НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2023 Том 23 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2023 Vol. 23 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2023-23-6-1247-1250
УДК 621.382

Проблемы защиты содержимого внутренней памяти микроконтроллеров Renesas

Кирилл Константинович Кондрашов[1], Алла Борисовна Левина[2]✉

[1,2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197022, Российская Федерация

[1] kondrashovkk@mail.ru, https://orcid.org/0000-0001-8889-320X
[2] alla_levina@mail.ru✉, https://orcid.org/0000-0003-4421-2411

Аннотация
Рассмотрена проблема защиты информации, содержащейся во внутренней памяти микроконтроллеров семейства Renesas RL78. Выявлена и исследована уязвимость этих микроконтроллеров, позволяющая извлекать данные из встроенной флэш-памяти с использованием программатора. Протестирован способ автоматизированного восстановления содержимого всей области памяти, в основе которого лежит специально разработанное программное обеспечение. Результаты исследования свидетельствуют о недостаточной эффективности реализованных производителем мер ограничения доступа. Описан вариант изменения управляющей команды программатора, ведущий к повышению защищенности данных. Представлена методика полного восстановления данных флэш-памяти, протестированная в программе, разработанной в среде LabVIEW.

Ключевые слова
информационная безопасность, микроконтроллер, Renesas RL78, флэш-память, извлечение данных

Благодарности
Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0014).

Ссылка для цитирования: Кондрашов К.К., Левина А.Б. Проблемы защиты содержимого внутренней памяти микроконтроллеров Renesas // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 6. С. 1247–1250. doi: 10.17586/2226-1494-2023-23-6-1247-1250

Internal memory data protecting problems of the Renesas microcontrollers

Kirill K. Kondrashov[1], Alla B. Levina[2]✉

[1,2] Saint Petersburg Electrotechnical University “LETI”, Saint Petersburg, 197022, Russian Federation

[1] kondrashovkk@mail.ru, https://orcid.org/0000-0001-8889-320X
[2] alla_levina@mail.ru✉, https://orcid.org/0000-0003-4421-2411

Abstract
The problem of protecting the information contained in the internal memory of the Renesas RL78 Family Microcontrollers is considered. The vulnerability of these microcontrollers has been identified and investigated, which allows extracting data from the built-in flash memory using a programmer. A method of automated recovery of the contents of the entire memory area, based on specially developed software, has been tested. The results of the study indicate the insufficient effectiveness of the access restriction measures implemented by the manufacturer. A variant of changing the programmer’s control command, leading to an increase in data security, is described. A technique for complete recovery of flash memory data is presented, tested in a program developed in the LabVIEW environment.

Keywords
information security, MCU, Renesas RL78, flash memory, data extraction

Acknowledgements
The work was supports by the Ministry of Science and Higher Education of the Russian Federation No. 075-01024-21-02 dated 09/29/2021 (project FSEE-2021-0014).

For citation: Kondrashov K.K., Levina A.B. Internal memory data protecting problems of the Renesas microcontrollers. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 6, pp. 1247–1250 (in Russian). doi: 10.17586/2226-1494-2023-23-6-1247-1250

В настоящее время микроконтроллеры общего назначения широко применяются в электронике. Зачастую они обрабатывают информацию конфиденциального характера, например: коды доступа, пароли и ключи шифрования. Данные такого рода, хранящиеся во внутренней памяти, должны надежно защищаться от угроз, связанных с посторонним вмешательством. Предусмотренные производителями способы ограничения доступа к устройствам с целью защиты информации иногда оказывается недостаточными. Эксплуатация конструктивных уязвимостей может оказаться эффективным способом для извлечения данных из внутренней памяти [1]. Особый интерес представляют неинвазивные методы получения информации, при использовании которых сохраняется целостность корпуса и работоспособность устройства. В зависимости от наличия внешнего воздействия на объект эти методы подразделяются на активные и пассивные [2]. Первый тип характеризуется большей гибкостью и в некоторых случаях позволяет открыть доступ к статической памяти при установленной производителем защите. В настоящей работе рассмотрена одна из серьезных проблем безопасности, обнаруженная в микроконтроллерах Renesas, применяемых в бытовой электронике. При исследовании этих микроконтроллеров поставлена задача анализа возможностей восстановления защищаемой информации с использованием только стандартных средств, предназначенных для программирования и отладки, без специализированного дорогостоящего оборудования.

