Методика разработки программы обеспечения целостности баз данных

Воробьева Диана Евгеньевна

соискатель ученой степени кандидата технических наук, АО «Невское проектно-конструкторское бюро», Санкт-Петербург, Россия, dinvor@mail.ru

АННОТАЦИЯ

Введение: Обеспечение целостности баз данных значимых объектов информационной инфраструктуры, к которым, в частности, относится база данных используемая в АСУ проектирования кораблей, является одной из главных задач, решаемых при обеспечении защиты критических информационных инфраструктур. **Постановка задачи:** В случае атаки со стороны внутреннего нарушителя возможно вместе с работой СУБД запустить на выполнение отладчик или трассировщик программ и таким образом получить возможность исследования программы с целью ее дальнейшего взлома. Возникает задача блокирования такой возможности, но технология «тонкого клиента» излишне сложна и не очень эффективна. Таким образом, требуется разработать достаточно простой и функциональный механизм для отечественных операционных систем. **Методы:** методы синтеза программных систем защиты информации. **Результаты**: методика разработки прототипа программной системы обеспечения целостности базы данных. **Практическая значимость**: обеспечение безопасной работы СУБД SQL в условиях заранее неизвестных компьютерных атак. **Обсуждение**: новизна предложенной задачи состоит в том, что предложен механизм упреждающего блокирования опасных воздействий на значимые объекты критической информационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА: целостность баз данных, защита от атак внутреннего нарушителя, программная система, блокировка опасных воздействий

Введение

Актуальность темы данной статьи обусловлена необходимостью защиты значимых объектов критической информационной инфраструктуры в условиях целенаправленных атак при отсутствии шаблонов безопасности для заранее неизвестных программно-технических воздействий на базы данных, используемые при проектировании кораблей [1-3].

Обеспечение целостности баз данных значимых объектов информационной инфраструктуры, к которым, в частности, относится база данных используемая в АСУ проектирования кораблей, является одной из главных задач, решаемых при обеспечении защиты критических информационных инфраструктур. В случае атаки со стороны внутреннего нарушителя возможно вместе с работой СУБД запустить на выполнение отладчик или трассировщик программ и таким образом получить возможность исследования программы с целью ее дальнейшего взлома. Возникает задача блокирования такой возможности, но технология «тонкого клиента» излишне сложна и не очень эффективна. Таким образом, требуется разработать достаточно простой и функциональный механизм для отечественных операционных систем.

В настоящее время назрел переход от теоретических исследований к нормальной схеме разработки средств защиты обеспечивающих гарантированную защищенность среды выполнения программ [4]. Это означает принудительную блокировку любых, как системных, так и других процессов, хотя бы потенциально могущих быть злонамеренными, в отличие от применяемого в настоящее время метода эталонных характеристик при построении механизмов защиты.

Для достижения поставленной цели создания системы гарантированного подавления опасных процессов необходимо решить следующие задачи:

- заблокировать саму возможность оператора иметь независимую от системы защиты функциональность рабочего места;
- обеспечить запуск защищаемой прикладной программы прямо из программы защиты (блокировки);
- оценить полученную защищенность на основе методов пентестинга [5-7].

Степень разработанности темы

На сегодня ссоздание программных средств защиты работы СУБД является достаточно малоисследованной задачей. Такие программы необходимы как для защиты серверов баз данных, так и для СУБД запускаемой на автоматизированных рабочих местах что накладывает определенные трудности на особенности их синтеза [8-12. При создании системы защиты СУБД от хакерских атак фундаментальной задачей остается эффективное использование и согласование ресурсов операционной системы в среде которой исполняется файл СУБД. Для решения такой задачи необходима разработка методов блокирования избыточной функциональности рабочего места оператора системы проектирования, которая использует базу данных в своей работе.

Анализ ранее проведенных исследований в области защиты СУБД и самих данных показал, что в известных работах были рассмотрены различные аспекты такой защиты:

- Архитектурное решение задачи повышения эффективности управления информационной инфраструктурой предприятия рассматривалось в работах Ю.В.Ланских, Я.В.Коновалова, но в них не рассматриваются вопросы сопряжения с ГосСОПКа.
- Доступность данных информационных систем рассматривалась в работах А.В.Ревнивых, А.М.Федотова, У.Франке, П.Джонсона, А.П.Мартина, Д.Хазанчи, К.Триверди, К.Ф.Раушера, но в них не проработаны вопросы анализа системами обнаружения вторжений (СОВ) запросов к базам данных, не разработаны соответствующие шаблоны для СОВ.
- Анализ функциональной стабильности критичных информационных систем был выполнен в работах Б.В. Соколова, П.В. Сундеева, но в данных работах нет теории и нормативно-методического аппарата анализа защищенности БД от целенаправленных воздействий.

