УДК 004.056.57

О. Ю. Юдін, м. Київ

ПРОГРАМНІ ЗАКЛАДКИ. ШЛЯХИ БОРОТЬБИ З НИМИ

Abstract. The paper describes the main characteristics of the program bugs and the submitted a proposal to fighting with them.

Вступ

На теперішній час створення та розвиток вітчизняних інформаційно-телекомунікаційних технологій характеризується широким застосуванням закордонного апаратного та програмного забезпечення, як загальносистемного, так і спеціального. Фірми-виробники комп'ютерної техніки не гарантують при цьому відсутність в обладнанні, що поставляється, вбудованих апаратно-програмних закладок, комп'ютерних вірусів та інших шкідливих недокументованих можливостей (типу Backdoors, Spyware та інших) [1, 12, 14]. Одним з аргументів відмови від гарантійних зобов'язань є наявність механізму впровадження програмних закладок [2] який полягає в тому, що закладка інтегрується за допомогою інструментальних засобів розробки та налагодження програм на етапі створення програмного забезпечення. Виявити такий тип закладок дуже складно. В першу чергу це пов'язано з тим, що програміст практично не має можливості контролювати програми, які створює, так як працює на рівні логічних конструкцій мовних засобів. Таким чином, зловмиснику достатньо впровадити, наприклад в компілятор, код який буде модифікувати вихідний код.

Поряд з тим ймовірність наявності деструктивних "зловмисних" компонентів в комп'ютерних засобах обумовлена високим рівнем розвитку закордонної мікропроцесорної елементної бази (розмір закладок може складати декілька кілобайт) та технологій транспортування і впровадження програм-агентів з глобальних телекомунікаційних систем (наприклад мережа Інтернет).

Враховуючи актуальність проблеми в статті пропонується розглянути загальні відомості щодо програмних закладок та визначити підходи до боротьби з ними.

Класифікація програмних закладок

Під програмною закладкою (program bug) будемо розуміти потайно впроваджену програму або недокументовані властивості програмного забезпечення, використання яких може надати зловмиснику можливість обійти комплекс засобів захисту інформації і/або порушити встановлену в комп'ютерній системі (далі – КС) політику безпеки.

До основних властивостей програмних закладок доцільно віднести:

- виконання операцій запису та зчитування з пам'яті КС;
- внесення довільних перекручувань в коди програм, які знаходяться в

оперативній пам'яті КС;

- перенос інформації з одних областей пам'яті КС в інші;
- перекручування інформації отриманої в результаті роботи інших програм, яка виводиться на пристрої КС або в канали зв'язку.

Відповідно до [3] програмні закладки можна класифікувати за:

1. Методом впровадження в КС:

- закладки, які знаходяться в коді апаратних пристроїв (як приклад BIOS);
- закладки завантаження, які впроваджуються з програмами початкового завантаження КС (як приклад завантаження операційної системи з boot-сектору);
- закладки в драйверах на пристрої КС;
- закладки в прикладному програмному забезпеченні;
- закладки в файлах що виконуються (наприклад в файлах з розширенням exe, com);
- закладки-імітатори, які мають інтерфейс як у легальних програм;
- замасковані закладки, які маскуються під архіватори, дефрагментатори та інші.

2. Способом активізації:

- резидентні закладки, які постійно знаходяться в оперативній пам'яті;
- нерезидентні закладки, які вивантажуються з оперативної пам'яті після настання визначених умов.

3. Деструктивними діями:

- копіювання інформації яка обробляється в КС;
- зміна алгоритмів функціонування програмного забезпечення;
- зміни режимів роботи КС;
- знищення інформації;
- пошкодження обладнання КС.

4. Умовами початку виконання:

- закладка повинна потрапити до оперативної пам'яті КС;
- повинні наступити умови, при яких закладка активізується.