Проблема защиты данных, содержащихся во внутренней памяти микроконтроллеров, является особенно актуальной в условиях широкого распространения электроники во всех сферах жизни. Практически в любых устройствах важно обеспечивать сохранность не только программного кода, заложенного производителем, но и разнообразных пользовательских данных конфиденциального характера. С целью ограничения стороннего доступа к такой информации в микроконтроллерах применяются различные способы защиты памяти.

Можно выделить несколько распространенных типов защиты от извлечения содержимого внутренней памяти при подключении микроконтроллера к программатору: бит секретности; установка пароля; шифрование данных; запрет поддержки операции чтения.

Установка бита секретности обеспечивает высокую степень защиты и является наиболее простым вариантом при технической реализации. Этими факторами обусловлено широкое распространение данного решения в продукции различных фирм-производителей. Несмотря на очевидные достоинства данного способа, исследования [3–5] показали, что защита может быть преодолена с помощью инвазивных и неинвазивных методов. Например, обойти бит секретности помогают манипуляции с напряжением питания некоторых устройств и облучение соответствующей ячейки на кристалле при локальном вскрытии корпуса [6].

Защита с помощью пароля более надежна по сравнению с установкой бита секретности, так как изменить каким-либо образом одновременно много битов или предотвратить обращение системы к ним без нарушения дальнейшего функционирования крайне затруднительно. Для хранения пароля может использоваться как отдельная область памяти, так и особая адресная зона в общем пространстве. В последнем случае в качестве пароля может выступать любая байтовая последовательность, которая изначально предназначена для других функций согласно коду микропрограммы. Такой подход упрощает реализацию защиты при сохранении эффективности и иногда встречается на практике [7].

Применение шифрования данных всей внутренней памяти или наиболее критичной к утечкам ее части является надежным способом защиты исходной информации, если обеспечивается высокая защищенность ключа. Очевидно, что для обработки данных требуется предварительная дешифровка, поэтому микроконтроллеру должен быть известен ключ. Хранение ключа в такой же энергонезависимой памяти на кристалле делает устройство уязвимым к различным методам анализа, в том числе по побочным каналам [8, 9]. В зависимости от алгоритма шифрования можно использовать один из множества способов, чтобы попытаться восстановить исходные данные, но дополнительная сложность возникает из-за большой трудоемкости и длительности процесса.

Невозможность произвести считывание по причине отсутствия поддержки микропроцессором такой операции, на первый взгляд, должна обеспечивать наилучшую защиту из всех возможных. Тем не менее, даже в таких условиях все еще доступно выполнение других операций с внутренней памятью. Как показывает практика, их определенная комбинация тоже может быть неявным способом обхода защиты и полного восстановления данных.

Семейство микроконтроллеров Renesas RL78 включает в себя множество моделей, которым свойственна широкая область применения[1]. Ключевой особенностью всех моделей этого семейства является принципиальное отсутствие возможности считывания содержимого внутренней памяти при подключении к программатору. Загрузка данных из флэш-памяти микроконтроллеров не предусмотрена производителем в целях обеспечения безопасности.

В настоящей работе исследованы 8-битные микроконтроллеры Renesas серии 78K0S[2], архитектура встро-

[1] Renesas RL78 Family Microcontrollers [Электронный ресурс]. Режим доступа: https://www.renesas.com/us/en/document/fly/rl78-family-microcontrollers-brochure, свободный. Яз. англ. (дата обращения: 10.07.2023).

[2] 78K0S/KY1+ 8-Bit Single-Chip Microcontrollers [Электронный ресурс]. Режим доступа: https://www.renesas.com/in/en/document/mah/78k0sky1-users-manual, свободный. Яз. англ. (дата обращения: 10.07.2023).

енной памяти которых аналогична устройствам семейства RL78. Принципиальные отличия нового семейства заключаются в сокращенном наборе команд программирования. Экспериментально выявлено, что микроконтроллеры обладают существенной уязвимостью, которая дает возможность восстанавливать содержимое флэш-памяти. Процедура восстановления основана на циклических операциях записи ячейки и считывания контрольной суммы массива флэш-памяти. Реализация данной методики оказалась возможной из-за того, что в серии 78K0S запись данных флэш-памяти производится побайтно, в отличие от серии 78K0, где запись выполняется блоками по четыре байта[1]. Ключевую роль играют конструктивные и схемотехнические особенности строения массива ячеек, вследствие которых запись нулевого байта (00h) поверх любого другого значения, хранящегося в ячейке, является допустимой и всегда проходит успешно без повреждения данных. Решающим фактором стало то, что расчет контрольной суммы флэш-памяти в серии 78K0S осуществлен побайтно по описанной в документации методике[2].

