УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03058 Київ, Україна

Модель загроз у розподілених мережах

Розглянуто питання захисту інформаційних ресурсів розподіленої обчислювальної мережі, наведено характеристику та механізми реалізації загроз у розподілених мережах, запропоновано модель загроз.

Ключові слова: *загроза, порушник, ресурси, модель загроз.*

Вступ

Побудова системи захисту інформаційних об'єктів розподіленої обчислювальної мережі (РОМ) передбачає детальний аналіз множини можливих загроз, визначення їхніх характеристик, механізмів і наслідків впливу. Узагальнену інформацію щодо цієї множини будемо називати моделлю загроз. Для побудови такої моделі розподілену обчислювальну мережу будемо розглядати як таку, яка складається з територіально рознесених програмно-технічних комплексів — вузлів РОМ, що входять до складу структурних підрозділів відомства (корпорації) і забезпечують функціонування РОМ. Будемо вважати, що структурно РОМ є ієрархічною автоматизованою системою, в якій визначаються певні рівні ієрархії. У свою чергу, вузли різних рівнів РОМ взаємодіють між собою за визначеними правилами (протоколами) та технологією [1].

Особливістю такої системи є те, що її компоненти розподілені в просторі й зв'язок між ними фізично здійснюється за допомогою мережних з'єднань і програмно — за допомогою механізму повідомлень. При цьому всі повідомлення й дані, що пересилаються між об'єктами розподіленої обчислювальної системи, передаються мережними комунікаціями у вигляді пакетів обміну. Ця особливість і є основною для розглянутих у статті атак (перш за все — віддалених атак) на інфраструктуру та протоколи розподілених обчислювальних мереж.

Будемо вважати (у більшості практичних випадків це є правилом), що в РОМ, як і в других типах комп'ютерних систем, для убезпечення від загроз інформаційним об'єктам, мережі чи її елементам застосовується певна множина програмно-технічних засобів захисту, наявність, можливості та характеристики яких можуть бути невідомими потенційним навмисним чи випадковим порушникам.

Аналіз і моделювання загроз у РОМ, включаючи їхню взаємодію із засобами захисту, надає змогу визначити як їхній склад і структуру, так і можливі значення величин залишкового ризику системи захисту в цілому чи по окремих функціональних властивостях захищеності інформаційних об'єктів та їхніх потоків.

Типові віддалені загрози в розподілених мережах. Розвідка, аналіз трафіка

РОМ є принадливою [1] для багатьох загроз як ненавмисних, так і зловмисних (у першу чергу, несанкціонованих) дій, і в певних випадках ці загрози можуть бути реалізованими успішно. Це пов'язано як із можливою високою професійністю порушників, так і з вразливістю всіх комп'ютеризованих систем. Дослідження й аналіз інформаційної безпеки різних розподілених обчислювальних систем [2–11] підтверджують той факт, що, незалежно від використовуваних мережних протоколів, топології, інфраструктури розподілених обчислювальних систем, механізми реалізації загроз у РОМ є інваріантними стосовно особливостей конкретної системи. Це пояснюється тим, що розподілені обчислювальні системи проектуються на основі однакових принципів, отже мають практично однакові проблеми безпеки. Тому виявляється, що причини успіху атак на різні РОМ однакові. Таким чином, з'являється можливість увести поняття типової віддаленої загрози.

***Типова віддалена загроза* (*ВЗ*)** — це віддалений інформаційний вплив, що програмно здійснюється каналами телекомунікаційної мережі з метою порушення тієї чи іншої функціональної властивості захищеності (конфіденційності, доступності, цілісності) інформаційних об'єктів, їхніх потоків чи елементів мережі та є характерним для будь-якої розподіленої обчислювальної системи.

Цілком зрозумілим є твердження про те, що, з метою успішності атаки більшість порушників здійснить хоча би поверхневий моніторинг структури мережі, побудови її мапи, визначення точок вразливостей мережі та мережного трафіка. Такий моніторинг часто відносять до окремого виду загроз, який називають **розвідкою**.

