DOI10.37882/2223–2966.2022.07.12

КОМПЛЕКСНАЯ ОЦЕНКА БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ РОБОТОВ

COMPREHENSIVE ASSESSMENT OF THE SECURITY OF THE OPERATING SYSTEM OF ROBOTS

G. Ivanov

Summary. The Robot Operating System (ROS) was not created for wide distribution outside of research laboratories, which is why the emphasis on ensuring the security of the platform was not made by its developers. However, now that this platform has been actively used to launch commercial robots in open networks, the issues of network security, user authorization, differentiation of access rights to resources, etc., have rapidly come to the fore. Despite the great advantages of ROS in creating a convenient user interface for developers and architecture aimed at achieving high platform performance, the lack of security leads to the emergence of vulnerabilities, using which attackers can gain access to ROS-based robots and cause serious damage.

This article provides a comprehensive assessment of the security of the operating system of robots based on the architecture of the platform, including the identification of current problems, vulnerabilities, threats and risks.

Keywords: robotic operating system, comprehensive assessment, security, problems, vulnerabilities, threats, risks.

Иванов Глеб Олегович
Пермский национальный исследовательский политехнический университет
gleb_molodoi5@mail.ru

Аннотация. Операционная система роботов (РОС) создавалась не для широкого распространения за пределами исследовательских лабораторий, ввиду чего акцент на обеспечение безопасности платформы ее разработчиками не делался. Однако теперь, когда эта платформа стала активно применяться для запуска коммерческих роботов в открытых сетях, вопросы обеспечения безопасности сети, авторизации пользователей, разграничения прав доступа к ресурсам и т.д., стремительно вышли на передний план. Несмотря на большие преимущества РОС по созданию удобного пользовательского интерфейса для разработчиков и архитектуры направленной на достижения высокой производительности платформы, недостаточный уровень безопасности приводит к появлению уязвимостей, воспользовавшись которыми злоумышленники могут получить доступ к роботам на базе РОС и причинить серьезный ущерб.

В данной статье проводится комплексная оценка безопасности операционной системы роботов на основе архитектуры платформы, включающая определение актуальных проблем, уязвимостей, угроз и рисков.

Ключевые слова: роботизированная операционная система, комплексная оценка, безопасность, проблемы, уязвимости, угрозы, риски.

Введение

Согласно концепции безопасности РОС, можно судить о критически низком уровне защищенности платформы [1]. Архитектурные особенности платформы были заложены с целью достижения задач производительности и удобства использования РОС для написания программного обеспечения роботов.

Широкое распространение РОС в коммерческом секторе создает новые условия ее использования, которые никак не учитывались ее разработчиками. Теперь любая ошибка, возникшая на платформе, может привести к ущербу, размер которого может быть огромным. В зависимости от сферы применения, это могут быть значительные денежные убытки, к примеру, если из-за ошибки робот-манипулятор не сможет собирать детали, производство в котором он участвует может полностью остановиться. В более серьезных случаях ошибка может стоить человеческой жизни, например, если она приведет к сбою робота-хирурга во время проведения операции на пациенте.

К возникновению ошибок могут привести не только сбои платформы, но и ранее не учитываемый фактор — злоумышленник. Теперь, когда РОС начинает функционировать в области общедоступных открытых сетей, появляется значительная угроза, исходящая именно от угрозы постороннего вмешательства. Зная какой ущерб это может причинить, возникает необходимость определить каким актуальным угрозам может быть подвержена платформа РОС, чтобы иметь возможность разработать меры для противостояния им.

Проведение комплексной оценки защищенности РОС позволит понять каким актуальным угрозам в информационном пространстве может быть подвержена платформа, чтобы иметь представление о том, какие решение следует применять для ее защиты.

1. Анализ проблем операционной системы роботов

Проблемы РОС не ограничиваются лишь одним аспектом. Они могут использовать любые существующие уязвимости платформы и привести к тому, что ущерб будет нанесен не только самой платформе, но и также роботу под ее управлением. Цепочка последствий может продолжаться и дальше, в результате приведя к худшему сценарию — созданию роботом опасности для человеческой жизни.

