить через нього, може виділяти у потоку даних код, який шукають. Відомий принцип фон-неймановської архітектури каже, що не існує різниці між даними та командами. Відповідно, для того, щоб визначити, що передається мережею – код або дані, необхідно використовувати певні особливості, які властиві реалізації мережевого обміну в конкретній розподіленій мережі або деякі особливості, притаманні конкретним типам файлів, що використовуються в даній локальній операційній мережі.

Виокремлюються два різних за метою види модифікації коду [7]:

- впровадження руйнуючих програмних засобів (РПЗ);
- зміна логіки роботи файла, що використовується.

В першому випадку при використанні РПЗ виконуючий файл модифікується за вірусною технологією: до файлу, що використовується, одним з відомих способів змінюється точка входу так, щоб вона вказувала на початок коду РПЗ, що впроваджується. Описаний спосіб нічим не відріз-

няється від стандартного зараження файлу, що виконується, вірусом, за винятком того, що файл виявився заражений вірусом або РПЗ в момент передачі його мережею.

Таке можливе лише при використанні системи впливу, яка побудована за принципом «хибний об'єкт».

Конкретний вид РПЗ, його цілі та задачі, в даному випадку не мають значення, але можливо розглянути, наприклад, варіант використання хибного об'єкта для створення мережевого хробака – найбільш складного на практиці віддаленого впливу в мережах, або в якості РПЗ використовувати програми мережеві шпигуни [1].

В другому випадку відбувається модифікація виконуючого коду з метою зміни його роботи. Даний вплив потребує попереднього використання роботи виконуючого файлу та, у випадку його проведення, може принести самі неочікувані результати. Наприклад, при запуску на сервері програми ідентифікації користувачів розподіленої бази даних хибний об'єкт може так модифікувати код цієї програми, що з'явиться можливість безпарольного входу з найвищими привілеями до бази даних [7].

Підміна інформації. Хибний об'єкт дозволяє не тільки модифікувати, але й підмінювати перехоплену їм інформацію. Якщо модифікація інформації призводить до її особистого спотворення, то підміна – до її повної зміни.

При виникненні в мережі певної події, яка контролюється хибним об'єктом, одному з учасників обміну посилається заздалегідь підготовлена інформація. При цьому така дезінформація в залежності від об'єкту, що контролюється, може бути сприйнята або як виконуючий код, або як дані. Розглянемо приклад подібного роду інформації.

Припустимо, що хибний об'єкт контролює подію, яка складається в підключенні користувача до серверу. В цьому випадку він очікує, наприклад, запуску відповідної програми входу в систему. У випадку, якщо ця програма знаходиться на сервері, при її запуску виконуючий файл передається на робочу станцію. Замість того, щоб виконати дану дію, хибний об'єкт передає на робочу станцію код заздалегідь написаної програми – захвату паролей. Ця програма виконує візуально такі ж самі дії, що і справжня програма входу в систему, наприклад, запитуючи ім'я та пароль користувача, після чого отримані дані посилаються на хибний об'єкт, а користувачеві виводиться повідомлення про помилку. При цьому користувач, порахував, що він невірно ввів пароль (пароль зазвичай не відображується на дисплеї) знов запустить програму підключення до системи (на цей раз справжню) ті з другого разу отримає доступ. Результат такої атаки – ім'я та пароль користувача, збережені на хибному об'єкті [1, 6, 7].

Відмова в обслуговуванні. Однією з основних задач, що висвітлюються на мережеву операційну систему, яка функціонує на кожному з об'єктів розподіленої мережі, є забезпечення надійного віддаленого доступу з будь-якого об'єкту мережі до даного об'єкта. В загальному випадку, в РКМ кожен об'єкт системи повинен мати можливість підключитися до будь-якого об'єкту розподіленої мережі та отримати у відповідності зі своїми правами віддалений доступ до її ресурсів. Зазвичай у комп'ютерних мережах можливість надання віддаленого доступу реалізується наступним чином. На об'єкті РКМ мережевої операційної мережі запускається ряд невиконаних програм сервера, що надають віддалений доступ до ресурсів даного об'єкта. Дані програми сервера входять до складу телекомунікаційних служб надання віддаленого доступу. Задача сервера полягає в тому, щоб знаходячись в пам'яті операційної системи об'єкта РКМ, постійно очікувати отримання запиту на підключення від віддаленого об'єкту. У випадку отримання такого запиту сервер повинен за можливістю передати на об'єкт, що запросив, відповідь, в якій або дозволити підключення, або відмовити (підключення до серверу описано схематично, оскільки подробиці в даному випадку не мають значення). За аналогічною схемою відбувається створення віртуального каналу зв'язку, по якому зазвичай взаємодіють об'єкти РКМ. В цьому випадку, безпосередньо, ядро мережевої операційної системи обробляє запроси, що приходять ззовні, на створення віртуального каналу та передає їх у відповідності з ідентифікатором запита прикладному процесу, яким є відповідний сервер [1, 5, 6, 7].