Найпоширенішим видом розвідки є аналіз мережного трафіка. Аналіз мережного трафіка дозволяє, по-перше, вивчити логіку роботи розподіленої обчислювальної системи, тобто одержати взаємно однозначну відповідність подій, що відбуваються в системі, і команд, що пересилаються один одному її об'єктами, у момент появи цих подій. Це досягається шляхом перехоплення й аналізу пакетів обміну на канальному рівні. Знання логіки роботи розподіленої обчислювальної системи дозволяє на практиці моделювати й здійснювати типові віддалені атаки. По-друге, аналіз мережного трафіка дозволяє перехопити потік даних, якими обмінюються об'єкти розподіленої обчислювальної системи. Таким чином, віддалена атака даного типу полягає в одержанні на віддаленому об'єкті несанкціонованого доступу до інформації, якою обмінюються два мережних абоненти. Відзначимо, що при цьому відсутня можливість модифікації трафіка, й сам аналіз можливий тільки всередині одного сегмента мережі. Прикладом перехопленої за допомогою даної типової віддаленої атаки інформації можуть служити ім'я та пароль користувача, що пересилаються в незашифрованому вигляді мережею.

Інформація, що отримується за результатами розвідки, може використовуватися для реалізації загроз (здійснення атак) того чи іншого типу.

Загрози інформаційним об'єктам у розподілених мережах

Як відомо [1], уся множина загроз, що реалізуються навмисними чи випадковими порушниками в будь-якій системі, у тому числі й у РОМ, може буди розглянута як сукупність атак на основні функціональні властивості захищеності інформаційних об'єктів та їхніх потоків — конфіденційність, цілісність, доступність інформаційних об'єктів, системи чи її елементів.

У [2–11] та інших джерелах досить детально розглянуто сукупність можливих загроз щодо ресурсів локальних обчислювальних мереж. Зокрема, показано, що шляхами реалізації таких загроз щодо *конфіденційності інформаційних ресурсів* є:

1) несанкціонований доступ до інформаційних ресурсів із подоланням засобів захисту в локальній мережі чи в елементах розподіленої мережі;

2) використання витоків інформації технічними каналами в локальній мережі чи в елементах розподіленої мережі;

3) подолання неавторизованим користувачем криптографічної захищеності інформаційних об'єктів (у разі її наявності) у локальній мережі чи в елементах розподіленої мережі;

4) використання спеціальних типів вірусних атак, спроможних збирати та передавати конфіденційну інформацію про користувача та інформаційні об'єкти даного хосту, згодом посилаючи її своїм «господарям» без відома власника хосту (так звані програми-шпигуни — spyware), або ж таких, що переводять захищений інформаційний ресурс із розряду конфіденційного до розряду відкритого.

У свою чергу, *загрозами порушення цілісності інформаційних об'єктів*, тобто несанкціонованої модифікації інформації тим чи іншим чином, є:

1) несанкціонований доступ до інформаційних ресурсів із подоланням засобів захисту в локальній мережі чи в елементах розподіленої мережі;

2) використання спеціальних впливів на інформацію технічними каналами в локальній мережі чи в елементах розподіленої мережі;

3) використання спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності (модифікацію чи підміну) інформаційного об'єкта.

І, нарешті, *загрозами порушення доступності інформаційних об'єктів*, тобто несанкціонованої організації блокування сервісу чи доступу тим або іншим чином (штучна відмова в доступі, в обслуговуванні), з урахуванням визначення цієї функціональної властивості в існуючих нормативних документах, є:

1) порушення цілісності інформаційного об'єкта за вже вищевизначених умов;

2) штучно створена відмова в обслуговуванні шляхом утримування потрібного користувачеві об'єкта чи сервісу в процесі використання з порушенням правил, які встановлені політикою безпеки щодо часу очікування авторизованим користувачем доступу до інформації (користувач очікує довше заданого (малого) проміжку часу, або інформація не знаходиться користувачем у той час, коли вона йому необхідна);

3) блокування зловмисником доступу до інформаційних об'єктів чи сервісів шляхом перевантаження системи управління доступом запитами з використанням атак типу «спрямований шторм» (Syn Flood), анонімної електронної пошти (spam) чи вірусних атак спеціального типу.

