Итоги спора с uuuvn. Блобы и прошивки с безопасностью

Арс Либрев 03.10.2023

Не так давно в нашем чате Matrix шла дискуссия между мной и uuuvn по некоторым важным вопросам. Дискуссия состояла из нескольких этапов, затрагивавших разные вопросы, и в конечном счете практически довела меня до нервного срыва. Что ж поделать, я человек эмоциональный и вспыльчивый, что для постоянных зрителей и читателей проекта, к коим uuuvn не относится, не является секретом. Поскольку со стороны uuuvn под конец, уже после того, как я начал срываться, полетели обвинения меня в стремлении замолчать неудобные факты, я решил сделать отдельную публикацию, разместив ссылки на нее не только в Matrix, но и в Telegram, в которой отразил то, что было выяснено в ходе дискуссии. Мне потребовалось немало времени, прежде чем я смог придти в себя и снова начал мыслить трезво. Надеюсь теперь мне удалось объективно отразить сведения по каждому вопросу и претензий ко мне не будет. Что касается моего поведения на этапе срыва, то об этом в конце.

Блобы в Linux

Первый вопрос касался блобов в ядре Linux. Напомню, что блобами называются объекты кода, распространяемые только в бинарном виде. Вопреки тому, что сказано, например, на сайте проекта GNU, uuuvn утверждал, что никаких блобов в обычном ядре Linux нет. В ходе дискуссии выяснилось следующее. В этой статье и в этой отмечается, что первые блобы в ядро были введены Торвальдсом еще в 1996 году. При этом, как сказано на сайте Linux-libre, в современных версий ядра, начиная с версии 4.14, вышедшей в 2018 году, были удалены прошивки. Это подтверждается словами одного из разработчиков самого Linux. Все это говорит о том, что ранее несвободные прошивки присутствовали в самом ядре. Поскольку ядро находится под свободной лицензией, они вероятно не были его частью формально, но являлись ей фактически, - так по крайней мере объясняют эту ситуацию на некоторых форумах. Поскольку это странно, желательно было бы заполучить в качестве дополнительного доказательства ссылки на непосредственные объекты кода. Однако все, что мне удалось найти это скриншот в статье, заметку на форуме. Пожалуй самым весомым была статья, как раз с непосредственными ссылками на фрагменты кода. Но увы, все ссылки оказались нерабочими. Проект Linux-libre, который по его словам ведет работу

по очищению ядра от блобов, приводит на своем сайте данные о том, что именно они удалили. Но опять же без ссылок на код. На некоторых форумах мне удавалось найти ссылки на их логи, где вроде как, должен был быть именно код. Но снова все они были нерабочими. По словам uuuvn, то что представлено на их сайте, это автоматически сгенерированные программные заголовки, механизмы для подтягивания и взаимодействия с прошивками, а также непонятные массивы чисел. В отношении последних, Linux-libre утверждают, что это обфусцированные объекты кода. Что это на самом деле — непонятно. Сам uuuvn высказывал несколько предположений - precomputed таблица, прекомпиленный код, код инициализации какого-то компонента - завершив эту цепочку словами «может быть вообще что угодно». То есть, в том числе и обфусцированный код. Нельзя не заметить, что разработчики самого Linux никогда нигде не опровергали заявлений о блобах в ядре. Это довольно странно, учитывая, что когда тот же проект GNU, искажал информацию по куда менее важному вопросу, его на этом тут же ловили. Дополнительно, проект Debian утверждал, что чистил ядро от блобов, но опять же без ссылок на соответствующие фрагменты кода. Все сказанное позволяет утверждать, что в прошлом, с достаточно высокой долей вероятности, несвободные прошивки представляли собой блобы в ядре. Об их выносе сообщал один из разработчиков Linux, о чистке ядра от них говорили Debian и Linux-libre. Сейчас же там есть непонятные массивы чисел, которые могут быть чем угодно. В общем-то, это все, что можно сказать. Но заметим, что Linux-libre вычищают из ядра механизмы для подтягивания несвободных прошивок и взаимодействия с ними. Обращение внимания на это подвело дискуссию к следующему вопросу.

