УДК 004.056

В. С. Коломойцев*
кандидат технических наук, доцент
К. Р. Коломойцева**
магистрант
*Санкт-Петербургский государственный университет
аэрокосмического приборостроения
**Университет ИТМО

КОНТРОЛЬ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Работа посвящена исследованию методов повышения качества построения эффективных систем защиты информации. В работе предлагается метод контроля за корректным применением средств защиты информации, которыми располагает система защиты информации. Для реализации метода используется алгоритм расчета хэш-сумм. Проведено сравнение эффективности работы систем, использующей предложенный метод и без него в вопросе вносимых задержек обслуживания для систем с поэтапным обслуживанием поступающих запросов в систему. Показано, что системы, использующие данный метод уступают во вносимых задержках обслуживания. Однако, при этом, метод позволяет повысить степень защищенности системы от сложных информационных атак, за счет контроля порядка применения средств защиты.
Ключевые слова: защита информации; вычислительные системы; средства защиты информации; схема безопасного доступа; информационная безопасность; контроль работы.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
K. R. Kolomoytseva**
Postgraduate Student
*St. Petersburg State University of Aerospace Instrumentation
**ITMO University

MONITORING THE EFFECTIVENESS OF THE USE OF MEANS OF PROTECTION IN INFORMATION PROTECTION SYSTEMS

The work is devoted to the study of methods for improving the quality of designing effective information protection systems. The paper proposes a method for monitoring the correct use of means of information protection available to the information protection system. To implement the method, an algorithm for calculating hash sums is used. A comparison of the performance of information protection systems using the proposed method and without it in the issue of introduced service delays for systems with phased servicing of incoming requests to the system is made. It is shown that the systems using this method are inferior in the introduced service delays. At the same time, it allows you to increase the degree of protection of the system from sophisticated information attacks by controlling the order of application of means of protection.
Keywords: Information security; computer systems; means of information protection; pattern of secure access; information security; monitoring of operation.

Введение

В состав современных автоматизированных систем входит множество различных элементов, в том числе отвечающих за обеспечение информационной защищенности данных, обрабатываемых и хранящихся в ней. Путь данных поступающих на оконечные узлы автоматизированной системы лежит через эти элементы. От того, к какой категории можно отнести поступающие данные зависит какие средства, меры и методы защиты необходимо будет использовать системе защиты информации (СЗИ), чтобы обеспечить требуемый уровень информационной безопасности в системе. Таким образом, при построении эффективной СЗИ необходимо не только использовать наиболее совершенные решения в области защиты информации, но и также осуществлять контроль над тем, что данные решения действительно применяются при работе СЗИ и, более того, что они применяются в требуемом порядке.

В качестве объекта исследования возьмем СЗИ, построенную на распространенной в настоящее время схеме – «Связующий узел». В состав такой СЗИ входят: оконечные узлы (элемент системы, к которому необходимо обеспечить доступ); “связующие узлы” (вычислительные узлы на которых располагаются элементы защиты системы); маршрутизаторы (или любые другие устройства, необходимые для коммутации оконечных узлов со “связующими узлами” и “связующих узлов” с узлами не входящими в состав системы) [1], [2]. Будем считать, что на оконечных узлах системы либо нет никаких средств защиты, либо они не представляют серьезной угрозы для возможного нарушителя и, тем самым, при оценке системы ими можно пренебречь.

Метод подтверждения выполнения функций элементами системы защиты информации

Различных элементов, которые включены в состав СЗИ огромное множество. При этом для разных типов и видов данных необходимо применять разные методы и меры защиты, которыми располагает СЗИ. Более того, нередко бывает, что и порядок применение элементов защиты может играть существенную роль в обеспечении высоко уровня информационной защищенности системы. Предложим метод, позволяющий осуществить контроль над тем, какие средства, меры и методы защиты информации применялись и в каком порядке для конкретных данных (запросов), обрабатываемых в системе.

Работа метода контроля выглядит следующим образом.

1. Данные (запрос) перед тем, как попасть на оконечное устройство системы, направляются на анализ в СЗИ, включающей в себя некоторый набор элементов защиты. Попав на первый элемент защиты и успешно пройдя его, происходит вызов операции расчета хэш-суммы, на вход которой в качестве ключа подается уникальный идентификатор элемента защиты (серийный номер, код-слово обозначающее данный элемент, краткое описание элемента защиты или любая другая последовательность по которой можно однозначно определить элемент защиты среди всех остальных, входящих в состав СЗИ) и

сами данные (запрос). После успешного расчета хэш-суммы данные (запрос) поступают на следующий элемент защиты информации.

