Дамский. – М.: Рипол Классик, 2005. – 152 с.

3. Heinz E. Scalable Search in Computer Chess: Algorithmic Enhancements and Experiments at High Search Depths / E. Heinz. – Vieweg, Verlag, 1999. – 270_с.

4. Ананд В. Энциклопедия шахматных дебютов / В. Ананд. – Н.: Кипр, 1993. – 178 с.

5. AlphaZero, новый проект Google, громит Stockfish в матче из 100 партий [Електронний ресурс]. – Режим доступу: https://www.chess.com/ru/news/view/alphazero-novyi-proiekt-google-ghromit-stockfish-v-matchie-iz-100-partii

Модель прихованих загроз інформаційній безпеці в системах з використанням хмарних технологій

Глінський О.В.
Науковий керівник: к.т.н. доц. Чорненький В.І.
Хмельницький національний університет

Характерною особливістю сучасного середовища хмарних обчислень є активний характер суб'єктів і об'єктів інформаційної взаємодії. Це дозволяє розглядати цільову функцію системи безпеки як збереження конфіденційності, цілісності і доступності програмних і інфраструктурних сервісів, що надаються в режимі видаленого доступу в умовах динамічної зміни стану обчислювальних ресурсів. Побудова перспективних механізмів забезпечення безпеки в середовищі хмарних обчислень зв'язується не із захистом від виявлених вразливостей, а полягає в можливості запобігання новим невідомим методам проведення атак, в розробці нових моделей загроз і методів запобігання або віддзеркалення комп'ютерних атак на інформаційні ресурси, які використовують можливості предикативної ідентифікації прихованих каналів і потенційно небезпечних процесів інформаційної взаємодії [1].

Перспективним напрямком вирішення сформульованої задачі є використання технології між мережевого екранування з урахуванням специфіки захищеності середовища [2]. Для цього необхідна формалізація вимог розмежування доступу до інформаційних сервісів. Така формалізація може бути представлена з використанням динамічно формованого набору правил фільтрації, що забезпечує виконання вимог політики доступу. При цьому зростаюча складність алгоритмів фільтрації пред'являє високі вимоги до продуктивності між мережевих екранів, що робить необхідним використання методів паралельної обробки віртуальних з'єднань за допомогою віотуальних машин. У сучасній літературі підхід до створення складних технічних систем, зв'язаність яких забезпечується за рахунок організації процесів обміну інформацією з мережі, отримав назву мережево-центричний. Цей підхід стосовно задачі розмежування доступу вимагає

забезпечення ситуаційної обізнаності та локальності дій кожного з між мережевих екранів, що входять до складу віртуальних машин, які використовуються в СХО для реалізації політики доступу [3].

Важливим напрямом вдосконалення технологій захисту і систем інформаційної безпеки є протидія білатеральним загрозам, в яких суб'єкт і об'єкт процесів інформаційної взаємодії є потенційним носієм небезпечних дій. У таких випадках необхідно використовувати моделі загроз, які ідентифікують потенційні вразливості як на рівні процесів контролю доступу до ресурсів гостьових операційних систем (ОС) або додатків, так і на рівні системних викликів гіпервізора, який сам може стати джерелом руйнуючих дій що реалізовуються шляхом порушення функціонування планувальника завдань або диспетчера устаткування. Загрози, що виникають при цьому, необхідно не тільки оперативно виявляти, але і блокувати використовувані неавторизовані канали інформаційних дій, які в середовищі хмарних обчислень зазвичай реалізуються в прихованому для гостьових ОС режимах. Тому важливим чинником підвищення ефективності систем захисту від прихованих загроз є облік напряму передачі, синтаксису і контексту потоків даних, які передаються [4].

З врахуванням вищесказаного, захист від загроз, які можуть приводити до розкрадання даних, неконтрольованої модифікації програмного коду, порушенню доступності (блокуванню) або нав'язуванню помилкової інформації в середовищі хмарних обчислень є актуальним науково-технічним завданням, вирішенню якого присвячена дана магістерська робота [2].

Використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримка апаратних платформ різного класу) пропонованих програмно-технічних рішень і мінімізації витрат.

Застосування сучасних технологій адаптивних систем захисту інформації не дозволяє здійснювати «прозорий» контроль за інформаційними потоками середовища хмарних обчислень, оскільки вони функціонують на верхніх рівнях ієрархії.

