УДК 004.056

ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ ПРОВЕДЕНИЯ АТАК НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ С ДОВЕРИТЕЛЬНОЙ МОДЕЛЬЮ УПРАВЛЕНИЯ

Усова М.А. (Университет ИТМО)
Научный руководитель – к.т.н. Викснин И.И.
(Университет ИТМО)

В работе представлен аналитический обзор существующих методов проведения атак на кибер-физические системы с доверительной моделью управления, в число которых входят предвзятые рекомендации, непоследовательное поведение и атаки на идентичность. Особенности методов проведения каждого типа атак послужат основой для разработки методики обнаружения атак на доверительную модель управления.

Введение. Кибер-физические системы (КФС) являются основополагающим концептом Индустрии 4.0: это системы, в которых с помощью эффективной интеграции информационных и физических компонентов достигаются автономность, надежность и возможность адаптации к изменяющимся параметрам окружающей среды. На основе КФС создаются автономные системы в области умного производства, умной медицины, умного города и умного транспорта. Следствием быстрого распространения КФС стало возникновение новых угроз информационной безопасности, которые становятся особо опасными в критических информационных системах.

Основная часть. В настоящее время хорошо изучены классические методы атак на кибер-физические системы и методы защиты от них. Классические атаки направлены на нарушение всех трех свойств информации с точки зрения информационной безопасности: конфиденциальности, целостности и доступности. Корректное функционирование одного из элементов КФС может быть нарушено, что может негативно повлиять на работу системы в целом. Для своевременного отключения атакованных узлов была создана доверительная модель управления, основанная на социальных механизмах доверия и репутации. Доверие отражает субъективную оценку поведения одного элемента КФС другим. Репутация – показатель, формирующийся во времени в процессе определения истинности информации, получаемой от элемента КФС. При достижении критического значения доверия и репутации элемента КФС он отключается от системы и более не может оказывать деструктивное воздействие на систему в целом. Поскольку такая модель управления основана на оценивании одними элементами КФС других, возникает угроза занижения или завышения показателей доверия и репутации элементами-нарушителями. В связи с этим выделяют три типа атак на доверительную модель управления: предвзятые рекомендации, непоследовательное поведение и атаки на идентичность.

Первая категория атак осуществляется посредством неправильной оценки текущей ситуации и может быть проведена злонамеренным элементом или элементом, имеющим неверную информацию об объекте оценки, как индивидуально, так и по предварительному сговору с другими элементами. Предвзятые рекомендации содержат ложные негативные оценки и направлены на подрыв показателей репутации элементов КФС с целью захвата управления КФС. Выделяют следующие методы проведения атак с предвзятыми рекомендациями:

- атаки bad-mouthing: в этом типе атак злоумышленники сговариваются, выдумывая ложные негативные рекомендации относительно элемента с корректным поведением в системе, в результате система изолирует жертву. Элементы-нарушители продолжают реализовывать атаку относительно других элементов системы. Таким образом, они выглядят как беспристрастные рекомендатели;

- атаки методом вброса бюллетеней: в этом типе атак злоумышленники вступают в сговор и координируют свои действия, чтобы повысить репутацию целевого элемента, давая поддельные положительные рекомендации.

Атаки непоследовательного поведения характеризуются попыткой элемента КФС получения незаслуженной положительной репутации. Они могут быть классифицированы как атаки периодического действия, самореклама и отбеливание репутации:

- атаки периодического действия: в этом типе атак нарушитель сначала формирует высокую положительную репутацию, становясь одним из доверенных элементов системы, а затем выполняет деструктивные действия. При достижении репутации достаточно низких значений, цикл повышения репутации и повторного проведения атаки повторяется;
- самореклама: при проведении атаки саморекламы нарушитель информационной безопасности повышает уровень доверия к себе путем распространения положительных рекомендаций о себе с использованием уязвимостей алгоритма аутентификации;
- отбеливание репутации: нарушитель информационной безопасности после деструктивного воздействия на систему и снижения его репутации выходит из системы и использует новую идентичность для повторного входа в систему с целью инициализации более высокого уровня доверия и репутации по сравнению с теми же показателями до выхода из системы.

Атаки на идентичность проводятся на основе использования одного или нескольких идентификаторов элемента системы. Они могут быть проведены следующими методами:

- атака Сибиллы: нарушитель информационной безопасности является сущностью, получающей в рамках системы несколько идентичностей для воспроизведения злонамеренного поведения и более успешного использования других методов атак;
- атака «человек посередине»: нарушитель информационной безопасности перехватывает поток определенных служебных сообщений «честных» элементов системы и модифицирует их, в результате чего репутация и доверие «честного» элемента КФС понижается;
- подмена идентификатора: нарушитель информационной безопасности использует подмену идентификаторов, несанкционированный доступ к элементам системы и другие методы для снижения уровня доверия и репутации жертвы.

Выводы. Доверительная модель управления является широко используемой в кибер-физических системах. Задача управления доверием становится сложной из-за особенностей такого класса систем: количество элементов системы легко масштабируется, а окружающая среда быстро изменяется. В работе представлен обзор существующих методов проведения атак на кибер-физические системы с доверительной моделью управления, который послужит основой для разработки методики обнаружения различных типов атак на доверительную модель управления.

Усова М.А. (автор)

Викснин И.И. (научный руководитель)