цьому питанні, де під час практичної діяльності підрозділами НПУ було доведено їх ефективність.

Список бібліографічних посилань

1. Cellebrite official site. URL: https://www.cellebrite.com/en/home/ (дата звернення: 23.10.2018).

2. The Feds Can Now (Probably) Unlock Every iPhone Model In Existence. URL: https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite (дата звернення: 23.10.2018).

3. MSAB official site. URL: https://www.msab.com/ (дата звернення: 23.10.2018).

4. Mobiledit official site. URL: https://www.mobiledit.com/ (дата звернення: 23.10.2018).

Одержано 31.10.2018

УДК 004.056.53

Михайло Анатолійович СТРЕЛЬБІЦЬКИЙ,
доктор технічних наук, доцент
начальник (завідувач) кафедри зв'язку, автоматизації та кібербезпеки
Національної академії Державної прикордонної служби імені Богдана Хмельницького;
ORCID: https://orcid.org/0000-0001-8030-3228;
Олександр Степанович АНДРОЩУК,
доктор технічних наук, професор
начальник докторантури – головний науковий співробітник
Національної академії Державної прикордонної служби імені Богдана Хмельницького;
Віталій Вікторович РАВЛЮК,
викладач кафедри зв'язку, автоматизації та кібербезпеки
Національної академії Державної прикордонної служби імені Богдана Хмельницького

ПРОБЛЕМА СПІЛЬНОГО ФУНКЦІОНУВАННЯ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ НА ЗАГАЛЬНОМУ ПОЛІ ДАНИХ ГЕТЕРОГЕННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Математичний апарат формування систем розмежування доступу (СРД) для окремих інформаційних систем (ІС) на сьогодні досить добре розроблений. Разом із тим, як показав аналіз, існуючі моделі не передбачають їх спільного функціонування на загальному полі даних гетерогенної інформаційної системи. Разом із тим, під час модернізації відомчих територіально-розподілених інформаційних систем реального часу можливе виникнення ситуації, в якій на загальному полі даних повинні функціонувати різні версії ІС з власними СРД.

Для дослідження спільного функціонування різних версій моделей безпеки комп'ютерних системи обрано такі види моделей: дискреційного, рольового, мандатного та тематичного розмежування доступу.

Спільне функціонування моделей дискреційного розмежування доступу. Моделі дискреційного розмежування (Харісона–Руззо–Ульмана, типізованих матриць доступу, Take–Grant, розширена модель Take–Grant та інші) оперують матрицею доступу $M[s,o]$, рядки якої відповідають суб'єктам, стовбці об'єктам системи, а комірки визначають право доступу суб'єкта S на об'єкт O [1–5].

У разі спільного функціонування різних версій цих моделей можлива реалізація двох ситуацій, за яких можливе порушення політики безпеки. Перша, значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів різні, тобто $\exists s_i, \exists o_j$ за яких $M_1[s_i,o_j] \neq M_2[s_i,o_j]$, де $s_i \in S_1, s_i \in S_2, o_j \in O_1, o_j \in O_2$. У даному випадку існує порушення політики безпеки, тому що під час здійснення операції суб'єкта відносно до об'єкта, яку дозволяє СРД однієї версії є забороненою у іншій версії або навпаки. У другому випадку значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів однакові, тобто $M_1[s_i,o_j] = M_2[s_i,o_j]$, для $\forall s_i \in S_1, \forall s_i \in S_2, \forall o_j \in O_1, \forall o_j \in O_2$. Водночас наявність суб'єктів та об'єктів, які не входять до СРД іншої версії, дозволяє здійснити інформаційний потік в обхід політики безпеки однієї із версій.

Спільне функціонування моделей рольового розмежування доступу. Моделі рольового розмежування доступу є подальшим розвитком політики дискреційного розмежування доступу. Відмінністю є те, що права доступу суб'єктів системи об'єднуються, утворюючи групи з однаковими правами, які визначаються з урахуванням специфіки їх функціональних завдань у системі [6/30, 7/45]. Отже, у разі спільного функціонування двох СРД, які побудовані за принципом рольового розмежування доступу, можливе виникнення інформаційного потоку в обхід однієї із версій СРД аналогічно дискреційному розмежуванню доступу.

