Література: ***1.*** *Siegenthaler T. Correlation immunity of non-linear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, Vol.30, 1984. pp. 776-780.* ***2.*** *Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций, Дискретная математика, т. 3., вып. 2, 1991.* ***3.*** *Xiao G. Z. Correlation-immunity of Boolean functions // Electron. Lett. Vol.23. No.25. 1987.* ***4.*** *Yu. V. Tarannikov. On a method for the constructing of cryptographically strong Boolean functions. – Moscow State University, French-Russian Institute of Applied Mathematics and Informatics. Preprint No 6., Moscow, October 1999.* ***5.*** *Webster A. F., Tavers S. E. On the design of S-boxes, Advances in Cryptology, –Proc. Crypto'85, Springer-Verlag, 1986, pp. 523-534.* ***6.*** *Zhang X.-M., Zheng Y. Cryptographically Resilient Functions. // IEEE Trans. on Information Theory. 1997. Vol. 43. 5. pp. 1740-1747.* ***7.*** *Bierbrauer J., Gopalakrishnan K., Stinson D. R. Bounds on Resilient Functions and Orthogonal Arrays. // Advances in Cryptology: Crypto'94/ Lect. Notes in Comput. Sci. Vol. 839. New York: Springer-Verlag. 1994. pp. 247-256.* ***8.*** *Stinson D. R. Resilient Functions and Large Sets of Orthogonal Arrays. // Congressus Numerantium/ Vol. 92. 1993. pp. 105-110.* ***9.*** *Camion P., Carlet C., Charpin P., Sendrier N. On Correlation Immune Functions. // Advances in Cryptology: Crypto'91/ Lect. Notes in Comput. Sci. Vol. 576. New York: Springer-Verlag. 1992. pp. 86-100.* ***10.*** *Chee S., Lee S., Lee D., Sung S. H. On the Correlation Immune Functions and Their Nonlinearity. // Advances in Cryptology: ASIACRYPT'96/ Lect. Notes in Comput. Sci. Vol. 1163. New York: Springer-Verlag. 1996. pp. 232-243.* ***11.*** *Maitra S., Sarkar P. Highly Nonlinear Resilient Functions Optimizing Siegenthaler's Inequality. // Advances in Cryptology: Crypto'99/ Lect. Notes in Comput. Sci. Vol. 1666. New York: Springer-Verlag. 1999. pp. 198-215.* ***12.*** *Seberry J., Zhang X.-M., Zheng Y. On the Constructions and Nonlinearity of Correlation Immune Boolean Functions. // Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. Vol. 765. New York: Springer-Verlag. 1994. pp. 181-199.* ***13.*** *Carlet C. Partially-bent functions. // Designs Codes and Cryptography. 1993. 3. pp. 135-145.* ***14.*** *Filiol E., Fontaine C. Highly Nonlinear Balanced Boolean Functions with a Good Correlation-Immunity. // Advances in Cryptology: EUROCRYPT'98/ Lect. Notes in Comput. Sci. Vol. 1403. New York: Springer-Verlag. 1998. pp. 475-488.* ***15.*** *Millan W., Clark A., Dawson E. Heuristic Design of Cryptographically Strong Balanced Boolean Functions. // Advances in Cryptology: EUROCRYPT'98/ Lect. Notes in Comput. Sci. Vol. 1403. New York: Springer-Verlag. 1998. pp. 489-499.* ***16.*** *Maitra S. Correlation Immune Boolean Functions with Very High Nonlinearity. // http://www.eprint.iacr.org No. 2000/054.* ***17.*** *Serf P. The degrees of completeness of avalanche effect and of strict avalanche criterion for MARS, RC6, Rijndael, Serpent and Twofish with reduct number of rounds. Siemens AG, ZT IK 3, April3, 2000.*

УДК 681.3

ОЦІНКА ЗАГРОЗ В РОЗПОДІЛЕНИХ МЕРЕЖАХ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Розглядаються питання захисту інформаційних ресурсів комунікаційної мережі зв'язку розподіленої обчислювальної мережі, наводяться характеристики й механізми реалізації загроз в розподілених мережах, наводиться їх класифікація і пропонується модель загроз.**
Summary: **The questions of defense of informative resources of communication network of the distributed computer network are examined, description and mechanisms of realization of threats in the distributed networks is pointed, their classification is pointed and the model of threats is offered.**
Ключові слова: **Загроза, порушник, ресурси, модель. комунікаційна мережа.**

Вступ

Розподілену обчислювальну мережу (РОМ) будемо розглядати як таку, яка складається з територіально рознесених програмно-технічних комплексів (ПТК) – вузлів РОМ, що входять до складу структурних підрозділів відомства (корпорації) і забезпечують функціонування РОМ. Будемо вважати, що структурно РОМ є ієрархічною трьохрівневою автоматизованою системою, в якій визначаються центральний, регіональний і місцевий рівні. В свою чергу, вузли різних рівнів РОМ взаємодіють між собою за визначеними правилами (протоколами) та технологією.

Основною особливістю такої розподіленої системи є те, що її компоненти розподілені в просторі й зв'язок між ними здійснюється фізично за допомогою мережних з'єднань і програмно за допомогою механізму повідомлень. При цьому всі управляючі повідомлення й дані, що пересилаються між об'єктами розподіленої обчислювальної системи, передаються мережними з'єднаннями в вигляді пакетів обміну. Ця

особливість і є основною для розглянутих у статті атак (перш за все – віддалених атак) на інфраструктуру й протоколи розподілених обчислювальних мереж. Під час збору та обробки інформації центральний (ЦВ) та регіональні (РВ) вузли РОМ взаємодіють із зовнішніми користувачами з метою інформаційного забезпечення функціонування РОМ та надання відповідних інформаційних послуг користувачам.