Проблемы с прошивками

Второй вопрос касался того, какая схема использования прошивок более предпочтительна — вшитых непосредственно в оборудование, или подтягиваемых отдельно с помощью механизмов, от которых избавляют ядро Linux-libre. По этому вопросу, в ходе дискуссии, картина открылась следующая.

Во-первых, абсолютное большинство прошивок являются проприетарными. Например, для Wi-Fi карт свободных или хотя бы открытых прошивок нет вообще. Существуют проекты по их разработке, но оборудование для них не найдешь.

Во-вторых, дистрибутивы, использующие ядро Linux-libre, могут работать только с тем оборудованием, в которое прошивки внедрены непосредственно.

Как подчеркивал uuuvn, такие прошивки часто забагованы и насквозь дырявы. За доказательствами он рекомендовал по этому поводу обратится к отчетам Coreboot. С тем же оборудованием, в которое прошивки подтягиваются извне, например из самой ОС, такие дистрибутивы взаимодействовать не смогут, поскольку из ядра удалены механизмы для этого.

Еще раз, прошивка в любом случае проприетарна, но с обычным ядром будет подтягиваться свежая версия с закрытыми дырами и багами, а с очищенным ядром, работать будет только та, которая внедрена в оборудование. Не в каждое оборудование прошивка внедрена изначально. Если раньше эта проблема была характерна только для Wi-Fi, то сейчас и многие проводные сетевые карты и видеокарты поставляются без прошивки, и в дистрибутивах с Linux-libre, вроде Trisquel, не работают. С последними создается парадоксальная ситуация, когда карта от Nvidia, для которой разработчики поставляют только проприетарный драйвер — при этом написанный отдельно свободный работает хуже — все же работает благодаря встроенной прошивке. А карты от AMD, которые сами выпускают свободный драйвер с полноценной поддержкой графического ускорения, не работают, поскольку не могут получить прошивку.

Таким образом, как утверждает uuuvn, подкрепляя свой вывод ссылками на статью, и эту страницу, с обсуждением этого вопроса — проект GNU и FSF рекомендующие использовать дистрибутивы с Linux-libre, делают только хуже пользователям, поскольку те теряют функциональность, не получая при этом ни капли дополнительной свободы. А кроме того, страдает, якобы, еще и безопасность, поскольку старая прошивка может содержать незакрытые дыры. В подтверждение этого, были приведены факты того, что Linux-libre удалили возможность обновления микрокода процессоров Intel для защиты от атак Spectr и Miltdown, а также предупреждение об угрозе.

После долгих душевных терзаний (я же получается вводил в заблуждение сотни людей) и раздумий, я наконец сообразил, что в такой аргументации есть изъян. Поскольку в обоих случаях прошивки проприетарные, пользователь не может изменить ни ту ни другую. Но одну может изменить разработчик, а другую нет.

Если в прошивке имеются некоторые вредоносные функции, но разработчик при этом не имеет возможности добавлять новые, он имеет над вычислениями пользователя меньше контроля, чем если он в любой момент может внести дополнительные. Вот и получается, что обновляемая прошивка, это не всегда больше свободы, чем необновляемая. На это мне возразили, что прошивка подтягиваемая отдельно, легче поддается изучению и изменению, а значит даже будучи проприетарной дает пользователю больше свободы. Я парировал, что таков расклад только для продвинутого пользователя, который изучает обновления, а не слепо скачивает, как это делают большинство пользователей.

В добавок, закрытие уязвимостей разработчиком, позволяет снизить угрозы со стороны взломщиков, на которых еще нужно нарваться. Тогда как власть разработчика над пользователем, использующем его разработку присутствует на всем протяжении ее использования. Возможность изменять в одностороннем порядке прошивку, дает разработчику больше власти, ее отсутствие — меньше. Но на этом я не остановился и продолжил изучать вопрос, в частности аргументы участников проекта Debian. Например, вот это. Не грузя дальше тонкостями разговора, укажу, что итог его можно емко представить в виде следующей таблицы.