Виходячи з класифікації програмних закладок можливо зробити висновки, що:

1. Закладки можуть бути впроваджені в КС на будь-якому етапі її життєвого циклу. Одним із прикладів є впровадження в операційну систему Debian генератору випадкової послідовності, який створював передбачувальну послідовність. Зазначена послідовність використовувалась для створення секретних ключів SSH, OpenVPN, DNSSEC, а також ключів цифрового підпису за стандартом X.509 [16]. Таким чином зловмисник мав можливість атакувати систему електронного цифрового підпису або захищені системи передачі даних.

2. Закладки можуть впливати не тільки на інформацію але і виводити з ладу КС. Так, в 1990 році програмна закладка в одному електронному комутаторі телефонних каналів 4ESS (Class 4 telephone Electronic Switching

System) вивела з ладу телефонні мережі компанії AT&T на 9 годин. Деструктивні дії закладки полягали в тому, що всі комутатори 4ESS які були підключені до несправного комутатору отримували відмову в обслуговуванні, а потім надсилали такий саме сигнал до інших комутаторів і так далі.

3. Для запуску функціонування закладки повинні бути виконані умови необхідні для її активізації.

Ідентифікація програмних закладок

Як зазначається в [4] іноземні експерти стверджують, що програмні закладки на відмінність від апаратних закладок є найбільш витонченими та важко ідентифікуємими об'єктами. Тому промислово розвинені країни дуже обережно відносяться до використання імпортних інформаційних технологій. Так, американським законодавством жорстко обмежено застосування програмних засобів закордонного виробництва в інтересах забезпечення національної безпеки. Зазначене обумовлено в першу чергу тим, що на теперішній час для виявлення програмних закладок можуть бути застосовані тільки дуже дорогі методи контролю вихідних кодів текстів програм у сполученні з методами математичного моделювання процесів функціонування систем.

Одним із ефективних методів боротьби з програмними закладками є виявлення уразливих для програмних закладок місць системи захисту за допомогою груп експертів, які намагаються встати на місце зловмисника і розробити та впровадити в систему різного роду програмні закладки [5]. За допомогою такого підходу можуть бути виявлені слабкі місця захисту та напрацьовані рекомендації щодо уточнення адекватної політики безпеки з урахуванням загроз, які створюють програмні закладки. Такий підхід застосовується в корпорації Microsoft і має позитивні результати [13]. В той же час, зазначений підхід має певні недоліки, а саме:

- необхідність залучення чималої кількості експертів з високим рівнем кваліфікації;
- витрачання тривалого часу на проведення детального дослідження (для складних систем –декілька років);
- суб'єктивність, яка вноситься при застосуванні методу експертних оцінок;
- висока вартість обслуговування методу експертних оцінок.

Також, зазначений підхід майже неможливо застосувати для програмного забезпечення яке часто доопрацьовуються або взагалі перевипускається в нових версіях.

Виходячи з наведеного можна стверджувати, що підходи до виявлення програмних закладок в кожному конкретному випадку повинні визначатись окремо. З урахуванням різноманіття класів програмного забезпечення (системне, прикладне, інструментальне) та їх типів практично неможливо уніфікувати процес пошуку програмних закладок в масштабах України.

Враховуючи зазначене вище, можливо припустити, що в межах держави та на сучасному рівні розвитку техніки, коли апаратно-програмне

забезпечення змінюється кожен рік, а за 3-5 років вже морально застаріває і не задовольняє вимогам користувачів, витрачати роки праці сотень висококваліфікованих фахівців на аналіз та пошук програмних закладок неефективно.

