Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 73-76 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

УДК 004.056.5(075.8).

ПРОБЛЕМА ОБЩЕГО АНАЛИЗА ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

THE PROBLEM OF GENERAL ANALYSIS OF INFORMATION PROTECTION IN THE INFORMATION SYSTEM

Д. Басшықызы, старший преподаватель, НАО Каспийский университет технологий и инжиниринга им. Ш. Есенова, г Актау, Казахстан
D. Bashygyzy, Senior Lector, NAO Caspian University of Technology and Engineering named after Sh. Yessenova, Aktau, Kazakhstan

АННОТАЦИЯ. Все программы защищены от несанкционированного копирования, если в ней выполняется копия программы, позволяющая проверить саму программу, с целью определить, создана ли она с соблюдением всех необходимых технологий. Программа не может нормально работать, если нарушена технология создания копий. Таким образом, юридическое копирование приводит к использованию некоторой уникальной технологии создания копий. Любая копия или внутренний файл защищенной программы должен иметь «ключ " - один или несколько кодовых цифр. При проверке программа сравнивает ряд специфических признаков рабочей среды с предварительно закодированным ключом и по результатам сравнения формирует соответствующий знак. Таким образом, создание копии программы минимально: эта копия должна предоставить ключ, готовый к работе с реальным компьютером, чтобы быть работоспособной.

КЛЮЧЕВЫЕ СЛОВА: *информационная система, файл, программа, компонент, персонал*

ABSTRACT: All programs are protected from unauthorized copying if a copy of the program is executed in it, which allows you to check the program itself in order to determine whether it was created in compliance with all the necessary technologies. The program cannot work normally if the copying technology is violated. Thus, legal copying involves some unique copying technology. Any copy or internal file of a protected program must have a "key" - one or several code digits. When checking, the program compares a number of specific features of the working environment with a pre-encoded key and, based on the results of the comparison, forms the corresponding sign. Thus, the creation of a copy of the program is minimal: this copy must provide a dongle ready to work with a real computer in order to be functional.

KEYWORDS: *information system, file, program, component, personal*

Стандарт информационной безопасности создает основу для взаимодействия между производителями, потребителями и экспертами по квалификации продукции информационных технологий.

Важнейшие стандарты информационной безопасности (в хронологическом порядке): «критерии безопасности компьютерных систем Министерства обороны США (оранжевая книга. 1983)», «европейские критерии безопасности информационных технологий», «федеральные критерии безопасности информационных технологий США», "критерии единства безопасности информационных технологий".

Какими специфическими признаками может обладать компьютер, на котором работает программа, а именно программно - аппаратная среда.

Для IBM – совместимых ПК этими признаками могут быть:

1. тип ПК и тип операционной системы (версия);
2. Дата выхода и /или его контрольное соединение;

3. физическое место месяцев на дисковом носителе;
4. аппаратный состав;
5. наличие скрытых частей программы;
6. физические особенности носителя (в т. ч. дефекты).

Некоторые из этих признаков очень индивидуальны (например, физические особенности некачественного носителя), другие менее индивидуальны (тип ПК, версия друга). Программа может использовать один или несколько символов, чтобы проверить законность копии. Особое значение в этом случае имеет способ применения программы: если программа рассчитана на работу на конкретном ПК, выбираются одни метки, если она легко перемещается с одного компьютера на другой без потери работоспособности - выбираются другие. Назовем программы первого типа-стационарными, а второго - мобильными.

Во всех случаях проверка законности не должна влиять на быстрое действие программы или требовать от пользователя каких-либо дополнительных действий (например, может ли система, использующая пароль, считаться эффективной). Система защиты должна проверять копию, а не пользователя.

Эти проверки довольно просты, но не имеют высокой степени индивидуальности в том смысле, что могут быть сотни тысяч ПК одного типа, использующих одну и ту же ОС. Поэтому обычно эти проверки используются в сочетании с проверкой других отдельных симптомов и предназначены для защиты стационарных программ.

Тип ПК жазылған f0000: жазылған fffe записан в КОС по адресу,т. е. в байтах перед последним в мегабайтном адресном пространстве ПК. Значения этого байта могут быть следующими кодами (табл.1).

