УДК 004.056.53 Вестник УрФО № 4(50) / 2023, с. 77–88

Хорев А.А., Чумаков А.А.

DOI: 10.14529/secur230408

АНАЛИЗ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, С ИСПОЛЬЗОВАНИЕМ РАДИОМОДУЛЕЙ

Одним из направлений внедрения технологии RFID являются центральные процессоры средств вычислительной техники. Анализ спецификаций радиомодулей, устанавливаемых на подложке центральных процессоров компании Intel®, показал, что они имеют контакты для подключения двух антенн, линии шины SMBus, а также контакты питания и заземления. Память радиомодулей разделяется на два сегмента. Первый блок PIROM, содержит информацию о центральном процессоре (ядра, частота, объём кеш и т.д.). Данный блок памяти невозможно перезаписать. Второй блок EEPROM, является перезаписываемым сегментом памяти неизвестного объёма и неизвестного назначения. Высказано предположение, что данный блок может использоваться для промежуточного хранения перехваченной с СВТ конфиденциальной информации, или размещения специального программного обеспечения, реализующего функции несанкционированного доступа или несанкционированного воздействия на ЦП или СВТ. Рассмотрены два сценария атаки на СВТ при помощи радиомодуля. Первый основан на использовании для атаки шины SMBus и предполагает физический доступ злоумышленника к СВТ. Второй способ основан на удаленном управлении центральным процессором и устройствами СВТ с помощью радиомодуля по радиоканалу с использованием технологии Anti-Theft.

Ключевые слова: *средство вычислительной техники, центральный процессор, радиомодуль, RFID технологии, угрозы безопасности информации, несанкционированный доступ.*

ANALYSIS OF THE POSSIBILITY OF IMPLEMENTING THREATS TO THE SECURITY OF INFORMATION PROCESSED BY COMPUTER TECHNOLOGY USING RADIO MODULES

One of the directions of implementation of RFID technology is the central processors of computer equipment. An analysis of the specifications of the radio modules installed on the substrate of Intel ® central processors showed that they have contacts for connecting two antennas, SMBus bus lines, as well as power and ground contacts. The memory of radio modules is divided into two segments. The first PIROM block contains information about the central processor (cores, frequency, cache size, etc.). This memory block cannot be overwritten. The second EEPROM block is a rewritable memory segment of unknown size and unknown purpose. It is suggested that this block can be used for intermediate storage of confidential information intercepted from the electronic computer, or for the placement of special software that implements the functions of unauthorized access or unauthorized impact on the CPU or electronic computer. Two scenarios of an attack on electronic computer using a radio module are considered. The first one is based on the use of the SMBus bus for an attack and assumes the attacker's physical access to the electronic computer. The second method is based on remote control of the central processor and electronic computer devices using a radio module over a radio channel using Anti-Theft technology.

Keywords: *computer hardware, central processing unit, radio module, RFID technology, information security threats, unauthorized access.*

1. Принципы работы технологии RFID

Для идентификации объектов используется несколько технологий, к одной из которых относится радиочастотная идентификация (Radio Frequency Identification, далее – RFID) [1].

Известно, что любая RFID система состоит из радиомодуля и считывателя. Радиомодуль иногда называют радиометкой или радиотранспондером.

Считыватель, представляющий собой приемо-передающее устройство, генерирует радиосигнал, который наводится в антенне радиомодуля. Наведенный сигнал «выпрямляется» и используется для питания радиомодуля, что позволяет организовать обмен данными между считывателем и радиомодулем (рис. 1 [2]).

В зависимости от назначения RFID системы, используемые в ней радиомодули можно классифицировать по следующим параметрам: диапазону рабочих частот, типу источника питания и используемой памяти.

По используемому диапазону частот радиомодули подразделяются на низкочастотные, высокочастотные, ультравысокочастотные и микроволновые радиомодули [3], [4].

Низкочастотные радиомодули (LF) работают в диапазонах частот 125 – 134,2 кГц и 140 – 148,5 кГц. Они характеризуются низкой скоростью передачи данных и малой дальностью действия (до 0,15 м) [4].

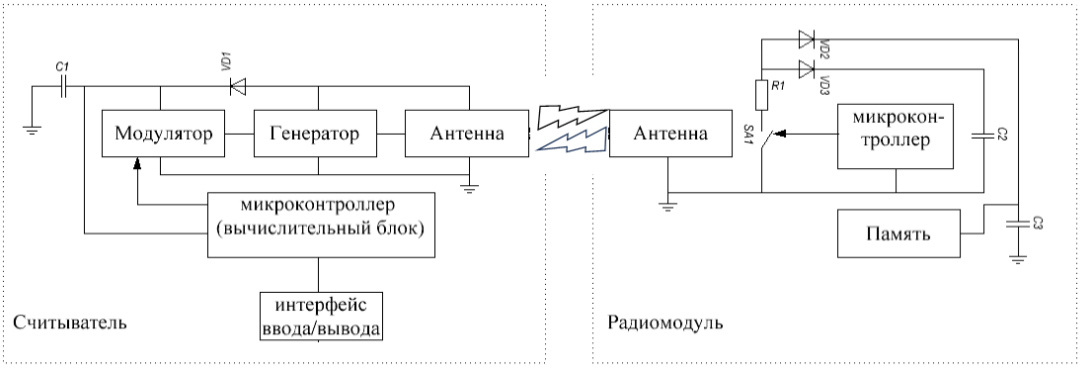


Рис. 1. Принцип работы технологии RFID

Высокочастотные радиомодули (HF) работают на частоте 13,56 МГц. Они характеризуются более высокими скоростями передачи данных и работают на дальностях от 0,8 до 1,5 м [4].