Очевидно, що мережева операційна система здатна мати тільки обмежене число відкритих віртуальних з'єднань та відповідати лише на обмежене число запитів.

Ці обмеження залежать від різних параметрів системи в цілому, основними з яких є швидкодія ЕОМ, об'єм операційної пам'яті та пропускної здатності каналу зв'язку, причому чим вона вища, тим більше число віртуальних запитів на одиниці часу буде обслуговано. Основна проблема полягає в тому, що при відсутності статистичної ключової інформації в РКМ ідентифікація запиту можлива тільки за адресою його відправника. Якщо в розподіленій системі не є передбаченим засоби

аутентифікації адреси відправника, тобто інфраструктура РКМ дозволяє з одного об'єкта системи передавати на інший об'єкт, що атакується, нескінчене число анонімних запитів на підключення від імені інших об'єктів, то в цьому випадку буде мати успіх віддалена тіньова атака (відмова в обслуговуванні). Результат застосування цієї віддаленої атаки порушення на об'єкті, що атакується, працездатності відповідної служби надавання віддаленого доступу, тобто неможливість отримання віддаленого доступу інших об'єктів РКМ до того, що атакується.

Другий різновид цієї тіньової віддаленої атаки полягає в передачі з однієї адреси такої кількості запитів на об'єкт, що атакується, яка дозволить трафік (направлений «шторм» запитів). В цьому випадку, якщо в системі не передбачені правила, що обмежують число запитів, що приймаються, з одного об'єкта (адреси) на одиницю часу, то результатом цієї атаки може бути як переповнення черги запитів та відмови однієї з телекомунікаційних мереж, так і повна зупинка комп'ютера із-за неможливості системи займатися нічим іншим, окрім обробки запитів.

І останнім третім різновидом атаки (відмова в обслуговуванні) є передача на об'єкт, що атакується, некоректного спеціально підібраного запиту. В цьому випадку при наявності помилок у віддаленій мережі можливе зациклювання процедури обробки запиту, переповнення буферу з подальшим зависанням системи. Типова віддалена атака (відмова в обслуговуванні) є активним методом, здійснюваним з метою порушення працездатності системи. Дана віддалена атака є односпрямованим впливом як між сегментами, так і внутрішньо сегментно, що здійснюється на транспортному та прикладному рівнях.

ВИСНОВКИ

Підводячи підсумки визначимо, що хоча захист інформації в розподілених комп'ютерних мережах та Internet є широкою та різноплановою темою, очевидно, що Internet-технології є рушійна силою розвитку в цьому секторі. Дослідження цієї проблеми дуже складний процес та отримання певних рішень дуже важливі для безпеки інформації.

Сучасним атакам та, в першу чергу, віддаленим, практично не можливо запобігти, тому маючи інформацію про типи та дії віддалених атак в розподілених мережах, можливо забезпечити боротьбу з ними або хоча б зменшити їх вплив на інформацію в розподілених комп'ютерних мережах та Internet.

ЛІТЕРАТУРА

[1] Ленков С.В. Методы и средства защиты информации в 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

[2] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки / В.Л. Бурячок. – К.: НАУ, 2013. – 432 с.

[3] Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

[4] Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП Україна», 2015. – 449 с.

[5] Поповский В.В. Защита информации в телекоммуникационных системах. В 2-х томах / В.В. Поповский, А.В. Перенков. – Харьков: ООО «Компания СМИТ», 2006.

[6] Козюра В.Д. Захист інформації в комп'ютерних системах / Козюра, В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. – Ніжин: ФОП Лук'яненкоВ.В.; ТПК"Орхідея", 2020. – 236 с.

[7] Браіловський М.М. Технології захисту інформації / М.М. Браіловський, С.В. Зибін, І.В. Піскун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.

