КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ МИКРОКОНТРОЛЛЕРОВ

Котенко И.В.[1], Левшун Д.С.[2], Чечулин А.А.[3], Ушаков И.А.[4], Красов А.В.[5]

Цель статьи *заключается в разработке комплексного подхода к обеспечению безопасности киберфизических систем на основе микроконтроллеров.*

Метод исследования: *системный анализ современных атак на киберфизические системы на основе микроконтроллеров и подходов к обеспечению их безопасности, разработка собственного подхода и его экспериментальная проверка.*

Полученный результат: *предложена обобщенная архитектура системы для управления инцидентами и противодействия целевым атакам в распределенных крупномасштабных критически важных системах, реализующая комплексный подход. Рассмотрена реализация данной архитектуры в рамках системы управления инцидентами безопасности для комплексной защиты элементов Умного дома, в том числе реализация надежной и доверенной шины данных, компонента обработки и корреляции событий безопасности, гибридного хранилища данных, компонента интеллектуального анализа событий безопасности, а также компонента расчета метрик безопасности.*

Область применения *предложенного комплексного подхода – формирование функциональных и нефункциональных требований к киберфизическим системам на основе микроконтроллеров, которые могут быть использованы в качестве входных данных для методик проектирования подобных систем, например DLSEDS (Design Lifecycle of Secure Embedded Devices System).*

Ключевые слова: *проектирование защищенных систем, целевые атаки, корреляция событий безопасности, интеллектуальный анализ событий безопасности, шина данных, гибридное хранилище, метрики безопасности, контрмеры, Интернет вещей, Умное здание.*

DOI: 10.21681/2311-3456-2018-3-29-38

Введение

Современные атаки на киберфизические системы для управления производственным процессом происходят одновременно на нескольких уровнях – от незаконного проникновения на территорию предприятия, до эксплуатации уязвимостей на уровне компьютерной сети. При этом сами атаки являются сложными, многошаговыми и растянутыми во времени, а также учитывают особенности целевой системы и её инфраструктуру. Для своевременного обнаружения таких атак, системам защиты необходимо анализировать совместно информацию, поступающую от множества гетерогенных источников как физического, так и кибернетического уровня [1]. При этом в большинстве существующих систем защиты, системы физической и кибернетической безопасности работают независимо друг от друга [2].

Поэтому, для соответствия современным вызовам, требуется реализовать комплексный подход к обеспечению киберфизической безопасности. С одной стороны, комплексность подхода заключается в совместном сборе, анализе и обработке событий систем физической и кибернетической безопасности в рамках единой системы. С другой стороны, не менее важным является учет необходимости обеспечения защищенности такой системы к атакам на неё ещё на этапе проектирования [3].

Отметим, что данная задача сама по себе является комплексной. Так, одной из ключевых особенностей микроконтроллеров является тот факт, что их функциональность определяется не только программной, но и аппаратной составляющей. При этом связи между программной частью устройства, с одной стороны, и аппаратной, с другой, обуславливают наличие дополнительных ограничений, влияющих существенным образом на процесс проектирования таких устройств. Это означает, что применение существующих решений для разработки безопасного программного обеспечения при создании защищенных систем на основе ми-

1 Котенко Игорь Витальевич, доктор технических, профессор, заведующий лабораторией проблем компьютерной безопасности, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

2 Левшун Дмитрий Сергеевич, младший научный сотрудник, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: levshun@comsec.spb.ru

3 Чечулин Андрей Алексеевич, кандидат технических наук, ведущий научный сотрудник, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: chechulin@comsec.spb.ru

4 Ушаков Игорь Александрович, старший преподаватель ФГБОУ ВО Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия. E-mail: ushakovia@gmail.com

5 Красов Андрей Владимирович, кандидат технических наук, доцент, заведующий кафедрой Защищенных систем связи, ФГБОУ ВО Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия. E-mail: krasov@inbox.ru

кроконтроллеров не позволит обеспечить их безопасность в полной мере.

Кроме того, существуют методики проектирования защищенных устройств на основе микроконтроллеров, применимые при компонентном подходе (например, в рамках платформ Arduino, Raspberry Pi, Beaglebone и Intel Galileo). Основная цель данных методик – выявление перечня возможных атак, которым может быть подвержено устройство, в соответствии с выбранной моделью нарушителя, а также используемыми программно-аппаратными компонентами ещё на этапе проектирования [4]. Ключевым недостатком компонентного подхода с точки зрения безопасности является его предопределенность, позволяющая злоумышленнику учитывать его при проведении атаки. Кроме того, применение подобных методик и дальнейшее объединение в рамках единой системы множества защищенных устройств не позволит разработать защищенную систему, т.к. не были учтены эмерджентные свойства полученной системы.

Одним из возможных решений проблемы учета эмерджентных свойств являются методики разработки и верификации сетевых систем на основе микроконтроллеров, исследования которых получили широкое распространение в последнее время. Основной целью данных методик является предоставление разработчикам информации о применимости отдельных интерфейсов и протоколов передачи данных для обеспечения соответствующего уровня надежности итоговой системы [5]. При этом безопасность системы не является непосредственной целью данных методик, однако отдельные аспекты безопасности учитываются при выборе интерфейсов и протоколов передачи данных. Однако, методики данного типа позволяют обеспечить надежность систем, состоящих только из микроконтроллеров, не рассматривая их взаимодействие с удаленными серверами, рабочими станциями и вебсервисами.

