Научная статья

Original article

УДК 004.056.53

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ДОВЕРЕННЫХ ТЕХНОЛОГИЙ

RESEARCH OF INFORMATION PROTECTION MECHANISMS USING TRUSTED TECHNOLOGIES

Симачев Антон Юрьевич, студент Бакалавриата, НИЯУ МИФИ

Simachev Anton Yuryevich, undergraduate student, National Research Nuclear University MEPhI, simachev.anton@mail.ru

Аннотация. Обеспечение безопасности и конфиденциальности данных, хранящихся в цифровых форматах, является в настоящее время актуальной задачей. 21 век - это век информации. С быстрым развитием информационных технологий часто происходят инциденты с информационной безопасностью, приводящие к серьезным ситуациям. Информационная безопасность касается национальной безопасности и стабилизации общества. Развитие методов и систем защиты необходимо для обеспечения национальной информационной безопасности. В киберпространстве допускается взаимодействие двух сетевых объектов без предварительных договоренностей или аутентификации. Чтобы решить эту проблему, необходим метод, позволяющий пользователям судить о достоверности взаимодействующего объекта и обеспечивать безопасность взаимодействия в киберпространстве. Таким образом, доверие является основой безопасного взаимодействия в киберпространстве. Понятие доверенной среды появилось в 1983 году и сейчас получает новое развитие. В статье рассматриваются методики защиты цифровой информации с использованием

доверенных технологий. Целью статьи является исследование методов защиты данных и выдача рекомендаций по их использованию. Рассмотрены такие методы, как изоляции процессов, безопасное обращение с памятью, сокрытие данных, глубокая защита и метод минимизации. В результате анализа построена таблица, включающая достоинства и недостатки методов.

Abstract. Ensuring the security and confidentiality of data stored in digital formats is currently an urgent task. The 21st century is the age of information. With the rapid development of information technology, information security incidents often occur, leading to serious situations. Information security concerns national security and the stabilization of society. The development of methods and systems of protection is necessary to ensure national information security. In cyberspace, the interaction of two network objects is allowed without prior agreements or authentication. To solve this problem, a method is needed that allows users to judge the reliability of the interacting object and ensure the security of interaction in cyberspace. Thus, trust is the basis for secure interaction in cyberspace. The concept of a trusted environment appeared in 1983 and is now receiving a new development. The article discusses methods of protecting digital information using trusted technologies. The purpose of the article is to study data protection methods and provide recommendations on their use. Methods such as process isolation, secure memory management, data hiding, deep protection and minimization method are considered. As a result of the analysis, a table is constructed that includes the advantages and disadvantages of the methods.

Ключевые слова: доверенные вычисления, защита информации, механизм, процесс, изоляция

Keywords: trusted computing, information security, mechanism, process, isolation

1. Введение

Доверенные вычисления - это новая технология обеспечения безопасности информационных систем. Она берет свое начало в человеческом обществе и применяет успешный опыт управления компьютерной системой и киберпространством для обеспечения безопасности и доверия [1-3].

Основным технологическим методом доверенных вычислений является создание корня доверия в компьютерной системе, доверие которой обеспечивается физической безопасностью, технической безопасностью и безопасностью управления совместно, а затем построение цепочки доверия, начиная от корня доверия до аппаратной платформы, операционной системы и приложений. Предыдущие исполняемые коды проверяют целостность следующего выполняемого компонента и передают «код доверия», после чего он распространялся на всю компьютерную систему.

К наиболее известным и широко используемым на практике механизмам защиты информации с использованием доверенных технологий относятся [4-6]: изоляции процессов; безопасное обращение с памятью; сокрытие данных; глубокая защита; метод минимизации.

2. Методы

Рассмотрим и проанализируем вышеприведенные методы защиты компьютерной информации с использованием концепции доверенных вычислений.

Изоляция процессов - концепция защиты информации, применяемая для исключения вмешательства одних процессов в другие посредством изоляции последних. Процессом можно назвать любую программу, запускаемую на устройстве [7]. Концепция изоляции процессов включает в себя три основных метода: разделение памяти; мультиплексирование с разделением по времени; отсутствие доверия. Их совокупность обеспечивает изоляцию процессов по времени и памяти, уменьшая вероятность вмешательства одних процессов в другие.

Данный метод позволяет гарантировать, что доступ к данным процесса получит только наш узел, который отправил задание.

Изоляция процессов реализуема в языке программирования python (рис.).

```
from process_isolation import import_isolated
sys = import_isolated('sys')
sys.stdout.write('Hello world\n')
```

Рис. Пример кода с использованием изоляции процессов

Метод безопасного обращения с памятью - метод, подразумевающий внедрение программного ядра безопасности, служащего связующим звеном между процессом и общей памятью [8].

Сокрытие данных - концепция, при которой данные процессов более высокого уровня будут скрыты от процессов более низкого уровня [9]. В связи с отсутствием информации о наличии данных, процесс не сможет даже пытаться получить к ним доступ. Только необходимые процессу данные предоставляются ему по запросу, а все действия с ними записываются в лог файлы.

В языке программирования python сокрытие данных реализуется за счет двойного подчеркивания (префикса) перед названием атрибута. Это делает атрибут приватным и скрывает его от пользователя.

Глубокая защита - концепция внедрения множества слоев защиты, с имеющимися профилактическими, поисковыми и корректирующими средствами на каждом [10]. Данная концепция позволяет избежать раскрытия данных при возникновении ошибки на одном из слоев. В контексте информационной безопасности слоем называется отдельный уровень защиты, который необходимо преодолеть атакующему для получения доступа к системе. Глубокая защита замедляет нападающего.