Комунікаційна мережа зв'язку (КМЗ) є складовою частиною РОМ і призначається для розв'язання задач підтримки процесів обміну інформацією між центральним, регіональними та місцевими (МВ) вузлами РОМ під час формування і внесення інформації до інтегрованої бази даних, процесів інформаційного обслуговування запитів зовнішніх користувачів РОМ та інформаційного обміну з іншими базами даних загальновідомчого (загально корпоративного) значення.

І Характеристика й механізми реалізації типових атак в розподілених мережах

КМЗ, як і будь-який інший елемент РОМ [2 – 12], є принадливою для багатьох загроз, як ненавмисних, так і зловмисних (в першу чергу, несанкціонованих) дій. До основних джерел вразливості КМЗ, внаслідок яких виникають ті чи інші загрози, слід віднести: технологічні недоліки, недоліки конфігурування і недоліки політики безпеки.

1. *Технологічні недоліки* пов'язані з наступними основними причинами:
   - більшість мережних технологій розроблялася для надання доступу користувачам до ресурсів мережі без врахування вимог забезпечення безпеки;
   - незахищеність стандартних протоколів (TCP/IP, UDP, HTTP, SNMP, Telnet, SMTP, POP3, FTP, TFTP і т. п.);
   - наявність вразливостей у мережному обладнанні (не декларовані можливості, помилки в програмному забезпеченні, відсутність або недостатність існуючої системи автентифікації користувачів);
   - недоліки операційних систем мережного обладнання.
2. *Недоліки конфігурування* мережного обладнання та програмного забезпечення, пов'язані з:
   - небезпечними налагодженнями обладнання, що використовується по замовчуванню;
   - небезпечними налагодженнями системи контролю доступу, протоколів маршрутизації та управління;
   - незахищеністю облікових записів користувачів і слабкими паролями.
3. *До недоліків політики безпеки* відносяться:
   - відсутність документу, що описує політику безпеки;
   - наявність розбіжностей у встановленій політиці безпеки;
   - відсутність відпрацьованої схеми контролю доступу до мережного обладнання;
   - відсутність контролю встановлення та зміни програмного забезпечення, що використовується;
   - відсутність відпрацьованої процедури аналізу інцидентів і відновлення роботи після атаки;
   - неадекватне адміністрування, моніторинг і аудит мережної безпеки;
   - невідповідність програмного забезпечення і технічних засобів захисту, що використовуються, встановленій політиці безпеки;
   - відсутність інформування користувачів про можливості атак;
   - відсутність інформування користувачів про вимоги політики безпеки;
   - часта заміна персоналу, що відповідає за реалізацію політики безпеки.

Дослідження й аналіз інформаційної безпеки різних розподілених обчислювальних систем підтверджують той факт, що незалежно від використовуваних мережних протоколів, топології і інфраструктури розподілених обчислювальних систем механізми реалізації загроз на РОМ є інваріантними щодо особливостей конкретної системи. Це пояснюється тим, що розподілені обчислювальні системи проектуються на основі однакових принципів, а, отже, мають практично однакові проблеми безпеки. Тому виявляється, що причини успіху атак на різні РОМ однакові. Таким чином, з'являється можливість ввести поняття типової віддаленої загрози.

Типова віддалена загроза (*ВЗ*) − це віддалений інформаційний руйнуючий вплив, що здійснюється віддалено каналами зв'язку і є характерним для будь-якої розподіленої обчислювальної системи. Введення цього поняття в сукупності з описом механізмів реалізації типових ВЗ дозволяє запропонувати методику дослідження безпеки, інваріантну щодо виду розподіленої обчислювальної системи.

Така методика дослідження безпеки полягає в послідовному здійсненні всіх типових віддалених впливів згідно з їхнім описом і характеристиками. *Аналіз мережного трафіка* будемо вважати при цьому основним елементом дослідження безпеки РОМ. Як пояснення останнього твердження розглянемо наступну аналогію: відладчик − основний засіб для хакера, відповідно аналізатор мережного трафіка − основний засіб для мережного хакера. Аналізатор мережного трафіка за своєю суттю є мережним

відладчиком. Отже, як методика дослідження інформаційної безпеки розподіленої обчислювальної системи пропонується виконання ряду тестових завдань, що оцінюють захищеність системи стосовно типових віддалених впливів. Розглянемо типові віддалені атаки й механізми їхньої реалізації.

Видами загроз, що реалізуються найчастіше, є: *розвідка, аналіз мережного трафіка, несанкціонований доступ, блокування сервісу, імітація (підміна) довіреного об'єкта або суб'єкта розподіленої обчислювальної системи, перш за все шляхом впровадження в розподілену обчислювальну систему помилкових об'єктів та маршрутів, модифікація інформації, підміна інформації, відмова в обслуговуванні*.

Розвідка представляє собою несанкціоноване виявлення структури мережі, побудову її мапи і моніторинг системи, послуг і точок вразливостей. Крім того, до розвідки слід віднести моніторинг мережного трафіка. Розвідка може бути пасивною або активною. Інформація, що отримується за результатами розвідки, може використовуватися для проведення атак іншого типу або для викрадення важливих даних.