- Вопросы моделирования непрерывности функционирования ИС были разработаны в трудах В.А.Герасименко, Ю.Г.Ростовцева, П.Л.Чебышева, А.А.Маркова, А.М.Ляпунова, П.Берстейна, Ф.Найта, Т.Авена, Д.Гольмана, Д.Скотта, но в них приведена только общая теория для информационных систем в целом.
- Задачи моделирования систем защиты информации были исследованы в работах П.Д.Зегжды, А.М.Ивашко, О.И.Береснева, В.Е.Ильина, но в них нет модели защищенной обработки транзакций в БД.
- Модели и механизмы управления безопасностью рассматривались в работах В.Н.Буркова, Е.В.Грацианского, П.Н.Девянина, С.И.Дзюбко, А.В.Щепкина, Дж.Вакка, но существующие модели и механизмы управления безопасностью нацелены только на защиту данных и не включают СУБД как отдельный вид ПО.
- Выбор критериев эффективности комплексных систем безопасности был выполнен в работах В.И.Васильева, Т.А.Иванова, А.А.Бакирова, С.М.Климова, Б.П.Пальчуна, М.П.Сычева, но существующие критерии эффективности не полностью учитывают целенаправленные воздействия.
- Мониторинг компьютерных атак рассматривался в работах С.А.Петренко, К.Мак-Клар, Л.Стюарта, Джоэл Скембрей, Дж.Курца, И.Д.Медведовского, П.В.Семьянова, В.В Платонова, но мониторинг компьютерных атак при взаимодействии с ГосСОПКа не описан в открытой литературе.
- Противодействие компьютерным атакам исследовано в работах С.А.Петренко, С.М.Климова, М.П.Сычева, А.В.Астахова, А.В.Лукацкого, А.Н.Лукашкина, но в них противодействие компьютерным атакам на СУБД описывается только с точки зрения криптографической защиты данных.
- Теория сетей Петри и моделирование систем подробно рассмотрена в работах Дж.Питерсона, но современных условиях требуется разработка моделей, адаптированных к определенным структурам и алгоритмам функционирования СУБД [13-17].

Таким образом, проведенный анализ известных работ в исследуемой предметной области позволил сформулировать противоречие в науке – между высокими требованиями к защищённости процессов функционирования АСУ проектирования кораблей и их СУБД и недостаточным уровнем развития научно-методического аппарата (моделей и методик) обеспечения целостности баз данных АСУ проектирования боевого корабля на основе самоконтроля семантики вычислений.

Исходя из вышеизложенного научная задача исследования заключается в разработке методики разработки прототипа программной системы обеспечения целостности БД (СУБД) АСУ ПК в условиях роста угроз безопасности на основе самоконтроля семантики функционирования СУБД.

Математической основой синтеза системы обеспечения целостности БД (СУБД) выступает теория трансляции.

Программа обеспечения целостности баз данных

Постановка задачи

Написать программу, которая будет загружаться вместе с операционной системой, формировать полный рабочий стол с ярлыками разрешенных программ и производить блокировку функциональных клавиш ОС (Ctrl+Alt+Del, Ctrl+F5, Alt+Tab), перекрывать доступ в систему, предоставляя для работы пользователю только возможность загрузки и работы с исполнимым файлом СУБД. Полный доступ к системе открывается только после ввода пароля.

Описание работы программы

После загрузки программа разворачивает окно на весь экран и включает блокировку функциональных клавиш операционной системы. Блокировка происходит с помощью функции Win API “SetWindowsHookEx”.

Описание функции:

function SetWindowsHookEx(idHook: Integer; lpfn: TFNHookProc; hmod: HINST; dwThreadId: DWORD): HHOOK;

Функция SetWindowsHookEx устанавливает определенную приложением процедуру ловушки в цепочку ловушек. Приложение устанавливает процедуру ловушки, чтобы контролировать некоторые типы событий в системе. Процедура ловушки может контролировать события, связанные со специфической нитью или со всеми нитями в системе.

