УДК 004.056.2

МОДЕЛЬ БЕЗОПАСНОСТИ С «ЧАСОВЫМ» МЕХАНИЗМОМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.В. ПОЛЯНСКАЯ[1], инженер, А.В. МОРОЗОВ[2], д-р. техн. наук,
С.Г. КРАСНОВ[3], адъюнкт

[1] Войсковая часть 21555, 214006, Смоленск, ул. Фрунзе, д. 47,
e-mail: glafira007@rambler.ru
[2] Военный инновационный технополис «ЭРА», 353456, Краснодарский край,
Анапа, Пионерский пр., д. 28, e-mail: glafira2190@mail.ru
[3] Военная академия воздушно-космической обороны
имени Маршала Советского Союза Г.К. Жукова,
170003, Тверь, ул. Жигарева, д. 50, e-mail: garvel568@yandex.ru

Основным направлением новой доктрины безопасности должна стать разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств, а также возможность гибкого управления безопасностью в зависимости от выдвигаемых требований, допустимого риска и расхода ресурсов. Задачей подсистемы контроля целостности ядра является обеспечение безопасности системы в процессе ее функционирования и обнаружение некорректного вмешательства субъектов системы в ее работу. В основе подсистем контроля целостности системы лежат две основные составляющие: статическая и динамическая. Частота срабатывания подсистемы контроля целостности ядра определяет интервал времени *T*, в котором система будет находиться в состоянии «утечки информации» в случае нарушения целостности системы. Существует два подхода к определению данного интервала времени: первый подход, вследствие наличия в системе подсистемы контроля целостности ядра, обеспечивает минимизацию потерь производительности системы, второй обеспечивает более высокий уровень безопасности при возможных потерях производительности системы.

Ключевые слова: модель безопасности, подсистема контроля целостности ядра, статистическая подсистема, динамическая подсистема, период срабатывания подсистемы.

DOI: 10.46573/2658-5030-2020-4-97-102

ВВЕДЕНИЕ

На сегодняшний день можно констатировать существенный разрыв между теоретическими моделями безопасности и современной парадигмой информационных технологий. Это приводит к несоответствию между моделями безопасности и их воплощением в программные реализации и выявлению недостатков современной научной базы обеспечения безопасности.

Такое положение обусловлено отсутствием общей теории защиты информации, комплексных моделей вычислительных систем, которые описывают механизм действий злоумышленников и разрушают программные средства (РПС) в реальных системах, а также отсутствием систем, позволяющих эффективно моделировать стойкость к атакам со стороны злоумышленников и РПС. Кроме того, в сфере безопасности нет даже общепринятой терминологии. Теория и практика существуют в разных плоскостях.

В результате практически все системы защиты основаны на анализе результатов успешно состоявшейся атаки.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Несмотря на то что прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий служит стимулом к развитию средств обеспечения безопасности, требуется во многом пересмотреть существующую научную парадигму информационной безопасности. Основным положением нового взгляда на безопасность должна являться разработка эффективных моделей безопасности, адекватных современному уровню развития программных и аппаратных средств, а также обеспечение возможности гибкого управления безопасностью в зависимости от выдвигаемых требований, допустимого риска и расхода ресурсов.

В 1987 г. Дэвид Кларк и Дэвид Уилсон представили модель целостности, которая существенно отличалась от уровнеориентированных моделей безопасности Белла и Лападула, а также от модели Биба. Впервые в своих положениях они обратились к термину «часовая процедура».

«Часовым» называется любой механизм или процедура, разработанная для снижения воздействия нежелательных событий до того, как они произошли. Это значит, что «часовые» процедуры являются предупредительным средством в том смысле, что они устанавливаются до того, как происходят события, от которых они обеспечивают защиту [2].

Задачей подсистемы контроля целостности ядра является обеспечение безопасности системы во время ее функционирования и обнаружение некорректного вмешательства субъектов системы в ее работу. В основу подсистем контроля целостности системы положены две главные составляющие: статическая (*подсистема обеспечения целостности ядра системы*) и динамическая (*подсистема контроля целостности ядра системы*).