Обнаруженная уязвимость состоит в изменении одного байта исходного массива, при котором изменяется контрольная сумма. Далее с помощью разработанного обратного алгоритма по известному значению контрольной суммы установлено первоначальное значение перезаписанного байта. При этом восстановление выполнено только по одному байту в инверсном порядке, начиная с адреса последней ячейки памяти. Контрольная сумма данных в устройствах семейства RL78 вычислено по алгоритму циклического избыточного кода (CRC)[3]. Значение CRC с математической точки зрения определено функцией f от набора байтов $b_0, \ldots, b_{N-1}$ для N ячеек памяти:

$$CRC = f(b_0, \ldots, b_{N-1}).$$

После замещения первого байта нулевым значением контрольная сумма массива имеет следующий вид:

$$CRC' = f(0, b_1, \ldots, b_{N-1}).$$

Первоначальное значение перезаписанного байта рассчитано в результате применения обратной функции к массиву, в котором байты $b_1, \ldots, b_{N-1}$ известны:

$$b_0 = f^{-1}(CRC, b_1, \ldots, b_{N-1}).$$

Методика полного восстановления данных флэш-памяти универсальна для любых устройств семейства Renesas RL78. Выделим следующие основные шаги методики.

Шаг 1. Считывание и сохранение контрольной суммы всей флэш-памяти.

Шаг 2. Запись нулевого байта в первую ячейку анализируемого микроконтроллера (с младшим адресом).

Шаг 3. Повторение шагов 1 и 2 для последующих ячеек, до предпоследней.

Шаг 4. Получение массива контрольных сумм, размерность которого равна объему памяти.

Шаг 5. Запуск специализированного программного обеспечения, которое предназначено для восстановления содержимого флэш-памяти по массиву контрольных сумм.

Шаг 6. Получение и сохранение результата.

Предложенная методика протестирована в программе, разработанной в среде LabVIEW. В программу был загружен массив контрольных сумм. Автоматизация вычислений позволила быстро восстановить всю область флэш-памяти микроконтроллера.

Защищенность микроконтроллеров семейства RL78 от доступа к данным флэш-памяти нельзя обеспечить установкой аппаратного запрета на операции записи, что возможно в устройствах других семейств. Обязательное предварительное стирание памяти перед записью, предусмотренное командой загрузки кода, является эффективной защитой от восстановления содержимого с использованием общедоступных средств.

В результате проведенных исследований выявлена уязвимость микроконтроллеров Renesas семейства RL78, позволяющая извлекать информацию из внутренней памяти. Защитные меры в виде отсутствия функции чтения памяти через программатор имеют серьезный вид, но оказываются недостаточными для обеспечения надежности хранения конфиденциальных данных. Относительная простота реализации доступа повышает уровень угрозы постороннего вмешательства. Возможность восстановления данных из всего адресного пространства открывает путь для копирования микропрограммного кода, охраняемого авторскими правами. Предварительное стирание памяти перед записью ограничивает применимость стандартных средств для извлечения информации, что ведет к повышению защищенности.

[1] 78K0/Kx2 8-Bit Single-Chip Microcontrollers Flash Memory Programming [Электронный ресурс]. Режим доступа: https://www.renesas.com/us/en/document/apn/78k0kx2-flash-memory-programming-programmer, свободный. Яз. англ. (дата обращения: 10.07.2023).

[2] 78K0S/Kx1+ 8-Bit Single-Chip Microcontrollers Flash Memory Programming [Электронный ресурс]. Режим доступа: https://www.renesas.com/in/en/document/apn/78k0skx1-flash-memory-programming-programmer, свободный. Яз. англ. (дата обращения: 10.07.2023).

[3] RL78 Microcontroller (RL78 Protocol B) Serial Programming Guide [Электронный ресурс]. Режим доступа: https://www.renesas.com/eu/en/document/apn/rl78-family-rl78-microcontroller-rl78-protocol-b-serial-programming-guide, свободный. Яз. англ. (дата обращения: 10.07.2023).