Параметры:

idHook: Определяет тип процедуры ловушки, которая будет установлена. Этот параметр может иметь одно из значений WH_.

lpfn: Указывает на процедуру ловушки. Если dwThreadId параметр, равен нулю или определяет идентификатор нити, созданного другим процессом, параметр lpfn должен указать на процедуру ловушки в библиотеке динамических связей (DLL). Иначе, lpfn может указывать на процедуру ловушки в коде, связанном с текущим процессом.

hMod: Идентифицирует DLL, содержащую процедуру ловушки, на которую указывает параметр lpfn. Параметр hMod должен быть установлен как NULL, если параметр dwThreadId определяет нить, созданную текущим процессом и если процедура ловушки - внутри кода, связанного с текущим процессом.

dwThreadId: Определяет идентификатор нити, с которым процедура ловушки должна быть связана. Если этот параметр - нуль, то процедура ловушки связана со всеми существующими нитями.

Возвращаемые значения

Если функция обработана, возвращаемое значение - дескриптор процедуры ловушки.

Если запрос провален, возвращаемое значение NULL.

Замечания

Ошибка может происходить, если параметр hMod равен NULL, и параметр dwThreadId - нуль или определяет идентификатор нити, созданного другим процессом.

Формирование цепочки к следующей процедуре ловушки (то есть вызов функции CallNextHookEx) по выбору. Приложение или библиотека может вызывать следующую процедуру ловушки или прежде, или после любой обработки в собственной процедуре ловушки. Хотя формирование цепочки на следующую ловушку выборочно, это строго рекомендуется; иначе, другие приложения, которые установили ловушки, не будут получать уведомления ловушки и могут в результате вести себя неправильно.

Перед завершением, приложение должно вызвать функцию UnhookWindowsHookEx, чтобы освободить ресурсы, связанные с ловушкой.

Контекст ловушки зависит от типа ловушки. Некоторые ловушки могут быть установлены только с контекстом системы; другие могут также быть установлены только для специфической нити, как показано в следующем списке:

WH_CALLWNDPROC - Нить или система (Thread or system)
WH_CBT - Нить или система (Thread or system)
WH_DEBUG Нить или система (Thread or system)
WH_GETMESSAGE - Нить или система (Thread or system)
WH_JOURNALPLAYBACK - Только система (System only)
WH_JOURNALRECORD - Только система (System only)
WH_KEYBOARD - Нить или система (Thread or system)
WH_MOUSE - Нить или система (Thread or system)
WH_MSGFILTER - Нить или система (Thread or system)
WH_SHELL - Нить или система (Thread or system)

WH_SYSMSGFILTER - Только система (System only)

Для определенного типа ловушки, сначала вызываются ловушки нити, затем ловушки системы.

Для автозагрузки программы используется динамически создаваемый ключ в реестре. Ключ создается в локальной области, отвечающей за автозагрузку, для всех пользователей системы. Запуск СУБД происходить с помощью стандартных средств языка Delphi. После ввода правильного пароля блокировка снимается с функциональных клавиш операционной системы, а приложение закрывается.

Оценка применимости предлагаемой программы в практических целях

Основной эффект обеспечения защищённости СУБД, как ясно из вышесказанного, достигается тем, что сама возможность сбросить рабочий стол с разрешенными ярлыками оператору нечем, так как все действия такого типа с клавиатуры запрещены. В результате, в отличие от технологии «тонкий клиент» нет необходимости перенастройки реестра операционной системы, а, самое главное, мониторинга возможных хакерских действий оператора [18-20].

Дальнейшая борьба с опасной функциональностью самой защищаемой программы достигается запуском программы из другой программы. Ярлык запуска не является в данном случае ярлыком операционной системы, а программируется в программе защиты. При привязке к ярлыку исполняемого файла в среде разработки становится доступна таблица функциональности всех органов управления в защищаемой программе. Приведем пример. Если таким образом создать запуск программы Word, то можно у кнопки «Open/Run» выключить неизвестно зачем введенную дополнительную функцию (если это только текстовый редактор) «Run» и оставить безопасную функцию «Open». Какие функции защищаемой программы являются потенциально опасными или не нужными в данном случае принимает решение разработчик программы защиты.

Моделирование атак на СУБД применяемую предприятием-заказчиком, защищенную описанной программой защиты, а также проверка корректности встраивания была произведена на средствах киберполигона ИТЦ «Ингрия» (Санкт-Петербург).

Заключение

Данная программа является программой обеспечения целостности баз данных, так как блокирует попытки оператора обойти ограниченную функциональность рабочего места.