	Свобода пользователя	Возможность изначально внедрить вредоносный функционал	Возможность внести новый вредоносный функционал	Возможность изучать и изменять для пользователя
Вшитая прошивка (не обновляемая)	Нет	Есть	Нет	Нет
Подтягиваемая прошивка (обновляемая)	Нет	Есть	Есть	Есть для продвинутого пользователя

Это представление имеет некоторую долю условности. Таков расклад для обычного пользователя. Пункт с продвинутым пользователем имеет место, поскольку, последний может выявить проблему и сообщить о ней, что позволит обычному пользователю предпринять определенные действия, например, откатить версию прошивки. Если пользователь продвинутый, хакер — изучает каждое обновление — он может в случае внедрения нового вредоносного функционала откатить версию. Если же он еще занимается обратной разработкой, то ему проще изучать прошивку, чтобы написать свободную. Таким образом, проблема с возможностью разработчика внедрить новый вредоносный функционал для него закрывается. И для него схема будет выглядеть так.

	Свобода пользователя	Возможность изначально внедрить вредоносный функционал	Возможность изучать и изменять для пользователя
Вшитая прошивка (не обновляемая)	Нет	Есть	Нет
Подтягиваемая прошивка (обновляемая)	Нет	Есть	Есть для продвинутого пользователя

Теперь картина ясна. Какой вариант более предпочтителен, пусть каждый решает для себя сам.

Безопасность операционных систем

Третий вопрос касался безопасности операционных систем. Точнее сформулировать его можно следующим образом. Является ли несвободная система, имеющая больше функций, направленных на предотвращение различных угроз, более безопасной, чем свободная, такими функциями не располагающая? Указывалось, что система MacOS имеет следующие функции. Свободные системы GNU/Linux всем этим похвастаться не могут, а потому, якобы, менее безопасны, чем проприетарная система от Apple. При этом uuuvn честно отметил, что у MacOS проблемы с приватностью, а также его использование приемлемо только в случае, если следование свободе не принципиально. Я возразил, что разделение свободы, приватности и безопасности неправомерно. Эти понятия взаимосвязаны, и низкий уровень приватности, неизбежно оборачивается низким уровнем безопасности — ведь корпорация, оставляющая себе возможность контроля над своей разработкой и собирающая данные о пользователе, имеет над пользователем власть. Информация о нем может быть использована против него, а механизмы контроля могут стать инструментами саботажа. К сожалению, мои возражения были сформулированы не так, как расписано здесь, поскольку к тому моменту эмоции уже захлестнули меня. Я просто сказал, что система корпорации, которая в своей Политике конфиденциальности, указывает, что собирает о пользователе данные, и за которой замечено немало гнусных практик, не может быть более безопасной, чем та, за которой всего этого нет. Позже uuuvn заявил, что готов разобрать свидетельства вредоносных особенностей программного обеспечения Apple, собранные проектом GNU, назвав их «бредом». Мне не известно, опубликовал ли он в итоге что-то, поскольку я с тех пор не заходил в

чат, по причинам о которых ниже. В любом случае, слежка корпорации — это факт, подтвержденный и их Политикой конфиденциальности и признаваемый самим uuuvn. Он при этом заметил, что если выпилить аналитику и Siri, то «вполне приемлемо». Что значит в данном случае «приемлемо» я не знаю. Также было заявлено, что в системы GNU/Linux, за счет совместной открытой разработки, у злоумышленников есть возможность внедрить свой вредоносный функционал. В качестве доказательств упоминался случай, как одна свободная разработка едва не приняла патч, содержащий бэкдор. Остановлено это было, только после того, как университет, который и создал патч, открыл, что проводили эксперимент по возможности внедрения подобных особенностей.
По всему этому, итог можно отразить с помощь следующей таблицы.