Аналіз мережного трафіка. Основною особливістю розподіленої обчислювальної системи є те, що її об'єкти розподілені в просторі й зв'язок між ними фізично здійснюється програмно по мережним з'єднанням − за допомогою механізму повідомлень. При цьому всі управляючі повідомлення й дані, що пересилають між об'єктами РОМ, передаються в мережі у вигляді пакетів обміну. Ця особливість приводить до появи специфічного для розподілених обчислювальних систем типового віддаленого впливу, що полягає в прослуховуванні каналу зв'язку. Назвемо даний типовий віддалений вплив *аналізом мережного трафіка* (або, скорочено, мережним аналізом).

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 пересилають один одному її об'єкти, 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 і пароль користувача, що пересилаються у незашифрованому виді мережею.

Несанкціонований доступ – це спроба порушника отримати доступ до мережних ресурсів без відповідного дозволу. Несанкціонований доступ передбачає: 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 – маскування, встановлення програмного забезпечення для здійснення подальших атак, розсилка зловмисного програмного забезпечення, несанкціоноване встановлення й використання з'єднань, несанкціоноване використання комунікаційних протоколів, використання комунікаційних з'єднань для атак, використання помилкових налагоджень, використання внутрішніх помилок, відторгнення комунікаційних відношень); підвищення прав доступу (отримання інформації або виконання процедур, що не є доступними при встановленому для користувача рівню доступу).

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 некоректними діями користувачів або адміністратора випадково, відмовами обладнання або навмисними діями порушників. Атаки блокування сервісів спрямовані проти маршрутизаторів периметра, бастіонного хоста або брандмауера.

Імітація (підміна) довіреного об'єкта або суб'єкта розподіленої обчислювальної системи. Однією з проблем безпеки розподіленої обчислювальної системи є недостатня ідентифікація й автентифікація її віддалених друг від друга об'єктів. Основні труднощі полягають у здійсненні однозначної ідентифікації повідомлень, переданих між суб'єктами й об'єктами взаємодії. Звичайно в 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). Однак, 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) використається передача одиночних повідомлень, які не потребують підтвердження.

Як відомо, для адресації повідомлень у розподілених обчислювальних системах використовується

мережна адреса, що є унікальною 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 використатися для ідентифікації об'єктів розподіленої обчислювальної системи. Однак мережна адреса досить просто підробляється й тому використати її як єдиний засіб ідентифікації об'єктів неприпустимо.

У тому випадку, коли розподілена обчислювальна система використовує нестійкі алгоритми ідентифікації віддалених об'єктів, виявляється можливою типова віддалена атака, яка полягає в передачі каналами зв'язку повідомлень від імені довільного об'єкта або суб'єкта РОМ. При цьому існують два різновиди даної типової віддаленої атаки:

атака при встановленому віртуальному каналі;

атака без установленого віртуального каналу.

У випадку встановленого віртуального з'єднання атака буде полягати в присвоєнні прав довірених суб'єктів взаємодії, які легально підключились до об'єкта системи, що дозволить атакуючому провести сеанс роботи з об'єктом розподіленої системи від імені довіреного суб'єкта. Реалізація віддалених атак даного типу звичайно складається в передачі пакетів обміну з атакуючого об'єкта на об'єкт атаки від імені довіреного суб'єкта взаємодії (при цьому передані повідомлення будуть сприйняті системою як коректні). Для здійснення атаки даного типу необхідно перебороти систему ідентифікації й автентифікації повідомлень, яка, в принципі, може використовувати контрольну суму, що обчислюється за допомогою відкритого ключа, динамічно виробленого при встановленні каналу, випадкові багатобітні лічильники пакетів і мережні адреси станцій.

Як було відмічено вище, для службових повідомлень у розподілених обчислювальних системах часто використовується передача одиночних повідомлень без підтвердження, тобто при цьому не потрібно створення віртуального з'єднання. У цьому випадку атака полягає в передачі службових повідомлень від імені мережних управляючих пристроїв, наприклад, від імені маршрутизаторів.

Очевидно, що при цьому для ідентифікації пакетів можливо використання лише статичних ключів, визначених заздалегідь, що досить незручно й потребує складної системи управління ключами. Однак, при відмові від такої системи ідентифікація пакетів без установленого віртуального каналу буде можлива лише за мережною адреси відправника, що легко підробити.

Посилка помилкових управяючих повідомлень може привести до серйозних порушень роботи розподіленої обчислювальної системи (наприклад, до зміни її конфігурації).

Отже імітація (підміна) має на увазі фальсифікацію IP-адреси, повторне відтворення повідомлень із метою захоплення сеансу зв'язку, зміну параметрів маршрутизації і змісту інформації, що передається.

До атак імітації відносяться *атаки посередників* (*"людина всередині"*), *впровадження в розподілену обчислювальну систему помилкових об'єктів, у тому числі шляхом нав'язування помилкового маршруту, а також шляхом використання недоліків алгоритмів віддаленого пошуку*.

Атака посередника (людина всередині) припускає участь в комунікаційній сесії трьох суб'єктів: клієнта, серверу і посередника-зловмисника, що знаходиться між ними. Таке положення дозволяє зловмиснику перехоплювати усі повідомлення, що циркулюють в обох напрямах і при бажанні підміняти їх.