В основе статической составляющей подсистемы контроля целостности ядра лежит модель целостности информации (например, модель Биба). Ядро системы должно находиться на самом привилегированном уровне безопасности, и к нему должен быть запрещен доступ по записи со стороны всех менее привилегированных субъектов системы. Реализация подсистемы обеспечения целостности информации должна опираться на аппаратную поддержку вычислительной системы.

В общем случае задачей подсистемы контроля целостности системы является динамический анализ целостности ядра системы с целью обнаружения возможных вмешательств в работу ядра системы со стороны менее привилегированных ее субъектов.

Подсистема контроля целостности ядра безопасности системы характеризуется двумя параметрами: множеством объектов, целостность которых подлежит контролю, и частотой срабатывания подсистемы контроля целостности. Рассмотрим влияние данных параметров на безопасность и производительность системы.

Влияние множества контролируемых объектов системы на ее производительность можно выразить следующим образом. Допустим, в цикле T проверяется целостность M объектов. Для $\forall m_i \in M$ существует параметр t_i, определяющий время, затрачиваемое системой на проверку целостности объекта m_i. Параметр t_i определяет сложность алгоритма проверки целостности объекта m_i системы и выражается в количестве тактов, в течение которых процессор проверяет целостность объекта m_i. При увеличении значения данного параметра, с одной стороны, повышается

надежность контроля целостности объекта m_i, а с другой – возрастает время, затрачиваемое на контроль целостности системы, и, как следствие, падает ее производительность.

Тогда однократная проверка системой целостности объектов ядра займет время

$$T_1 = \sum_{i=0}^{M} t_i. \quad (1)$$

Частота срабатывания подсистемы контроля целостности ядра определяет время, в течение которого система будет находиться в состоянии «утечки информации» в случае нарушения целостности системы. Иными словами, если подсистема контроля целостности работает один раз за временной промежуток T, то при нарушении целостности ядра система будет находиться в состоянии утечки информации в течение временного промежутка [0, T]. К определению интервала времени T возможны два подхода.

Первый подход характерен минимизацией потери производительности системы благодаря наличию подсистемы контроля целостности ядра. При этом подсистема контроля целостности ядра срабатывает в том случае, если субъекты системы не используют процессорное время в течение промежутка времени T. При этом частота срабатывания подсистемы контроля целостности ядра нерегулярна, так как она имеет низкий приоритет по сравнению с остальными субъектами системы, но при этом не происходит потери производительности системы.

Второй подход обеспечивает более высокий уровень безопасности при возможных потерях производительности системы. В данной ситуации подсистема контроля целостности ядра имеет высокий приоритет и срабатывает независимо от условий функционирования системы один раз за период времени T. Нижней границей, определяющей значение T, является выражение, определяющее максимально возможное время, которое система может провести в состоянии утечки информации. Это время вычисляется исходя из вероятности преодоления подсистемы контроля целостности. Будем считать подсистему контроля целостности нарушенной в том случае, когда субъект нарушитель смог изменить алгоритм подсистемы контроля целостности. Для этого ему необходимо преодолеть подсистему обеспечения целостности. Таким образом, для стопроцентного детектирования появления канала утечки информации, возникающего вследствие нарушения целостности системы, необходимо, чтобы подсистема контроля целостности срабатывала за временной интервал, не превышающий минимальное время, необходимое для преодоления субъектом-нарушителем подсистемы обеспечения целостности и модификации подсистемы контроля целостности.

Для определения времени, необходимого для изменения алгоритма контроля целостности, необходимо для синтезированной системы контроля и обеспечения целостности построить граф, отражающий все возможные пути преодоления подсистемы обеспечения целостности и модификации подсистемы контроля целостности [1]. Пример данного графа приведен на рисунке. Узлами данного графа являются компоненты подсистемы обеспечения целостности, а конечной вершиной каждого пути на данном графе – подсистема контроля целостности. Характеристикой каждого узла графа служит время, необходимое для преодоления данного компонента подсистемы обеспечения целостности, а также вероятность преодоления данного компонента, в предположении, что предыдущий компонент данного пути преодолен. Для первого элемента каждого пути данная вероятность полагается равной единице.