	Свобода пользователя	Сбор данных о пользователе	Ограничения пользователя	Возможность проверки безопасности	Возможность внедрить вредоносный функционал разработчиком	Возможность внедрить вредоносный функционал сторонним разработчиком	Разделение через песочницы	Проверка подлинности процесса загрузки
GNU/Linux	Есть	Нет	Нет	Облегчена	Есть	Есть	Возможно	Нет
MacOS	Нет	Есть	Есть	Возможна	Есть	Нет	Есть	Есть

Здесь необходимо дать несколько оговорок. В таблицу я не стал включать упомянутый uuuvn инструмент для предотвращения перебора паролей — поскольку не успел узнать, как с ним обстоят дела в GNU/Linux, а также Guarded Exception Level и инструменты усложнения установки имплантов в ядро, поскольку непонятно к чему именно это относится — сугубо к ПО или оборудованию. По поводу возможности проверки, я отсылаю вас к статье «FLOSS Security», которую уже разбирал в одной из своих заметок. В ней показано, какие преимущества для проверки дает свободное ПО, и какие возможности имеются у программистов для проверки проприетарного. Также необходимо заметить, что существуют инструменты, которые позволяют решить проблемы отсутствия разделения активности через песочницы в GNU/Linux, например виртуализация. Учитывая это, а также тот факт, что возможность внедрения вредоносного функционала разработчиком присутствует при любой схеме, таблицу можно упростить следующим образом.

	Свобода пользователя	Сбор данных о пользователе	Ограничения пользователя	Возможность проверки безопасности	Возможность внедрить вредоносный функционал сторонним разработчиком	Проверка подлинности процесса загрузки
GNU/Linux	Есть	Нет	Нет	Облегчена	Есть	Нет
MacOS	Нет	Есть	Есть	Возможна	Нет	Есть

Картина наглядна. Какой вариант более предпочтителен, пусть также каждый решает для себя сам.

Чудовище внутри

Теперь хотелось бы сказать о самом по себе ходе дискуссии и моем поведении. Те, кто внимательно следит за проектом, знают, что в прошлом я неоднократно под воздействием критики менял свои рекомендации, хотя порой по началу и реагировал на такую критику с некоторым пренебрежением. В этот раз, однако, моя объективность дала сбой.
Эта дискуссия начиналась вполне в рамках приличий. Быстро отобразилась противоречивость сведений о блобах в Linux. Потратив несколько дней на поиск и изучение информации я не только устал, но и начал путаться в своих собственных оценках ситуации, - плохо или нет наличие таких механизмов в ядре? Оппонент же мой решил пойти дальше и поднял вопрос о взаимодействии дистрибутивов с прошивками и проблемах подхода тех, кто строго следует рекомендациям GNU, к этому вопросу. Изучив аргументацию, я осознал, что возможно я все это время давал нерациональные рекомендации сотням, а то и тысячам людей. Естественно, сначала это обернулось чувством глубокого негодования, затем отчаяния. А затем, спустя много часов, мой мозг все-таки нашел изъян в аргументации оппонента. В ответ я получил порцию критики, по сути повторяющую ту, которую разбирал до этого, только с более сильным акцентом на возможностях обновляемой прошивки. В добавок ко всему uuuvn проявлял при этом непонимание того, что вообще подразумевается, когда говорится о свободе в контексте программного обеспечения. До того он уже демонстрировал непонимание этого, лишь смутно припоминал критерии GNU, и мне пришлось объяснять корректность этих критериев, их соотношение с понятием свободы, как таковым, и другими взглядами на этот вопрос. Оппонент тогда ничего на это не ответил, что я расценил как его согласие. Однако он снова и снова демонстрировал непонимание видения свободы в контексте ПО. Из этого же становилось ясно, что он не является зрителем или читателем проекта, и не желает изучать его материалы. В чате же проекта он тусуется безостановочно, разводя со своими знакомыми оффтоп по разным вопросам. Я не возражал, хоть мне это и не нравилось. Но в той ситуации, это поспособствовало усилению эмоциональной реакции. С этого момента во мне стало разрастаться чувство, которое, как я думал, уже не захватит мою душу. Я начал раздражаться. А оппонент не унимался. Я все еще сохранял способность рассуждать, и я продолжал искать и проверять информацию. В конце концов, нерациональность моих

рекомендаций, стала более очевидной. К тому моменту я от всего этого уже дико устал. А чтобы до конца во всем разобраться мне нужно было время. Мне нужно было спокойно все взвесить и обдумать. В конце своих длинных рассуждений, показывающих изъяны в аргументации uuuvn, я признал, что в предпочтении загружаемых прошивок есть рациональное зерно. Допустил, что возможно был неправ и рекомендации проекта придется поменять.