В низкочастотных и высокочастотных модулях в качестве антенн наиболее часто используются катушки индуктивности.

Ультравысокочастотные радиомодули (UHF) работают в диапазоне частот 433, 860 – 960 МГц [5]. Эти системы имеют одну из самых высоких скоростей передачи данных и дальность действия. В качестве антенн в радиомодулях используются диполи [3], [4].

Микроволновые радиомодули (SHF) работают в диапазоне частот 2,45 – 5,8 ГГц. Эти системы строятся в основном на компонентах, имеющих нелинейные характеристики (диоды, варикапы).

В России ограничения на использование низкочастотных и высокочастотных радиомодулей не вводятся. Разрешено использование ультравысокочастотных радиомодулей, работающих в полосах радиочастот 433 МГц, 864 – 865 МГц, 866 – 868 МГц, 868,7 – 869,2 МГц с максимальной эффективной мощностью излучения 25 мВт [5], [7].

Частотный диапазон 2,45 – 5,8 ГГц для RFID на территории РФ не выделен [6].

Ультравысокочастотные радиомодули имеют обширный перечень поддерживаемых и разрабатываемых протоколов и стандартов, как, например, разработанный организацией EPCglobal (Electronic Product Code™) и адаптированный для РФ ГОСТ Р 58701-2019 (ИСО/МЭК 18000-63:2015) «Информационные технологии. Идентификация радиочастотная для управления предметами. Параметры радиоинтерфейса для связи в диапазоне частот от 860 МГц до 960 МГц Тип С» [3], [8], [9].

По типу питания радиомодули подразделяют на: пассивные, полуактивные и активные [10].

В пассивных радиомодулях нет встроенного источника питания. Они работают за счёт электрического тока, индуцированного в антенне электромагнитным излучением считывателя. Они имеют малые размеры и практически неограниченный срок службы. К недостаткам пассивных радиомодулей можно отнести малую дальность действия и низкое качество передаваемого сигнала [10].

Полуактивные радиомодули имеют маломощный источник питания, например, конденсатор, заряжаемый электрическим током, индуцированным в антенне электромагнитным излучением считывателя. Дальность их действия несколько больше, чем пассивных радиомодулей [10].

Активные радиомодули имеют встроенный источник питания и микроконтроллер, позволяющий обеспечить самую стабильную передачу информации на значительных расстояниях. Сроком работы таких модулей ограничен сроком работы встроенной аккумуляторной батареи [10].

Применяемые подходы к использованию памяти радиомодулей [10]:

RO (Read Only) – однократная запись (чаще всего аппаратная), произведённая на заводе-изготовителе. Такие радиомодули используются исключительно для идентификации (отправки идентификатора). Новую информацию в них записать невозможно.

WORM (Write Once Read Many) – модуль кроме идентификатора содержат блок памяти, подверженного однократной записи, и многократному считыванию.

RW (Read and Write) – блок памяти для многократного чтения/записи информации.

В настоящее время технологии RFID стали использоваться не только для идентифика-

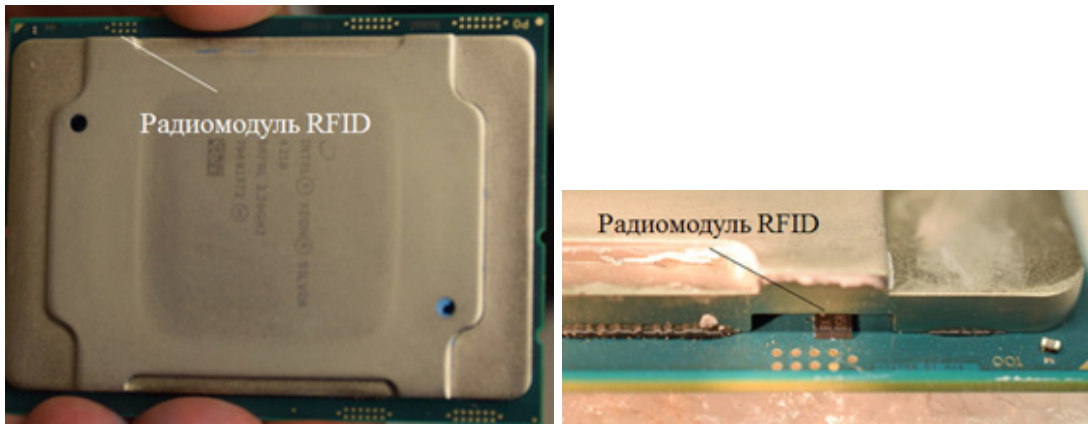
ции объектов, но и управления и контроля доступом, осуществления бесконтактных платежей путём эмулирования физических карт пользователей, оплаты проезда в общественном транспорте и т.д. [1], [11].

2. Анализ радиомодулей, работающих на базе технологии RFID, интегрированных на подложку центральных процессоров средств вычислительной техники

Одним из направлений внедрения технологии RFID являются центральные процессоры (далее – ЦП) средств вычислительной техники (далее – СВТ) [12].

Например, на подложке ЦП компании Intel® устанавливаются радиомодули, находящиеся на шине System Management Bus (далее – SMBus) [13]. Ниже представлены снимки серверного процессора Intel® xeon® silver 4210, на которых виден радиомодуль (рис. 2). Радиомодуль размещается под теплораспределительную крышку ЦП в труднодоступном для визуального обнаружения месте. На снимке ЦП Intel® Core® i9-7940X радиомодуль расположен в правом верхнем углу процессора (рис. 3).