2. После того, как данные успешно прошли второй элемент защиты, происходит повторный расчет хэш-суммы. Однако в сравнении с расчетом хэш-суммы на первом этапе, в данном случае на вход алгоритма вместо самих данных будет подаваться ранее полученная хэш-сумма. В качестве ключа, как и на первом этапе, выступает идентификатор текущего элемента защиты.

3. Данный процесс (шаг 2) повторяется вплоть до момента, когда не закончатся все требуемые для анализа запроса элементы защиты (и таким образом, будет n-раз произведен расчет хэш-сумм, где n – количество задействованных в проверке элементов защиты).

4. По окончанию всех проверок элементами защиты, запрос покидает СЗИ и направляется на оконечный узел системы. Оконечный узел системы имеет информацию об идентификаторах элементов защиты и порядке (правильном) их применения для конкретных данных (запроса). Он производит повторный расчет хэш-суммы, с учетом известной ему информации по элементам защиты и полученным данным и, в случае совпадения полученной и повторно рассчитанной хэш-суммы, делает заключение о корректности примененных средств и методов защиты. Если совпадение не происходит то оконечный узел отбрасывает данный запрос, как неудовлетворяющий правилам информационной безопасности.

Простота внедрения данного метода контроля за корректностью работы средств защиты СЗИ, обусловлена возможностью его использования в виде программного компонента (службы) в составе СЗИ. Таким образом, операция расчета хэш-суммы может быть вызвана на вычислительном узле в любой требуемый момент. В свою очередь, так как все средства защиты располагаются также на вычислительном узле (входят в его состав), то получить информацию о состоянии их работы, а также их контрольные параметры (в том числе идентификаторы) – не представляется сложным.

Оценка влияния метода на работу вычислительной системы

Пусть СЗИ представляет из себя вычислительный узел, в состав которого входит набор средств защиты, реализуемых программно или аппаратно-программно. Средства защиты можно активировать последовательно (поэтапно) в любом порядке. Вычислительный узел представим в виде одноканальной системы массового обслуживания (СМО) с общей бесконечной очередью и поэтапным выполнением запросов [3].

Запрос, попавший в СЗИ, с вероятностью $(1 – P_i)$ попадает на каждый последующий этап обслуживания системы $(i + 1)$. В случае, когда элемент системы обнаруживает какую-либо угрозу в поступающем запросе, то с вероятностью P_i – данный запрос покидает систему и начинается обслуживание следующего запроса из очереди. На этапе R запрос покидает систему как в случае обнаружения угрозы, так и в ином случае. Время выполнения этапов будем считать распределенным по показательному закону [3].

СМО типа *M/G/1* является частным случаем СМО с поэтапным обслуживанием [3]. Используя формулу Полячика-Хинчина, учитывая, что в состав СЗИ входит *M*-систем, ведущих обслуживание поступающих запросов, среднее время пребывания запроса в системе *T*, можно определить как [3]:

$$T_S = \bar{x} + \frac{\lambda \cdot x^{(2)}}{2(M - \lambda \bar{x})}.$$

Здесь $\bar{x}$ – среднее время обслуживания запроса; $x^{(2)}$ – второй начальный момент; λ – интенсивность входного потока.

В случае, когда время обслуживания каждого этапа – случайная величина, распределенная по показательному закону для определения первого и второго начальных моментов можно воспользоваться следующей формулой [4]:

$$B(s) = \left(\frac{\mu_1}{s+\mu_1}\right)P_1 + \left(\sum_{i=2}^{R-1} P_i \left(\prod_{j=1}^{i=1}(1-P_j)\right) \cdot \prod_{j=1}^{i-1}\left(\frac{\mu_j}{s+\mu_j}\right)\right) + \prod_{i=1}^{R}\left(\frac{\mu_i}{s+\mu_i}\right) \cdot \left(\prod_{j=1}^{R-1}(1-P_j)\right), \quad (1)$$

где μ_i и P_i – интенсивность обслуживания и вероятность покидания системы запросом (устранение угрозы на *i*-м этапе обслуживания); *R* – количество этапов обслуживания (обнаружения и устранения угроз и/или расчета хэш-сумм). P_i – можно определить по формуле расчета вероятности обнаружения и устранения угрозы СЗИ, состоящей из *i*-элементов [2].

Используя формулу $\overline{X^n} = (-1)^n A^{*(n)}(0)$, можно вычислить *n*-ый начальный момент случайной величины [3]. Первая производная *B(s)* соответствует первому начальному моменту, а также математическому ожиданию, а вторая производная *B(s)* соответствует второму начальному моменту.