"Посередник" прикидається сервером для клієнта і клієнтом для сервера. У разі використання сервером процедур "сертифікації" така атака неможлива. Це викликано тим, що під час діалогу про встановлення безпечного з'єднання з сервером необхідно надати сертифікат, підписаний сертифікаційним центром. У цьому сертифікаті розміщується загальнодоступний ключ серверу, його ім'я і ім'я емітента сертифікату. Клієнт веріфікує підпис сертифікату, а потім перевіряє ім'я емітента.

Якщо посередник надає підроблений сертифікат, то він не пройде перевірку підпису, оскільки зловмисник не може знати секретного ключа серверу.

Впровадження в розподілену обчислювальну систему помилкових об'єктів. У разі, якщо в розподіленій обчислювальній системі недостатньо надійно вирішені проблеми ідентифікації мережних управляючих пристроїв (наприклад, маршрутизаторів), що виникають при взаємодії останніх з об'єктами системи, то подібна розподілена система може піддатися типовій віддаленій атаці, пов'язаній зі зміною маршрутизації й впровадженням зловмисниками у систему помилкових об'єктів. Це досить легко реалізується у випадку, коли інфраструктура мережі для взаємодії об'єктів потребує використання алгоритмів віддаленого пошуку, що дозволяє впровадити в систему "помилковий об'єкт РОМ".

Впровадження в розподілену обчислювальну систему помилкового об'єкта шляхом нав'язування помилкового маршруту. Сучасні глобальні мережі представляють собою сукупність сегментів мережі, пов'язаних між собою через мережні вузли. При цьому маршрутом називається послідовність вузлів мережі, якою дані передаються від джерела до приймача. Кожен маршрутизатор має спеціальну таблицю

маршрутизації, в якій для кожного адресата вказується оптимальний маршрут. Відзначимо, що таблиці маршрутизації існують не тільки в маршрутизаторів, але й у будь-яких хостів у глобальній мережі. Для забезпечення ефективної й оптимальної маршрутизації в розподілених обчислювальних систем застосовуються спеціальні управляючі протоколи, що дозволяють маршрутизоторам обмінюватися інформацією один з одним, повідомляти хости про новий маршрут, віддалено управляти маршрутизаторами. Важливо відзначити, що всі описані вище протоколи дозволяють віддалено змінювати маршрутизацію в мережі, тобто є протоколами управління мережею.

По цьому абсолютно очевидно, що маршрутизація в глобальних мережах відіграє найважливішу роль й, як наслідок цього, може піддаватися атаці. *Основна мета атаки, пов'язаної з нав'язуванням помилкового маршруту*, полягає в тому, щоб змінити вихідну маршрутизацію на об'єкті розподіленої обчислювальної системи так, щоб новий маршрут проходив через помилковий об'єкт − хост атакуючого.

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

Для зміни маршрутизації необхідно протоколами управління мережею послати мережею спеціальні службові повідомлення від імені мережних управяючих пристроїв (наприклад, маршрутизаторів). У результаті успішної зміни маршруту атакуючий одержить повний контроль над потоком інформації, якою обмінюються два об'єкти розподіленої обчислювальної системи, і атака перейде в другу стадію, пов'язану з прийманням, аналізом і передачею повідомлень, одержуваних від дезінформованих об'єктів РОМ.

Впровадження в розподілену обчислювальну систему помилкового об'єкта шляхом використання недоліків алгоритмів віддаленого пошуку. У розподіленої обчислювальної системи часто виявляється, що її віддалені об'єкти споконвічно не мають достатньої інформації, необхідної для адресації повідомлень. Звичайно такою інформацією є апаратурні (адреса мережного адаптера) і логічні (IP−адреса, наприклад) 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.

В випадку використання розподіленою обчислювальною системою механізмів віддаленого пошуку існує можливість на атакуючому об'єкті перехопити посланий запит і послати на нього помилкову відповідь, в якій слід вказати дані, використання яких приведе до адресації на атакуючий помилковий об'єкт. Надалі весь потік інформації між суб'єктом й об'єктом взаємодії буде проходити через помилковий об'єкт РОМ.

Інший варіант впровадження в РОМ помилкового об'єкта використовує недоліки алгоритму віддаленого пошуку й складається в *періодичній передачі на об'єкт, що атакується, заздалегідь підготовленої помилкової відповіді* без приймання пошукового запиту. Справді, для того, щоб послати помилкову відповідь, не завжди обов'язково чекати приймання запиту. При цьому атакуючий може спровокувати об'єкт, що атакується, на передачу пошукового запиту, і тоді його помилкова відповідь буде негайно мати успіх. Дана типова віддалена атака надзвичайно характерна для глобальних мереж, коли в атакуючого через знаходження його в іншому сегменті щодо мети атаки просто немає можливості перехопити пошуковий запит.

Використання помилкового об'єкта для організації віддаленої атаки на розподілену обчислювальну систему. Одержавши контроль над потоком інформації між об'єктами, помилковий об'єкт РОМ може застосовувати різні методи впливу на перехоплену інформацію. У зв'язку з тим, що впровадження в розподілену обчислювальну систему помилкового об'єкта є метою багатьох віддалених атак й являє серйозну загрозу безпеці РОМ у цілому, в наступних пунктах будуть докладно розглянуті методи впливу на інформацію, перехоплену помилковим об'єктом.