SMBus – это последовательный протокол



а) б)

Рис. 2. Процессор Intel® xeon® silver 4210: а) вид сверху; б) вид сбоку

Рис. 3. Процессор Intel® Core® i9-7940X и интегрированный радиомодуль

обмена данными, предложенный компанией Intel®. Он является подмножеством протокола I2C, но в нем использует более низкий уровень напряжения (3.3В). Протокол используется для обмена данными с устройствами питания и внутренними устройствами СВТ. Шина, использующая данный протокол, имеет одноимённое название и является составной частью системной (главной) шины СВТ. Радиомодули, размещаемые в ЦП компании Intel®, имеют контакты для подключения к шине SMBus [13], [14]. Схематично схема связи RFID с устройства СВТ через системную шину приведена рис. 4.

По данным компании Intel®, представленным авторам:

– радиомодули устанавливаются на всех процессорах серверов и рабочих станций (включая серию X) и используются для логистических нужд; [15]

– по умолчанию радиомодуль отключен и не может быть включен без специального программного обеспечения;

– радиомодуль не влияет и не воздей-

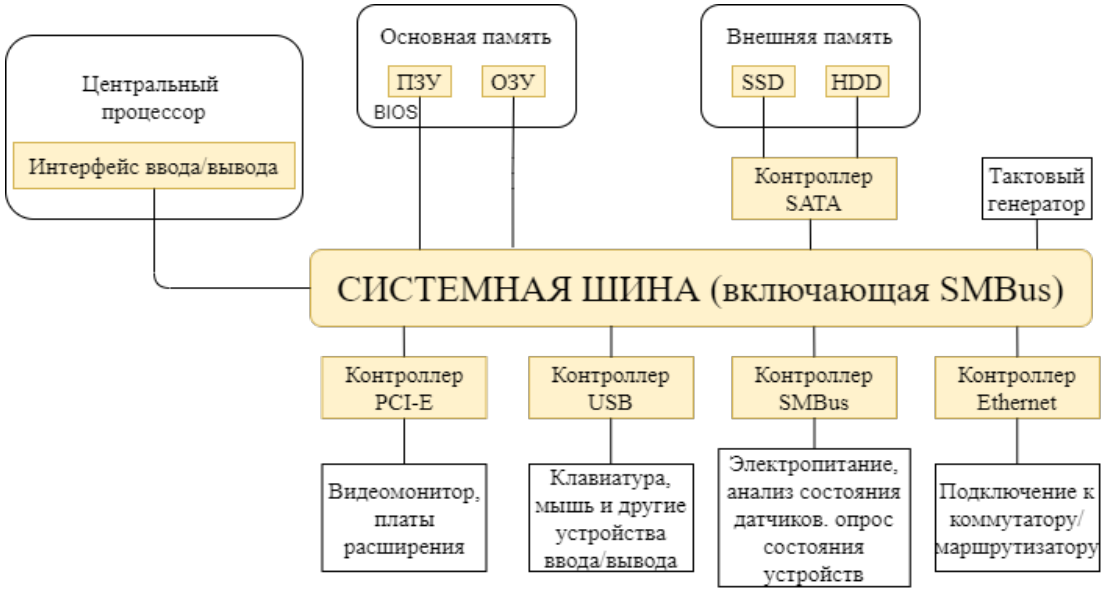


Рис. 4. Схема связи RFID с устройства СВТ через системную шину, включающую SMBus

ствует процессор и не оказывает никакого влияния на его производительность или работу;

– процессор разработан и предназначен для использования с радиомодулем. Наличие радиомодуля проверяет при загрузке, а затем он отключается. Не рекомендуется удалять радиомодуль, без него процессор работать не будет.

Если радиомодуль не влияет на работу процессора, то почему компания Intel® не может гарантировать возможность функционирования СВТ без радиомодуля?

В доступной литературе отсутствует описание радиомодулей, установленных на центральных процессорах.

Путём анализа снимков процессоров компании было обнаружено, что радиомодуль интегрируется с 1998 года преимущественно в серверные решения Intel®, однако намечается тенденция на интеграцию радиомодулей в ЦП, используемые в персональных компьютерах.

Для выяснения целей внедрения и характеристик радиомодулей в ЦП СВТ проведён анализ трёх спецификаций серверных процессоров Intel® Xeon® Processor, в которых имеется упоминание о радиомодулях RFID [15].

Первая спецификация от апреля 2011 года посвящена процессорам Intel® Xeon® Processor E7-8800/4800/2800 на микроархитектуре Westmere [16]. Вторая спецификация от февраля 2014 года посвящена процессорам Intel® Xeon® Processor E7-8800/4800/2800 v2 на микроархитектуре Ivy Bridge [17]. Третья спецификация от апреля 2019 года посвящена масштабируемым процессор Intel® Xeon® второго поколения [18].

Из первой спецификации удалось найти данные об используемом радиомодуле. В соответствие с приведённым в 5-м разделе спецификации было установлено, что данная микросхема, используемая в серверных процессорах, имеет называние PIROM (Processor Information ROM). Далее указано: PIROM – запоминающее устройство, расположенное на процессоре и доступное через шину управления системой SMBus, которое содержит информацию о функциях процессора. Это устройство используется совместно с Scratch EEPROM, программируется во время производства и защищено от записи.

