Перелік посилань
1. Michelle Bailey. The Economics of Virtualization: Moving Toward an Application- Based Cost Model. IDC.URL: http://www.vmware.com/files/pdf/Virtualization-
2. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. URL: http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf

Метод захисту від загрозливих програм, заснований на реалізації контролю доступу до файлових об'єктів

Казіміров В.О., Мостовий С.В., Нагребецький О.В., Орленко В.С.
Хмельницький національний університет

Використання сучасних систем інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях та нових загроз, а з іншого - з урахуванням реальних характеристик апаратного та програмного забезпечення корпоративних мереж та систем. Процедура придбання пристроїв захисту інформації проста. Набагато складніше вирішити проблему - як захистити і які заходи безпеки застосовувати, мінімізуючи витрати. Впроваджуючи різні засоби захисту, необхідно визначити баланс між можливим збитком від несанкціонованого витоку інформації та обсягом інвестицій, які витрачаються на забезпечення безпеки інформаційних ресурсів. З метою підвищення ефективності захисту інформаційних ресурсів необхідно дослідити підходи до оцінки рівня їх захисту та систем захисту. Ця оцінка для кожного випадку індивідуальна і залежить від багатьох факторів (вартості інформації, статусу організації, важливості інформації, рівня технічного та програмного забезпечення тощо).

В роботі здійснено дослідження основних типів загрозливих програм, та запропоновано класифікацію шкідливого програмного забезпеченні (ШПЗ) за способом їх виконання. Враховуючи аналіз існуючої статистики зроблено висновок, що найбільш актуальними для захисту є виконувані двійкові і файли сценаріїв.

Можна виділити два найбільш поширених способи зараження: соціальна інженерія; технічні прийоми впровадження ШПЗ, що заражається без відома користувачf [1].

Ці види ШПЗ передбачають обов'язкове збереження файлу на вінчестері перед виконанням.

Тому можна зробити висновок що застосування розмежувальної політики доступу до виконуваних об'єктів, дозволяє мінімізувати загрози.

Проведено дослідження існуючих підходів до оцінки ефективності методів і засобів захисту від загрозливих програм, в результаті якого зроблені

висновки про неможливість з використанням відомих підходів ні кількісно оцінити актуальність окремої загрози для інформаційної системи в цілому (з урахуванням безлічі інших потенційних загроз), в тому числі загрози занесення і запуску загрозливих програм, ні кількісно оцінити основні стохастичні характеристики безпеки системи від загрозливих програм. В результаті чого сформульована задача розробки відповідних математичних моделей і наступного проведення на них досліджень, що дозволяють отримати необхідні кількісні оцінки.

Бінарні та скриптові виконувані файли будуть діяти як об'єкти доступу. Розглянемо варіант, коли всі користувачі мають однакові права доступу.

У Windows найпоширеніші двійкові виконувані файли. Найпоширеніший їх тип - аплікація. Додатки мають розширення EXE і можуть працювати самостійно. Крім того, існують динамічні бібліотеки (їх розширення - DLL), які містять загальні функції для різних додатків. Існують також драйвери (DRV або VXD) - спеціальні програми, необхідні для того, щоб система могла взаємодіяти з конкретними моделями певних пристроїв. Виконувані файли (особливо в Windows) можуть залежати один від одного: наприклад, для запуску будь-якої програми потрібні певні системні динамічні бібліотеки, а вони, в свою чергу, потребують драйверів [2].

Слід зазначити, що виконувані файли містять не тільки самі програми, але і різні додаткові дані. Це можуть бути різні графічні ресурси, що відображаються програмою, тексти написів, описи діалогових вікон тощо. Яскравим прикладом цього є архіви, які містять великі обсяги упаковки з метою зменшення її обсягу при передачі або зберіганні інформації [3].

Отже суб'єктом доступу є будь-який користувач системи $S_i : S = \{S_1, \dots, S_k\}$. Об'єкти доступу поділяються на виконувані, системні та інформаційні: $O = \{ O_{вик1}, \dots, O_{викq}, O_{сист1}, \dots, O_{системт}, O_{інф1}, \dots, O_{інфп} \}$.

Системні файли мають розширення: *.config, *.manifest, *.fon, *.ttf, *.log.

Ми додамо захист від виконуваних файлів сценарію. Для їх виконання потрібно встановити інший інтерпретатор, в якому запуститься виконуваний файл. Основою моделі захисту від виконуваних файлів сценарію є захист від витоку повноважень на зміну функцій дозволеної програми. Особливістю методу є поділ методу доступу "Запис" для створення нового об'єкта доступу («*ЗпН*») та зміни існуючого об'єкта доступу шляхом перейменування («*ЗпІ*»). Введемо додатково право доступу - заборона читання («*~~Чт~~*») [4].