Аналіз цієї множини дозволяє визначити в їхньому складі основну загрозу — загрозу несанкціонованого доступу, яка є умовою порушення всіх функціональних властивостей захищеності інформаційних об'єктів та їхніх потоків, а також підмножини вірусних атак, які є специфічними кожній із функціональних властивостей захищеності (використання спеціальних типів вірусних атак). Що ж стосується атак, пов'язаних із використанням витоків та спеціальних впливів на інформацію технічними каналами, то їхнє використання в РОМ є малоймовірним, і тому вони надалі не розглядаються.

Несанкціонований доступ у розподілених мережах. Механізми його реалізації

Несанкціонований доступ представляє собою спробу порушника отримати доступ до мережних ресурсів без відповідного дозволу. Несанкціонований доступ дозволяє: неавторизовану маніпуляцію даними (читання, модифікацію, копіювання або переміщення файлів, підробку мережних адрес, переключення з'єднань, зміну маршрутів); доступ до системи (реєстрація зі «стороннім» обліковим записом — імітація, маскування, встановлення та розсилка зловмисного програмного забезпечення для здійснення подальших атак, несанкціоноване встановлення й використання мережних з'єднань, несанкціоноване використання комунікаційних протоколів, використання комунікаційних з'єднань для атак, використання хибних налагоджень, використання внутрішніх помилок, відторгнення комунікаційних відношень); підвищення прав доступу (отримання інформації або виконання процедур, що не є доступними при встановленому для користувача рівні доступу).

У розподілених мережах несанкціонований доступ може реалізовуватися такими специфічними прийомами як подолання:

— систем адміністрування доступом до захищеного інформаційного об'єкта, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані тощо). У межах даної статті цей тип НСД не розглядається;

— систем адміністрування доступом до робочих станцій, локальних мереж і т.п., заснованих на атрибутах робочих станцій чи засобів управління доступом і маршрутизації відповідних мереж (файрволів, проксі-серверів, маршрутизаторів тощо).

Останній тип НСД ***використовує недостатню стійкість відповідних механізмів ідентифікації та автентифікації*** й може мати характер ***імітації, маскування довіреного об'єкта або суб'єкта*** шляхом:

— підміни довіреного об'єкта або суб'єкта розподіленої обчислювальної системи;

— впровадження в розподілену обчислювальну систему хибного об'єкта, зокрема, шляхом нав'язування хибного маршруту (зміна маршрутизації) чи з використанням недоліків алгоритмів віддаленого пошуку (атаки типу «людина всередині»).

Імітація має на увазі фальсифікацію (порушення цілісності) IP-адреси, повторне відтворення повідомлень (порушення доступності) з метою захоплення сеансу зв'язку, зміну параметрів маршрутизації й змісту інформації, що передається. Згадана вище недостатня ідентифікація й автентифікація віддалених один від одного об'єктів полягає, перш за все, у труднощах здійснення однозначної

ідентифікації повідомлень, переданих між суб'єктами й об'єктами взаємодії. Звичайно, у розподілених обчислювальних системах ця проблема вирішується в такий спосіб: у процесі створення *віртуального каналу* об'єкти РОМ обмінюються певною інформацією, що унікально ідентифікує даний канал. Такий обмін, звичайно, називається «рукостисканням» (handshake). Для надійної ідентифікації й автентифікації повідомлень, у принципі, можна використати, по-перше, гешфункції, які обчислюються за допомогою, наприклад, відкритого ключа, динамічно виробленого при встановленні каналу, й, по-друге, випадкові багатобітні лічильники пакетів і мережні адреси станцій. Однак на практиці, наприклад, у протоколі TCP для ідентифікації використаються лише два 32-бітних лічильники.

Відзначимо, що не завжди для зв'язку двох віддалених об'єктів у РОМ створюється віртуальний канал. Практика показує, що найчастіше, особливо для службових повідомлень (наприклад, від маршрутизаторів) використовується передача одиночних повідомлень без підтвердження.