Актуальными являются следующие проблемы:

- Отсутствие защищенной сети, которая делая связь между узлами небезопасной и подверженной различным атакам;
- Отсутствие идентификации пользователей, в следствии которой невозможно установить кто получает физический доступ к платформе;
- Отсутствие аутентификации узлов, что приводит к несанкционированному доступу с использованием стандартных тем сообщений;
- Отсутствие конфиденциальности из-за передачи сообщений в открытом виде, без применения криптографических алгоритмов, что приводит к перехвату и раскрытию информации;
- Отсутствие проверки целостности, вызванной использованием протокола без кэширования и проверки контрольных сумм, в результате чего сообщения могут быть скомпрометированы;
- Отсутствие разграничения доступа к ресурсам, в результате чего конфигурация платформы может быть изменена пользователями, не имеющими на то прав;
- Отсутствие механизма самовосстановления делает платформу не способной противостоять продолжительным во времени атакам, ухудшающим производительность платформы из-за ее неспособности своевременно отреагировать на ошибки и сбои.
- Отсутствие обновлений текущих версий РОС приводит к появлению устойчивых уязвимостей. Проблема связана с тем, что для РОС еще не было разработано стабильной версии. Вместо исправления уязвимостей для текущей версии, разработчики выпускают новую, учитывая все найденные проблемы, но оставляя старые версии без исправлений;
- Отсутствие IDS-решений делает невозможным обнаружение сигнатур и поиск аномального поведения, что приводит к повышенной угрозе заражения вредоносным ПО;
- Отсутствие тестирования на проникновение приводит к возникновению угроз безопасности стабильных соединений узлов;

2. Анализ уязвимостей операционной системы роботов

Роботизированные системы подвержены различным уязвимостям, которые могут повлиять на их работоспособность как с точки зрения производительности, так и обеспечения безопасности обрабатываемых данных. Уязвимости могут привести к частичному или полному отказу функционала платформы.

Актуальными являются следующие уязвимости:

- Уязвимости сети из-за отсутствия мер обеспечения безопасности связи, делающих платформу уязвимой для различного рода проводных и беспроводных атак, таких как прослушивание трафика, “человек по середине”, сканирование системы, подмена данных и т.д.;
- Уязвимость обновления включает в себя отсутствие постоянных обновлений библиотек. Библиотека от независимого издателя может содержать критические бреши, через которые злоумышленник может провести атаку на узел, подписавшийся на соответствующую тему библиотеки. В силу обстоятельств, издатель может оказаться недобросовестным, в результате чего бреши в библиотеки останутся без изменений;
- Уязвимость программного кода заключается в отсутствии тестирования и оценивания его на наличие ошибок кодирования или совместимости. Если протокол обмена сообщениям между узлами полностью соблюдается, то по подписке узлу может быть передан программный код, который не может быть корректно скомпилирован, что повлияет на производительность платформы;
- Уязвимость узлов состоит в том, что по модели подписки на заданную тему злоумышленник может выполнить атаку типа “отказ в обслуживании”. Если узел является издателем, то на него может одновременно подписаться огромное количество узлов, для каждого из которых потребуется обработать запрос, установить соединение и передать сообщения. Если узел является подписчиком, то при наличии подписки на определенную тему, он может начать получать огромное количество сообщений с данной темой, которые потребуется обработать;
- Уязвимость гетерогенности сети состоит в наличии ошибок в относительно новых языках программирования, которые поддерживаются платформой, что может привести к возникновению каскадного эффекта, поскольку, порты для поддержки новых языков программирования также находятся в разработке;
- Уязвимость управления заключается в отсутствии службы контроля за приоритетом выполнения

операций. Ошибочная последовательность запуска критических узлов может привести к нарушениям в работоспособности платформы.

3. Анализ угроз операционной системы роботов

Угрозы могут исходить из разных источников, будучи являясь частью киберпреступлений, кибервойн, кибершпионажа или даже кибертерроризма.

К актуальным источникам угроз относятся:

- Инсайдеры. Это, как правило, мошенники или ненадежные сотрудники, которые стремятся либо украсть конфиденциальную информацию платформы, либо проникнуть внутрь, помогая аутсайдерам проводить свои атаки удаленно, злоупотребляя привилегиями. Инсайдеры также могут нанести физический через прямое подключение к платформе;
- Аутсайдеры стремятся получить доступ к платформе удаленно, через общественную сеть Интернет. Их целью является получение доступа к информации для вызова сбоев или нарушения работоспособности платформы путем внедрения поддельных или вредоносных данных;
- Конкуренты. Обычно конкуренты преследует цель сохранить лидирующие позиции в области робототехнике. Многие их методы могут опираться на взаимодействие через инсайдеров с целью осуществления промышленного шпионажа через утечки конфиденциальных документов или нанесение репутационного ущерба;
- К некомпетентным разработчикам относятся плохие производители или программисты, которые неосознанно допускают ошибки при установке или настройке платформы, а также в результате написания программного кода, в последствии, приводящих к возникновению ошибок функционирования платформы;
- Некомпетентные пользователи могут неосознанно допускать ошибки в результате эксплуатации платформы из-за невнимательности или недостаточного объема знаний. В редких случаях пользователь может злонамеренно пытаться использовать платформу, с целью нанести ей ущерб из личных побуждений;
- Киберпреступники, включая хакеров, целью которых является применение своих возможностей для реализации кибератаки путем сканирования, поиска пробелов в безопасности или уязвимостей программного обеспечения платформы;
- Организованные преступники, в отличии от киберпреступников, проводят осознанное вторжение с целью получения физического доступа к платформе и ее компонентам для их последующего похищения и продажи;
- Злонамеренные разработчики специально оставляют бэкдоры в конфигурации платформы для удаленного получения доступа к информации без ведома ее владельца. Кроме того, они могут проводить сбор конфиденциальной и не конфиденциальной информации на платформе в автоматическом режиме и периодически отправлять ее в виде отчетов. На самом деле многие разработчики специально оставляют дефекты в программной структуре, чтобы при необходимости воспользоваться ими как черным ходом для восстановления доступа к платформе;
- Спонсируемые государством хакеры обычно вербуются для проведения кибератак с целью выполнения оборонительных или наступательных задач, приводящих к получению политической выгоды. Целью таких атак являются сферы значительно влияния, где применяется платформа, например, оборонная. Так, атака на платформу может привести к выведению из строя военного робота, утечке секретной информации;
- Террористы преследуют цели взлома платформы для получения доступа к военным роботам или промышленным, преимущественно используемых на объектах критической инфраструктуры. Цели взлома направлены на выведены платформы из строя, что позволит создать аварийную ситуацию опасную для жизни людей и окружающей инфраструктуры. Как правило, террористы стремятся нанести наибольший деструктивный ущерб;
- Шпионы постоянно используются для проведения кибершпионажа и диверсионных операций, как правило, между соперничающими странами. Их отличительной чертой является высокий профессионализм и неясность преследуемых целей, которые напрямую зависят от поставленных им задач. Атака шпионов в киберпространстве могу носить каскадный характер и длиться продолжительное время. Объектами атаки могут стать любые сферы применения платформы, как правило для того, чтобы найти устойчивые точки входа и постепенно наращивать потенциал шпионажа.

Исходя из существующих проблем безопасности платформы, злоумышленникам доступны разные типы угроз, которые способны оказать разный эффект на платформу и роботов под ее управлением. Выбор типа угрозы напрямую зависит от того, кто будет являться ее источником.

К актуальным типам угроз относятся:

- Беспроводные помехи. Связь между узлами платформы может быть подвержена различным

атакам на доступность, которые могут привести к возникновению помех, нарушающих или прерывающих соединение по сети. Это может привести к полной или частичной потере связи с узлами;

- Разведка и сканирование. Платформа подвержена различным аналитическим атакам, целью которых является оценка уровня ее защищенности, сбор информации об используемых программных модулях, поиск адресов задействованных узлов, сбор данных об актуальной версии и т.д. Полученные данные могут позволить обнаружить уязвимости и бреши в платформе, которые могут быть использованы для проведения будущих атак;
- Раскрытие информации. Создание каналов утечки информации, может проводиться как через физическое взаимодействие с платформой, так и удаленно, с помощью кибератак. Полученная информация может быть и конечной, и промежуточной целью. Во втором случае также создаются условия для проведения будущих атак;
- Нарушение привилегий. События, когда неавторизированные пользователи нарушают физическую или логическую связь между элементами управления платформы, чтобы получить несанкционированный доступ для выполнения неразрешенных задач для их уровня привилегий;
- Сбор информации. В отличии от разведки и сканирования, данный тип угрозы направлен не напрямую к платформе, а к окружающей ей элементам информационной среды. Так, сбор может происходить через утечку данных от операторов платформы, побочное излучение физических объектов, с помощью которых поддерживается платформа, и так далее;
- Перехват информации. За счет отсутствия защиты сети и шифрования проходящих по ней сообщений, возникает возможность проведения различных атак перехвата и задержки информации, которые могут привести к полному нарушению конфиденциальности, целостности и доступности;
- Модификация информации. Угроза, реализуемая теми же способами, что перехват, но с дополнительным последующим шагом — модификацией или подменой полезной нагрузки перехваченных сообщений. Модификация может позволить дольше оставаться злоумышленнику незамеченным, а также нанести большей вред самой платформе;
- Отслеживание и мониторинг. Через уязвимости отдельных библиотек может осуществляться мониторинг информации, передаваемой узлом, использующим данную библиотеку. Сбор информации происходит тайно и долгое время оставаться нераскрытым.