Подытоживая вышесказанное, отметим, что на данный момент не существует единого комплексного подхода к обеспечению безопасности киберфизических систем на основе микроконтроллеров, а существующие решения не лишены недостатков и нуждаются в доработке. В рамках данной статьи рассматривается реализация комплексного подхода к обеспечению безопасности на начальном этапе – этапе формирования требований к системе. Предлагается обобщенная архитектура системы для управления инцидентами и противодействия целевым атакам в распределенных крупномасштабных критически важных системах, позволяющая обеспечить необходимый функционал и взаимодействие с внешними системами. Кроме того, представляется реализация данной архитектуры в рамках прототипа системы управления инцидентами безопасности для комплексной защиты элементов Умного дома.

Обобщенная архитектура системы

Существующие системы управления инцидентами безопасности преимущественно имеют трехуровневую архитектуру «агент» – «сервер» – «база (хранилище) данных», которая разворачивается поверх корпоративной сети, при необходимости включая филиалы. Агенты осуществляют сбор данных об инцидентах безопасности, выполняют их первоначальную обработку и фильтрацию, после чего передают на анализ серверу приложений, который является основой системы. Сервер приложений анализирует собранную с помощью агентов информацию и преобразует ее в более высокоуровневое и удобное для анализа представление. Вся информация, собранная агентами, а также результаты анализа ее сервером приложений сохраняются в хранилище (базе данных, хранилище).

На основе данных архитектурных уровней и особенностей перспективных систем управления инцидентами безопасности критически важных объектов, представляется целесообразным выделить в архитектуре следующие компоненты:

- внешние источники данных (сенсоры);
- надежная и доверенная шина данных;
- компонент обработки и корреляции событий безопасности;
- гибридное хранилище данных;
- компонент интеллектуального анализа событий безопасности;
- компонент расчета метрик безопасности;
- компонент выбора контрмер;
- внешние системы, реализующие выбранные контрмеры.

Рассмотрим цикл обработки данных в перспективной системе управления инцидентами безопасности критически важных объектов, включающих все вышеперечисленные компоненты (рис. 1).

Поток данных начинается с внешних сенсоров, предоставляющих события безопасности от физических и кибернетических систем безопасности в разных форматах. Затем через внешние компоненты системы события безопасности поступают на надежную и доверенную шину данных. Далее через шину данных события безопасности поступают в компонент обработки и корреляции событий безопасности [6], а затем в гибридное хранилище информации и событий безопасности [7]. После этого данные обрабатываются в компоненте интеллектуального анализа событий безопасности. В указанном компоненте производится обнаружение в реальном времени сложных многошаговых целевых атак на основе технологий интеллектуального анализа информации и событий безопасности, а также, анализ истории событий безопасности и прогнозирование действий нарушителей и их последствий [8,9]. Данные, получаемые от компонентов корреляции событий, интеллектуального анализа событий и гибридного хранилища отправляются в компонент расчета метрик безопасности для расчета первичных и интегрированных метрик безопасности [10]. Обнаруженные атаки, рассчитанные метрики и результаты анализа истории и прогнозирования действий нарушителей поступают в компонент выбора контрмер, где осуществляется автоматизированный выбор наиболее эффективных контрмер для противодействия целевым информационно-программным и физическим воздействиям. Далее, выбранные контрмеры отправляются внешним системам безопасности, реализующим выбранные контрмеры.

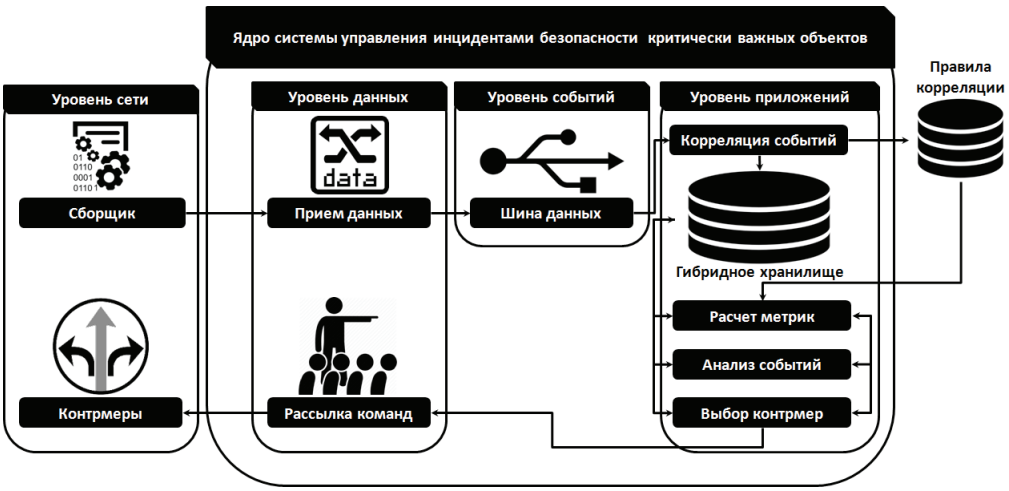

Рис. 1. Обобщенная архитектура перспективной системы управления инцидентами безопасности критически важных объектов

Комплексный подход

Реализация предложенной архитектуры в рамках системы управления инцидентами безопасности для комплексной защиты элементов Умного дома, состоит из нескольких основных частей (рис. 2):

1. аппаратных источников информации (АИ);
2. программных источников информации (ПИ);
3. концентраторов (HUB):;
4. центрального сервера Умного дома;
5. модуля аналитической обработки данных и визуализации (АОДВ);
6. модуля интеграции с системами управления информацией и событиями безопасности (СУИСБ).