Окрім того відомо, що для адресації повідомлень у розподілених обчислювальних системах використовуються мережні адреси, що є унікальними для кожного об'єкта системи (на канальному рівні моделі OSI — це апаратурна адреса мережного адаптера, на мережному рівні — адреса визначається залежно від використовуваного протоколу мережного рівня (наприклад, IP-адреса). Мережна адреса також може використовуватися для ідентифікації об'єктів розподіленої обчислювальної системи. Однак мережна адреса не є прихованою інформацією й досить просто підробляється. Звідси випливає, що ***одним із механізмів несанкціонованого доступу є підробка*** (*для об'єктів взаємодії — порушення цілісності*) ***мережних адрес*** тих об'єктів, що атакують. Тому використовувати мережні адреси, як єдиний засіб ідентифікації об'єктів, неприпустимо.

У цьому випадку є можливою також типова віддалена атака, яка полягає в передачі мережею повідомлень від імені довільного об'єкта або суб'єкта РОМ (*маскування*).

Реалізація механізму віддалених атак щодо несанкціонованого доступу з підробкою (порушенням цілісності) мережних адрес звичайно складається з:

1) передачі пакетів обміну з атакуючого об'єкта на мету атаки від імені довіреного суб'єкта взаємодії (при цьому передані повідомлення будуть сприйняті системою як коректні);

2) передачі службових повідомлень від імені мережних керуючих пристроїв, наприклад, від імені маршрутизаторів.

Наступним механізмом ***несанкціонованого доступу є зміна параметрів маршрутизації***. Це пов'язано з тією особливістю РОМ, що сучасні глобальні мережі представляють собою сукупність сегментів мережі, пов'язаних між собою через мережні вузли. Для забезпечення ефективної й оптимальної маршрутизації в розподілених обчислювальних системах застосовуються спеціальні керуючі протоколи, що дозволяють маршрутизаторам обмінюватись інформацією один з одним, повідомляти хости про новий маршрут, віддалено управляти маршрутизаторами. При цьому абсолютно очевидно, що маршрутизація в глобальних мережах відіграє найважливішу роль і, як наслідок цього, може піддаватися атаці. Основна мета атаки, пов'язаної з нав'язуванням хибного маршруту, полягає в тому, щоб змінити (*порушити цілісність*, модифікувати) вихідну маршрутизацію на об'єкті розподіленої обчислювальної системи так, щоб новий маршрут проходив через

хибний об'єкт — хост атакуючого. Реалізація даної типової віддаленої атаки складається в несанкціонованому використанні протоколів керування мережею для зміни вихідних таблиць маршрутизації.

Для зміни маршрутизації атакуючому необхідно послати по мережі для протоколів керування мережею спеціальні службові повідомлення від імені мережних керуючих пристроїв (наприклад, маршрутизаторів). У результаті успішної зміни маршруту атакуючий одержить повний контроль (можливість *порушення конфіденційності, цілісності та доступності*) над потоком інформації, яким обмінюються два об'єкти розподіленої обчислювальної системи, і атака перейде до другої стадії, пов'язаної з прийманням, аналізом і передачею повідомлень, одержуваних, наприклад, від дезінформованих (у разі *порушення цілісності*) об'єктів РОМ.

У розподіленій обчислювальній системі часто виявляється, що її віддалені об'єкти споконвічно не мають досить інформації, що необхідна для адресації повідомлень. Звичайно, такою інформацією є апаратурні (адреса мережного адаптера) і логічні (наприклад, IP-адреса) адреси об'єктів РОМ. Для одержання подібної інформації в розподілених обчислювальних системах використовуються різні *алгоритми віддаленого пошуку*, що полягають у передачі мережею спеціального виду пошукових запитів і очікуванні відповідей на запит із шуканою інформацією. Після одержання відповіді на запит суб'єкт РОМ, що запросив, має всі необхідні дані для адресації. Керуючись отриманими з відповіді відомостями про шуканий об'єкт, суб'єкт РОМ, що запросив, починає адресуватися до нього, маючи можливості *порушення конфіденційності та доступності* певної інформації чи шуканого об'єкта.

У випадку використання розподіленої обчислювальної системи механізмів віддаленого пошуку існує можливість на атакуючому об'єкті перехопити посланий запит і надіслати на нього хибну відповідь (*здійснити маскування*), де вказати дані, використання яких приведе до адресації на атакуючий хибний об'єкт. Надалі весь потік інформації між суб'єктом й об'єктом взаємодії буде проходити через хибний об'єкт РОМ.