Я надеялся, что после этого станет понятна ситуация, и я смогу наконец спокойно разобраться во всем. Мне стоило прекратить посещать чат до тех пор, пока я окончательно во всем не разберусь. Но я не прекратил.
Оппонента не устраивал мой ответ. Более того, он снова и снова пытался вызвать меня на прямой разговор через видео, полагая, что это каким-то образом поможет быстрее во всем разобраться. Я объяснил ему, что мне это неудобно, поскольку мне для осмысления аргументов, обнаружения изъянов и составления ответа нужно время. То что я стал включаться в дискуссию эмоционально тоже не способствовало ясности мысли. Но он все это просто игнорировал, снова и снова прося прямого разговора. Такое игнорирование моих слов меня раздражало еще больше.
Итак, он игнорировал мои слова и раз за разом просил о том, от чего я обоснованно отказался. Он игнорировал мои слова о том, что первостепенным для проекта является вопрос свободы, и все иные вопросы о ПО рассматриваются через его призму. Он постоянно разводил оффтоп в чате, отказываясь понимать, для чего он на самом деле был создан. Все это бесило. И здесь я не заметил как переступил черту. Теперь уже не важно было — за кем рациональность. Эмоции захлестнули меня. Злоба — вот что отвечало на претензии uuuvn дальше. Мы отправились по кругу в своем споре. На свою беду, критикуя позицию оппонента, я вскользь упомянул о его давнишних рекомендациях MacOS, не помня о тех оговорках, которые он при этом давал. Оппонент возразил на это. Я признал, что был не прав, при этом отметив, что раз чат о свободном ПО, то рекомендовать здесь такую вещь как MacOS, просто не уместно. К сожалению, я не смог это сделать спокойно и с акцентом именно на неуместность. Я обмолвился о безопасности MacOS. Несмотря на все, я однако еще сохранял какие-то остатки рассудительности. Продолжал изучать информацию по вопросу. Я смог полноценно оценить ситуацию с прошивками — для меня стал ясно, что текущие рекомендации проекта, действительно в этом плане нерациональны. И я даже понял, какие именно были бы действительно рациональными. Об этом я написал в своем ответе. И даже поблагодарил uuuvn за то, что он развил дискуссию о прошивках. Увы, из-за злости это было окружено яростной критикой аргументов uuuvn. К