У загальному випадку не є обов'язковим рівність прав кожної ролі в умовах спільного функціонування різних версій СРД. У даному випадку, якщо існує роль r_i^1 – старої та r_j^2 – нової СРД за яких права на об'єкт O_k відрізняються, то існує порушення політики безпеки однієї із версій СРД, тому що під час здійснення операції користувача з роллю r_i^1 відносно об'єкта, яку дозволяє СРД однієї версії є забороненою операцією в ролі r_j^2 іншої версії або навпаки.

У результаті досліджень інформаційних потоків у разі спільного функціонування різних версій систем рольового розмежування доступу висунуто гіпотезу, що для дотримання політики безпеки при спільному функціонуванні обох версій рольового розмежування доступу необхідно та достатньо рівності множин прав доступу ролей різних версій СРД для спільних об'єктів.

Спільне функціонування моделей мандатного розмежування доступу. Моделі мандатного розмежування доступу (класична модель Белла–ЛаПадули, модель безпечного переходу, модель систем воєнних повідомлень, політика low–watermark, модель цілісності Біба й інші) передбачають аналіз умов, під час виконання яких неможливий інформаційний потік від об'єктів з більшим рівнем конфіденційності до об'єктів з меншим рівнем конфіденційності [7–12].

Виникнення недозволеного інформаційного потоку в одній із версій СРД у разі спільного їх функціонування можливе у випадку: невідповідності решіток рівнів конфіденційності об'єктів СРД, що може призвести до забороненого в одній із версій інформаційного потоку або невідповідності матриць доступу $M[s,o]$;

Доцільно зазначити, що наявна нормативно-правова база чітко визначає решітку рівнів конфіденційності об'єктів, тому виникнення недозволеного інформаційного потоку у перший спосіб є малоймовірним. Водночас реалізація другого способу можлива аналогічно моделі дискреційного розмежування доступу.

Спільне функціонування моделей тематичного розмежування доступу. Моделі тематичного розмежування доступу оперують тематичним ієрархічним класифікатором (рубрикатором), що включає кінцеву множину тематичних рубрик, на яких встановлений частковий порядок, який визначається кореневим деревом [1, 8]. У моделях тематичного розмежування доступу множина сутностей $X = S \cup O$ тематично класифікується на основі відображення на множину мультирубрик, які визначені на кореневому дереві ієрархічного рубрикатора.

Виникнення недозволеного інформаційного потоку в одній із версій тематичного розмежування доступу під час спільного їх функціонування можливе у разі невідповідності тематик сутностей системи.

Як приклад наведемо два випадки суперечностей інформаційних потоків різних версій тематичного розмежування доступу для чотирьох спільних об'єктів, а саме:

– перший, $СРД_1$ об'єкти o_1 та o_2 знаходяться в непорівнюваних за тематикою сутностями і, як наслідок, такі потоки є забороненими. Водночас в $СРД_2$ зазначені об'єкти знаходяться в одній тематиці, тому інформаційний потік між ними дозволений;

– другий, СРД$_1$ об’єкт O_3 знаходиться в сутності з більш широкою тематикою, а O_4 з більш вузькою, тому такий потік є забороненим. Водночас у СРД$_2$ зазначені об’єкти знаходяться в одній тематиці, тому інформаційний потік між ними дозволений.

У результаті досліджень інформаційних потоків у разі спільного функціонування різних версій систем тематичного розмежування доступу висунуто гіпотезу, що для дотримання політики безпеки при спільному функціонуванні обох версій тематичного розмежування доступу необхідно та достатньо ієрархічної рівності тематичних класифікаторів різних версій СРД для спільних об’єктів.