При этом на уровне сбора данных расположены аппаратные и программные источники информации; на уровне управления данными — концентраторы; а на уровне анализа данных — сервер Умного дома, модуль АОДВ и модуль интеграции с СУИСБ.

В соответствии с обобщенной архитектурой перспективной системы управления инцидентами безопасности, компоненты сбора данных должны поддерживать следующие операции:

1. автоматическая коррекция погрешности;
2. самовосстановление при возникновении единичного дефекта;
3. автоматическая оптимизация параметров и алгоритмов работы.

Реализация данных компонентов в рамках системы управления инцидентами безопасности для комплексной защиты элементов Умного дома представлена в виде аппаратных и программных источников информации. Их задача – сбор данных от гетерогенных источников и их последующая передача на центральный сервер. Примеры событий: срабатывание извещателя в определенном режиме работы системы; выход показаний датчика за допустимые пределы; нелегитимный переход между состояниями пользователя в системе; потеря связи с устройством; и т.д.

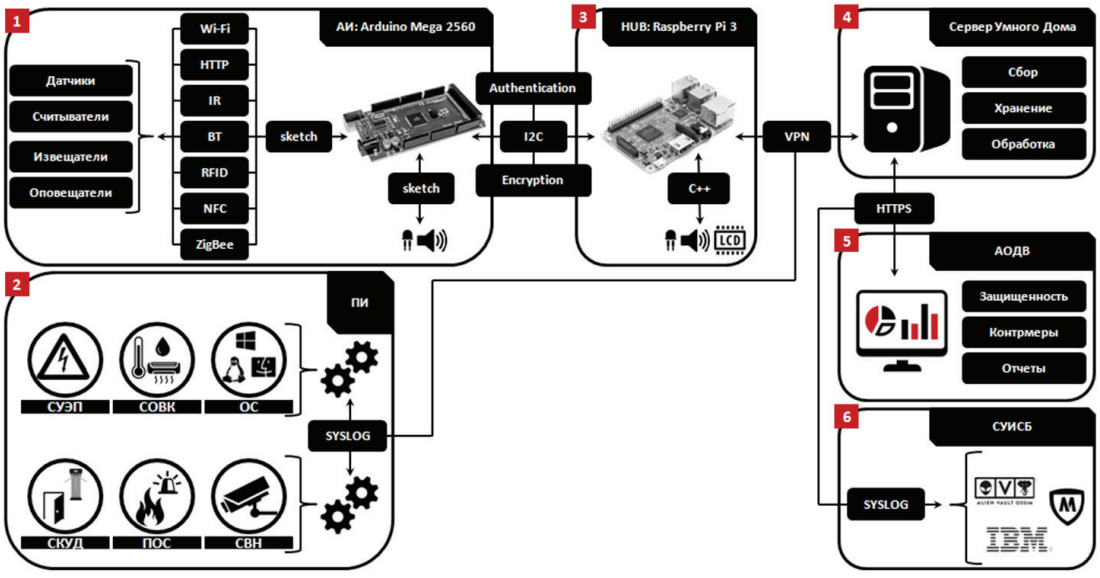

Рис. 2. Взаимодействие элементов системы управления инцидентами безопасности для комплексной защиты элементов Умного дома

Аппаратные источники, представляющие собой микроконтроллеры платформы Arduino[6], подключаются к системам Умного дома на уровне извещателей, оповещателей, датчиков и внешних электронных компонентов посредством специальных адаптеров, позволяя собирать показания системы контроля и управления доступом и системы отопления, вентиляции и кондиционирования. При этом каждый адаптер соответствует стандартному проводному или беспроводному интерфейсу передачи данных, используемому в рамках концепции Интернета вещей.

Программные источники информации подключаются к системам дома посредством специальных драйверов, позволяя собирать показания агентов рабочих станций, а также события серверов баз данных, серверов приложений и web-сервисов. При этом драйверы могут использовать как уже существующие интерфейсы программирования приложений, так и специально разработанные агенты для сбора необходимых данных. Надежность и достоверность соединения между программными источниками информации и сервером Умного дома обеспечивается за счет VPN-соединения на основе технологии OpenVPN[7].

Для обеспечения надежного и доверенного сбора данных от внешних сенсоров предлагается использовать шину данных. При этом в соответствии с обобщенной архитектурой, доверенность шины данных обеспечивается за счет применения следующих решений:

1. взаимной аутентификации устройств на основе MAC;
2. надежного шифрования передаваемых данных на основе открытых и закрытых ключей.

Надежность шины данных, в соответствии с обобщенной архитектурой, достигается за счет применения следующих решений:

1. динамической адресации подключенных устройств;
2. мониторинга состояния подключенных устройств;
3. отсутствия неконтролируемых потерь показаний датчиков, извещателей, оповещателей и считывателей;
4. проверки целостности передаваемых данных.

В рамках разработанного прототипа системы управления инцидентами безопасности для комплексной защиты элементов Умного дома, аппаратные источники информации и концентраторы объединены надежной, доверенной шиной данных на основе протокола I2C[8]. При таком соединении, один из аппаратных интерфейсов выступает в качестве главного микроконтроллера последовательной шины данных, а соединенные с ним микроконтроллеры в качестве подчиненных. При этом допустимый диапазон адресов подчиненных микроконтроллеров лежит в диапазоне от 8 до 127 (рис. 3). Для минимизации избыточности сообщений, в рамках разработанного протокола, производится предобработка каждого сообщения методом прямой коррекции ошибок, присваивающей номера пакетам. А переотправка пакетов осуществляется только тогда, когда данные можно восстановить только из потерянного подмножества переданных пакетов.