сожалению, я не смог дать ответ по поводу MacOS и с акцентом именно на неуместность. Я обмолвился о безопасности MacOS. Оппонент высказал сомнение наличия в нем бэкдоров, и сказал что они скорее есть в GNU/Linux. Я возразил, напомнив еще раз о чем чат. Но оппонент меня не слышал. Он разразился тирадой о полезных функциях MacOS, коих нет в GNU/Linux, и заявил, что я мол не хочу знать технические детали того, о чем веду проект. В том-то и дело, что я не веду проект о MacOS, при чем тут его детали? Я не сказал этого. Не сообразил. После этого его ответа, эмоции накрыли меня окончательно. А uuuvn опять просил прямого разговора, хотя я уже неоднократно объяснил, что мне это не удобно. Снова настаивал, что, якобы, просто излагает технические факты. Если бы он ранее просто перечислял характеристики MacOS, то да, это были бы просто факты. Но он же писал, что ее можно использовать, если следование свободе не принципиально. Такая речь не факт — это рекомендация. Чат проекта о свободном ПО — здесь следование свободе не может быть не принципиально. Если бы он просто писал, чем отличаются современные смартфоны Android, от смартфонов на базе GNU/Linux, то это были бы просто технические факты. Но он же писал, что использовать смартфоны с GNU/Linux «боже упаси». Это уже не факт, а рекомендация — рекомендация не использовать более свободные устройства. Но uuuvn ничего этого не видел, и отказывался понимать, что находится в чате проекта, популяризирующего свободное ПО, и потому продвижение проприетарного здесь не уместно. Конечно, мог иметь место вопрос, а почему использование свободного ПО настолько важно, что проект на нем настаивает? На него я давал ответ в статье о свободном программном обеспечении и комплексной статье. Я постоянно указывал uuuvn на них, надеясь, что знакомство с ними прояснит для него этот вопрос. Но он просто игнорировал их. Он говорил про приемлемость использования проприетарного ПО при выпиливании вредоносного функционала (аналитика в MacOS и т.д.). Я не знаю, что в его представлении «приемлемо», каким образом можно убедиться, что все проблемы выпилины, а главное, почему сторонник свободного ПО должен пользоваться несвободной системой, пусть и без вредоносных особенностей. Сам uuuvn говорил, что он всеми руками за свободное ПО. При этом использование MacOS, судя по тому что он пишет (он писал, что пересел на нее со свободных систем), является его сознательным выбором, а не вынужденной мерой. Как в голове одного человека сочетаются приверженность свободному ПО и предпочтение использования несвободного, при наличии возможности использовать первое — мне непонятно. Оппонент указал, что он против «фанатизма». Но если принципиальное использование свободного ПО, это фанатизм, то чем отличается его «нефанатичный» сторонник, от того, кто к

нему вообще равнодушен? От всего этого нервы мои сдали. В бешенстве я сходу коротко ответил uuuvn по некоторым пунктам, буквально послав его при этом.

Потом не спал почти всю ночь. Гнев сменялся отчаянием, а отчаяние гневом. Я раз за разом представлял себе дальнейшее развитие спора с uuuvn, орал, бешенство сотрясало меня. Как вдруг обнаружил себе тем, кем казалось перестал быть давно. Тем, кто ненавидит весь мир и самого себя. Кто считает, что гнев добродетель. И что категоричность — достоинство. А любой, кто не рассуждает категорично — ничтожество. Но ведь это то, что рождает столько страданий в мире. Нет, это не то, что позволительно культивировать. Неужели uuuvn был прав, когда говорил о «фанатизме»? Подумав о нем, я снова не смог противиться гневу.

Поскольку я не могу быть уверенным, что ненависть и ярость не поглотят меня снова, я вынужден отказаться от участия в переписках. Собственно, после того ответа, в котором вместо меня заговорило то худшее, что как оказалось, все еще сидит во мне, я и не посещал чат. Потому не знаю, что там писали после этого. Только собирая ссылки на сообщения для этой заметки, краем глаза заметил, что uuuvn, что-то писал еще. Больше я это не стану. Я осознаю, что из-за этого могу пропустить какие-то важные сведения, но если я окончательно тронусь башкой, это точно не пойдет на пользу проекту. Да и к тому же сейчас и в чате Matrix, и в чате Telegram за сутки набегает такое количество сообщений, что читать их все становится физически невозможно. Если я продолжу делать новые публикации, то буду выкладывать их в пабликах. Но читать переписки более не стану. По крайней мере до тех пор, пока не пойму, что эмоции не возобладают. Тем, кто пишет лично, буду продолжать стараться отвечать.

Теперь те из вас, кто дочитал до этого места, все знают. Я напоминаю, что все это происходило в публичном чате, и я специально оставил прямые ссылки на сообщения, чтобы каждый мог проверить все сам и убедиться, что я ничего не исказил и из контекста не вырвал. Я осознаю, что повел себя недостойно. Я намеренно не стал здесь пытаться давать какие-то рекомендации, чтобы каждый смог сам оценить ситуацию и принять решение, сообразно со своими принципами и потребностями, что ему следует использовать.