Селекція потоку інформації і збереження її на помилковому об'єкті РОМ. Однією з атак, що може здійснювати помилковий об'єкт РОМ, є перехоплення переданої між суб'єктом й об'єктом інформації взаємодії. Важливо відзначити, що факт перехоплення інформації (файлів, наприклад) можливий через те, що при виконанні деяких операцій над файлами (читання, копіювання й т. д.) зміст цих файлів передається мережею, а, виходить, надходить на помилковий об'єкт. Найпростіший спосіб реалізації перехоплення − це збереження у файлі всіх одержуваних помилковим 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 помилковому об'єкті динамічний семантичний аналіз потоку інформації для його селекції.

Модифікація інформації. Однієї з особливостей будь-якої системи впливу, побудованої за принципом помилкового об'єкта, є те, що вона здатна модифікувати перехоплену інформацію. Слід особливо зазначити, що це один із способів, що дозволяють *програмно модифікувати потік інформації між об'єктами РОМ із іншого об'єкта.* Адже для реалізації перехвату інформації в мережі необов'язково атакувати розподілену обчислювальну систему за схемою "помилковий об'єкт". Ефективніше буде атака, яка здійснює аналіз мережного трафіка, що дозволяє одержувати всі пакети, що проходять каналом зв'язку, але, на відміну від віддаленої атаки за схемою "помилковий об'єкт", вона не здатна до модифікації інформації.

Далі розглянемо два види модифікації інформації: модифікація переданих даних; модифікація переданого коду.

Однією з функцій, яку може мати система впливу, побудована за принципом "помилковий об'єкт", є модифікація переданих даних. У результаті селекції потоку перехопленої інформації і його аналізу система може розпізнавати тип переданих файлів (програмний або текстовий). Відповідно, у випадку виявлення текстового файлу або файлу даних з'являється можливість його модифікувати. Особливу загрозу ця функція представляє для мереж обробки конфіденційної інформації.

Іншим видом модифікації може бути модифікація переданого коду. Помилковий об'єкт, проводячи семантичний аналіз інформації, що роходить через нього, може виділяти з потоку даних код, що виконується. Відомий принцип неймановскої архітектури говорить, що не існує розходжень між даними й командами. Отже, для того, щоб визначити, що передається мережею − код або дані, необхідно використати певні особливості, властиві реалізації мережного обміну в конкретній розподіленій обчислювальній системі або деякі особливості, властиві конкретним типам файлів, що виконуються в даній локальній ОС.

Представляється можливим виділити два різних за метою види модифікації коду: впровадження руйнуючих програмних засобів (РПЗ); зміна логіки роботи файлу, що виконується.

У першому випадку при впровадженні РПЗ файл, що виконується, модифікується за вірусною технологією: до файлу, що виконується, одним з відомих способів дописується тіло РПЗ, а також одним з відомих способів змінюється точка входу так, щоб вона вказувала на початок впровадженого коду РПЗ. Описаний спосіб, у принципі, нічим не відрізняється від стандартного зараження вірусом файлу, що виконується, за винятком того*, що файл виявився уражений вірусом або РПЗ у момент передачі його мережею*. Таке можливе лише при використанні системи впливу, побудованої за принципом "помилковий об'єкт". Конкретний вид РПЗ, його мета й завдання в цьому випадку не мають значення, але можна розглянути, наприклад, варіант використання помилкового об'єкта для створення мережного хробака − найбільш складного на практиці віддаленого впливу в мережах, або як РПЗ використати мережні шпигуни.

У другому випадку відбувається модифікація коду, що виконується, з метою зміни логіки його роботи. Даний вплив вимагає попереднього дослідження роботи файлу, що виконується, і, у випадку його проведення, може принести несподівані результати. Наприклад, при запуску на сервері ідентифікації користувачів розподіленої бази даних помилковий об'єкт може так модифікувати код цієї програми, що з'явиться можливість беспарольного входу з найвищими привілеями в базу даних.

Підміна інформації. Помилковий об'єкт дозволяє не тільки модифікувати, але й підмінювати перехоплену ним інформацію. Якщо модифікація інформації приводить до її часткового викривлення, то підміна − до її повної зміни.

При виникненні в мережі визначеної контрольованої події одному із учасників обміну помилковий об'єкт посилає заздалегідь підготовлену дезінформацію. При цьому така дезінформація залежно від контрольованої події може бути сприйнята або як код, що виконується, або як дані. Розглянемо приклад подібного роду дезінформації.

Припустимо, що помилковий об'єкт контролює подію, що складається в підключенні користувача до сервера. В цьому випадку він очікує, наприклад, запуску відповідної програми входу в систему. У випадку, якщо ця програма перебуває на сервері, то при її запуску файл, що виконується, передається на робочу станцію. Замість того, щоб виконати дану дію, помилковий об'єкт передає на робочу станцію код заздалегідь написаної спеціальної програми − загарбника паролів. Ця програма виконує візуально ті ж дії, що й чинна програма входу в систему, наприклад, запитуючи ім'я й пароль користувача, після чого отримані відомості посилаються на помилковий об'єкт, 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 чинну) і з другого разу одержить доступ. Результат такої атаки − ім'я й пароль користувача, збережені на помилковому об'єкті.

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 служби надання віддаленого доступу, тобто неможливість одержання віддаленого доступу з інших об'єктів РОМ має назву "Відмова в обслуговуванні".

У загальному випадку кожен суб'єкт розподіленої обчислювальної системи повинен мати можливість підключитися до будь-якого об'єкта РОМ й одержати відповідно до своїх прав віддалений доступ до його ресурсів. Звичайно в обчислювальних мережах можливість надання віддаленого доступу реалізується в такий спосіб: на об'єкті РОМ в 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. 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, у якій або дозволити підключення, або ні (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 запити, що приходять іззовні, 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 (чим вона вище, тим більшим є число можливих запитів в одиницю часу).