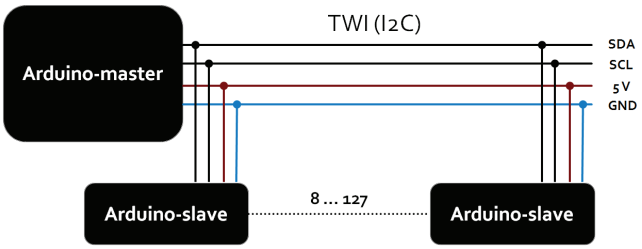

Рис. 3. Надежная, доверенная шина данных на основе протокола I2C

Потоковая обработка данных осуществляется в рамках технологии Complex Event Processing [11]: данные, собранные аппаратными источниками информации, передаются по защищенному каналу на концентраторы, задача которых снизить нагрузку на сервер Умного дома за счет предварительной обработки, обобщения и нормализации. Предварительная обработка и обобщение данных, в соответствии с обобщенной архитектурой, заключаются в применении следующих операций:

1. операция добавления метки времени и идентификатора источника к показаниям извещателей, оповещателей и считывателей систем;
2. операция добавления метки времени и идентификатора источника к показаниям агентов рабочих станций системы;
3. операция добавления метки времени и идентификатора источника к событиям серверов баз данных, серверов приложений и web-сервисов системы.

В рамках процесса нормализации данных, в соответствии с обобщенной архитектурой, применяются следующие методы:

1. метод приведения показаний датчиков, извещателей, оповещателей и считывателей систем к общесистемному формату;
2. метод приведения показаний агентов рабочих станций системы к общесистемному формату;
3. метод приведения событий серверов баз данных, серверов приложений и web-сервисов к общесистемному формату.

Сервер Умного дома подвергает процессу фильтрации данные, собранные посредством аппаратных и программных источников информации, перед их непосредственной записью в гибридное хранилище. Фильтрация данных основывается на операции удаления нерелевантных данных в соответствии с заранее заданными правилами.

В соответствии с обобщенной архитектурой, гибридное хранилище должно быть разработано по методике построения, ориентированной на концепцию сервис-ориентированной архитектуры. Данная концепция выделяет в архитектуре гибридного хранилища следующие уровни: уровень хранения и уровень

6 Официальный сайт сообщества разработчиков решений на основе микроконтроллеров платформы Arduino. – URL: https://www.arduino.cc. (дата обращения: 28.05.2018).

7 Официальный сайт проекта OpenVPN. – URL: https://openvpn.net/. (дата обращения: 28.12.2017).

8 Официальная документация по библиотеке Wire.h, реализующей взаимодействие по протоколу I2C между микроконтроллерами платформы Arduino. – URL: https://www.arduino.cc/en/Reference/Wire. (дата обращения: 28.05.2018).

реализации веб-сервисов. Уровень хранения включает в себя реляционную базу данных, базу XML-данных и базу RDF-данных. Уровень реализации веб-сервисов содержит компоненты доступа к данным, реализации веб-сервисов и представления данных. В рамках разработанного прототипа системы управления инцидентами безопасности для комплексной защиты элементов Умного дома, гибридное хранилище основано на технологии OpenLink Virtuoso9. При этом реляционная база данных отвечает за хранение показаний датчиков, извещателей, оповещателей, считывателей и агентов рабочих станций; хранение событий серверов баз данных, серверов приложений и web-сервисов системы; хранение событий и инцидентов полученных на основе процесса корреляции событий безопасности. База XML-данных отвечает за хранение правил процесса корреляции событий безопасности, а также за хранение шаблонов многошаговых атак. База RDF-данных отвечает за хранение знаний о взаимосвязи элементов системы с объектом защиты, а также за хранение знаний о возможных конфликтах между элементами системы. Применение гибридного хранилища позволяет методам, моделям, методикам и алгоритмам анализа истории событий безопасности, прогнозирования действий нарушителей и их последствий иметь релевантный источник данных, позволяющий повысить оперативность анализа и выявлять в режиме реального времени наиболее вероятный следующий шаг атаки, изъяны системы защиты, а также точки входа нарушителей.

В соответствии с предложенной архитектурой перспективной системы управления инцидентами безопасности критически важных объектов, данные, записанные в гибридное хранилище, подвергаются процессу корреляции событий безопасности для выявления инцидентов безопасности, сценариев атак и аномальной активности. При этом к использованию рекомендуются следующие методы [12-15]:

1. методы на основе машины конечных состояний;
2. методы на основе правил;
3. методы на основе Байесовской и нейронной сети.

Существо метода на основе правил заключается в преобразовании политики безопасности организации в правила, понятные модулю обработки событий. Эти правила позволяют, например, формировать конечные состояния сотрудников или гостей объекта защиты в рамках системы. При этом возможные переходы между полученными конечными состояниями задаются с помощью методов на основе конечных автоматов. Конечные состояния, а также возможные переходы между ними, позволяют в режиме реального времени выявлять нарушения политики безопасности объекта защиты.

