DOI10.37882/2223–2966.2022.07.11

ПРОБЛЕМА ИНТЕГРАЦИИ ЗАЩИЩЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ РОБОТОВ С ПРИМЕНЕНИЕМ МЕХАНИЗМОВ ЗАЩИТЫ

THE PROBLEM OF INTEGRATION OF THE PROTECTIVE ROBOT OPERATION SYSTEM WITH THE USE OF PROTECTION MECHANISMS

G. Ivanov

Summary. The robotic operating system (ROS) is one of the most popular platforms for implementing robot control systems and software development. However, the ROC was created for a research and development purpose and was not designed for use in a commercial industry, so this system does not provide any protection methods. This is due to the fact that regulatory protection methods require certain resources to function, which is revealed in the form of increased productivity and performance efficiency, and also leads to an increase in delays in the processing of control signals. To date, a general solution has not yet been created to close all vulnerabilities in ROS, since the practical implementation of the robot system is unique and requires a personalized approach, identification of priority threats and performance restrictions on danger.

This article describes a robot based on ROS, the power to increase productivity, reveals the relevance of the "man in the middle" attack, uses the selection of protection mechanisms against this attack and an assessment of their impact on the performance of the robot.

Keywords: robotic operating system, performance, achievements, protection mechanisms, evaluation.

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

Аннотация. Роботизированная операционная система (РОС) является одной из самых популярных платформ для реализации систем управления роботами и разработки программного обеспечения. Однако, РОС изначально создавалась для научно-исследовательских задач и не предполагалась для использования в коммерческой индустрии, ввиду чего в данной системе не предусмотрены какие-либо методы защиты. Это объясняется тем, что традиционные методы защиты требуют определенных ресурсов для функционирования, что выливается в виде дополнительных нагрузок и снижения производительности, а также приводит к появлению задержек при обработке управляющих сигналов. На сегодняшний момент еще не создано единого решения для закрытия всех уязвимостей в РОС, поскольку, каждая практическая реализация операционной системы роботов уникальна и требует персонализированного подхода, ввиду наличия приоритетных угроз и ограничений по нагрузке на производительность.

В данной статье приводится описание робота на базе РОС, имеющего ограничения по снижению производительности, подтверждается актуальность атаки "человек посередине", проводится подбор механизмов защиты от данной атаки и оценивается их влияние на производительность робота.

Ключевые слова: роботизированная операционная система, производительность, ограничения, механизмы защиты, оценка влияния.

Введение

По своей задумке механизмы защиты должны интегрироваться в платформу РОС и вносить структурные изменения в процессы хранения и обработки данных, не изменяя ключевых особенностей архитектуры. Это позволяет добавить промежуточные вычислительные этапы способные обеспечить защиту от большинства известных атак, при этом не создавая изменений в логике работы РОС. Однако, не существует одного универсального механизма для закрытия всех известных уязвимостей. Различными группа разработчиков ведется создание множества механизмов защиты, имеющих свои сильные и слабые стороны.

Ключевым недостатком разработанных механизмов защиты является использование традиционных методов защиты по умолчанию. Такие решения как использование криптографии для шифрования данных, использование рукопожатий для проведения аутентификации, применения кэширования для проверки целостности данных и другие, обеспечивают защиту в ущерб производительности. Так, в попытке защитить платформу РОС от широкого спектра атак традиционными методами, разработчики механизмов идут против основной концепции РОС, ставя задачу обеспечения защиты выше производительности. [1]

В ситуациях, когда РОС функционирует в условиях наличия требований к производительности, применение механизмов, использующих традиционные методы защиты, может само по себе создать условия возникновения инцидента, без необходимости участия злоумышленника, против которого и вводятся механизмы защи-

ты. Особо серьезно это касается роботов на базе РОС, которые активно взаимодействуют с людьми.

1. Описание модели применения робота на базе РОС

В качестве объекта исследования выберем промышленного робота-манипулятора модели "M-900iB/280", от компании "FANUC", используемого на химическом производстве для совершения манипуляций с опасными веществами, работающего на базе РОС.

Данный тип робота обладает полностью модернизированной рукой, обеспечивающую максимальную жесткость конструкции. Один из его ключевых показателей — очень высокий уровень статической податливости. Благодаря этому качеству робот идеально подходит для решения задач, требующих высокой точности.