Основна проблема полягає в тому, що при відсутності статичної ключової інформації у РОМ ідентифікація запиту можлива тільки за адресою його відправника. Якщо в розподіленій обчислювальній системі не передбачено засобів автентифікації адреси відправника, тобто інфраструктура РОМ, дозволяє з одного об'єкта системи передавати на інший об'єкт, що атакується, нескінченне число анонімних запитів на підключення від імені інших об'єктів, то в цьому випадку буде мати успіх типова віддалена атака "Відмова в обслуговуванні". Результат застосування цієї віддаленої атаки − порушення на атакованому об'єкті 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 з однієї адреси такої кількості запитів на об'єкт, що атакується, яку дозволить трафік (спрямований "шторм" запитів). У цьому випадку, якщо в системі не передбачені правила, що обмежують число прийнятих запитів з одного об'єкта (адреси) в одиницю часу, то результатом цієї атаки може бути як переповнення черги запитів і відмова однієї з телекомунікаційних служб, так і повна зупинка комп'ютера через неможливість системи займатися нічим іншим, крім обробки запитів.

І останнім, третім різновидом атаки "Відмова в обслуговуванні" є передача на об'єкт, що атакується, не коректного, спеціально підібраного запиту. В цьому випадку при наявності помилок у віддаленій системі можливе зациклення процедури обробки запиту, переповнення буфера з наступним зависанням системи ("Ping Death") і т. п.

II Класифікація віддалених атак на розподілені обчислювальні системи

Основна мета будь-якої класифікації полягає в тому, щоб запропонувати такі класифікаційні ознаки, використовуючи які можна найбільш точно описати явища або об'єкти, що класифікуються. Тому для більше точного опису віддалених атак використана класифікація, наведена в табл. 1 [2 – 11].

Отже, віддалені атаки можна класифікувати за наступними ознаками:

За характером впливу:

1. пасивний (клас 1.1);
2. активний (клас 1.2).

Пасивним впливом на розподілену обчислювальну систему назвемо вплив, що не здійснює безпосереднього впливу на роботу системи, але може порушити її політику безпеки. Саме відсутність безпосереднього впливу на роботу розподіленої обчислювальної системи приводить до того, що пасивний віддалений вплив практично неможливо виявити. Прикладом пасивного типового віддаленого впливу у РОМ служить прослуховування каналу зв'язку в мережі.

Під активним впливом на розподілену обчислювальну систему будемо розуміти вплив, що здійснює безпосередній вплив на роботу системи (зміна конфігурації РОМ, порушення працездатності й т. д.) і що порушує прийняту в ній політику безпеки. Практично всі типи віддалених атак є активними впливами. Це пов'язано з тим, що само природа руйнуючого впливу містить активний початок. Очевидною особливістю

активного впливу порівняно з пасивним є принципова можливість його виявлення (природно, з більшим або меншим ступенем складності), тому що в результаті його здійснення в системі відбуваються певні зміни.

За метою впливу:

1. порушення конфіденційності інформації або ресурсів системи (клас 2. 1);
2. порушення цілісності інформації (клас 2. 2);
3. порушення доступності (працездатності) системи (клас 2. 3).

Ця класифікаційна ознака є прямою проекцією трьох основних типів загроз − конфіденційності, цілісності й доступності (відмови в обслуговуванні).

Таблиця 1. Класифікація типових віддалених атак на розподілені обчислювальні системи

Типова віддалена атака	Характер впливу		Ціль впливу			Умова початку здійснення впливу			Наявність зворотного зв'язку з об'єктом, що атакує		Розташування суб'єкта атаки щодо об'єкта, що атакує		Рівень моделі OSI						
Клас впливу	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Аналіз мережного трафіка	+	−	+	−	−	−	−	+	−	+	+	−	−	+	−	−	−	−	−
Підміна довіреного об'єкта РОМ	−	+	+	+	−	−	+	−	+	+	+	+	−	−	+	+	−	−	−
Впровадження в РОМ помилкового об'єкта шляхом нав'язування помилкового маршруту	−	+	+	+	+	−	−	+	+	+	+	+	−	−	+	−	−	−	−
Впровадження в РОМ помилкового об'єкта шляхом використання недоліків алгоритмів віддаленого пошуку	−	+	+	+	−	+	−	+	+	−	+	+	−	+	+	+	−	−	−
Відмова в обслуговуванні	−	+	−	−	+	−	−	+	−	+	+	+	−	+	+	+	+	+	+

Основна мета практично будь-якої атаки − одержати несанкціонований доступ до інформації. Існують дві принципові можливості доступу до інформації: перехоплення й викривлення. Можливість перехоплення інформації означає одержання до неї доступу, але неможливість її модифікації. Отже, перехоплення інформації може мати наслідком порушення її конфіденційності. Прикладом перехоплення інформації може служити прослуховування каналу в мережі (п. 3. 2. 1). У цьому випадку є несанкціонований доступ до інформації без можливості її викривлення. Очевидно також, що порушення конфіденційності інформації є пасивним впливом.