Ще одним механізмом ***несанкціонованого доступу є використання недоліків алгоритму віддаленого пошуку***, наслідком чого є ***впровадження*** зловмисниками в систему об'єктів, що мають назву ***«Хибних об'єктів РОМ»***. Цей варіант впровадження в РОМ хибного об'єкта складається в *періодичній передачі на об'єкт, що атакується, заздалегідь підготовленої хибної відповіді* без приймання пошукового запиту. Справді, для того щоб послати хибну відповідь, не завжди обов'язково чекати приймання запиту (може, в принципі, не бути можливості перехоплення запиту). При цьому атакуючий може спровокувати об'єкт, що атакується, на передачу пошукового запиту, і тоді його хибна відповідь буде негайно мати успіх. Дана типова віддалена атака надзвичайно характерна для глобальних мереж, коли просто немає можливості перехопити пошуковий запит. Використання хибного об'єкта для організації віддаленої атаки на розподілену обчислювальну систему дає змогу одержати контроль над потоком інформації між об'єктами й застосовувати різні методи впливу на перехоплену інформацію. Одним із таких методів є **селекція потоку інформації й збереження її на хибному об'єкті РОМ** шляхом перехоплення переданої між суб'єктом й об'єктом взаємодії інформації. Важливо відзначити, що перехоплення інформації (наприклад, файлів) можливе

через те, що при виконанні деяких операцій над файлами (читання, копіювання тощо) зміст цих файлів передається мережею, а надходить на хибний об'єкт. Найпростіший спосіб реалізації перехоплення — це збереження у файлі всіх одержуваних хибним об'єктом пакетів обміну. Проте, даний спосіб перехоплення інформації виявляється недостатньо інформативним. Це відбувається внаслідок того, що в пакетах обміну крім полів даних існують службові поля, що не представляють у цьому випадку для атакуючого безпосереднього інтересу. Отже, для того щоб одержати безпосередньо переданий файл, необхідно проводити на хибному об'єкті динамічний семантичний аналіз потоку інформації для його селекції.

Специфічні загрози

Подолання конфіденційності інформаційних об'єктів. Окрім ознайомлення зі змістом інформаційних об'єктів унаслідок несанкціонованого доступу, можливі й деякі види специфічних загроз. До специфічних загроз конфіденційності можна віднести використання витоків технічними каналами та специфічних вірусних атак шляхом впровадження програм-шпигунів (spyware), які збирають про користувача даного ПК інформацію, згодом посилаючи її своїм «господарям» без відома власника комп'ютера. Встановлюються вони автоматично під час Web-серфінгу або поставляються разом із поширюваними через Internet додатками (особливо безкоштовними). Для очищення комп'ютера від spyware розумно використовувати тільки спеціалізоване ПО, оскільки антивіруси класифікують багато шпигунів як безпечні програми. Вручну ж видалити шпигуна достатньо важко, оскільки він прописується в численних ключах реєстру й не завжди в явному вигляді може створювати свої копії в різних місцях файлової системи.

Порушення цілісності (вилучення, зміна чи підміна) інформаційного об'єкта є можливим шляхом тієї чи іншої, у залежності від задач порушника, модифікації переданих даних чи програмного коду. Для випадку текстових файлів або файлів даних несанкціонований доступ забезпечує можливість будь-якої модифікації. Для випадку модифікації програмного коду представляється можливим виділити два різних за метою види модифікації коду: по-перше, впровадження руйнуючих програмних засобів (РПЗ), по-друге, зміна логіки роботи програмного файлу. Нарешті, внаслідок модифікації чи підміни одному з учасників обміну може бути посланою заздалегідь підготовлена дезінформація. При цьому така дезінформація, залежно від контрольованої події, може бути сприйнята або як програмний код, або як дані. Приклад такої дезінформації — впровадження спеціального коду заздалегідь написаної спеціальної програми-загарбника паролів. Ця програма виконує візуально ті ж дії, що й дійсна програма входу в систему, наприклад, запитує ім'я та пароль користувача, після чого отримані відомості пересилаються на хибний об'єкт (об'єкт, створений зловмисником), а користувачеві виводиться повідомлення про помилку. При цьому користувач, вважаючи, що він неправильно ввів пароль (пароль, звичайно, не відображається на екрані) знову запустить програму підключення до системи (цього разу дійсну) і з другого разу одержить доступ. Результат такої атаки — ім'я та пароль користувача, збережені на хибному об'єкті.