Класичні методи пошуку шкідливого програмного коди не дозволяють виявляти нові зразки шкідливого ПО, що реалізовує технології DKOM і VICE, оскільки вони вбудовуються в операційну систем на «нижчому» рівні, ніж модулі адаптивних систем захисту.

Традиційні методи перехоплення системних функцій гостьових ОС не дозволяють виявляти програмні «закладки», що вшиваються в ОС на етапі завантаження.

Для боротьби з такими загрозами актуальною є розробка нових засобів захисту інформації, заснованих на методах оперативної ідентифікації потенційних вразливостей, що виникають як на рівні процесів контролю доступу до ресурсів гостьових ОС, так і на рівні системних викликів гіпервізора, які за певних умов самі можуть ставати джерелами різних видів

руйнівних впливів. Метою дослідження є підвищення рівня захищеності обчислювальних систем на основі розробки моделей, методів і алгоритмів протидії прихованим загрозам в середовищі хмарних обчислень.

Для досягнення поставленої мети вирішуються наступні завдання:

– розроблена модель прихованих загроз інформаційній безпеці в середовищі хмарних обчислень, що враховує активний характер суб'єктів і об'єктів інформаційної взаємодії.

– розроблена модель операцій, що відбуваються з даними при їх обробці в середовищі хмарних обчислень, що дозволяє формалізувати опис інформаційних процесів у вигляді мультиграфа транзакцій.

– розроблений метод протидії прихованим загрозам з використанням запропонованої моделі операцій, заснований на характеризації ієрархії транзакцій.

– розглянемо компоненти гіпервізора як джерело загрози при проведенні атак зловмисником з подальшим розповсюдженням шкідливого програмного забезпечення на серверах віртуалізації.

Користувачі можуть атакувати компоненти гіпервізора, посилаючи некоректні запити на обробку модулям програмного забезпечення гіпервізора і використовуючи недокументовані можливості системного і прикладного програмного забезепечення, встановленого на серверах віртуалізації. Логіка виконання програм повинна контролюватися з точки зору відмови в обслуговуванні. Це підвищує ризики при реалізації прихованих загроз, не тільки функціональних можливостей, але і безпеки, яка оцінюється величиною ризику їх не документованої роботи. Приховані загрози, що приводять до порушення роботи середовищі хмарних обчислень, реалізуються за допомогою дій з боку шкідливого програмного забезпечення, від яких немає захисту на рівні гостьової ОС].

Під реалізацією прихованих загроз маються на увазі використання механізмів створення і зміни контексту виконання потоків, за допомогою яких можуть передаватися дані від сутностей з високим рівнем безпеки до сутностей з низьким рівнем безпеки в обхід правил і може порушуватися стан захищеності самого гіпервізора.

Гіпервізор забезпечує ізоляцію різних ОС одна від одної, розділення і управління ресурсами. Гостьові ОС – це операційні системи віртуальних машин, що запускаються під управлінням гіпервізора.

У гіпервізорі, як і в будь-якій операційній системі, створюється множина сутностей (об'єктів і суб'єктів доступу) з різним рівнем безпеки. Операція породження суб'єктів $Create\left(Subi, Om\right) \to Subj$ називається породженням з контролем незмінності об'єкту, якщо для будь-якого моменту часу $t > \mathrm{t0}$, в який активізована операція породження об'єкту $Create$, породження об'єкту $Subj$ можливо тільки при тотожності об'єкту-джерела

щодо моменту $t0: Om[t] = Om[t0]$, де Sub – суб'єкт, O – об'єкт доступу. У разі середовища хмарних обчислень суб'єкти і об'єкти доступу можуть мінятися ролями [8].

Тому для протидії прихованим загрозам в середовищі хмарних обчислень, в якому діє породження суб'єктів з контролем незмінності об'єкту, необхідно, щоб у момент часу $t0$ через будь-який суб'єкт до будь-якого об'єкту існували тільки потоки, що не суперечать умові коректності: монітор безпеки повинен реалізувати спеціальні механізми ідентифікації контексту контрольованих потоків даних як для суб'єктів, так і для об'єктів доступу, а будь-який суб'єкт доступу (ініціатор доступу) повинен використовувати тільки дозволені механізми доступу. З цією метою вводиться набір який підходить для створення об'єктів доступу, так і при породженні об'єктів у вигляді кортежу $(s, Ord, Context\_type)$.