Робот работает вместе с людьми и выполняет определенные манипулятивные действия, например, подъем и фиксацию, перемещение объекта в пространстве. Всякий раз, когда человек приближается к роботу, тот должен замедляться или даже останавливаться, если человек находится слишком близко. Для контроля скорости робота существует области, которые для простоты обозначим номерами от 0 до 2, где 0 означает отсутствие человека, 1 означает нахождение человека в зоне совместной работы (работа с пониженной скоростью), а 2 означает нахождение человека в опасной зоне (робот полностью останавливается). Робот оснащен датчиками, которые фиксируют и обрабатывают данные об окружении, в частности, о попадании человека в одну из пронумерованных областей.

Сеть состоит из самого робота, двухдиапазонного маршрутизатора, который позволяет подключаться по беспроводной сети к компьютеру вне робота, и внешнего сервера, который выполняет определенные действия. Робот общается с сервером через темы РОС.

Алгоритм контроля скорости робота строится следующим образом:

- Датчики фиксирует человека в 0 области или ни в какой другой, робот работает с нормальной скоростью, датчики не передают сообщения;
- Датчики фиксируют попадание человека в 1 или 2 область и начинают постоянно генерируют сообщения размером 3 КБ с текущем положением человека;
- Сообщения обрабатываются платформой РОС и передаются встроенным в робота узлам, отвечающим за изменение его скорости;
- Узлы робота изменяют скорость в соответствии с полученными сообщениями;
- РОС отправляет сообщение серверу об изменении скорости робота;
- Сервер может прислать ответное сообщение с повышенным приоритетом, самостоятельно устанавливая скорость робота.

Области контроля скорости данной модели робота рассчитаны таким образом, что если датчики непрерывно генерируют 140.000 сообщений размером 3 КБ и передают их узлам, отвечающим за изменение скорости робота, с частотой 200 Гц, то они должны быть переданы не более чем за 10 мс, при допустимой потере сообщений не более 0,1% от общего количества. Если данное условие не выполняется, то считается, что человек смог попасть во 2 область и робот не успел полностью остановиться, что создает угрозу опасности для жизни человека.

2. Алгоритм проведения атаки

Целью атаки является незаметно перехватить, изменить и заблокировать сообщения между сервером и роботом, чтобы создать аварийную ситуацию. Имея злоумышленника в той же сети что и узлы РОС, мы можем использовать атаку "человек по середине" чтобы передать все данные с сервера через компьютер злоумышленника, предварительно проанализировав и модифицировав их.

Атака проводилась в три этапа: сначала проводится анализ сети, затем перехватывались данные, и, наконец, был получен контроль над передачей данных.

Анализ сети проводился с использованием инструмента nmap для поиска IP-адресов сервера и робота. С IP-адресами злоумышленник знает расположение двух концов TCP-соединения, по которым передаются целевые данные.

Как только IP-адреса конечных точек были обнаружены, была запущена атака "человек посередине", чтобы поместить компьютер злоумышленника между этими точками. Злоумышленник отправлял вредоносный TCP-пакет на широковещательный канал маршрутизатора, с установленным флагом SYN, после получения ответа с флагами SYN+ACK производилась отправка пакета ACK, содержащего легитимный порядковый номер на подключение. Подобрать номер удалось с помощью полученного ответа, где содержался данный номер, уменьшенный на единицу. Теперь компьютер злоумышленника соединен с роботом и сервером.

Последним шагом потребовалось включить IP-переадресацию, чтобы убедиться, что полученные пакеты

будут перенаправлены в исходное место назначения. Теперь, когда данные проходят через машину злоумышленника, нужен способ изменить или заблокировать их. Для этого использовалась библиотека Linux под названием Netfilter Queue. С помощью этого инструмента можно создавать правила прохождения трафика и обработки пакетов через машину злоумышленника.

В результате реализованной атаки "человек посередине", компьютер злоумышленника получил возможность просматривать и изменять весь проходящий трафик между роботом и сервером. Для создания аварийной ситуации с роботом злоумышленник может подделать сообщение от лица сервера и изменить скорость работы робота, тем самым создав угрозу для человека, находящегося непосредственно вблизи, в областях 1 или 2.