Методы на основе Байесовской или нейронной сети могут использоваться для выявления аномальной активности в рамках Умного дома. Предполагается, что обнаружение аномалий позволит выявлять атаки, использующие недостатки политики безопасности объекта защиты. В основе Байесовской сети лежит модель направленного ациклического графа. Суть метода заключается в расположении в вершинах графа признаков. При этом связывающие их направленные дуги представляют собой отношение условной независимости одного признака от другого. В основе нейронной сети лежит математическая модель, также состоящая из признаков, имеющих собственное состояние, и линий связи, определяющих зависимость одних признаков от других. При реализации данных методов в рамках системы управления инцидентами безопасности для комплексной защиты элементов Умного дома, в качестве переменных или искусственных нейронов используются как отдельные события или атаки, характерные для модуля обработки центрального сервера, так и обобщенные характеристики множества событий и атак. Рассмотрим несколько примеров.

Пример 1. В соответствии с политикой безопасности, сотрудник предприятия может находиться в одном из четырех состояний (рис. 4): – сотрудник вошел в здание; – сотрудник начал сеанс работы с операционной системой; – сотрудник завершил сеанс работы с операционной системой; – сотрудник вышел из дома.

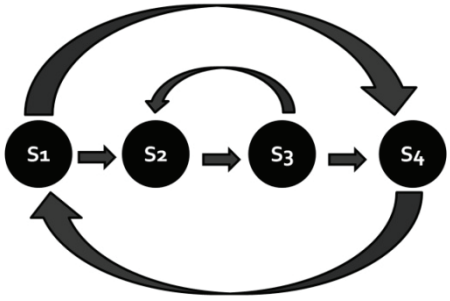

Рис. 4. Конечный автомат

В течение рабочего дня, модуль обработки событий с помощью методов на основе правил и машины конечных состояний выявил подозрительную активность: от операционной системы пришло событие об авторизации учетной записи секретаря, притом, что события о входе секретаря в здание от системы контроля и управления доступом не приходило. Это означает, что переход в состояние был осуществлен некорректным образом, т.е. была нарушена политика безопасности. На основе этих фактов система управления инцидентами безопасности для комплексной защиты элементов Умного дома создает инцидент безопасности и формирует рекомендацию о необходимости анализа записей, поступивших от системы видеонаблюдения за данный период времени.

Пример 2. В течение рабочего дня сотрудник вошел в здание (состояние S_1) и авторизовался на рабочем месте (состояние S_2). При этом модуль обработки событий с помощью методов на основе Байесовской и нейронной сетей обнаружил аномальную сетевую активность: трафик от компьютера сотрудника к базе данных, хранящей персональные данные сотрудников организации. Такой трафик является аномальным, так как при нормальном функционировании системы доступ к базе данных осуществляется через специальное клиентское приложение. На основе этих фактов система управления инцидентами безопасности для комплексной защиты элементов Умного дома создает инцидент безопасности и формирует вывод о необходимости блокировки учетной записи данного сотрудника до выяснения причин.

9 Официальный сайт проекта OpenLink Virtuoso. – URL: https://virtuoso.openlinksw.com. (дата обращения: 28.12.2017).

Также, в рамках процесса корреляции событий безопасности, в соответствии с обобщенной архитектурой, применяются следующие правила для выявления ложных срабатываний датчиков или их подмены:

1. правила сопоставления показаний одинаковых датчиков;

2. правила сопоставления изменений показаний одних датчиков с данными от датчиков, показания которых также должны были измениться.

Рассмотрим несколько примеров.

Пример 3. Система управления инцидентами безопасности для комплексной защиты элементов Умного дома получает информацию от системы пожарной сигнализации о наличии пожара в одном из помещений. При этом на основании данных от системы отопления, вентиляции и кондиционирования известно, что в момент поступления сигнала о пожаре в помещении температура и влажность оставались в пределах нормы. На основе этих фактов система управления инцидентами безопасности для комплексной защиты элементов Умного дома создает инцидент безопасности и формирует вывод о необходимости проверки пожарного извещателя на предмет ложных срабатываний, а также формирует рекомендацию о необходимости анализа записей, поступивших от системы видеонаблюдения за данный период времени.

Пример 4. Нарушитель с целью формирования отказа в обслуживании на стороне чувствительного серверного оборудования подменил информацию от датчиков температуры системы отопления, вентиляции и кондиционирования, установленных на объекте защиты. Система управления инцидентами безопасности для комплексной защиты элементов Умного дома получает информацию от системы отопления, вентиляции и кондиционирования о достижении оптимального диапазона температур в серверном помещении. С целью повышения энергоэффективности, кондиционирование помещения было временно приостановлено. При этом на основании данных от операционных систем источников бесперебойного питания и серверов известно, что температура в помещении постепенно увеличивается, что не соотносится с данными от системы отопления, вентиляции и кондиционирования. На основе этих фактов система управления инцидентами безопасности для комплексной защиты элементов Умного дома создает инцидент безопасности и формирует вывод о необходимости проверки датчиков температуры системы отопления, вентиляции и кондиционирования в серверном помещении на предмет ложных срабатываний, а также формирует рекомендацию о необходимости анализа записей, поступивших от системы видеонаблюдения за данный период времени.