Таблиці дозволених зв'язків об'єктів і суб'єктів доступу, за допомогою яких здійснюється контроль транзакцій операцій породження нових об'єктів, необхідно розширити на випадок прихованих загроз.

Предикативна функція ідентифікації прихованих загроз - це відображення 8-рівневої моделі операцій на множину його можливих станів - небезпечні, безпечні і невизначені. В цьому випадку модель прихованих загроз описується у вигляді розширеного кортежу:

$$M = \langle Source, Services, Devices, \{proc\}, Actions, \{hv\}, \{vm\}, Security\ Roles \rangle$$

де $Source$ - суб'єкт доступу або процес, джерело загрози; $Services$ - набір шаблонів правил безпеки, використовуваних традиційними СЗІ (наприклад, правила фільтрації для МСЕ тощо); $Devices$ - пристрої, що встановлені на серверах віртуалізації і використовувані гостьовими операційними системами ВМ (диск, мережний контролер тощо), як об'єкт доступу; $\{proc\}$ - множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.); $Actions$ - (дії) виконання операцій суб'єктом по відношенню до об'кту доступу (виконання команд read, write, append, create, execute…); $\{hv\}$ - середовище взаємодії процесів ВМ у гіпервізорі, що представляє собою множину компонентів $\mathrm{mod}i$; $\{vm\}$ - об'єкти впливу (множина ВМ); $Security\ Roles$ - процедури багаторівневої рольової ПБ для протидії прихованим загрозам, які реалізуються у вигляді набору міток безпеки. Набір міток являють собою значення кортежу $(s, Ord, Context\_type)$.

В рамках пропонованої моделі загроз середовище хмарних обчислень розглядається як система взаємодії гіпервізорів, встановлених на серверах віртуалізації. В рамках направленої схеми «суб'єкт-дія-об'єкт» активний характер суб'єктів і об'єктів інформаційної взаємодії передбачає ту

обставину, що вони можуть мінятися місцями. Розглянемо ситуацію, в якій зловмисник(суб'єкт) атакує сервер віртуалізації(об'єкт), модифікує компоненти гіпервізора шляхом реалізації нових загроз, приведених в таблиці

У будь-якій обчислювальній системі існують інтерфейсні рівні взаємодії між різними модулями(компонентами), що дозволяють використовувати недокументовані можливості, з одного боку, для проведення атак зловмисником, з іншої – для реалізації механізмів моніторингу з боку систем контролю і захисту ПЗ середовища хмарних обчислень.

Загроза порушення доступу до конфіденційної інформації породила необхідність розробки нових методів захисту ПЗ та предикативного алгоритму на основі розробленої моделі операцій, що допомагає систематизувати функціональні рівні, використовувані зловмисником для вбудовування до гостьової ОС і гіпервізора, і протидіяти впровадженню шкідливих кодів та загроз, які формують послідовності запитів до некоректних програмним модулів гіпервізора або використовують недекларовані можливості системного і прикладного програмного забезпечення. Різні компоненти гіпервізора розглядаються в якості потенційного джерела загроз кібербезпеці, які реалізується шляхом поширення шкідливого програмного забезпечення або ініціалізації процесів, що руйнують стан захищеності ресурсів середовища хмарних обчислень.

Література

1. Моляков А.С. KPROCESSOR_CID_TABLE факторинг – новый метод в теории компьютерного анализа вирусного кода и поиска программных закладок / А.С. Моляков // Проблемы информационной безопасности. Компьютерные системы. - СПб.: Изд-во Политех. Ун-та, 2009. - №1. - с. 17-19.

2. Козак І.В Аналіз проблем захисту інформації в середовищі хмарних обчислень / І.В. Козак, С.О. Пашков, О.В. Огнєвий // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 51. – С.177-185.

3. Гладких А.А. Концептуальная модель функционирования обманной системы в условиях информационного противоборства. / А. А. Гладких, Р.Р. Зелимов // Сб. рефератов депонированных.- М: ЦВНИ МО РФ, 2004. - с. 12-15.

4. Муляр І.В. Розробка математичної моделі та методу її вирішення для підвищення ефективності використання обчислювальних ресурсів на основі технології віртуалізації / І.В. Муляр , Г.В. Гусляков , Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського НУ імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 54. – С. 134-143.