Можливість викривлення інформації означає або повний контроль над інформаційним потоком між

об’єктами системи, або можливість передачі повідомлень від імені іншого об’єкта. Таким чином, очевидно, що викривлення інформації веде до порушення її цілісності. Даний інформаційний руйнуючий вплив є яскравим прикладом активного впливу. Прикладом віддаленої атаки, ціллю якої є порушення цілісності інформації, може служити типова віддалена атака (ВА) “Помилковий об’єкт РОМ”.

Принципово іншою метою атаки є порушення доступності − працездатності системи, наприклад, шляхом її перевантаження. У цьому випадку не передбачається одержання атакуючого несанкціонованого доступу до інформації. Його основна мета − домогтися, щоб вийшла з ладу операційна система на об’єкті, що атакується, й для всіх інших об’єктів системи доступ до ресурсів атакованого об’єкта був би неможливий. Прикладом віддаленої атаки, метою якої є порушення доступності – працездатності системи, може служити типова ВА “Відмова в обслуговуванні”.

За умовою початку здійснення впливу

Віддалений вплив, як і будь-який інший, може здійснюватися тільки за певних умов. У розподілених обчислювальних системах існують три види умов початку здійснення віддаленої атаки:

1. *Атака за запитом від об’єкта, що атакується,* (*клас* 3. 1).

У цьому випадку атакуючий очікує передачі від потенційної цілі атаки запиту певного типу, що і буде умовою початку здійснення впливу. Важливо відзначити, що даний тип віддалених атак найбільш характерний для розподілених обчислювальних систем.

2. *Атака за настанням очікуваної події на об’єкті, що атакується* (клас 3. 2).

У цьому випадку атакуючий здійснює постійне спостереження за станом операційної системи віддаленої мети атаки й при виникненні певної події в цій системі починає вплив. Як і в попередньому випадку, ініціатором здійснення початку атаки виступає сам об’єкт, що атакується.

3. *Безумовна атака* (клас 3. 3).

У цьому випадку початок здійснення атаки є безумовним стосовно цілі атаки, тобто атака здійснюється негайно й безвідносно до стану системи й об’єкта, що атакується. Отже, у цьому випадку атакуючий є ініціатором початку здійснення атаки.

За наявністю зворотного зв’язку з об’єктом, що атакується:

1. із зворотним зв’язком (клас 4.1);
2. без зворотного зв’язку (односпрямована атака) (клас 4.2).

Віддалена атака, здійснювана за наявності зворотного зв’язку з об’єктом, що атакує, характеризується тим, що на деякі запити, передані на об’єкт, що атакується, потрібно одержати відповідь, а, отже, між атакуючим і ціллю атаки існує зворотний зв’язок, що дозволяє атакуючому адекватно реагувати на всі зміни, що відбуваються на об’єкті, що атакується. Подібні віддалені атаки найбільш характерні для розподілених обчислювальних систем.

На відміну від атак зі зворотним зв’язком віддаленим атакам без зворотного зв’язку не потрібно реагувати на які-небудь зміни, що відбуваються на об’єкті, що атакується. Атаки даного виду звичайно здійснюються передачею на об’єкт, що атакується, одиночних запитів, відповіді на які атакуючому не потрібні. Подібну ВА можна називати односпрямованою віддаленою атакою. Прикладом односпрямованих атак є типова ВА “Відмова в обслуговуванні”.

За розташуванням суб’єкта атаки щодо об’єкта, що атакується:

1. внутрішньосегментні (клас 5.1);
2. міжсегментні (клас 5.2).

З погляду віддаленої атаки надзвичайно важливо, як відносно один до одного розташовуються суб’єкт й об’єкт атаки, тобто в одному або в різних сегментах вони перебувають. У випадку внутрішньо сегментної атаки, як витікає з назви, суб’єкт й об’єкт атаки перебувають в одному сегменті. При міжсегментній атаці суб’єкт й об’єкт атаки перебувають у різних сегментах.

Дана класифікаційна ознака дозволяє судити про так звану “ступені віддаленості” атаки.

Зрозуміло, що на практиці міжсегментну атаку здійснити значно складніше, ніж внутрішньо сегментну. Важливо відзначити, що міжсегментна віддалена атака являє набагато більшу небезпеку, чим внутрішньо сегментна. Це пов’язане з тим, що у випадку міжсегментної атаки об’єкт її й безпосередньо атакуючий можуть перебувати на відстані багатьох тисяч кілометрів один від одного, що може істотно перешкодити заходам щодо відбиття атаки.

За рівнем еталонної моделі ISO/OSI, на якому здійснюється вплив:

1. фізичний (клас 6.1);
2. канальний (клас 6.2);
3. мережний (клас 6.3);
4. транспортний (клас 6.4);
5. сеансовий (клас 6.5);

6. представницький (клас 6.6):
7. прикладний (клас 6.7).

III Модель загроз в КМЗ

Модель загроз та їх ідентифікація з можливими діями порушників щодо об'єктів захисту наведена в табл. 2 [12]. В ній відображено перелік загроз з констатацією можливих дій порушників щодо відповідних об'єктів, на порушення властивостей захищеності яких вони спрямовані – порушення конфіденційності (к), цілісності (ц), доступності (д), спостереженості та керованості (с), оцінка ймовірності здійснення загроз та рівень збитків (шкоди) від порушень по кожному з видів порушень, а також джерело виникнення – які внутрішні чи зовнішні суб'єкти можуть ініціювати загрозу.