Тогда нижнюю границу периода срабатывания подсистемы контроля целостности информации можно записать как

$$T_2 \le \min(T_{p1}, T_{p2}, ..., T_{pn}), \tag{2}$$

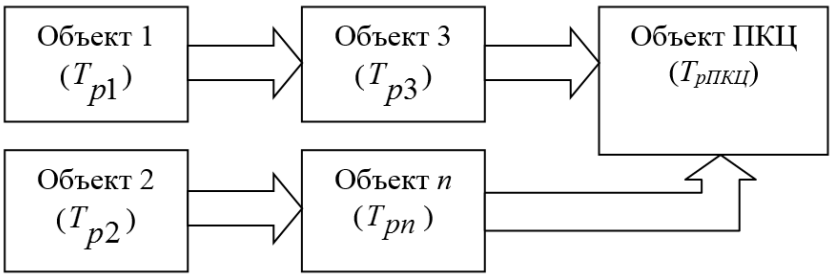
где T – время преодоления системы, соответствующее пути m на графе;

$$T_{pm} = \sum_i \frac{T_{p_i m}}{P_{i,i-1}}, \tag{3}$$

где $T_{p_i m}$ – время преодоления подсистемы i, принадлежащей пути m; $P_{i,i-1}$ – вероятность преодоления подсистемы i при условии преодоления подсистемы i – 1.

Для первого элемента в пути, ведущем к преодолению подсистемы контроля целостности, P = 1, т.е. предполагается, что данное звено в системе некорректно. При выполнении условия (2) преодолеть подсистему контроля целостности не удастся [3].

На рисунке показаны возможные пути нарушения подсистемы целостности информации (здесь ПКЦ – подсистема контроля целостности, а $T_{pПКЦ}$ – время разрушения подсистемы контроля целостности).



Пути нарушения подсистемы целостности информации

На данном рисунке показано два пути нарушения подсистемы контроля целостности. Для пути 1 суммарное время нарушения подсистемы контроля целостности $T_{нар1} = T_{p1} + T_{p3} + T_{pПКЦ}$. Для пути 2 суммарное время нарушения подсистемы контроля целостности $T_{нар1} = T_{p2} + T_{pn} + T_{pПКЦ}$. Таким образом, период функционирования подсистемы контроля целостности должен удовлетворять условию

$$T \le \min(T_{нар1}, T_{нар2}).$$

Выражение (2) определяет нижнюю границу возможного значения периода функционирования подсистемы контроля целостности.

С целью повышения производительности системы должно выполняться условие $T \to max$, т.е. чем реже выполняется контроль целостности ядра системы, тем меньше потеря производительности. Из данного выражения может быть вычислена верхняя граница T-периода срабатывания подсистемы контроля целостности информации:

$$T_4 \ge \sum_i^N \frac{t_i}{P-1}. \tag{4}$$

Таким образом, период срабатывания подсистемы контроля целостности для второго подхода может быть выбран исходя из выражений (2) и (4). Если значение периода срабатывания, полученное из выражения (2), больше, чем значение, полученное из (4), то удастся спроектировать систему с заданной потерей производительности и с гарантией контроля целостности. Если значение, полученное из выражения (2), меньше или равно значению, полученному из (4), то спроектирована система с заданной потерей производительности и подсистема контроля целостности не будет преодолена с вероятностью

$$P = \frac{T_4 - T_2}{T_4}, \quad (5)$$

где T_4 – период срабатывания подсистемы контроля целостности, вычисленный исходя из уравнения (4); T_2 – период срабатывания подсистемы контроля целостности, вычисленный исходя из выражения (2).

При $T_2 > T_4$ для достижения приемлемых безопасности и потери производительности следует изменить алгоритмы контроля целостности системы.

ЗАКЛЮЧЕНИЕ

Проведение защитных действий до причинения какого-либо вреда имеет ряд особенностей:

1. Интеграция в процессе проектирования. Поскольку «часовые» должны находиться в работоспособном состоянии до возникновения угрозы, то их следует идентифицировать и установлить в систему на стадии разработки и проектирования.

2. Противостояние угрозам. Если определенную угрозу нельзя допустить ни в коем случае, то метод «часовых» подходит как нельзя лучше, поскольку в такой ситуации принятие мер защиты после произошедшего нежелательного события не имеет смысла.