Канали передачі інформації які використовують програмні закладки

Теоретично, програмні закладки можуть використовувати будь-які інтерфейси КС як канали передачі даних, або як канали для отримання команд активування. Однак найбільшу загрозу становить поєднання прихованих каналів (covert channel) та програмних закладок. Це твердження випливає з того, що у разі, коли програмна закладка використовує приховані канали для передачі даних виявити її становиться майже неможливо. Як приклад можливо навести деякі програми які реалізують приховані канали:

- Loki2 [6] для Linux використовує приховування інформації в полі даних ICMP-пакетів та DNS-запитів і відповідях;

- інструмент ReverseWWWShell, який розроблений Ван Хаузером (vanHauser) [7], використовує протокол http. Сервер ReverseWWWShell створює зворотне з'єднання з клієнтом та періодично "проштовхує" запит на отримання команд з клієнту і "витягує" команди, після виконання команди результат "проштовхується" зворотно. Зазначені програми передають дані в полі даних пакету та можуть бути відносно швидко виявлені;

- більш скритним методом є використання некритичних полів пакетів. Такий метод описаний в роботі Крэйга Х. Роулэнда (CraigH. Rowland) [8]. Розроблений їм інструмент Covert TCP використовує заміну інформації в службових полях протоколів IP та TCP.

Окрім зазначених "примітивних" прихованих каналів програмна закладка може використовувати більш витончені канали, як приклад передачу інформації за допомогою цифрового підпису. Один з таких механізмів був описаний в статті [9] та полягав в тому, що в реалізації алгоритму ГОСТ Р 34.10-2001 замість псевдовипадкового числа k підставлялось інше значення. Це значення отримував зловмисник.

Програмні закладки які використовують звичайні канали передачі даних ідентифікуються більш легко. Наприклад, в операційній системі AOS (Alcatel Operating System) версії 5.1.1, яка використовується в комутаторах Alcatel Omni Switch 7700/7800, була знайдена програмна закладка що запускала telnet-сервіс на порту 6778/TCP та надавала віддаленому зловмиснику повний доступ до керування комутатором [15]. Закладка виявлена завдяки несанкціонованому використанню порту, і це можна відстежити без застосування спеціалізованих програмно-апаратних комплексів.

З урахуванням викладеного можливо припустити, що у разі використання програмними закладками, для передачі інформації, прихованих каналів, її виявлення шляхом аналізу потоку інформації на виході КС майже неможливо. Такий висновок підтверджується іншими дослідженнями, як приклад [10, 11, 14].

Висновки

Виходячи з викладеного та спираючись на проведений аналіз можливо зробити наступні висновки:

1. Пошук та нейтралізація програмних закладок дуже трудомісткий процес який потребує багато часу та ресурсів.

2. Підходи до виявлення програмних закладок в кожному конкретному випадку повинні визначатись окремо. Тобто неможливо уніфікувати процес пошуку та нейтралізації програмних закладок.

3. Розробка уніфікованого засобу пошуку програмних закладок призначеного для будь-якого програмного забезпечення КС практично неможлива і як наслідок недоцільна.

4. В межах України, як держави в якій на національному рівні не існує визначеного набору базового програмного забезпечення, доцільно використовувати підхід боротьби з програмними закладками що полягає в контролі за їх впровадженням на всіх етапах життєвого циклу програмного забезпечення та усунення каналів їх активізації. В той же час, слід зазначити, що ефективність такого підходу буде досягнута лише за умов прийняття рішення щодо розробки та впровадження, як мінімум в органах державної влади, національного програмного забезпечення.

1. Информационная безопасность эргасистем: нетрадиционные угрозы, методы, модели [Електронний ресурс] / Д. Ловцов. – Режим доступу: http://viperson.ru/wind.php?ID=554830. – Назва з екрану.

2. *О. В. Казарин*. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2003. – 213 с.

3. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) [Електронний ресурс] / С. Охрименко, Г. Черней. – Режим доступу: http://security.ase.md/publ/ru/pubru05.html. – Назва з екрану.

4. *Ефимов А.И.* Проблемы безопасности программного обеспечения военной техники и других критических систем / А.И. Ефимов, П.А. Кузнецов, А. Лукашкин // Защита информации. – 1994. - № 2. С. 11-16.