Загрози доступності. Нагадаємо, що доступність — це властивість ресурсу системи (послуги, об'єкта, інформації), яка полягає в тому, що користувач і/або процес, який має відповідні повноваження, може використовувати ресурс відповідно до правил, установлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, у місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Наразі в мережах вирізняють такі атаки доступності як блокування того чи іншого сервісу (послуги) та організацію штучної відмови в обслуговуванні.

Блокування сервісу означає спробу порушити або зупинити роботу мережі, всієї системи або окремих сервісів, що веде до відмови в обслуговуванні запитів авторизованих користувачів. Відмова в обслуговуванні може бути викликана випадково некоректними діями користувачів або адміністратора, відмовами обладнання або навмисними діями порушників. Атаки блокування сервісів спрямо-вані проти маршрутизаторів периметра, бастіонного хоста або брандмауера.

Відмова в обслуговуванні (*DoS атака*). Одним з основних завдань, покладених на мережну ОС, що функціонує на кожному з об'єктів розподіленої обчислювальної системи, є забезпечення надійного віддаленого доступу з будь-якого об'єкта мережі до даного об'єкта. Порушення працездатності відповідної послуги надання віддаленого доступу, тобто неможливість одержання віддаленого доступу з інших об'єктів РОМ — «Відмова в обслуговуванні».

У загальному випадку в розподіленій обчислювальній системі кожен суб'єкт системи повинен мати можливість підключитися до будь-якого об'єкта РОМ й одержати у відповідності зі своїми правами віддалений доступ до його ресурсів. Звичайно в обчислювальних мережах можливість надання віддаленого доступу реалізується в такий спосіб: на об'єкті РОМ у мережній ОС запускаються на виконання ряд програм-серверів (наприклад, FTP-сервер, WWW-сервер і т.п.), що надають віддалений доступ до ресурсів даного об'єкта. Дані засоби входять до складу телекомунікаційних послуг надання віддаленого доступу. Завдання сервера полягає в тому, щоб, перебуваючи в пам'яті операційної системи об'єкта РОМ, постійно очікувати одержання запиту на підключення від віддаленого об'єкта. У випадку одержання подібного запиту сервер повинен по можливості передати на об'єкт, що запросив, відповідь, в якій або дозволити підключення, або заборонити його (підключення до сервера спеціально описано дуже схематично, тому що подробиці в цей момент не мають значення). За аналогічною схемою відбувається створення віртуального каналу зв'язку, яким звичайно взаємодіють об'єкти РОМ. У цьому випадку безпосереднє ядро мережної ОС обробляє зовнішні запити на створення віртуального каналу (ВК) і передає їх відповідно до ідентифікатора запиту (порт або сокет) прикладному процесу, яким є відповідний сервер.

Очевидно, що мережна операційна система здатна мати тільки обмежене число відкритих віртуальних з'єднань і відповідати лише на обмежене число запитів. Ці обмеження залежать від різних параметрів системи в цілому, основними з яких є швидкодія ЕОМ, обсяг оперативної пам'яті й пропускна здатність каналу зв'язку — максимальний трафік (чим він вище, тим більше число можливих запитів за одиницю часу).

Інфраструктура РОМ дозволяє з одного з її об'єктів (якщо в розподіленій обчислювальній системі не передбачено засобів автентифікації адреси відправника),

передавати на інший об'єкт, що атакується, нескінченне число запитів (можливо анонімних) на обробку запитів чи на підключення. У цьому випадку буде мати успіх типова віддалена атака «Відмова в обслуговуванні». Результат застосування цієї віддаленої атаки — порушення на об'єкті, що атакований, працездатності відповідної служби надання віддаленого доступу, тобто неможливість одержання віддаленого доступу з інших об'єктів РОМ — відмова в обслуговуванні.