PIROM предназначено для предоставления информации о процессоре. При воздействии на радиомодуль по шине SMBus или по каналу RFID партнёрам компании Intel® предоставляется исчерпывающая информация о ЦП СВТ. Перечень выводимых данных представлен в таблице 5.1 спецификации на ЦП [16]. Из спецификации следует, что данные в PIROM защищены от перезаписи с целью исключения их преднамеренных или случайных изменений. Способы обеспечения защиты данных не указаны.

EEPROM – перезаписываемая программируемая память. Ее описание и цели использования в спецификации не отражены. PIROM использует лишь малую часть всей памяти радиомодуля, поэтому можно предположить,

что компания Intel® оставшуюся память помечает как EEPROM и использует для своих собственных нужд, поэтому и предусмотрена защита от записи.

Так как EEPROM и PIROM являются составляющими блоками общей памяти радиомодуля, то можно утверждать, что через шину SMBus/I2C имеется прямой доступ к системной шине [16].

Далее были определены контакты, подходящие к EEPROM, и их назначение. Сигналы SMBDAT (SDA), SMBCLK(SCL) и SM_WP(WP) относятся к шине SMBus. VCC33 напряжение 3.3. В используется для питания микросхемы и SMBus. SKTID [2:0] (A [2:0]) необходимы для получения данных из PIROM о ЦП. Предположительно, контакты для подключения антенн. GND – заземляющий вывод [16].

Шина SMBus в связке с блоком PIROM радиомодуля используется ЦП для получения сервисной информации (число ядер, тип сокета, диапазона рабочих частот, напряжения питания, для обозначения наборов, поддерживаемых процессором инструкций и т.д.) [16]. В спецификации описано на каких адресах находится эта информация [16].

Анализ двух других спецификаций показал, что информация, касающаяся радиомодуля, идентична. Незначительный отличия встречаются при описании адресов PIROM. Главное отличие спецификаций 2019 и 2014 годов от спецификации 2011 года в том, что информация, описывающая структуру и назначение радимодуля, была значительно сокращена. Так, например, пропала функциональная схема подключения радиомодуля к ЦП, а также удалено описание зарезервированных адресов в PIROM [16] – [18]. Данное действие компании можно расценивать, как стремление скрыть назначение и принцип функционирования радиомодуля.

Вероятно, необнародованные данные о радиомодуле могут описывать алгоритм взаимодействия, позволяющий передавать любые данные, хранимые и обрабатываемые процессором, заинтересованным в этих данных лицам, а также управлять поведением радиомодуля вплоть до сокрытия факта наличия радиомодуля на системной шине SMBus от любого пользователя СВТ.

Таким образом, в ходе анализа спецификаций ЦП компании Intel® возник следующий вопрос: зачем для логистических нужд создавать данный модуль в виде отдельной микросхемы и помещать его на системную шину SMBus?

Использование данных радиомодулей для ведения складской логистики кажется неубедительным. Известны UHF метки, которые могут быть выполнены в виде миниатюрной наклейки и установлены на упаковку [19]. Это значительно выгоднее, чем интегрировать отдельно создаваемый модуль на подложку ЦП.

Не ясна также цель создания и применения в радиомодуле отдельного блока с перезаписываемой памятью. Информацию по данному вопросу не удалось найти ни в указанных выше спецификациях, ни в открытых источниках.

Компания Intel® не описывает, как осуществляется механизм считывания данных с радиомодуля, и какова цель его размещения на шину SMBus. Можно предположить, что использование радиомодуля в виде отдельной микросхемы необходимо для создания дополнительных возможностей управления ЦП, в том числе и реализации угроз безопасности информации, обрабатываемой СВТ.

3. Анализ способов несанкционированного доступа к информации, обрабатываемой на СВТ, с использования интегрированных в центральный процессор радиомодулей

Радиомодуль, интегрируемый в ЦП компании Intel®, производит взаимодействие с элементами СВТ путём обмена данных по шине SMBus. Так как SMBus является подмножеством шины I2C, то сказанное ниже к шине I2C будет иметь равное отношение к шине SMBus.

Ввиду наличия уникального алгоритма общения с радиомодулем, поддержка работы со стандартными устройствами шины I2C (мастер-устройствами) не возможна. Стоит учитывать, что мастер устройство шины I2C представляет из себя микросхему, являющуюся частью чипсета (набор микросхем, объединённых одним кристаллом). Ввиду того, что чипсет и ЦП производит и разрабатывает Intel®, то можно утверждать, что в программу управления контроллера шины I2C заведомо интегрирован алгоритм взаимодействия с радиомодулями.

Проведенный анализ показал, что возможны следующие угрозы безопасности информации, обрабатываемой СВТ, с использованием шины SMBus/I2C и радиомодуля:

1. **Осуществление анализа (перехват) данных между устройствами шины I2C и арбитром (мастером) шины.** В роли

устройств помимо радиомодуля могут выступать также извещатели, микросхемы памяти, аналого-цифровые преобразователи (далее – АЦП), цифро-аналоговые преобразователи (далее – ЦАП) и т.п., а также микроконтроллеры устройств или ЦП. В схеме подключения I2C/SMBus используется одно мастер-устройство (арбитр шины) и множество подключенных к нему по общей шине подчинённых устройств (slave).

При подключении логического анализатора к контактам шины I2C/SMBus можно произвести накопление данных, которые циркулируют по шине, для последующего анализа. Подключение к шине можно осуществить через любое устройство I2C, подключённое к ней, следить за поведением устройств и выявить наличие радиомодуля. Зная алгоритм взаимодействия радиомодуля с мастер-устройством, можно осуществить несанкционированное копирование конфиденциальной информации. В EEPROM может содержаться конфиденциальная информация, ключей, журналов и т. д., которые ЦП разместил туда для возможного хранения. Протокол SMBus способен обеспечивать обмен данными до 3 уровня модели OSI включительно. Следовательно, злоумышленник может подключиться как на прямую к контактам шины I2C/SMBus, так и через сеть, если сетевая карта имеет поддержку работы с протоколом I2C/SMBus и может быть обнаружена в сети [14].