RANGE ATTACKS IN DISTRIBUTED COMPUTER NETWORKS AND INTERNET

In this article, typical remote attacks and their implementation mechanisms are discussed in detail, as well as network traffic is analyzed, which allows to investigate the logic of work of a distributed computer network, i.e. to obtain an unambiguous correspondence of events that occur in the system and commands that are transmitted between objects system at the time of occurrence of these events. Based on network security research and information availability analysis, those possible remote information destructive effects (remote attacks) that can appear as unwanted effects at any time are described. Types of modification of information and information code are also considered in detail. It was determined that although the protection of information in distributed computer networks and the Internet is a broad and diverse topic, it is clear that Internet technologies are the driving force of development in this sector. Researching this problem is a very complex process and obtaining certain solutions is very important for information security. Modern attacks and, first of all, remote ones, are practically impossible to prevent, therefore, having information about the types and actions of remote attacks in distributed networks, it is possible to ensure the fight against them or at least reduce their impact on information in distributed computer networks and the Internet.

Key words: computer network, distributed computer networks, remote attack, Internet, network traffic.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Khoroshko, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Браіловський Микола Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і захисту інформації Київського національного університету імені Тараса Шевченка.
Mykola Brailovskyi, PhD in Engineering Science, Associate Professor, Associate Professor of department of Cybersecurity and Information Protection of the Taras Shevchenko National University of Kyiv.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Yuliia Khokhlachova, PhD of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Капустян Марія Вікторівна, кандидат технічних наук, доцент, доцент кафедри систем і захисту інформації Хмельницького національного університету.
Mariia Kapustian, PhD of technical sciences, associate professor, associate professor of the department of systems and information protection of Khmelnitsky National University.
E-mail: kapustian.mariia@gmail.com.
Orcid ID: 0000-0001-9200-1622.

DOI: 10.18372/2410-7840.24.17266
УДК 004.681.3

МАТРИЧНИЙ ПОМНОЖУВАЧ ЗА МОДУЛЕМ ДЛЯ КРИПТОГРАІЧНИХ ПЕРЕТВОРЕНЬ

Максим Луцький, Сахибай Тинимбаєв, Сергій Гнатюк, Рат Бердібаєв, Юлія Поліщук

Сьогодні для шифрування даних найбільш широко застосовують три види шифраторів: апаратні, програмно-апаратні і програмні. Їх основна відмінність полягає не лише у способі реалізації шифрування та ступеня надійності захисту даних, але й ціною, що часто стає для користувачів визначальним чинником. Незважаючи на те, що ціна апаратних шифраторів істотно вища ніж програмних, різниця в ціні не спів-ставна із значним підвищенням якості захисту інформації. Апаратне шифрування має низку вагомих переваг перед програмним шифруванням, одна з яких – більш висока швидкодія. Апаратна реалізація гарантує цілісність процесу шифрування. При цьому генерування і збереження ключів, а також шифрування, здійснюється у самій платі шифратора, а не в операційній пам'яті комп'ютера. З огляду на це, розробка швидкодіючих операційних блоків апаратних процесорів для асиметричного шифрування, не дивлячись на їх високу вартість, є актуальною науковою та прикладною задачею. У цій статті проводиться аналіз сучасних підходів до множення чисел за модулем, виділено їх сильні та слабкі сторони. Досліджено алгоритм множення з покроковим формуванням часткових і проміжних залишків, що в свою чергу, не потребує ви-конання попередніх обчислень, а всі обчислення не виходять за діапазон розрядної сітки модуля. Як результат, розроблено синхронний матричний помножувач, який містить n блоків схем I, n-1 FPR і єдиний FIR з регістром проміжного залишку, що буде корисним для криптографічних перетворень в системах з підвищеними вимогами до швидкодії та рівня інформаційної безпеки (наприклад, в критичній інформаційній інфраструктурі).

Ключові слова: *криптосистема з відкритим ключем, апаратне шифрування, формувач залишків, помножувач.*

ВСТУП

В асиметричних криптосистемах процедура шифрування і дешифрування даних проводиться піднесенням числа a до степеню x за модулем P (a^x modP), якого можна реалізувати програним, програмно-апаратним і апаратним засобами [1, 2].

Апаратне шифрування має низку вагомих переваг перед програмним шифруванням, одна з яких (і ймовірно найбільш суттєва) – більш висока швидкодія. Апаратна реалізація гарантує цілісність процесу шифрування. При цьому генерування і збереження ключів, а також шифрування здійснюється безпосередньо у самій платі шифратора, а не в операційній пам'яті комп'ютера.

Сьогодні, розробка швидкодіючих операційних блоків апаратних процесорів для асиметричного шифрування, не дивлячись на їх високу вартість, є актуальною науково-прикладною задачею.