Таблица 2. Коды значений байта

Код	Тип БД
FF	PC
FE	XT
FD	PCjr
FC	AT

Проверка сроков выхода и контрольной суммы фур. Постоянное запоминающее устройство (пси) является неделимой составной частью любого IBM, объединенного с ПК. Состав НПС учитывает особенности реализации конкретных ПК и может отличаться от компьютеров каждого типа.

При этом в конце фур (по адресу$F000:$FFFS) обычно записывается срок ее выхода, поэтому даже для однотипных ПК (даже при наличии одной фирмы - изготовителя) контрольная сумма фур отличается на разных экземплярах ПК.

Дата выхода НПС находится по адресу SFOOO: $FFF5 и состоит из 8 смешанных байтов. Данные хранятся символически в формате MM/DD/YY (MM – символы номера месяца, DD – номер даты, YY –номер года), например «26.06.92». Эта проверка используется для защиты стационарных программ.

Хорошей индивидуальностью обладает физический номер кластера, который начинается на жестком диске с файлом с защищенной программой. Действительно, в аппаратно-программной среде ПК что-то другое (кроме состава оперативной памяти) динамично меняется, как и файловая структура жесткого диска. При создании легальной копии исходный номер кластера для файловой программы на жестком диске в общем случае будет случайным. Если при отправке программа проверит этот номер,то в большинстве случаев она легко обнаружит незаконное копирование.

Такой способ защиты нельзя считать идеальным по многим причинам. Проверка номера кластера выполняется не так просто, как проверка даты выхода и типа ПК. Но первоначальный недостаток заключается в другом: любое изменение места файла в пределах хотя бы одного каталога приводит к незаконности ранее установленной копии.

Программа может проверить эффективный объем оперативной памяти, наличие и объем расширенной памяти, тип центрального процессора и приблизительную скорость его работы, наличие математического сопроцессора, тип и количество дисководов для гибких дисков, параметры физического жесткого диска, количество логических дисков, тип и количество каналов для подключения внешних устройств. Каждая из этих характеристик может повторяться на тысячах других ПК, но все они достаточно индивидуальны в комплексе и поэтому могут с большим успехом использоваться для защиты стационарных программ [1].

Некоторые зарубежные фирмы выпускают электронные ключи для защиты мобильных приложений - несколько более дешевых устройств, которые подключаются к стандартному каналу последовательного или параллельного ввода – вывода перед отправкой защищаемого приложения. Электронные ключи реализуются на основе заказанных микросхем и осуществляют взаимодействие с защищенной программой в необходимом интерфейсе.

Для компьютеров класса IBM AT используется специальная энергоемкая КМОП - память, которая хранит полезную информацию о составе аппаратных средств ПК, в том числе – эффективную память. Информацию о периферийных устройствах формирует Equipm в КМОП-памяти.

Наиболее эффективным способом защиты (в основном для мобильных приложений) является создание и использование скрытых частей программы и/или особенности физических носителей информации.

Скрытые части программы-это область носителя диска, которая тем или иным способом связана с программой, но не записана в виде файлов ОС. В подавляющем большинстве случаев в программе нет необходимости искусственно создавать такие территории, так как они будут«за» любым файлом.

Не очень эффективный способ защиты заключается в создании и использовании дополнительных скрытых кластеров. Такие кластеры могут быть помечены как неверные или «потерянные» в FAT (т. е. не соответствующие ни одному зарегистрированному файлу). (Во всех случаях, независимо от того, находится ли ключ за файлом или в отдельном кластере, защита может быть легко нейтрализована, если копирование дискета «из блока в блок " используется с помощью системной утилиты DISKCOPY или аналогичных несистемных программ).

Лучшей способностью противостоять незаконному копированию обладает система защиты, основанная на учете индивидуализированных особенностей, прежде всего дискет в анализе неустранимых дефектов. В этом случае система проверки защиты «знает» список дефектных секторов оригинальной дискеты и пытается их отформатировать. Если после форматирования обмен информацией с сектором прошел правильно, то соответствующий сектор - без дефекта и, следовательно, мы намерены работать с нелегальной копией дискеты. Главное достижение этого способа защиты приводит к принципиальной невозможности создания дефекта, который не устраняется программными средствами на правильной дискете.