Разработанная программная модель системы защиты была предложена к реализации в виде программного комплекса, который должен также обеспечивать защиту работы СУБД в случае наличия закладок в операционной системе или хакерских действий по сети с удаленного компьютера по отношению к рабочему месту в интересах проекта Сейфнет НТИ РФ и апробирована на площадке киберполигона ИТЦ «Ингрия» (Санкт-Петербург) в 2022 году. Применение предложенной технологии защиты позволяет сделать следующий шаг к требуемым системам безопасности значимых объектов критической информационной инфраструктуры.

Литература

1. *Воробьева Д.Е.* Система мониторинга безопасности технологических операций на основе квантового блокчейна // Известия СПБГЭТУ «ЛЭТИ». 2023.№9. С. 54-59.

2. *Воробьев Е.Г., Воробьева Д.Е.* Безопасное функционирование инфраструктуры телерадиовещания в аспекте влияния на цифровую экономику//«Защита информации. Инсайд». 2023. №1. С.2-6.

3. *Воробьев Е.Г., Воробьева Д.Е.* Модели оценки киберустойчивости транзакций в СУБД // «Защита информации. Инсайд». 2022. №6. С.67-70.

4. Безопасность объектов критической информационной инфраструктуры. Общие рекомендации. М.:АРСИБ, 2019. 52 с.

5. *Петренко А.С.* Квантово-устойчивый блокчейн. С.-Пб: Изд-во Питер, 2022. 320 с.

6. *Горбань И. И.* Феномен статистической устойчивости. М.:Наука, 2018. 444 с.

7. *Крамаров С.О.* Криптографическая защита информации. М.: Риор, 2019. 112 с.

8. *Мельников В.П.* Защита информации. М.: Академия, 2019. 320 с.

9. *Баранова Е.К.* Информационная безопасность и защита информации. М.: Риор, 2018. 400 с.

10. *Хорев, П.Б.* Программно-аппаратная защита информации. М.: Форум, 2018. 352 с.

11. *Parker, Donn B.* Fighting Computer Crime : A New Framework for Protecting Information : [англ.]. N. Y. : John Wiley & Sons, 2019. 528 p. ISBN 0-471-16378-3.

12. *Krutz, Ronald L.* The CISM Prep Guide : Mastering the Five Domains of Information Security Management : [англ.] / Ronald L. Krutz, Russell Dean Vines. N. Y.: John Wiley & Sons, 2020. 433 p. ISBN 0-471-45598-9.

13. *McCarthy, C.* Digital Libraries : Security and Preservation Considerations // Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management : [англ.] / Bidgoli, H.. John Wiley & Sons, 2020. Vol. 3. ISBN 9780470051214.

14. *Schlienger, Thomas*. Information security culture : From analysis to change : [англ.] / Thomas Schlienger, Stephanie Teufel // South African Computer Journal. Pretoria, South Africa, 2018. Vol. 31.

15. *Samonas, S.* The CIA Strikes Back : Redefining Confidentiality, Integrity and Availability in Security : [англ.] / Samonas, S., Coss, D. // Journal of Information System Security. Washington DC, USA : Information Institute Publishing, 2021. Vol. 10, no. 3.

16. *Jacques, R. J.* The True Costs of Paper-Based Business : [англ.] // Fulcrum Blog. Spatial Networks, Inc, 2018 13 January. Дата обращения: 27.06.2018.

17. *Pettey, Christy*. Gartner Says Digital Disruptors Are Impacting All Industries; Digital KPIs Are Crucial to Measuring Success : [англ.]. Gartner, Inc., 2017. 2 October. Дата обращения: 27.06.2018.

18. *Forni, Amy Ann, van der Meulen*, *Rob*. *Gartner Survey* Shows 42 Percent of CEOs Have Begun Digital Business Transformation : [англ.]. Gartner, Inc., 2017. 24 April. Дата обращения: 27.06.2018.

19. 2021 Global Information Security Workforce Study : Benchmarking Workforce Capacity and Response to Cyber Risk EMEA : [PDF] : [англ.] // (ISC)². Frost & Sullivan, 2017. Дата обращения: 27.06.2018.

20. Crime in the age of technology : Europol's serious and organized crime threat assessment 2017 : [англ.] : press release. Europol, 2017. 9 March. Дата обращения: 27.06.2018.