Также перехватить данные можно путём воздействия на контроллер шины (позволяет опередить мастера, если их в системе несколько), который находится в чипсете (набор микросхем) СВТ. Чипсет разрабатывается компанией Intel®, следовательно, путём воздействия на контроллер шины при помощи проприетарных программных инструментов партнёры компании могут получить доступ к любым данным, которые циркулируют на шине I2C/SMBus.

2. **Анализ и последующее изменение данных в контроллерах, буферах и микросхемах памяти устройств, подключенных к шине I2C.** Если данные на устройстве не защищены, злоумышленник может их модифицировать (изменить). Изменение данных в названных сегментах СВТ может привести к повреждению системы или выводу её из строя. Например, путём воздействия через шину PMBus (шина управления питанием – подмножество шины I2C) можно изменить конфигурационные данные питающих узлов серверов, что может привести к ситуациям, когда поведение системы может быть непредсказуемым. Нестабильное питание ЦП и контроллеров устройств может вызывать сбой в работе встроенных программных и аппаратных алгоритмов защиты, ввиду выхода оборудования и устройств за пределы допустимых диапазонов питающих напряжений. Имеются данные, что пониженное напряжение питания ЦП приводит к сбою аппаратной защиты, что позволяет злоумышленнику получить доступ ко всем блокам памяти ЦП [20].

3. Подключенное к шине I2C/SMBus устройство, к которому злоумышленник получил доступ, может быть использовано для воздействия на тактовый генератор шины с целью вызова в нём сбоя. Изменяя частоту тактирования при передаче сигналов между конкретным устройством (радиомодулем) и мастером можно вызвать сбои и задержки в передаче данных и в последующем осуществить несанкционированный доступа (НСД) к информации, содержащейся в радиомодуле [21].

Можно предположить следующий сценарий атаки на СВТ при помощи радиомодуля и его шины SMBus:

При непосредственном доступе к СВТ необходимо установить микросхемы, имеющих подключение к I2C или отвечающих за их функционирование, и определить контакты подключения на плате СВТ.

Далее осуществляется подключение к шине и перехват сигналов, передаваемых по шине, с последующим сравнением их с известными (штатными устройствами, подключаемыми к шине). При наличии логического анализатора или специально разработанных программ можно осуществить накопление и анализ всех данных, передаваемых по шине. Логический анализатор способен отображать сигналы на линиях SDA и SCL шины I2C/SMBus.

Далее при помощи декодирования и сравнения сигналов согласно временной диаграмме протокола можно получить информацию о том, к какому адресу (устройству) происходит обращение и какие данные передаются на шине.

В случае, если методом сравнения полученных результатов не удалось описать адрес или данные на шине, необходимо при помощи устройства, которое способно выполнять функции мастер-устройства, подключиться к шине и осуществить попытку воздействия на

данный адрес и инициировать выгрузку всех данных устройства, которые содержит устройство по данному адресу.

Для доступа напрямую к конкретному устройству или блоку памяти необходимо описание алгоритма работы с ним, прописанного в его техническом описании. Имея информацию о том, как устройство взаимодействует с шиной, злоумышленник способен написать программу, реализующую алгоритм взаимодействия с устройством или микросхемой.

Устройство взаимодействия, содержащее в себе программу взаимодействия с анализируемым (атакуемым) устройством или микросхемой, можно подсоединить напрямую к шине или подсоединиться специальной контактной клипсой к самой микросхеме. В случаях отсутствия возможности подключения возможно отпаивание микросхемы и подключение напрямую к её выходам I2C для дальнейшего взаимодействия с блоками памяти.

Таким образом, для осуществления несанкционированного доступа к СВТ при помощи радиомодуля злоумышленнику необходимо непосредственное подключение к шине SMBus. Однако в случае, если злоумышленником выступает разработчик аппаратной платформы, которым может являться компания Intel®, необходимость в использовании описанного алгоритма отпадает. Ввиду наличия контроля за устройством управления злоумышленник в лице разработчика может получить любые данные из любого подключенного к шине устройства и передать его любым возможным способом за пределы СВТ.

С помощью радиомодуля теоретически можно организовать удалённое управление устройствами СВТ. По информации из открытых источников в 2012 году Intel® внедрила в свои ЦП технологию, позволяющую удалённо при помощи RFID отключать и дистанционно управлять ЦП, даже если компьютер не подключен к Интернету или не включен. Данной технологии было дано название Anti-Theft 3.0 [22]. Сделано это было по заявлению компании для осуществления невозможности работы ПК в случае его кражи.

Таким образом, можно предположить, что данная технология уже внедрена в радиомодуль и позволяет удалённо при помощи радиоканала RFID управлять и отключать аппаратно-связанные с ним ЦП или устройства СВТ (искажать прошивки по шине I2C).

Реализация такой функции позволит не только отслеживать перемещение СВТ, даже когда он не подключен к сети или питанию, но и ставит под угрозу безопасность данных, обрабатываемых СВТ. Нет гарантий, что злоумышленник не воспользуется данным каналом и не перехватит информацию, передаваемую по радиоканалу, или не выведет ЦП или СВТ из строя.