3. Нерациональное расходование ресурсов. Важным аспектом работы «часовых», который необходимо принимать во внимание, является оценка дополнительного времени и ресурсов, затрачиваемых на предотвращение событий, которые и так не могут произойти. Вычислительные системы некритического применения могут и не нуждаться в «часовых», использование которых в подобном случае представляет собой неоправданную трату ресурсов.

4. Сложности в оценке повышения безопасности. Еще одна проблема при использовании «часовых» связана с тем, что не всегда можно установить, действительно ли «часовой» работает. Конечно, это выполнимо в случаях, когда неудачные попытки нападения могут быть зафиксированы. Однако в тех случаях, когда нельзя определить, что данный «часовой» действительно предотвратил потенциальную атаку, оценить его эффективность довольно сложно. Можно применять статистические или вероятностные методы (например, использование системы с установленным и неустановленным «часовым»), но при этом все равно будет оставаться некоторая степень неопределенности.

ЛИТЕРАТУРА

1. Барзилович Е.Ю. Модели технического обслуживания сложных систем. М.: Высшая школа, 1982. 231 с.

2. Зегжда П.Д., Зегжда Д.П., Корт С.С. Теоретические основы информационной безопасности. СПб.: ВГТУ, 1998. 70 с.

3. Корпеев Д.О., Бондаренко Р.А., Яковлев Д.С. Методы однократной случайной выборки и последовательного случайного контроля защищенности информации

в компьютерных системах и пути повышения их эффективности // *Информация и безопасность.* 2010. № 3. С. 351–358.

Для цитирования: Полянская Ю.В., Морозов А.В., Краснов С.Г. Модель безопасности с «часовым» механизмом системы защиты информации // Вестник Тверского государственного технического университета. Серия «Технические науки». 2020. № 4 (8). С. 97–102.

SECURITY MODEL WITH THE "TIMING" MECHANISM OF THE INFORMATION SECURITY SYSTEM

Yu.V. POLYANSKAYA[1], Engineer, A.V. MOROZOV[2], Dr. Sc., S.G. KRASNOV[3], Adjunct

[1] Military unit 21555, 47, Frunze st., 214006, Smolensk, Russian Federation,
e-mail: glafira007@rambler.ru
[2] Military innovation technopolis "ERA" 28, Pionersky st., 353456, Krasnodar territory,
Anapa, Russian Federation, e-mail: glafira2190@mail.ru
[3] Military Academy of Aerospace Defense named after Marshal of the Soviet Union
G.K. Zhukov, 50, Zhigareva st., 170003, Tver, Russian Federation,
e-mail: garvel568@yandex.ru

The main point of the new approach to security should be the development of effective security models that are adequate to the current level of development of software and hardware, as well as the possibility of flexible security management depending on the requirements, acceptable risk and resource consumption. The task of the kernel integrity control subsystem is to ensure the security of the system during its operation and detect incorrect interference of system subjects in its operation. The system integrity control subsystems are based on two main components: static and dynamic. The frequency of the kernel integrity control subsystem actuation determines the time that the system will be in the "information leak" state in the event of a violation of the system integrity. There are two approaches to determining the time interval *T*: the first approach is characterized by minimizing the loss of system performance due to the presence of the kernel integrity control subsystem in the system, the second approach is characterized by the fact that it provides a higher level of security in case of possible losses of system performance.

Keywords: security model, kernel integrity control subsystem, statistical subsystem, dynamic subsystem, the subsystem response period.

REFERENCES

1. Barzilovich E.Yu. Modeli tekhnicheskogo obsluzhivaniya slozhnykh sistem. [Models of technical maintenance of complex systems]. Moscow: Vysshaya shkola, 1982. 231 p.

2. Zegzhda P.D., Zegzhda D.P., Kort S.S. Teoreticheskiye osnovy informatsionnoy bezopasnosti [Theoretical foundations of information security]. St-Petersburg: VGTU, 1998. 70 p.

3. Karpeev D.O., Bondarenko R.A., Yakovlev D.S. Methods of single random sampling and sequential random control of information security in computer systems and ways to improve their efficiency *Informatsiya i bezopasnost*. 2010, No. 3, pp. 351–358. (In Russian).

Поступила в редакцию/received: 02.07.2020; после рецензирования/revised: 28.08.2020;
принята/accepted 15.09.2020