Висновок. Під час розробки складових інформаційних систем формалізується та реалізовується певна політика безпеки, яка базується на відомих моделях інформаційної безпеки. Їх використання в окремих ІС та підсистемах забезпечує виконання функцій забезпечення дотримання властивостей інформаційного ресурсу. Водночас під час модернізації наявних складових ІС або інтеграції нових виникає ситуація спільного функціонування систем розмежування доступу на загальному полі даних. Показано, що спільне функціонування різних версій систем розмежування доступу, які побудовані на розглянутих моделях безпеки комп’ютерних систем, передбачає наявність можливих шляхів виникнення інформаційних потоків в обхід політики безпеки однієї із версій системи розмежування доступу.

Список бібліографічних посилань

1. Гайдамакин Н. А. Теоретические основы компьютерной безопасности : учеб. пособие. Екатеринбург : изд-во Урал. Ун-та, 2008. 212 с.

2. Докучаев А. А., Мошенский С. А. Защита данных в системах обработки экономической и финансовой информации : учебн. пособие. Спб., 1994. 25 с.

3. Баришев Ю. В., Каплун В. А., Неуйміна К. В. Дискреційна модель та метод розмежування прав доступу до розподілених інформаційних ресурсів. *Наукові праці Вінницького національного технічного університету*. 2017. № 2. 8 с. URL: https://praci.vntu.edu.ua/index.php/praci/article/view/506 (дата звернення: 17.10.2018).

4. Семенов С. Г., Зміївська В. М., Голубенко А. В. Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі. *Системи обробки інформації*. 2015. № 3. С. 99-102.

5. Потенко О. С. Аналіз моделей безпеки в аспекті експертизи спеціалізованих інформаційних систем. *Моделювання та інформаційні технології* : Зб. наук. пр. К.: ІПМЕ ім. Г. Є. Пухова НАН України, 2009. Вип. 52. 8 с. URL: http://dspace.nbuv.gov.ua/handle/123456789/29642 (дата звернення: 17.10.2018).

6. Мазулевський О. Є. Аналіз прихованих каналів витоку інформації в телекомунікаційних системах військового застосування. *Збірник наукових праць Військового інституту телекомунікацій та інформатизації*

Національного технічного університету України Київський політехнічний інститут. 2013. № 2. С. 39-47.

7. Жора В. Підхід до моделювання рольової політики безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2003. Вип. 7. С.45-49.

8. Девянин П. Н. Модели безопасности компьютерных систем : учеб. пособие для студ. высш. учеб. заведений. М. : Издательский центр «Академия», 2005. 144 с.

9. Бабенко Л. К., Басан А. С., Макаревич О. Б. Мандатный доступ в СУБД. *Известия Южного федерального университета*. Технические науки. 2005. № 4 (48). С. 133-136.

10. Баранов П. А. Проблемы реализации мандатного доступа (модель Белла-ЛаПадулы) к ресурсам вычислительных систем. *Проблемы информационной безопасности. Компьютерные системы* 2005. № 1. С. 7-14.

11. Яковів І., Корнейко О., Черноног О. Класифікація і аналіз моделей систем захисту інформації в комп'ютерних системах. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні* : науково-технічний збірник. 2001. Вип. 3. С. 71-76.

12. Кононович І. В. Динаміка кількості інцидентів інформаційної безпеки. *Інформатика та математичні методи в моделюванні*. 2014. № 1. С. 35-43.

Одержано 17.10.2018

УДК 343.346.8:004.056.53

Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент
завідуючий кафедри інформаційних технологій
факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-4722-3159;
Дмитро Юрійович УЗЛОВ,
кандидат технічних наук,
начальник Управління інформаційно-аналітичної підтримки
ГУНП в Харківській області;
ORCID: https://orcid.org/0000-0003-3308-424X;
Олексій В'ячеславович ВЛАСОВ,
заступник начальника Управління інформаційно-аналітичної підтримки
ГУНП в Харківській області

МАКСИМІННИЙ КРИТЕРІЙ ВИЗНАЧЕННЯ ПЕРВИННИХ ЦЕНТРІВ В АЛГОРИТМАХ КЛАСТЕРИЗАЦІЇ K-MEANS

В базах даних органів внутрішніх справ на поточний момент накопичено десятки мільйонів записів кримінально значимої інформації. І кожного дня кількість цих даних зростає. Результати