Таким образом, для СЗИ, включающей три элемента защиты информации, в конце работы которых происходит подтверждение их работы, путем расчета хэш-сумм (шесть этапов обслуживания) и, зная, что $\mu_i = V_i^{-1}$, а также приняв $s = 0$, получим среднее время обслуживания:

$$\begin{aligned}\bar{x} = V_1P_1 + (1-P_1)\cdot P_2\cdot(V_0+V_1+V_2) + (1-P_1)\cdot(1-P_2)\cdot P_3\cdot(2V_0+V_1+V_2+V_3) + \\ +(1-P_1)\cdot(1-P_2)\cdot(1-P_3)\cdot(3V_0+V_1+V_2+V_3),\end{aligned} \quad (2)$$

где V_i – среднее время обслуживания i-го средства ЗИ, V_0 – среднее время расчета хэш-суммы.

Зная, что $\mu_i = V_i^{-1}$ и приняв $s = 0$, получим второй начальный момент:

$$\begin{aligned}x^{(2)} = 2\cdot P_1\cdot V_1^2 + (1-P_1)P_2\cdot(2V_1^2+3V_0V_2+4V_0^2+V_1+V_2+V_0V_1) + \\ +(1-P_1)(1-P_2)P_3\cdot(4V_0V_1+4V_0V_2+4V_0V_3+6V_0^2+2V_1V_3+2V_2V_3 + \\ +2V_3^2+2V_2^2+2V_1^2+2V_1V_2) + (1-P_1)(1-P_2)(1-P_3)(8V_0V_1+4V_0V_2 + \\ +9V_0V_3+12V_0^2+2V_3^2+2V_1^2+V_2V_3+2V_2^2+2V_1V_2).\end{aligned} \quad (3)$$

Для стандартного вида СЗИ (без использования предлагаемого метода подтверждения), получим, что математическое ожидание и второй начальный момент равны:

$$\bar{x} = V_1P_1 + (1-P_1)P_2(V_1+V_2) + (1-P_1)(1-P_2)(V_1+V_2+V_3), \quad (4)$$

$$x^{(2)} = 2(V_1^2(P_1 + P_2(1-P_1)) + V_2^2P_2(1-P_1) + V_1V_2P_2(1-P_1) + V_3^2(1-P_1)\times$$
$$\times(1-P_2)) + (V_1^2 + V_1V_2 + V_2^2)(1-P_1)(1-P_2) + 2V_3(V_1+V_2)(1-P_1)(1-P_2). \quad (5)$$

В результате среднее время обслуживания для СЗИ, использующей предлагаемый метод будет равно: $T = T_S + T_{check} = T_S + n \cdot V_0 / (1 - \lambda_{end} \cdot n \cdot V_0)$, где n – количество элементов защиты в СЗИ, подтверждение работы которых требуется провести; λ_{end} – интенсивность входного потока для оконечных узлов, $\lambda_{end} = \lambda \cdot (1 - P_R)$. Однако в зависимости от использованного алгоритма хэширования T_N может иметь существенно меньшее значение.

В рамках данного исследования, в качестве алгоритма хэширования, возьмем алгоритм SHA-3 (Keccak). Данный алгоритм является последней версией алгоритма семейства SHA и позволяет за крайне короткие сроки проводить операцию хэширования больших объемов данных. Также, что немаловажно при использовании предлагаемого метода контроля работы средств защиты, алгоритм имеет возможность сократить время расчета хэш-сумм при реализации процедуры проверки хэш-суммы (повторный расчет) [4].

Пусть элементы СЗИ имеют следующие параметры:

- Вероятности обнаружения и устранения угрозы информационной безопасности СЗИ: $P_1 = 0{,}01$ (1%), $P_2 = 0{,}5$ (5%), $P_3 = 0{,}1$ (10%) – после одного, двух, трех элементов защиты, соответственно. Иными словами, система выполняет свои функции в штатном режиме и подвергается некоторым атакам разного вида (часть запросов являются зловредными и система может с ними бороться).
- Среднее время обслуживания: $V_1 = 1$ мс, $V_2 = 2$ мс, $V_3 = 3$ мс, $V_0 = 0{,}01$ мс.
- Вероятность успешного расчета хэш-суммы (P_0) и проверки корректности расчета хэш-сумм (P_N) – будем считать равной 1 (100%).
- Кратность резервирования равна: $M = 5$.
- Длина идентификатора – 256 бит.
- Алгоритм хэширования – SHA-3 (256 бит).
- Интенсивность входного потока, поступающего на оконечные узлы: $\lambda_{end} = 0.9 \cdot \lambda$

Тогда для СЗИ, использующей метод подтверждения (T_1) и СЗИ без подтверждения (T_2), в состав которых входит три элемента защиты, получим зависимость показанную на рис. 1.

В табл. 1, представлены некоторые значения задержек обслуживания для рассмотренных методов, а также оценена разница в задержке обслуживания между ними.

Как видно из таблицы, задержки обслуживания в системе растут в зависимости от интенсивности входного потока. При этом разница между вариантами построения СЗИ становится более существенной с увеличением значения интенсивности входного потока.