METHODOLOGY FOR DEVELOPING A DATABASE INTEGRITY PROGRAM

DIANA EV. VOROBIEVA
JSC "Nevskoye Design Bureau",
St Petersburg, Russia dinvor@mail.ru

ABSTRACT

Introduction: Ensuring the integrity of databases of significant information infrastructure facilities, which, in particular, include the database used in the ship design control system, is one of the main tasks solved in ensuring the protection of critical information infrastructures. **Problem statement**: In the event of an attack by an internal intruder, it is possible to run a debugger or a program tracer along with the DBMS and thus get the opportunity to study the program for its further hacking. There is a problem of blocking such a possibility, but the "thin client" technology is unnecessarily complex and not very effective. Thus, it is necessary to develop a sufficiently simple and functional mechanism for domestic operating systems. **Methods**: methods of synthesis of information security software systems. **Results**: methodology for developing a prototype of a software system for ensuring the integrity of the database. **Practical significance:** ensuring the safe operation of SQL DBMS in the face of previously unknown computer attacks. **Discussion:** the novelty of the proposed task lies in the fact that a mechanism for proactively blocking dangerous impacts on significant objects of critical information infrastructure is proposed.

Keywords: database integrity, protection against insider attacks, software system, blocking dangerous actions

REFERENCES

1. Vorobieva D.E. A system for monitoring the security of technological operations based on a quantum blockchain. //Izvestia of ETU "LETI"2023.№9. Pp. 54-59.
2. Vorobiev E.G., Vorobieva D.E. Safe Functioning of TV and Radio Broadcasting Infrastructure in the Aspect of Influence on the Digital Economy. Information security.Inside. 2023. №1. Pp.2-6.
3. Vorobiev E.G., Vorobieva D.E. Models for assessing cyber stability of transactions in DBMS. // Information security. Inside. 2022. №6. Pp.67-70.
4. Security of critical information infrastructure facilities. General recommendations. Moscow: ARSIB, 2019. 52 p.
5. Petrenko A.S. Quantum-resistant blockchain. St. Petersburg: Piter Publ., 2022. 320 p.
6. Gorban I. I. Phenomenon of Statistical Stability. Moscow: Nauka, 2018. 444 p.
7. Kramarov S.O. Cryptographic Information Protection. Moscow, Rior Publ., 2019. 112 p.
8. Melnikov V.P. Information Protection. Moscow, Akademiya Publ., 2019. 320 p.
9. Baranova E.K. Information Security and Information Protection. Moscow, Rior Publ., 2018. 400 p.
10. Khorev, P.B. Software and hardware information protection. - Moscow, Forum Publ., 2018. 352 p.
11. Parker, Donn B. Fighting Computer Crime : A New Framework for Protecting Information : N. Y. : John Wiley & Sons, 2019. 528 p.
12. Krutz, Ronald L. The CISM Prep Guide : Mastering the Five Domains of Information Security Management : / Ronald L. Krutz, Russell Dean Vines. N. Y. : John Wiley & Sons, 2020. 433 p.
13. McCarthy, C. Digital Libraries : Security and Preservation Considerations // Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management :] / Bidgoli, H.. John Wiley & Sons, 2020. Vol. 3.
14. Schlienger, Thomas. Information security culture : From analysis to change : / Thomas Schlienger, Stephanie Teufel // South African Computer Journal. Pretoria, South Africa, 2018. Vol. 31.
15. Samonas, S. The CIA Strikes Back : Redefining Confidentiality, Integrity and Availability in Security / Samonas, S., Coss, D. // Journal of Information System Security. Washington DC, USA : Information Institute Publishing, 2021. Vol. 10, no. 3.
16. Jacques, R. J. The True Costs of Paper-Based Business // Fulcrum Blog. Spatial Networks, Inc, 2016. 13 January.
17. Pettey, Christy. Gartner Says Digital Disruptors Are Impacting All Industries; Digital KPIs Are Crucial to Measuring Success : Gartner, Inc., 2017. 2 October.
18. Forni, Amy Ann, van der Meulen, Rob. Gartner Survey Shows 42 Percent of CEOs Have Begun Digital Business Transformation : Gartner, Inc., 2017. 24 April.
19. 2017 Global Information Security Workforce Study : Benchmarking Workforce Capacity and Response to Cyber Risk EMEA : [PDF] : // (ISC)². Frost & Sullivan, 2017.
20. Crime in the age of technology : Europol's serious and organised crime threat assessment 2017 : press release. Europol, 2017. 9 March.