Фактически, перечисленные типы угроз затрагивают напрямую безопасность именно самой платформы РОС, что в результате отражается и на связанных с ней элементах. Следует заметить, что отдельные типы угроз могут быть направлены не на саму платформу, а на обрабатываемую в ней конфиденциальную информацию. Отсюда возникают следующие типы угроз информации:

- Угроза конфиденциальности. Сюда относится, помимо использования вредоносных программ для пассивного анализа трафика (например, подслушивание), кража конфиденциальных данных, внедрение вредоносного кода, раскрытие конфиденциальной информации, атака по побочным каналам излучения, фишинг и так далее;
- Угроза целостности. Включает в себя активный анализ трафика (например, “человек посередине”), слежку, подмену и модификацию данных, внедрение вредоносных программ, внедрение ложных данных, физическую или логическую компрометацию обрабатывающей платформы, использование бэкдоров, руткитов, повышение привилегий и так далее;
- Угроза доступности. Состоит из кражи служебных данных, отказа в обслуживании или прерывания работы, нарушения или прерывания сетевого взаимодействия, истощения ресурсов и переполнения буфера, создания помех, внедрения вредоносных программ и вирусов, физического ущерба обрабатывающей платформе, повторные атаки и так далее;
- Угроза аутентификации. Структура объединяет использование вредоносных сторонних приложений и сервисов, методы фишинга, злоупотребление привилегиями, кражи ключей доступа, отсутствие надлежащего контроля доступа, развертывание поддельных узлов и так далее.

4. Анализ рисков операционной системы роботов

При возникновении различных проблем безопасности и кибербезопасности платформы, связанных с наличием актуальных угроз и уязвимостей, появляются риски способные привести к возникновению негативных последствий.

Актуальными являются следующие риски:

- Системные недостатки безопасности. Эти риски влияют на нормальную обработку и производительность платформы, а также могут стать следствием нарушения производственных и промышленных процессов, что приведет к финансовым потерям. Также, это может повлечь за собой блокировку платформы, перехват информации, утечку данных;

- Бэкдоры. Плохо сконфигурированные пакеты со сторонним доступом приводят к появлению различных атак через бэкдор или с использованием руткитов. Это позволит собрать информацию об активных узлах в платформе, поставить их на мониторинг и начать сбор конфиденциальной информации;
- Удаленный доступ. Открытые по умолчанию порты в платформе могут привести к получению злоумышленниками удаленного доступа, что позволит им провести успешную кибератаку. Также, риск удаленного доступа связан с использованием портов по умолчанию, что может привести к таргетированной атаке;
- Кража устройств. Поскольку для практического применения платформы требуется физическое устройство (робот), на базе которого будет функционировать платформа, существует риск получения несанкционированного доступа путем кражи физического оборудования. Злоумышленник получит возможность деаутентифицировать легитимных пользователей;
- Поддельные пакеты. Платформа поддерживает интеграцию программного обеспечения сторонних специалистов, в связи с чем злоумышленники могут замаскировать вредоносный код под легитимный пакет. В состав такого пакета для отвлечения может входить рабочий программный код, но при этом параллельно будет работать и вредоносная часть кода, к примеру, состоящая из программ-вымогателей, бэкдоров, шпионских программ, ботнетов, червей, троянов и так далее. Пока пакет выполняет полезную нагрузку и не привлекает к себе внимания, в это время атаке может подвергаться конфиденциальная информация;
- Резервное восстановление. Отсутствие надлежащего и проверенного резервирования данных может привести к их повреждению и потере, в случае возникновения сбоев в работе платформы. Фактически, без резервных копий данных любая атака может вывести платформу из режима нормального функционирования и привести к ее полному отказу;
- Системный сбой. Во время проведения кибератак, платформа подвержена различным проблема, включая возникновение крупных и каскадных сбоев, приводящих к нарушению ее функционирования. Неспособность своевременно реагировать на возникающие ошибки несет в себе накопительный эффект, перерастающий в эти самые сбои. [2]

Итоги

Проведенная комплексная оценка безопасности POC показала, что использование платформы в чистом виде является небезопасным и может повлечь за собой возникновение инцидентов за счет воздействия злоумышленника. Данная проблема делает маловероятным выбор платформы в качестве решения задач робототехнической области, особенно в коммерческой сфере, в связи с чем возникает потребность в разработке и использовании методик защиты POC, способных обеспечить безопасность платформы и не допустить возникновение инцидентов в результате воздействия злоумышленника на платформу.

ЛИТЕРАТУРА

1. Ruffin White and Dr. Henrik I. Christensen. SROS: Securing ROS over the wire, in the graph, and through the kernel // Springer — 2018.
2. Jean-Paul A. Yaacoub, H. Noura, O. Salman, A. Chehab. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations // Springer — 2021.

Журнал «Современная наука: актуальные проблемы теории и практики»