Другий різновид цієї типової віддаленої атаки складається в передачі на одну адресу (на один об'єкт, що атакується) такої кількості запитів (спрямований «шторм» запитів), яку дозволить мережний трафік. У цьому випадку, якщо в системі не передбачені правила, що обмежують число прийнятих запитів за одиницю часу, то результатом цієї атаки може бути як переповнення черги запитів і відмова однієї з телекомунікаційних служб, так і повна зупинка хосту, який атакується, через неможливість його системи займатися нічим іншим, крім обробки запитів. Для організації такого типу атаки потрібна координація зусиль певної групи об'єктів, що, з погляду об'єкта, який атакується, є злочинним угрупуванням.

І останнім, третім різновидом атаки «Відмова в обслуговуванні» є передача на об'єкт, що атакується, некоректного, спеціально підібраного запиту. У цьому випадку за наявності помилок у віддаленій системі можливе зациклювання процедури обробки запитів, переповнення буфера з наступним «зависанням системи» («Ping Death») тощо.

Модель загроз у РОМ

Розглянутий досить детальний аналіз множини можливих загроз дозволяє здійснити наступний крок у визначенні сукупності потрібних засобів захисту інформаційних об'єктів відповідної РОМ і побудові системи захисту. Цим кроком є побудова моделі загроз. Приклад моделі загроз та їхньої ідентифікації з можливими діями порушників щодо об'єктів захисту, тобто перелік загроз із констатацією можливих дій порушників щодо відповідних об'єктів, на порушення властивостей захищеності яких вони спрямовані — порушення конфіденційності (к), цілісності (ц), доступності (д) інформаційних об'єктів РОМ, а також оцінка ймовірності здійснення загроз і рівень збитків (шкоди) від порушень по кожному з видів порушень; джерело виникнення — які внутрішні чи зовнішні суб'єкти можуть ініціювати загрозу, наведено в таблиці.

Методика розроблення такої моделі полягає в тому, що в один зі стовпчиків таблиці заноситься по можливості повний перелік видів загроз; у наведеному прикладі такий перелік наведено в стовпчику 2. Надалі для кожної з можливих загроз шляхом їхнього аналізу (можливо й методом експертних оцінок) необхідно визначити:

— ймовірність виникнення таких загроз. Як перший крок визначення такої ймовірності можна використати її якісні оцінки. У таблиці можуть бути наведені якісні оцінки їхньої ймовірності — неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька (стовпчик 3);

— на порушення яких функціональних властивостей захищеності інформації (стовпчик 4) вона спрямована (порушення конфіденційності — к, цілісності — ц, доступності — д);

— можливий (такий, що очікується) рівень шкоди (стовпчик 5). Приклад цієї оцінки наведено також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока). Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної із властивостей захищеності інформації;

— механізми реалізації (можливі шляхи здійснення загроз) (стовпчик 6). Наявність такої інформації дозволяє побудувати загальну модель системи захисту; оцінити значення залишкового ризику, як функцію захищеності по кожній із функціональних властивостей захищеності; визначити структуру системи захисту та її основні компоненти.

Модель загроз у РОМ

№№ з/п	Вид загроз	Імовірність	Що порушує	Рівень шкоди	Механізм реалізації
1	2	3	4	5	6
Моніторинг (розвідка) мережі					
1	Розвідка, аналіз трафіка	висока	к, ц, д	відсутня	Перехоплення інформації, що пересилається, у незашифрованому вигляді в широкомовному середовищі передачі даних, відсутність виділеного каналу зв’язку між об’єктами РОМ
Несанкціонований доступ до інформаційних ресурсів із РОМ					
1	Підміна (імітація) довіреного об’єкта або суб’єкта РОМ із підробкою мережних адрес тих об’єктів, що атакують	висока	к, ц, д	середній	Фальсифікація (підробка мережних адрес IP-адреси, повторне відтворення повідомлень при відсутності вір туального каналу, недостатні ідентифікації та автентифікації при наявності віртуального каналу
2	Зміна маршрутизації	неприпустимо висока	к, ц, д	низький	Зміна параметрів маршрутизації й змісту інформації, що передається, внаслідок відсутності контролю за маршрутом повідомлень чи відсутності фільтрації пакетів із невірною адресою
3	Селекція потоку інформації та збереження її шляхом впровадження в розподілену обчислювальну систему хибних об’єктів (атаки типу «людина всередині»)	висока	к, ц, д	високий	Використання недоліків алгоритмів віддаленого пошуку