Однако как уже было упомянуто ранее, на данный момент широкое распространение получили комплексные атаки, одновременно происходящие на разных уровнях – от незаконного проникновения в помещение до эксплуатации уязвимостей на уровне компьютерной сети. При этом при построении перспективных систем управления инцидентами безопасности критически важных объектов необходимо также учитывать многошаговость таких атак. С этой целью в модуле обработки на сервере Умного дома, в соответствии с обобщенной архитектурой, используются элементы аналитического моделирования. Так, посредством методики обнаружения в реальном времени сложных многошаговых целевых атак на основе технологий интеллектуального анализа информации и событий безопасности осуществляется сравнение цепочки обнаруженных событий с хранимыми в гибридном хранилище шаблонами многошаговых атак с целью ещё на ранних этапах выявить наиболее вероятный следующий шаг атаки. Рассмотрим пример многошаговой атаки.

Пример 5. От системы контроля и управления доступом на сервер Умного дома поступило уведомление о подозрительной, но легитимной активности:

1. на объект защиты осуществлен вход в нерабочее время по карте сотрудника с правами администратора;

В дальнейшем, на сервер Умного дома от системы контроля и управления доступом поступило ещё одно уведомление о подозрительной, но легитимной активности:

2. в серверное помещение объекта защиты в нерабочее время был осуществлен вход по карте сотрудника с правами администратора, при этом данные карты совпадают с данными, предоставленными при входе на объект защиты;

Далее на сервер Умного дома от системы отопления, вентиляции и кондиционирования серверной поступило уведомление о подозрительной, но легитимной активности:

3. режим работы кондиционеров был изменен на «обогрев»;

Спустя некоторое время на сервере Умного дома на основе данных от системы отопления, вентиляции и кондиционирования серверной был сформирован инцидент безопасности:

4. температура в серверном помещении вышла за пределы допустимого диапазона;

Ещё некоторое время спустя на сервер Умного дома от подсистемы мониторинга сетевого оборудования начинают приходить уведомления:

5. отказ в обслуживании со стороны сетевого оборудования.

Подозрительная, но легитимная активность шагов 1-3 многошаговой атаки, при использовании только стандартных средств защиты, позволит системе управления инцидентами безопасности для комплексной защиты элементов Умного дома выявить вредоносную активность только после наступления 4 шага, а сценарий атаки после наступления 5 шага. Однако благодаря методике обнаружения в реальном времени сложных многошаговых целевых атак, при осуществлении сравнения цепочки подозрительной активности на шагах 1-3 с хранимым в гибридном хранилище шаблоном соответствующей многошаговой атаки, атака будет обнаружена на более ранней стадии. Это позволит уведомить отдел защиты и избежать отказа в обслуживании со стороны сетевого оборудования.

Методика обнаружения в реальном времени сложных многошаговых целевых атак, в соответствии с обобщенной архитектурой, опирается на следующие модели, методики и алгоритмы:

1. модели для прогнозирования действий нарушителя;

2. методы, методики и алгоритмы анализа истории событий безопасности для формирования профиля нарушителя;

3. методики определения наиболее вероятных предыдущих и последующих действий нарушителя;

4. методы, методики и алгоритмы определения последствий возможных действий нарушителя;

5. методы, методики и алгоритмы анализа истории событий безопасности для связи событий безопасности с одним или разными нарушителями.

На основе полученных результатов, в модуле аналитической обработки данных и визуализации генерируются отчеты, вырабатываются контрмеры и осуществляется оценка защищенности охраняемого объекта.

При этом в качестве первичных метрик безопасности используются следующие метрики:

1. метрика нахождения показаний температуры воздуха в пределах заданного интервала;

2. метрика нахождения показаний влажности воздуха в пределах заданного интервала;

3. метрика нахождения концентрации определенных газов в пределах заданного интервала;

4. метрика успешной или неуспешной попытки начала сеанса с операционной системой;

5. метрика успешной или неуспешной попытки прохода в помещение;

6. метрика отсутствия срабатываний датчика движения в пределах заданного временного интервала.

В качестве интегрированных метрик безопасности, в соответствии с обобщенной архитектурой, используются следующие метрики:

1. метрика отсутствия нелегитимных переходов пользователей системы между допустимыми состояниями;

2. метрика наличия или отсутствия противоречий между показаниями источников данных;

3. метрика общего числа зафиксированных инцидентов безопасности определенной критичности;

4. метрика среднего числа зафиксированных инцидентов безопасности определенной критичности;

5. метрика процентного отношения числа зафиксированных инцидентов безопасности определенной критичности на отдельном устройстве к числу зафиксированных инцидентов безопасности определенной критичности в системе или подсистеме в целом.

При этом методики вычисления интегрированных метрик безопасности будут основаны на методиках вычисления первичных метрик и общем подходе, объединяющим метрики, вычисленные в соответствии с имеющимися в конкретный момент времени данными.

Такой подход позволит иметь адекватную имеющимся данным интегрированную оценку защищенности в заданный момент времени за счет применения следующих методов:

1. анализа статистических данных для выявления текущих показаний и динамики их изменения;

2. анализа произошедших инцидентов для выявления изъянов системы защиты и точек входа нарушителя;

3. анализа ущерба в результате воздействий на инфраструктуру системы;

4. анализа ущерба в результате воздействий на элементы инфраструктуры системы;

5. анализа ущерба в результате воздействий на сервисы системы.

В соответствии с обобщенной архитектурой, в процессе автоматизированного реагирования на целевые информационно-программные и физические воздействия в модуле аналитической обработки и визуализации данных системы будут осуществляться следующие операции:

1. уведомление оператора об обнаруженных инцидентах, сценариях атак и аномальной активности;

2. уведомление о необходимости усиления физического контроля инфраструктуры системы или её отдельных элементов;

3. уведомление о необходимости изменения правил доступа к сервисам системы.