Не так давно появилась информация об атаках с использованием уязвимостей типа Sprectre [23] и Meltdown [24]. Способы их закрытия не гарантируют абсолютной безопасности. Существуют риски совместного использования данных уязвимостей вместе с интегрированным радиомодулем.

Вредоносный код, использующий данные уязвимости, может внедрятся через радиоканал в пользовательскую память радиомодуля, и в последующем отправляться в оперативную память СВТ или же напрямую в кэш-память ЦП. Ввиду того, что радиомодуль по SMBus напрямую связан с процессором, а также имеет доступ к оперативной памяти, риск очевиден. В дальнейшем код может, например, эксплуатируя уязвимость Spectre, изъять из памяти СВТ конфиденциальные данные такие, как пароли аутентификации, банковские пароли и т.д. В последующем достаточно лишь выгрузить их обратно в пользовательскую память радиомодуля и считать их по RFID.

Даже если атаки типа Spectre и Meltdown, использующие уязвимость «спекулятивного» выполнения команд и развитого предсказания ветвлений, удастся закрыть, то это не решит обозначенных выше проблем. В апреле 2021 года была опубликована статья исследователей из инженерной школы Университета Вирджинии, в которой говорится о том, что была обнаружена линия атаки, которая ломает всю защиту от уязвимости Spectre [25].

Таким образом, осуществление несанкционированного доступа к конфиденциальным данным при помощи радиомодуля и эксплуатации уязвимостей Spectre и Meltdown представляют серьёзный риск неконтролируемой утечки этих данных по специально создаваемому радиоканалу или системной шине SMBus.

Ввиду связи через шину SMBus со всеми периферийными устройствами СВТ, может существовать возможность получения не только информации из оперативной памяти,

кэш-памяти процессора, но также из буферов периферийных устройств и т.д. Следовательно, злоумышленник теоретически может удалённо перехватить конфиденциальные данные пользователей, содержащиеся в потенциально уязвимых частях памяти, среди которых могут быть информация об идентификаторах пользователей, сведения, позволяющие осуществить аутентификацию от их лица, конфиденциальные документы, файлы и т.д.

В виду того, что устройства на шине могут обмениваться данными при отсутствующем питании, появляется возможность доступа к узлам СВТ без запуска операционной системы СВТ. Это создаёт возможность управления шиной и подключенными к ней устройствами в обход установленной на СВТ операционной системы. Единственное, что необходимо – это наличие питания 3.3 В на материнской плате, являющегося дежурным, либо радиомодуль может получать питание от считывателя RFID. Ввиду того, что радиомодуль никак не отображается в операционной системе, контроль над устройством происходит на аппаратном уровне самим процессором или с помощью микрокоманд, отправляемых мастером шины SMBus.

Заключение

Одним из направлений внедрения технологии RFID являются центральные процессоры средств вычислительной техники.

Анализ спецификаций радиомодулей, устанавливаемых подложке центральных процессоров компании Intel®, показал, что они имеют контакты для подключения двух антенн, линии шины SMBus, а также контакты питания и заземления. Память радиомодулей разделяется на два сегмента. Первый блок PIROM, содержит информацию о центральном процессоре (ядра, частота, объём кеш и т.д.). Данный блок памяти невозможно перезаписать. Второй блок EEPROM, является перезаписываемым сегментом памяти неизвестного объёма и неизвестного назначения. Высказано предположение, что данный блок может использоваться для промежуточного хранения перехваченной с СВТ конфиденциальной информации, или размещения специального программного обеспечения, реализующего функции несанкционированного доступа или несанкционированного воздействия на ЦП или СВТ.

Рассмотрены два сценария атаки на СВТ при помощи радиомодуля.

Первый сценарий основан на использовании для атаки шины SMBus и предполагает физический доступ злоумышленника к СВТ. Однако в случае, если злоумышленником выступает разработчик аппаратной платформы, которым может являться компания Intel®, необходимость в физическом доступе к СВТ злоумышленника отпадает.

Второй сценарий основан на удаленном управлении центральным процессором и устройствами СВТ с помощью радиомодуля по радиоканалу с использованием технологии Anti-Theft.

Таким образом, с использованием радиомодулей, установленных на центральном процессоре, возможно не только отслеживать перемещение СВТ, даже когда он не подключен к сети или питанию, но и осуществлять перехват данных, обрабатываемых СВТ, и управлять центральным процессором или отключать аппаратно-связанные с центральным процессором устройства СВТ.

Направлениями дальнейших исследований является создание лабораторного стенда, позволяющего моделировать и исследовать угрозы безопасности информации, реализуемые с использованием радиомодулей, установленных на центральном процессоре.

Литература

1. Применения RFID // Wikipedia. URL: https://clck.ru/Tzote (дата обращения: 07.12.2023).

2. RFID-Technology // SMART-TEC URL: https://www.smart-tec.com/en/auto-id-world/rfid-technology (дата обращения: 27.03.2023).

3. ГОСТ Р 58701-2019 (ИСО/МЭК 18000-63:2015) Информационные технологии (ИТ). Идентификация радиочастотная для управления предметами. Параметры радиоинтерфейса для связи в диапазоне частот от 860 МГц до 960 МГц (Тип С). – Москва: Стандартинформ, 2020.

4. RFID-Technology // SMART-TEC URL: https://www.smart-tec.com/en/auto-id-world/rfid-technology (дата обращения: 27.03.2023).

5. ГОСТ Р ИСО 17363-2010 Применение радиочастотной идентификации (RFID) в цепи поставок. Контейнеры грузовые, М.: Стандартинформ, 2019 год, ¬¬ 20 с.