Продовження таблиці

1	2	3	4	5	6
4	Подолання систем адміністрування доступом до робочих станцій, локальних мереж і захищеного інформаційного об'єкта, заснованих на атрибутах робочих станцій чи засобів управління доступом і маршрутизації (маскування) відповідних мереж — (файрволів, проксі-серверів, маршрутизаторів тощо)	висока	к, ц, д	високий	Використання недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.). Недостатні ідентифікації та автентифікації об'єктів РОМ, зокрема, адреси відправника
Специфічні загрози інформаційним об'єктам					
1	Подолання криптографічної захищеності інформаційних об'єктів, що перехоплені	низька	к	високий	Використання витоків технічними каналами, вилучення із мережі специфічних вірусних атак шляхом впровадження програм-шпигунів (spyware) із розкриттям ключових наборів
2	Подолання криптографічної захищеності інформаційних об'єктів робочих станцій	низька	к	високий	Несанкціонований доступ до інформаційних об'єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.) із розкриттям ключових наборів
3	Модифікація переданих даних, даних чи програмного коду, що зберігаються в елементах обчислювальних систем	висока	ц, д	високий	Модифікація чи підміна інформаційних об'єктів (програмних кодів) чи їхніх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності
					Викривлення певної кількості символів інформаційного об'єкта із використанням спеціальних впливів на інформацію технічними каналами в локальній мережі чи в елементах розподіленої мережі

Продовження таблиці

1	2	3	4	5	6
4	Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні)	висока	д	високий	Використання атак типу «спрямований шторм» (Syn Flood), передачі на об’єкт, що атакується, некоректних, спеціально підібраних запитів
					Використання анонімних (чи із модифікованими адресами) запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу

Слід урахувати, що наведені оцінки ймовірностей і величини можливої шкоди кожної із загроз у даному прикладі моделі загроз носять ілюстративний характер. Для випадків конкретних РОМ ці величини повинні бути визначеними фахівцями служби захисту відповідного підприємства за окремими методиками.

Таким чином, запропонований у статті аналіз множини можливих типових віддалених загроз у розподілених мережах дає можливість із застосуванням нескладної методики побудови моделі таких загроз визначити складові політики безпеки інформаційних об’єктів відповідної РОМ і визначити сукупність потрібних засобів захисту інформаційних об’єктів від можливих загроз із середовища РОМ.

1. *Матов О.Я., Василенко В.С., Будько М.М.* Оцінка захищеності в локальних обчислювальних мережах // Вісті Академії інженерних наук України. — К., 2005. — № 2. — С. 59−73.

2. Maximum Security: A Hacker’s Guide to Protecting Your Internet Site and Network. — http://zaphod.redwave.net/books/hackg/index.htm

3. TCP під прицілом. — http://www.hackzone. ru/articles/tcp.html

4. Деякі проблеми FTP. — http://www. hackzone.ru /articles/ftp.html

5. Атака на DNS, або нічний кошмар мережного адміністратора. — http://www.hackzone.ru/articles/dns−poison.html

6. *Медведовский И.Д. Семьянов П.В. Леонов Д.Г.* Атака на Интернет. — М.: Видавництво ДВК, 1999.

7. *Соболев К.И.* Дослідження системи безпеки з Windows NT 4.0 HackZone: Територія злому. — 1998. — № 1−2.

8. Переповнення буфера в WIN32. — http://www.void.ru/stat/9907/20.html

9. EXPLOITи переповнення буфера на PERL’е (http://www.void.ru/stat/0102/02.html).

10. Теорія та практика атак FORMAT STRING. — http://www.void.ru/stat/0102/27.html+http://www.void. ru/stat/0102/28.html

11. Перехоплення пакетів TCP: Захист від флуда. — http://www.void. ru/stat/9907/19.html

Надійшла до редакції 05.11.2007