Как видно из опыта, часть дискет (не менее 1%) состоит из заводских выходных дефектов, поэтому при большом выпуске коммерческих программ такие дефекты приходится создавать искусственно. Для этого иногда используют лазеры, а чаще – обычную булавку. После нескольких упражнений вы можете оставить царапину на слое носителя, когда угодно, или вы можете перевернуть дискету, чтобы сохранить работоспособность большей ее части. Но царапины и вмятины поверхности дискеты могут повредить головки некоторых носителей.

Под информационной безопасностью понимается поддержание инфраструктуры под случайным или предопределенным воздействием естественного или искусственного характера, грубо ущемляющего защиту информации и субъектов информационных отношений, в том числе владельца и пользователей информации, и поддержка инфраструктуры [2].

1. типичные атаки на операционные системы

Угроза-это потенциальная возможность реального нарушения информационной безопасности. Попытка осуществить угрозу называется нападением, а такого стремящегося – злоумышленником. Социальных злоумышленников называют источником угрозы.

Прежде всего, угроза исходит из-за наличия уязвимого места в защите информационных систем (например, возможность доступа посторонних лиц к крайне необходимому оборудованию или ошибке в программном обеспечении).

Типичные атаки:

1. сканирование файловой системы: злоумышленник сканирует файловую систему компьютера и пытается прочитать (или скопировать, или стереть) все файлы подряд.

2. Кража ключевой информации: в простейшем случае-злоумышленник видит пароль, набранный пользователем.

3. выбор пароля.

4.сбор мусора: во многих операционных системах информация, удаленная пользователем, физически не удаляется, помечается как удаленная. С помощью специальных программных средств эта информация (мусор) может быть впоследствии восстановлена. Сбор мусора может осуществляться не только на дисках, но и в оперативной памяти.

5. повышение полномочий: для реализации данной угрозы злоумышленник, используя ошибки в программном обеспечении операционной системы либо/или политике безопасности, получает больше полномочий, чем ему было предоставлено в соответствии с политикой безопасности. Обычно это происходит либо путем запуска программы от имени другого пользователя, либо переключением динамически загружаемой библиотеки. Эта угроза представляет большую опасность для операционных систем (UNIX), которые позволяют временно увеличить полномочия пользователя.

6. программный. В качестве средств вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (как правило - полоса пропускания сетей, вычислительные возможности процессоров и оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и отключенное. При сбое в конфигурации системы локальная программа монополизирует процессор или/или физическую память, снижая скорость выполнения других программ до нуля.

Одним из опасных способов атаки является проникновение вредоносного программного обеспечения в атакующую систему.

7.исключение штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы [3-5].

Защищенными называют ОС, рассматривающие средства защиты от основных классов угроз. Защищенная ОС обязательно должна содержать средства ограничения доступа пользователя к своим ресурсам, а также средства проверки подлинности пользователя, начиная работу с ОС. Кроме того, защищенная ОС должна содержать средства противодействия случайному или непреднамеренному выходу ОС из строя.

ЛИТЕРАТУРА

1. Айтхожаева Е.Ж., И Син Фу Е.В. Язык программирования баз данных xBase. /Методические указания к лабораторным работам по дисциплинам «Системы баз данных», «Базы данных». / - Алматы: КазНТУ, 2006.
2. Айтхожаева Е.Ж., И Син Фу Е.В. Визуальное проектирование компонентов систем баз данных. /Методические указания к лабораторным работам по дисциплинам «Системы баз данных», «Базы данных». / - Алматы: КазНТУ, 2004.
3. Айтхожаева Е.Ж., Дрогнова Н.Ф., И Син Фу Е.В. Разработка приложений баз данных. /Методические указания к курсовой работе/ - Алматы: КазНТУ, 2005.
4. Sergiy Gnatyuk , Maksim Iavich , Giorgi Iashvili , Andriy Fesenko ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019
5. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019