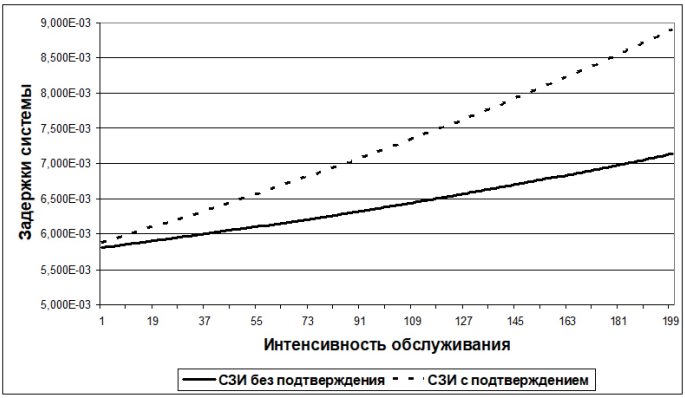

Рис. 1. Зависимость задержек обслуживания между способами построения СЗИ

Таблица 1

Выборочные значения задержек обслуживания

λ	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**	**160**	**170**	**180**	**190**	**200**
T_1, мс	5,85	5,9	5,96	6	6,07	6,13	6,19	6,26	6,31	6,38	6,81	6,89	6,97	7,05	7,14
T_2, мс	5,98	6,11	6,23	6,36	6,5	6,63	6,77	6,91	7,06	7,2	8,17	8,35	8,53	8,71	8,9
T_1 / T_2, %	2,2	3,4	4,6	5,7	6,9	8,12	9,3	10,5	11,7	12,8	20	21,1	22,3	23,5	24,7

С момента разработки и внедрения алгоритма хэширования SHA-3 было проведено несколько исследований по изучению влияния его работы на производительность вычислительных систем [5]. Проведенные исследования показали, что производительность систем в среднем снижается на 3-5%, с достижением скорости хэширования в 320 Мбит/сек. Учитывая данный факт и полученные результаты, показанные в Таблице 1, можно сказать, что разница во вносимых задержках обслуживания в СЗИ, использующих предлагаемый метод и без него, будет даже более существенной, чем показано в таблице. Вызвано это тем, что «потерянные» вычислительные ресурсы СЗИ может использовать на работу элементов защиты и, тем самым, используя предлагаемый метод, эффективность работы элементов защиты будет снижена. Стоит также учитывать, что при применении данного метода, помимо полезных данных, в канале будут присутствовать пакеты, содержащие хэш-суммы, что в некоторой степени будет снижать его пропускную способность.

Однако одним из важных факторов использования метода может стать то, что так как в случае нарушения порядка применения необходимых средств защиты итоговая хэш-сумма будет иной, то для злоумышленника снижается вероятность успешной реализации сложных атак, зависящих от анализа связанного набора данных (нескольких запросов) [6].

Заключение

В работе предложен метод контроля корректности применения методов и средств по защите информации в рамках системы защиты информации, использующей схему построения «Связующий узел», использующий алгоритм расчета хэш-сумм. Метод позволяет проконтролировать какие элементы защиты, имеющеюся в системе защиты информации были применены и в каком порядке.

Проведено исследование эффективности метода с точки зрения вносимых им задержек обслуживания в сравнении с типовым видом системы защиты информации. Показано, что система, использующая предложенный метод контроля обладает большими задержками обслуживания, чем типовая система. Также с ростом интенсивности входного потока разница между вариантами построения схем увеличивается.

Библиографический список

1. Kolomoitcev V. S. "Effectiveness of Options for Designing a Pattern of Secure Access ‘Connecting Node’," 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2020. P. 1-5, doi: 10.1109/WECONF48837.2020.9131509.

2. Коломойцев В. С., Богатырев В. А. Эффективность поэтапного применения средств защиты с пересечением областей обнаружения угроз // Программные продукты и системы. 2018. Т. 32. № 3. С. 557-564

3. Клейнрок Л. "Теория массового обслуживания", Пер. с англ./Пер. И.И.Грушко; ред. В.И.Нейман. М.:Машиностроение, 1979. 432 с.

4. Chang Shu-jen, Perlner Ray, Burr William E., Turan Meltem Sonmez, Kelsey John M. Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition. NIST: National Institute of Standards and Technology. 2012. Режим доступа: https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf [Дата обращения 22.03.21]

5. San Jose C.C.G. "Comparative and security performance analysis of SHA-3", Journal of Advanced Research in Dynamical and Control Systems. Volume 11, Issue 11 Special Issue, 2019, Pages 960-966

6. Shterenberg, S.I., Poltavtseva, M.A. A Distributed Intrusion Detection System with Protection from an Internal Intruder. Aut. Control Comp. Sci. 52, 945–953 (2018).