6. Какие частоты разрешены для RFID. — Текст: электронный // rfctest: [сайт]. — URL: https://rfctest.ru/stati/kakie-chastoty-razresheny-dlya-rfid/ (дата обращения: 18.12.2023).

7. Заседание ГКРЧ от 07.05.2007 (протокол № 07-20) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

8. UHF RFID PROTOCOLS AND STANDARTS. — Текст: электронный // TraceID: [сайт]. — URL: https://www.trace-id.com/protocols-and-standards-of-uhf-rfid/ (дата обращения: 24.03.2023).

9. EPCglobal. — Текст: электронный // gs1: [сайт]. — URL: https://www.gs1.org/epcglobal (дата обращения: 24.03.2023).

10. RFID // Wikipedia. URL: https://ru.wikipedia.org/wiki/RFID (дата обращения: 27.03.2023).

11. FAQ RFID: от описаний к фактическим применениям // Gaw.ru URL: http://www.gaw.ru/html.cgi/txt/publ/other/rfid.htm (дата обращения: 27.03.2023).

12. Jean, Elyan Avec le RFID, Intel veut mieux recenser le matériel des datacenters / Elyan Jean. — Текст: электронный // Le Monde Informatique: [сайт]. — URL: https://www.lemondeinformatique.fr/actualites/lire-avec-le-rfid-intel-veut-mieux-recenser-le-materiel-des-datacenters-61331.html (дата обращения: 07.12.2023).

13. RFID-Tag im Intel Core X-Prozessor // HEISE ONLINE. URL: https://www.heise.de/newsticker/meldung/RFID-Tag-im-Intel-Core-X-Prozessor-3730254.html (дата обращения: 07.12.2023).

14. System Management Bus (SMBus) Specification, 2018. System Management Interface Forum, Inc., pp: 85.

15. Под крышкой процессоров Intel Core i9 скрывается микросхема NFC либо RFID // ixbt. URL: https://www.ixbt.com/news/2017/06/05/intel-core-i9-nfc-rfid.html (дата обращения: 07.12.2023).

16. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 Product Families. Datasheet Volume 1 of 2. - Reference Number: 325119-001 изд. INTEL®, April 2011. - 174 с.

17. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 v2 Product Family Datasheet - Volume One Electrical, Mechanical and Thermal Specifications - Volume 1 of 3. - Reference Number: 329594-001 изд. INTEL®, February 2014. - 190 с.

18. INTEL® Second Generation Intel® Xeon® Scalable Processor. Datasheet, Volume One: Electrical. - Reference Number: 338845-001US изд. INTEL®, April 2019. - 134 с.

19. UHF RFID метка на фары автомобиля ZKTeco UHF Waterproof Tag (самоклеящаяся). — Текст: электронный // Системы безопасности US-PLAST: [сайт]. — URL: https://us-plast.ru/product/new-uhf-waterproof-tag/ (дата обращения: 07.12.2023).

20. В массовых процессорах AMD нашлась «дыра», которую невозможно закрыть. В опасности все пользователи. — Текст: электронный // CNews: [сайт]. — URL: https://www.cnews.ru/news/top/2023-05-03_v_narodnyh_protsessorah (дата обращения: 07.12.2023).

21. Hardware Attacks on Mobile Robots: I2C Clock Attacking / Jiménez-Naharro Raúl, G. *. Fernando, Medina-García Jonathan, Sánchez-Raya,and,Juan,Antonio Manuel. — Текст: непосредственный // Robot 2015: Second Iberian Robotics Conference. — 2016. — С. 147-159.

22. Intel Developing RFID Tracking and Remote Controlled 'Kill Switch' for Laptops // The hacker news. URL: https://thehackernews.com/2014/06/intel-developing-rfid-tracking-and.html (дата обращения: 07.12.2023).

23. Spectre (уязвимость)// Википедия. Свободная энциклопедия URL: https://ru.wikipedia.org/wiki/Spectre_(уязвимость) (дата обращения: 07.12.2023).

24. Meltdown (уязвимость)// Википедия. Свободная энциклопедия URL: https://ru.wikipedia.org/wiki/ Meltdown_(уязвимость) (дата обращения: 07.12.2023).

25. X. Ren, L. Moody, M. Taram, M. Jordan, D. M. Tullsen, A. Venkat, «I See Dead μops: Leaking Secrets via Intel/AMD Micro-Op Caches». URL: https://www.cs.virginia.edu/venkat/papers/isca2021a.pdf (дата обращения: 24.12.2023).

References

1. Primeneniya RFID // Wikipedia. URL: https://clck.ru/Tzote (data obrashcheniya: 07.12.2023).

2. RFID-Technology // SMART-TEC URL: https://www.smart-tec.com/en/auto-id-world/rfid-technology (data obrashcheniya: 27.03.2023).

3. GOST R 58701-2019 (ISO/MEK 18000-63:2015) Informatsionnyye tekhnologii (IT). Identifikatsiya radiochastotnaya dlya upravleniya predmetami. Parametry radiointerfeysa dlya svyazi v diapazone chastot ot 860 MGts do 960 MGts (Tip S). – Moskva: Standartinform, 2020.

4. RFID-Technology // SMART-TEC URL: https://www.smart-tec.com/en/auto-id-world/rfid-technology (data obrashcheniya: 27.03.2023).

5. GOST R ISO 17363-2010 Primeneniye radiochastotnoy identifikatsii (RFID) v tsepi postavok. Konteynery gruzovyye, M.: Standartinform, 2019 god, ¬¬ 20 c.