Выводы

Методы, модели, методики, алгоритмы и архитектуры, выбранные в соответствии с обобщенной архитектурой перспективной системы управления инцидентами безопасности критически важных объектов, могут быть успешно реализованы для управления инцидентами безопасности в рамках комплексной защиты элементов Умного дома. При этом комплексность защиты достигается за счет:

1. анализа событий в режиме реального времени для обнаружения сложных многошаговых атак на ранних этапах развития (проактивность);

2. адаптивности мер защиты к состоянию объекта защиты (динамичность);

3. совместного анализа событий физического и кибернетического уровня (многоаспектность).

Динамический подход в управлении инцидентами реализован за счет применения облачных сервисов, которые позволяют поддерживать в актуальном состоянии следующие базы знаний:

- базы знаний правил процесса корреляции событий безопасности;
- базы знаний шаблонов многошаговых атак;
- базы знаний возможных конфликтов между элементами системы.

В качестве основы для проектирования прототипа Умного дома, как объекта управления инцидентами безопасности, были выбраны встроенные устройства на основе микроконтроллеров платформы Arduino в качестве аппаратных источников информации и встроенные устройства на основе одноплатного компьютера платформы Raspberry Pi в качестве концентраторов и серверов. Выбранные встроенные устройства позволяют организовать коммуникации в рамках структурированной кабельной системы по протоколу I2C, программно-аппаратная реализация которого на физических устройствах обеспечивает возможность подключения до 128 микроконтроллеров платформы Arduino к одному одноплатному компьютеру платформы Raspberry Pi. Целевая система представляет собой совокупность систем управления зданием, содержащую большое количество разнородных контролирующих, считывающих и управляющих устройств. В основе данной системы лежит трехуровневая модель, представленная в рамках обобщенной архитектуры. Нижний уровень данной системы представлен программными и аппаратными источниками информации, предназначенными для подключения к различ-

ным система Умного дома. На промежуточном уровне реализована сетевая инфраструктура, объединяющая отдельные программные и аппаратные источники информации в единую систему сбора, хранения и предобработки информации и событий безопасности. Верхний уровень представляет собой сервер Умного дома, позволяя реализовать процесс управления инцидентами безопасности.

Предложенный комплексный подход позволяет сформировать функциональные и нефункциональные требования к подобным системам. Данные требования могут быть направлены на вход методикам проектирования защищенных систем на основе встроенных устройств, например DLSEDS [16]. Подход DLSEDS представляет собой объединение подхода к разработке безопасного программного обеспечения, методики проектирования защищенных встроенных устройств, а также разработанной авторами методики проектирования защищенной системы на основе встроенных устройств. При этом последняя методика выступает связующим звеном, формулирующим требования как к методике проектирования защищенных встроенных устройств, так и к подходу к разработке безопасного программного обеспечения, а также обеспечивает защищенность среды передачи данных между элементами системы.

Кроме того, полученные результаты могут быть интересны компаниям, а также физическим лицам, которые занимаются разработкой и внедрением систем Умного дома. Внедрение данных результатов позволит повысить защищенность охраняемого объекта, объединить разнородные физические и кибернетические источники данных в единую систему комплексной защиты, а также упростить управление информацией, касающейся событий и инцидентов безопасности за счет интеллектуальных методов их обработки.

Кроме того, подход к разработке системы управления инцидентами безопасности для комплексной защиты элементов Умного дома также можно использовать в обучающих и исследовательских целях в области информационной безопасности, Интернета вещей и встроенных устройств.

Также, результаты работы прототипа системы управления инцидентами безопасности для комплексной защиты элементов Умного дома могут быть использованы в качестве входных данных для систем управления информацией и событиями безопасности. Интеграция с системами такого типа необходима для более детальной и высокоуровневой обработки обнаруженных инцидентов безопасности, сценариев атак и аномальной активности.

Рецензент: *Молдовян Александр Андреевич, доктор технических наук, профессор, заведующий отделом проблем информационной безопасности ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург, Россия. E-mail: maal305@yandex.ru*

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482 и 18-07-01488) и бюджетной темы АААА-А16-116033110102-5.