Литература

1. Tunstall M. Smart card security // Smart Cards, Tokens, Security and Applications. Springer, Cham, 2017. P. 217–251. https://doi.org/10.1007/978-3-319-50500-8_9
2. Spreitzer R., Moonsamy V., Korak T., Mangard S. Systematic classification of side-channel attacks: A case study for mobile devices // IEEE Communications Surveys and Tutorials. 2018. V. 20. N 1. P. 465–488. https://doi.org/10.1109/comst.2017.2779824
3. Кондрашов К.К., Денисов А.К., Лучинин В.В. Неразрушающая методика контроля данных ПЗУ по каналу энергопотребления // Петербургский журнал электроники. 2017. № 2-3. С. 97–102.
4. Skorobogatov S.P. Semi-invasive attacks — A new approach to hardware security analysis / University of Cambridge, Computer Laboratory. 2005. Technical Report No. 630. [Электронный ресурс]. URL: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf, свободный. Яз. англ. (дата обращения: 10.07.2023).
5. Kaur S., Singh B., Kaur H. Stratification of hardware attacks: Side channel attacks and fault injection techniques // SN Computer Science. 2021. V. 2. N 3. P. 183. https://doi.org/10.1007/s42979-021-00562-3
6. Лучинин В.В., Садовая И.М. Информационная безопасность смарт-микросистем и технологий. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2015. 157 с.
7. Семейство микроконтроллеров MSP430. Рекомендации по применению: пер. с англ. М.: Компэл, 2005. 544 с. (Библиотека Компэла)
8. Кондрашов К.К., Ершов М.И., Гасников А.О. Современное состояние диагностики микропроцессорных систем по нетрадиционным побочным каналам // Известия СПбГЭТУ «ЛЭТИ». 2016. № 3. С. 3–9.
9. Alashik K., Efe A. Side channel attack // Gazi University Journal of Science. Part A: Engineering and innovation. 2019. V. 6. N 3. P. 61–73.

References

1. Tunstall M. Smart card security. *Smart Cards, Tokens, Security and Applications*. Springer, Cham, 2017, pp. 217–251. https://doi.org/10.1007/978-3-319-50500-8_9
2. Spreitzer R., Moonsamy V., Korak T., Mangard S. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Communications Surveys and Tutorials*, 2018, vol. 20, no. 1, pp. 465–488. https://doi.org/10.1109/comst.2017.2779824
3. Kondrashov K.K., Denisov A.K., Luchinin V.V. Non-destructive method for ROM data monitoring via the energy consumption channel. *Petersburg Electronics Journal*, 2017, no. 2-3, pp. 97–102. (in Russian)
4. Skorobogatov S.P. *Semi-invasive attacks — A new approach to hardware security analysis*. University of Cambridge, Computer Laboratory. 2005. Technical Report No. 630. Available at: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf. (accessed: 10.07.2023).
5. Kaur S., Singh B., Kaur H. Stratification of hardware attacks: Side channel attacks and fault injection techniques. *SN Computer Science*, 2021, vol. 2, no. 3, pp. 183. https://doi.org/10.1007/s42979-021-00562-3
6. Luchinin V.V., Sadovaia I.M. *Information Security of Smart Microsystems and Technologies*. St. Petersburg, Saint Petersburg Electrotechnical University “LETI” Publ., 2015, 157 p. (in Russian)
7. *MSP430 Family of Microcontrollers*. Usage Tips. Moscow, Kompel, 2005, 544 p. (in Russian)
8. Kondrashov K.K., Ershov M.I., Gasnikov A.O. Side-channel diagnostics for microprocessor devices: current state. *Proceedings of Saint Petersburg Electrotechnical University Journal*, 2016, no. 3, pp. 3–9. (in Russian)
9. Alashik K., Efe A. Side channel attack. *Gazi University Journal of Science. Part A: Engineering and innovation*, 2019, vol. 6, no. 3, pp. 61–73.

Авторы

Кондрашов Кирилл Константинович — младший научный сотрудник, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197022, Российская Федерация, https://orcid.org/0000-0001-8889-320X, kondrashovkk@mail.ru

Левина Алла Борисовна — кандидат физико-математических наук, доцент, доцент, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197022, Российская Федерация, sc 56427692900, https://orcid.org/0000-0003-4421-2411, alla_levina@mail.ru

Authors

Kirill K. Kondrashov — Junior Researcher, Saint Petersburg Electrotechnical University “LETI”, Saint Petersburg, 197022, Russian Federation, https://orcid.org/0000-0001-8889-320X, kondrashovkk@mail.ru

Alla B. Levina — PhD (Physics & Mathematics), Assiciate Professor, Associate Professor, Saint Petersburg Electrotechnical University “LETI”, Saint Petersburg, 197022, Russian Federation, sc 56427692900, https://orcid.org/0000-0003-4421-2411, alla_levina@mail.ru

Статья поступила в редакцию 31.07.2023
Одобрена после рецензирования 19.10.2023
Принята к печати 10.11.2023

Received 31.07.2023
Approved after reviewing 19.10.2023
Accepted 10.11.2023