Тоді в моделі будемо використовувати таку множину прав:

$$R = \{ Чт, \sout{Чт}, В, Зп, \sout{ЗпН}, \sout{ЗпІ}, \sout{Пв}, \sout{ПвВ}, \sout{Д} \}.$$

Права адміністратора:

- читання, інсталювання і запуск виконуваних файлів;
- читання, інсталювання системних файлів;
- читання і запис інформаційних файлів;
- все інше забороняти.

Опишемо права інших користувачів:

- читання і запуск виконуваних файлів, які вже знаходяться на системному диску;
- заборонити створення нового файлу, зміни існуючого, перейменування існуючого виконуваного файлу, видалення існуючих виконуваних файлів на системному диску;
- читання системних файлів;
- заборонити для системних файлів створення нового, зміну та перейменування існуючого файлу;
- читання і запис інформаційних файлів;
- заборонити запис, перейменування і видалення системних файлі;
- заборонити перейменування і видалення інформаційних файлів;
- заборонити для інформаційних файлів перейменування існуючого файлу, видалення;
- все інше заборонити.

	$O_{вик1}, \dots, O_{викq}$	$O_{сист1}, \dots, O_{системm}$	$O_{інф1}, \dots, O_{інфn}$
S_1	Чт, В, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, Зп, ~~Пв~~, ~~ПвВ~~, ~~Д~~
...		...	
S_k	Чт, В, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, Зп, ~~Пв~~, ~~ПвВ~~, ~~Д~~
M = VM_1	~~Чт~~, В, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, Зп, ~~Пв~~, ~~ПвВ~~, ~~Д~~
...		...	
VM_j	~~Чт~~, В, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~	Чт, Зп, ~~Пв~~, ~~ПвВ~~, ~~Д~~
A	Чт, Зп, В	Чт, Зп	Чт, Зп

Запропоновано модель захищеної системи, яка дає можливість сформувати вимоги з точки зору запобігання витоку прав доступу.

Такий підхід дає нам впевненість що такі права доступу не дадуть змогу бінарним і скриптовим виконуваним загрозливим файлам зашкодити

безпеці системи.

Але потрібно забороняти співпадання будь-якого користувача з Адміністратором [5] .

Отже в роботі досліджено існуючі способи впровадження та запуску загрозливих програм, в результаті чого зроблено висновок про те, що найбільш актуальними для захисту є виконувані бінарні і скриптові файли і про те, що дані класи загрозливих програм передбачають обов'язкове збереження загрозливого файлу на жорсткому диску перед його виконанням (читанням). Це дозволило зробити висновок щодо того, що захист від загрозливих програм може будуватися реалізацією контролю (розмежування прав) доступу до файлів.

Запропоновано загальний підхід до реалізації захисту від загрозливих програм, заснований на реалізації контролю доступу до файлів по їх типам, які можуть бути ідентифіковані розширеннями файлів. Можливість використання подібного підходу обґрунтована проведеним дослідженням засобів захисту.

Розглянута модель засобів захисту дозволяє сформулювати вимоги до експлуатаційних параметрів засобів захисту - до інтенсивності виявлення помилок засобами захисту, що дозволяє здійснити успішну атаку, та інтенсивності їх виправлення, виконання яких забезпечує необхідні значення експлуатаційних характеристик засобів захисту.

Перелік посилань

1. Лебедев А. Защита компьютера от вирусов, хакеров и сбоев / Алексей Лебедев. – М.: Питер, 2013. – 157 с.

2. Исполняемые файлы: расширения, форматы. // Справочник типов файлов. [Електронний ресурс]. Режим доступу: http://open-file.ru/types/executable/, свободный (10.10.2020).

3. *Cuff P*. Distributed channel synthesis / P. Cuff // IEEE. Trans. Inf. Theory. – 2013. – Vol. 59(11). – P. 7071-7096.

4. Джулій В.М. Оцінка актуальності загрози впровадження загрозливих програм для інформаційної системи / В.М. Джулій, В.О. Бойчук, О.О. Кушнерик, -Хмельницький: Наука й економіка, 2018. - Вип. № 2. – С.107-115

5. Schieler C. Rate-distortion theory forsecrecy systems / C. Schieler, P. Cuff // IEEE Trans. on Inf. Theory. – 2014. – Vol. 66(12). – P.7584-7605.

6. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

7. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.