5. Программные закладки в защищенных системах [Електронний ресурс] / В. Проскурин. – Режим доступу: http://www.crime-research.ru/library/progwir98.htm. – Назва з екрану.

6. LOKI2 (the implementation) [Електронний ресурс] / Daemon9 // Phrack Magazine. - 1997. - Vol. 7, issue 51. - Art. 6. – Режим доступу: http://www.phrack.org/issues.html?issue=51&id=6. – Назва з екрану.

7. Placing Backdoors Through Firewalls [Електронний ресурс] / Van Hauser. - 2005. - Режим доступу: http://www.thc.org/papers/fw-backd.htm. – Назва з екрану.

8. Covert channels in the TCP/IP protocol suite / C.H. Rowland // First Monday. – 1997. - Vol. 2, N 5. - Art. 6.

9. *Белим С. В.* Исследование скрытых каналов передачи информациив алгоритме цифровой подписи ГОСТ Р 34.10-2001 / С. В. Белим, А. М. Федосеев // Известия челябинского научного центра. -2007. - № 2 (36). – С. 17-20.

10. *Галатенко В. А.* О скрытых каналах и не только / Алексей Галатенко // Информационный бюллетень JetInfo. – 2002. - №11 (114). – С. 12-20.

11. *Тимонина Е. Е.* Скрытые каналы (обзор) / Е. Е. Тимонина // Информационный бюллетень JetInfo. – 2002. - №11 (114). – С. 3-11.
12. Программные закладки в бизнес-приложениях [Електронний ресурс] / Илья Шабанов. Режим доступу: http://www.anti-malware.ru/software_backdoors. – Назва з екрану.
13. Vulnerability Notes Database [Електронний ресурс] / Software Engineering Institute. Режим доступу: http://www.kb.cert.org/vuls/id/319331. – Назва з екрану.
14. *Галатенко В. А.* О каналах скрытых, потайных, побочных и не только / Алексей Галатенко // Информационный бюллетень JetInfo. – 2006. - №1. – С. 13-21.
15 Vulnerability Notes Database. CERT® Advisory CA-2002-32 Backdoor in Alcatel Omni Switch AOS. Software Engineering Institute [Електронний ресурс] / Software Engineering Institute. Режим доступу: http://www.cert.org/advisories/CA-2002-32.html. – Назва з екрану.
16. DSA-1571-1 openssl -- predictable random number generator [Електронний ресурс] / Debian Security Advisory. – 2008. Режим доступу: http://www.debian.org/security/2008/dsa-1571. – Назва з екрану.

Поступила 17.02.2014р.

УДК 004.032.24+004.312.44

І.Г. Цмоць, д.т.н., О.В. Скорохода, к.т.н., В. Я. Антонів, В.Б. Красовський
Національний університет «Львівська політехніка», м. Львів

МЕТОДИ ТА НВІС-СТРУКТУРИ УЗГОДЖЕНО-ПАРАЛЕЛЬНОГО ОБЧИСЛЕННЯ МАКСИМАЛЬНИХ І МІНІМАЛЬНИХ ЗНАЧЕНЬ

Анотація. Запропоновано алгоритм і спеціалізовані НВІС-структури для визначення максимальних і мінімальних значень та проведено оцінку їхніх основних характеристик.

Аннотация. Предложен алгоритм и специализированные СБИС-структуры для определения максимальных и минимальных значений и проведена оценка их основных характеристик.

Abstract. Algorithm and specialized VLSI structure to determine the maximum and minimum values have been proposed, evaluation of their basic characteristics has been conducted.

Ключові слова: узгоджено-паралельне обчислення, максимальне значення, мінімальне значення, НВІС-реалізація.

Ключевые слова: согласовано-параллельное вычисление, максимальное значение, минимальное значение, СБИС-реализация.

Keywords: coordinated-parallel computation, maximum value, minimum value, VLSI-implementation.