Минимизация - концепция, подразумевающая наличие только минимально-необходимой функциональности программы или устройства [11]. Минимизация уменьшает количество путей компрометации системы для нападающего. Путем отключения ненужных возможностей программ, блокировки неиспользуемых портов и в уменьшения размера кода достигается безопасность программы и простота работы с ней.

3. Результаты

На основе проведенного анализа была составлена таблица характеристик методов.

Таблица. Достоинства и недостатки механизмов защиты информации с использованием доверенных технологий

Метод	Достоинства	Недостатки
Изоляции процессов	Позволяет защитить процессы	Процессы должны

	от коллизий и получения доступа к данным, которые им не нужны	использовать только связи коммуникации, определенные операционной системой
Безопасное обращение с памятью	Позволяет избежать ошибок переполнения буфера и истощения памяти	Требует установки специального программного обеспечения
Сокрытие данных	Позволяет защититься от случайного использования некорректных данных при работе программы	Возможное недовольство пользователя при отсутствии доступа для завершения задачи
Глубокая защита	Позволяет обезопасить сервер на нескольких уровнях	Множество независимых слоев требуют раздельного управления для обеспечения полной защиты. Требует установки специального программного обеспечения
Метод минимизации	Обеспечивает удобство разработки и простоту поддержки программного кода	Расширение возможностей кода в дальнейшем будет затруднено

4. Заключение

Таким образом, можно сказать, что доверенные информационные технологии включают доверенное техническое обеспечение (компьютер в общем смысле) и программное обеспечение (некую изолированную операционную систему), которые будут обеспечивать функционирование приложений, требующих приватного выполнения. Рассмотренные методы могут применяться как по отдельности, так и в сочетаниях под конкретные задачи в соответствии с разработанной таблицей.

Литература

1. Shen C. X. et al. Research on trusted computing and its development //Science China Information Sciences. – 2010. – Т. 53. – №. 3. – С. 405-433.

2. Challener D. et al. A practical guide to trusted computing. – Pearson Education, 2007.
3. Shen Z. et al. Cloud computing system based on trusted computing platform //2010 International Conference on Intelligent Computation Technology and Automation. – IEEE, 2010. – Т. 1. – С. 942-945.
4. Новиков С. В., Зима В. М., Андрушкевич Д. В. Подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры //Информатика и автоматизация. – 2015. – Т. 1. – №. 38. – С. 34-57.
5. Котенко И. В. и др. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах //Информатика и автоматизация. – 2012. – №. 20. – С. 27-56.
6. Сырчин В. К., Панасенко С. П. Научно-технические аспекты защиты конфиденциальной информации: проблемы, способы, решения //Высокотехнологичное право: генезис и перспективы. – 2021. – С. 338-345.
7. Mao J. K., Xu Y. F. Research on gateway security isolation technology based on trusted computing //Advanced Materials Research. – Trans Tech Publications Ltd, 2014. – Т. 846. – С. 1656-1659.
8. Felber P. et al. Safe exception handling with transactional memory //Transactional Memory. Foundations, Algorithms, Tools, and Applications. – Springer, Cham, 2015. – С. 245-267.
9. Yesilyurt M., Yalman Y. New approach for ensuring cloud computing security: using data hiding methods //Sādhanā. – 2016. – Т. 41. – №. 11. – С. 1289-1298.
10. Hassan M. M. et al. A robust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment //IEEE Internet of Things Journal. – 2020. – Т. 8. – №. 12. – С. 9611-9621.
11. Erway J. B., Gill P. E. A subspace minimization method for the trust-region step //SIAM Journal on Optimization. – 2010. – Т. 20. – №. 3. – С. 1439-1461.

References

1. Shen C. X. et al. Research on trusted computing and its development //Science China Information Sciences. – 2010. – Т. 53. – №. 3. – С. 405-433.

2. Challener D. et al. A practical guide to trusted computing. – Pearson Education, 2007.
3. Shen Z. et al. Cloud computing system based on trusted computing platform //2010 International Conference on Intelligent Computation Technology and Automation. – IEEE, 2010. – Т. 1. – С. 942-945.
4. Novikov S. V., Zima V. M., Andrushkevich D. V. Approach to the construction of secure distributed data processing networks based on trusted infrastructure //Computer science and automation. - 2015. – Vol. 1. – No. 38. – pp. 34-57.
5. Kotenko I. V. et al. Application of information and security event management technology to protect information in critical infrastructures //Computer science and automation. - 2012. – No. 20. – pp. 27-56.
6. Syrchin V. K., Panasenko S. P. Scientific and technical aspects of confidential information protection: problems, methods, solutions //High-tech law: genesis and prospects. – 2021. – pp. 338-345.
7. Mao J. K., Xu Y. F. Research on gateway security isolation technology based on trusted computing //Advanced Materials Research. – Trans Tech Publications Ltd, 2014. – Т. 846. – С. 1656-1659.
8. Felber P. et al. Safe exception handling with transactional memory //Transactional Memory. Foundations, Algorithms, Tools, and Applications. – Springer, Cham, 2015. – С. 245-267.
9. Yesilyurt M., Yalman Y. New approach for ensuring cloud computing security: using data hiding methods //Sādhanā. – 2016. – Т. 41. – №. 11. – С. 1289-1298.
10. Hassan M. M. et al. A robust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment //IEEE Internet of Things Journal. – 2020. – Т. 8. – №. 12. – С. 9611-9621.
11. Erway J. B., Gill P. E. A subspace minimization method for the trust-region step //SIAM Journal on Optimization. – 2010. – Т. 20. – №. 3. – С. 1439-1461.

© Симачев А. Ю. 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Симачев А. Ю. ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ДОВЕРЕННЫХ ТЕХНОЛОГИЙ// Научно-образовательный журнал для студентов и преподавателей «StudNet» 6/2022