Методика розроблення такої моделі полягає в тому, що в один із стовпчиків таблиці заноситься можливо повний перелік видів загроз; в наведеному прикладі такий перелік (на погляд автора, досить повний) наведено в стовпчику 2. Надалі для кожної із можливих загроз шляхом їх аналізу (можливо і методом експертних оцінок) необхідно визначити:

ймовірність виникнення таких загроз; в таблиці наведена якісна оцінка їх ймовірності – неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька (стовпчик 3);

на порушення яких властивостей інформації або КМЗ вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності – к, цілісності – ц, доступності – д інформації, а також порушення спостереженості та керованості – с АС) (стовпчик 4);

можливий (такий, що очікується) *рівень шкоди* (стовпчик 5); ця оцінка здійснена також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока);.

джерела виникнення (які суб'єкти КМЗ, зовнішні чи внутрішні відносно неї, можуть ініціювати загрозу) (стовпчик 6).

Наявність оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної з властивостей захищеності інформації, а також побудувати загальну модель системи захисту, на основі характеристик її складових оцінити кількісні значення залишкового ризику, визначити структуру системи захисту та її основні компоненти.

Для створення цього прикладу моделі автор намагався проаналізувати якомога більшу кількість доступних інформаційних джерел та спирався на власний досвід розроблення політики безпеки інформації для досить складних АС у вигляді розподілених обчислювальних мереж (за класифікацією НД ТЗІ – АС класу 3.КЦД).

Таблиця 2 – Модель загроз в КМЗ

№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Джерело
Пасивні атаки					
1	Перехоплення даних	висока	к, ц, с	високий	внутр. зовн.
2	Перехоплення ідентифікаційних даних користувача	висока	к, ц, д, с	високий	внутр. зовн.
3	Аналіз трафіка	висока	к, ц, д, с	високий	
Активні атаки					
1	Повторення або затримка інформації	низька	д, с	низький	внутр. зовн.
2	Вставлення і видалення даних	висока	к, ц, с	високий	внутр. зовн.
3	Зміна даних	висока	к, ц, с	високий	внутр. зовн.
4	Бойкот комунікаційної системи (відмова в обслуговуванні)	висока	д, с	високий	зовн.
5	Робота під чужим ідентифікатором (маскування)	висока	к, ц, д, с	високий	внутр. зовн.
6	Одностороння відмова від передавання даних	низька	к, ц, с	низький	внутр. зовн.
7	Атака "людина в середині"	висока	к, ц, д, с	високий	внутр. зовн.

Таблиця 2 – Модель загроз в КМЗ

№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Джерело
Непередбачені помилки					
1	Помилки маршрутизації	низька	к, ц, д, с	високий	внутр. зовн.
2	Програмні помилки	низька	к, ц, д, с	середній	внутр. зовн.
3	Відмови в роботі апаратури, що обумовлені впливом зовнішнього середовища	низька	к, ц, д, с	середній	внутр. зовн.
4	Фактор людини	висока	к, ц, д, с	високий	внутр. зовн.

Слід врахувати, що наведені оцінки ймовірностей та величини можливої шкоди кожної із загроз в даному прикладі моделі загроз носять ілюстративний характер. Для випадків конкретних АС ці величини мають бути визначені фахівцями служби захисту відповідного підприємства.

Література: ***1****. Буточнов О. М., Гончар Г. В., Деревянко С. М., Короленко М. П. Захист інформації в комунікаційній мережі зв'язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 37 − 58.* ***2.*** *Maximum Security: AHacker'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/dn s−poison.html);* ***6.*** *Медведовский И. Д. Семьянов П. В. Леонов Д. Г."Атака на Інтернет" М.:Видавництво ДВК 1999;* ***7.*** *Соболоев К. И. Дослідження системи безпеки з Windows NT 4.0 HackZone: Територія злому. №1−2, 1998.* ***8.*** *Переповнення буфера в WIN32 (http://www.void.ru/stat/9907/20.html).* ***9.*** *EXPLOIT'и переповнення буфера на PERL'е (http://www.void.ru/stat/0102/02.html).* ***10.*** *Теорія й 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).* ***12.*** *Матов О. Я., Василенко В. С., Будько М. М Оцінка захищеності в локальних обчислювальних мережах. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 59 − 73.*

УДК 681.5:621.391

ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДКРИТИХ СИСТЕМ. ЧАСТИНА 3. ІЄРАРХІЯ СИСТЕМ ТА ВИМОГ ДО БЕЗПЕКИ

Володимир Кононович, Ірина Кононович*, Тетяна Тардаскіна**

Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком",
**Інститут комп'ютерних технологій ОДАХ, **Одеська національна академія зв'язку*

Анотація: **З позицій теорії систем та синергетики аналізуються основні ієрархічні властивості інформаційної безпеки складних відкритих систем, що розвиваються. Формулюється ієрархія вимог до інформаційної безпеки відкритих систем.**

Summary: **It is analyzed, from positions of theory of the systems and synergetic, basic hierarchical properties in relation to information security of the difficult open systems which develop. The hierarchy of requirements to informative safety of the open systems is formulated**.

Ключові слова: **Інформаційна безпека, відкриті системи, кібернетика, ієрархічні системи, параметри порядку, саморганізація.**

I Вступ

Дане дослідження стосується сфери технічного захисту інформації та інформаційної безпеки систем, які об'єднуються під загальною назвою – інформаційні технології з акцентом на відкриті системи. Проблематика дослідження, аналіз стану досліджень наведені в частинах 1, 2 цієї роботи [1, 2].