Зорин В.А.

Атака на робототехнические системы как способ информационно-технического воздействия

Аннотация: Рассмотрены основные виды атак на робототехнические системы, которые могут быть использованы в качестве информационно-технического воздействия.

Ключевые слова: информационно-техническое воздействие, робототехническая система

Робототехнические системы повсеместно используются в гражданских целях. Во многих домохозяйствах внедрены технологии умных домов, интернета вещей, используются роботы-пылесосы и робот-ассистенты. Активно внедряются робототехнические системы во все отрасли народного хозяйства от сельского хозяйства и медицины до систем, поддерживающих обороноспособность государства. Недавний случай в США с уязвимостью в безопасности китайских роботов-пылесосов Ecovacs Deebot X2, наглядно показал, что робототехнические системы могут стать средством информационно-технического воздействия, в том числе на объекты критической информационной инфраструктуры.

Рост числа атак на робототехнические системы (далее – РТС) ставит под сомнение развертывание систем в определенных областях деятельности. Выход из строя медицинских РТС или РТС на опасном производстве потенциально способен поставить под угрозу жизнь и здоровье граждан. А перехват управления РТС военного назначения чревато потерей суверенитета.

Для понимания механизмов, с помощью которых злоумышленники свершают попытки завладеть РТС, рассмотрим основные виды атак.

1. Атаки на аппаратную часть

Могут варьироваться от фишинга до аппаратных троянских программ, которые могут привести к использованию бэкдоров злоумышленниками для получения несанкционированного доступа, в том числе полного, к используемым роботам.

РТС подвержены атакам по сторонним каналам и атакам на сбои, которые могут привести к потере конфиденциальных данных или нарушениям в эксплуатации системы, что недопустимо для критической инфраструктуры.

2. Атаки на коды прошивки

Обновление операционной системы робототехнических систем осуществляется через подключение к сети Интернет через специальные коды прошивки, которые хранятся во флэш-памяти. Операционная система подвержена DoS и DDoS-атакам, а также выполнению произвольного кода.

3. Атаки приложений

Реализуются через вредоносные программы (вирусы, черви, программных троянов), а также атаки переполнения буфера и атаки внедрения вредоносного кода.

Атаки червей нацелены на РТС, используя уязвимости в безопасности подключенных к сети устройств до их самораспространения и саморепликации для заражения других роботизированных устройств, а также нацелены на промышленные системы управления. Например, червь Stuxnet, перехватывающий работу АСУ ТП Siemens, который был разработан совместным национальным подразделением (ISNU) США и Израиля SIGnal INTelligence (SIGINT), подразделением 8200 в рамках операции «Олимпийский» для нацеливания на ядерные активы Ирана.

Атаки программ-шифрователей направлены на захват данных, связанных с РТС, а также на блокировку резервных копий, предотвращая повторный доступ к ним владельцев систем.

Атаки типа «троянский конь» с произвольным доступом, которые маскируются под легитимное приложение и могут быть реализованы с помощью фишингового электронного письма. Обычно такие атаки нацелены на процессы аутентификации.

Атаки руткитов позволяют конкретному злоумышленнику иметь привилегированный контролируемый доступ на уровне администратора. Цель состоит в том, чтобы изменить данные робототехнических систем, оставив при этом бэкдор для будущих атак или установив скрытое шпионское ПО, которое влияет на

аспекты конфиденциальности, целостности, аутентификации и неприкосновенности частной жизни.

Атаки ботнетов обычно используются для проведения D-DoS-атак на медицинские и промышленные РТС. Ботнеты могут быть основаны на вредоносных кодах, используемых для заражения незащищенных устройств.

Атаки шпионского ПО используются для сбора информации и данных о роботах, подключенных устройствах и отправки информации третьей стороне, что дает возможность отслеживать активность роботов, их перемещения и использование.

Атаки с переполнением буфера направлены на использование уязвимости для манипулирования памятью робототехнического устройства и захвата. Переполнение на основе стека – переполнение буфера представляет собой непрерывное пространство в памяти, используемое для организации данных, связанных с вызовами роботизированных функций. Переполнение буфера на основе кучи – тип переполнения буфера в области данных кучи. Переполнение кучи эксплуатируется иначе, чем переполнение на основе стека. Память в куче динамически выделяется во время выполнения и обычно содержит данные программы. Эксплуатация выполняется путем повреждения этих данных для вынужденной перезаписи внутренних структур.

4. Атаки на коммуникации роботов

Атаки глушения для нарушения коммуникации между роботами с целью приостановить дальнейшую деятельность и прервать связь всех каналов управления.

Атаки идентификации и аутентификации, направленные на временное, периодическое или отключение РТС, чтобы получить возможность подключиться к своему первоначальному оператору, чтобы захватить робота путем получения контроля, раскрыть оператора.

Сниффинг-атаки используются, поскольку РТС часто используют открытую беспроводную связь и включают в себя прослушивание текущего трафика между роботами и их контроллерами, а также извлечение важной информации без обнаружения. Пассивный мониторинг трафика по зашифрованным и незашифрованным открытым каналам связи может помочь в

сборе и извлечении конфиденциальной информации о роботизированных системах и их текущих операторах.

Атака «человек посередине» с перехватом данных при обмене информацией между РТС или узлами, изменять информацию и внедрять.

Атаки с помощью скомпрометированных роботов, размещенных в сети для генерации ложных данных.

5. Противодействие

При проектировании роботов производители должны учитывать безопасность в качестве ключевого компонента при разработке любой прошивки, операционной системы, оборудования и приложений. Использовать постоянный мониторинг уязвимостей для обеспечения безопасности. Мониторинг активности позволит отследить аномалии поведения робототехнических систем. Внедрение улучшенных способов управления доступом, для предотвращения атак, направленных на перехват управления. Внедрение усовершенствованных криптографических решений и протоколов для защиты данных и каналов коммуникации, также внедрение безопасных каналов связи на физическом уровне.

Внедрение механизмов мгновенного отключения робота при обнаружении угрозы безопасности, в том числе через реализацию закладки для саморазрушения управляющего контроллера или процессора.

Сомов С.К.

Способы сокращения вычислительной сложности алгоритмов поиска оптимального размещения массивов данных в распределенных системах обработки данных

Аннотация: В работе приведены несколько утверждений теорем, использование которых при решении задач поиска оптимального размещения копий массивов данных в распределенных системах позволяет сократить вычислительную сложность данных задач. Представлено несколько методов, которые способствуют уменьшению