3. Подбор механизмов защиты

Для защиты робота от атаки "человек посередине" можно использовать один из следующих механизмов защиты:

Securing ROS. Дополнение к API и экосистеме ROC, разработанное для закрытия основных уязвимостей ROC. Обеспечивает безопасность транспортного уровня (TLS) для всех сокетов ROC, создает доверительные цепочки между узлами используя сертификат x.509, определяет пространство имен и разрешенные роли для ограничения узлов ROC.

Secure ROS. Решение предоставляет альтернативные версии пакетов ROC, которые обеспечивают безопасную связь между узлами. Основной упор сделан на обеспечение безопасного соединения для обычных пользователей, для чего вводится IP-расширение безопасности (IPSec). IPSec используется в транспортном режиме, таким образом шифруя и аутентифицируя полезную нагрузку передаваемых сообщений. Кроме того, транспортный и прикладной уровень защищаются хэшем, поэтому, они не могут быть изменены извне.

SECURE-ROS-TRANSPORT. Архитектура работает на уровне приложений, используя выделенный сервер аутентификации, обеспечивая безопасную связь между узлами ROC, используя криптографические методы, обеспечивая конфиденциальность и целостность данных. Данная реализация включает модификацию основных пакетов ROC и обеспечивает создание защищенного канала связи, позволяющего узлам ROC безопасно обмениваться сообщениями. Для TCP используется TLC, а для UDP используется DTLS, что позволяет повысить защищенность связи между главным и побочными узлами. [2]

4. Оценка влияния механизмов на производительность

Для проведения оценки будем осуществлять передачу сообщений между узлами робота со следующими параметрами:

1. Тип сообщения: string;
2. Размер сообщения: 3 КБ;
3. Количество отправляемых сообщений: 140.000;
4. Частота отправки: 200 Гц.

В итоге, были получены следующие результаты:

Перед отправкой 140000 сообщений размером 3 КБ каждому механизму потребовалось дополнительное время на обработку данных. Чистая версия ROS обеспечила задержку в 0,288 мс. Задержка Securing ROS была выше на 4102,778% от значения чистой версии ROS, Secure ROS — выше на 121,153%, Secure-ROS-Transport — выше на 4082,292%.

Затраченное время отправки всех сообщений для чистой версии ROS составило 3,615 мс. Затраченное время Securing ROS было больше на 807,441% от значения чистой версии ROS, Secure ROS — больше на 330,776%, Secure-ROS-Transport — больше на 760,775%.

В результате невозможности поддерживать заданную частоту в 200 Гц и разовых ошибок на уровне программы, присутствовала потеря пакетов. Чистая версия ROS смогла передать все 140.000 без потерь. Securing ROS смог передать на 39,234% меньше от значения чистой версии ROS, Secure ROS — меньше на 0,002%, Secure-ROS-Transport — меньше на 33,701%.

Итоги

Для исследуемой модели системы робота на основе ROC была успешно реализована атака "человек посередине". Для обеспечения защиты от выявленной угрозы был определен и интегрирован перечень механизмов защиты, использующих традиционные методы защиты по умолчанию.

Проведенная оценка производительности каждого механизма показала, что их наличие приводит к созданию значительной нагрузки на систему. Расчет затраченного времени и потери пакетов позволил определить, что для заданной модели робота на базе ROC, механизмы защиты Securing ROS, Secure ROS и Secure-ROS-Transport не могут использоваться, поскольку, их влияние на производительности приводит к нарушению ограничений для областей контроля скорости робота-манипулятора, тем самым создавая условия для возникновения угрозы опасности для жизни человека, находящегося вблизи робота.

ЛИТЕРАТУРА

1. Б. Дибер, Б. Брейлинг, С. Таурер, С. Качянка, С. Расс и П. Шартнер. Безопасность операционной системы робота. Робототехника и автономные системы, 98: 192–203, 2017.
2. П. Эстефо, Дж. Симмондс, Р. Роббс и Дж. Фабри. Операционная система робота: повторное использование пакетов и динамика сообщества. Журнал систем и программного обеспечения, 151: 226–242, 2019.

Журнал «Современная наука: актуальные проблемы теории и практики»

г. Пермь