6. Kakiye chastoty razresheny dlya RFID. — Tekst: elektronnyy // rfctest: [sayt]. — URL: https://rfctest.ru/stati/kakie-chastoty-razresheny-dlya-rfid/ (data obrashcheniya: 18.12.2023).

7. Zasedaniye GKRCH ot 07.05.2007 (protokol № 07-20) // Ministerstvo tsifrovogo razvitiya, svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii.

8. UHF RFID PROTOCOLS AND STANDARTS. — Tekst: elektronnyy // TraceID: [sayt]. — URL: https://www.trace-id.com/protocols-and-standards-of-uhf-rfid/ (data obrashcheniya: 24.03.2023).

9. EPCglobal. — Tekst: elektronnyy // gs1: [sayt]. — URL: https://www.gs1.org/epcglobal (data obrashcheniya: 24.03.2023).

10. RFID // Wikipedia. URL: https://ru.wikipedia.org/wiki/RFID (data obrashcheniya: 27.03.2023).

11. FAQ RFID: ot opisaniy k fakticheskim primeneniyam // Gaw.ru URL: http://www.gaw.ru/html.cgi/txt/publ/other/rfid.htm (data obrashcheniya: 27.03.2023).

12. Jean, Elyan Avec le RFID, Intel veut mieux recenser le matériel des datacenters / Elyan Jean. — Tekst: elektronnyy // Le Monde Informatique: [sayt]. — URL: https://www.lemondeinformatique.fr/actualites/lire-avec-le-rfid-intel-veut-mieux-recenser-le-materiel-des-datacenters-61331.html (data obrashcheniya: 07.12.2023).

13. RFID-Tag im Intel Core X-Prozessor // HEISE ONLINE. URL: https://www.heise.de/newsticker/meldung/RFID-Tag-im-Intel-Core-X-Prozessor-3730254.html (data obrashcheniya: 07.12.2023).

14. System Management Bus (SMBus) Specification, 2018. System Management Interface Forum, Inc., pp: 85.

15. Pod kryshkoy protsessorov Intel Core i9 skryvayetsya mikroskhema NFC libo RFID // ixbt. URL: https://www.ixbt.com/news/2017/06/05/intel-core-i9-nfc-rfid.html (data obrashcheniya: 07.12.2023).

16. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 Product Families. Datasheet Volume 1 of 2. - Reference Number: 325119-001 izd. INTEL®, April 2011. - 174 s.

17. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 v2 Product Family Datasheet - Volume One Electrical, Mechanical and Thermal Specifications - Volume 1 of 3. - Reference Number: 329594-001 izd. INTEL®, February 2014. - 190 s.

18. INTEL® Second Generation Intel® Xeon® Scalable Processor. Datasheet, Volume One: Electrical. - Reference Number: 338845-001US izd. INTEL®, April 2019. - 134 s.

19. UHF RFID metka na fary avtomobilya ZKTeco UHF Waterproof Tag (samokleyashchayasya). — Tekst: elektronnyy // Sistemy bezopasnosti US-PLAST: [sayt]. — URL: https://us-plast.ru/product/new-uhf-waterproof-tag/ (data obrashcheniya: 07.12.2023).

20. V massovykh protsessorakh AMD nashlas' «dyra», kotoruyu nevozmozhno zakryt'. V opasnosti vse pol'zovateli. — Tekst: elektronnyy // CNews: [sayt]. — URL: https://www.cnews.ru/news/top/2023-05-03_v_narodnyh_protsessorah (data obrashcheniya: 07.12.2023).

21. Hardware Attacks on Mobile Robots: I2C Clock Attacking / Jiménez-Naharro Raúl, G. *. Fernando, Medina-García Jonathan, Sánchez-Raya,and,Juan,Antonio Manuel. — Tekst: neposredstvennyy // Robot 2015: Second Iberian Robotics Conference. — 2016. — S. 147-159.

22. Intel Developing RFID Tracking and Remote Controlled 'Kill Switch' for Laptops // The hacker news. URL: https://thehackernews.com/2014/06/intel-developing-rfid-tracking-and.html (data obrashcheniya: 07.12.2023).

23. Spectre (uyazvimost')// Vikipediya. Svobodnaya entsiklopediya URL: https://ru.wikipedia.org/wiki/Spectre_(uyazvimost') (data obrashcheniya: 07.12.2023).

24. Meltdown (uyazvimost')// Vikipediya. Svobodnaya entsiklopediya URL: https://ru.wikipedia.org/wiki/ Meltdown_(uyazvimost') (data obrashcheniya: 07.12.2023).

25. X. Ren, L. Moody, M. Taram, M. Jordan, D. M. Tullsen, A. Venkat, «I See Dead μops: Leaking Secrets via Intel/AMD Micro-Op Caches». URL: https://www.cs.virginia.edu/venkat/papers/isca2021a.pdf (дата обращения: 24.12.2023).

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Зеленоград, площадь Шокина, дом 1. E-mail: horev.ya@yandex.ru

HOREV Anatoly Anatolevich, doctor of technical Sciences, Professor, head of the Department «Information security», National Research University of Electronic Technology. 124498, Zelenograd, Shokin square, house 1. E-mail: horev.ya@yandex.ru

ЧУМАКОВ Андрей Александрович, аспирант кафедры «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Зеленоград, площадь Шокина, дом 1. E-mail: mr.jordan99@yandex.ru

CHUMAKOV Andrey Aleksandrovich, postgraduate student of the Department of Information Security, National Research University MIET. 124498, Zelenograd, Shokin Square, building 1. E-mail: mr.jordan99@yandex.ru

* Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.. The authors declare no conflicts of interests.