Литература

1. Kotenko I.V., Levshun D.S., Chechulin A.A. Event correlation in the integrated cyber-physical security system // Soft Computing and Measurements (SCM), 2016 XIX IEEE International Conference on. – IEEE, 2016. – С. 484-486.
2. Desnitsky V.A., Levshun D.S., Chechulin A.A., Kotenko I.V. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System // JoWUA. – 2016. – Т. 7. – №. 2. – С. 60-80.
3. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. – 2016. – Т. 5. – №. 48. – С. 5-31.
4. Ruiz J.F., Desnitsky V.A., Harjani R., Manna A., Kotenko I.V., Chechulin A.A. A methodology for the analysis and modeling of security threats and attacks for systems of embedded components // Parallel, Distributed and Network-Based Processing (PDP), 2012 20th Euromicro International Conference on. – IEEE, 2012. – С. 261-268.
5. Stefanni F. A Design & Verification Methology for Networked Embedded Systems. Ph.D. Thesis. University of Verona, Department of Computer Science, Italy. – April 7, 2011. –143 с.
6. Kruegel C., Valeur F., Vigna G. Intrusion detection and correlation: challenges and solutions. – Springer Science & Business Media, 2004. – Т. 14.
7. Fedorchenko A.V., Kotenko I.V., Doynikova E.V., Chechulin A.A. The ontological approach application for construction of the hybrid security repository // Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on. – IEEE, 2017. – С. 525-528.
8. Kotenko I.V., Doynikova E.V., Chechulin A.A. Security metrics based on attack graphs for the Olympic Games scenario //Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. – IEEE, 2014. – С. 561-568.
9. Kotenko I.V., Chechulin A.A. Attack modeling and security evaluation in SIEM systems //International Transactions on Systems Science and Applications. – 2012. – Т. 8. – С. 129-147.
10. Kotenko I.V., Doynikova E.V. Selection of countermeasures against network attacks based on dynamical calculation of security metrics // The Journal of Defense Modeling and Simulation. – 2017. – С. 1-23. DOI: 10.1177/1548512917690278.
11. Buchmann A., Koldehofe B. Complex event processing // IT-Information Technology Methoden und innovative Anwendungen der Informatik und Informationstechnik. – 2009. – Т. 51. – №. 5. – С. 241-242.
12. Sadoddin R., Ghorbani A. Alert correlation survey: framework and techniques // Proceedings of the 2006 international conference on privacy, security and trust: bridge the gap between PST technologies and business services. Article No. 37. – ACM, 2006. – 15 с.
13. Müller A. Event correlation engine // Department of Information Technology and Electrical Engineering-Master's Thesis, Eidgenössische Technische Hochschule Zürich. – 2009.
14. Tiffany M. A survey of event correlation techniques and related topics // Research paper, Georgia Institute of Technology. – 2002.
15. Denise W. Guerer, Khan I., Ogler R., Keffer R. An artificial intelligence approach to network fault management // Sri international. – 1996. – Т. 86.
16. Levshun D.S., Chechulin A.A., Kotenko I.V. Design lifecycle for secure cyber-physical systems based on embedded devices //Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 9th IEEE International Conference on. – IEEE, 2017. – Т. 1. – С. 277-282.

INTEGRATED APPROACH TO PROVIDE SECURITY OF CYBER-PHYSICAL SYSTEMS BASED ON MICROCONTROLLERS

Igor Kotenko[10], Dmitry Levshun[11], Andrey Chechulin[12], Igor Ushakov[13],Andrey Krasov[14]

The purpose of the paper *consists in development of the integrated approach to provide security of cyber-physical systems based on microcontrollers.*

Research method: *systems analysis of modern attacks against cyber-physical systems based on microcontrollers and approaches to provide their security, development of the new approach and its experimental validation.*

The result obtained: *the paper considers an integrated approach for ensuring the security of cyber-physical systems based on microcontrollers. It proposes a generalized architecture of the system for managing incidents and counteracting targeted attacks in distributed large-scale critical systems. This architecture realizes the proposed approach. The implementation of this architecture is considered in the framework of the security incidents management system for complex protection of Smart Home elements, including the implementation of a reliable and trusted data bus, a security event processing and correlation, a hybrid data store, an intelligent security event analysis, and a security metrics calculation.*

The area of use of the proposed integrated approach is the formation of functional and non-functional requirements for cyber-physical systems based on microcontrollers, which can be directed as an input data of the design techniques for such systems development, for example, DLSEDS (Design Lifecycle of Secure Embedded Devices System).

Keywords: *the design of secure systems, advanced persistent threats, alert correlation, intelligent alert analysis, data bus, hybrid storage, security metrics, countermeasures, Internet of things, smart home.*

DOI: 10.21681/2311-3456-2018-3-XX-YY

References

1. Kotenko I.V., Levshun D.S., Chechulin A.A. Event correlation in the integrated cyber-physical security system // Soft Computing and Measurements (SCM), 2016 XIX IEEE International Conference on. – IEEE, 2016. – P. 484-486.
2. Desnitsky V.A., Levshun D.S., Chechulin A.A., Kotenko I.V. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System // JoWUA. – 2016. – T. 7. – №. 2. – P. 60-80.
3. Desnitsky V.A., Chechulin A.A., Kotenko I.V., Levshun D.S., Kolomeec M.V. Kombinirovannaya metodika proektirovaniya zashchishchennyh vstroennyh ustrojstv na primere sistemy ohrany perimetra // Trudy SPIIRAN. – 2016. – T. 5. – №. 48. – P. 5-31.
4. Ruiz J.F., Desnitsky V.A., Harjani R., Manna A., Kotenko I.V., Chechulin A.A. A methodology for the analysis and modeling of security threats and attacks for systems of embedded components // Parallel, Distributed and Network-Based Processing (PDP), 2012 20th Euromicro International Conference on. – IEEE, 2012. – P. 261-268.
5. Stefanni F. A Design & Verification Methology for Networked Embedded Systems. Ph.D. Thesis. University of Verona, Department of Computer Science, Italy. – April 7, 2011. – 143 p.
6. Kruegel C., Valeur F., Vigna G. Intrusion detection and correlation: challenges and solutions. – Springer Science & Business Media, 2004. – T. 14.
7. Fedorchenko A.V., Kotenko I.V., Doynikova E.V., Chechulin A.A. The ontological approach application for construction of the hybrid security repository // Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on. – IEEE, 2017. – P. 525-528.
8. Kotenko I.V., Doynikova E.V., Chechulin A.A. Security metrics based on attack graphs for the Olympic Games scenario //Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. – IEEE, 2014. – P. 561-568.
9. Kotenko I.V., Chechulin A.A. Attack modeling and security evaluation in SIEM systems //International Transactions on Systems Science and Applications. – 2012. – T. 8. – P. 129-147.
10. Kotenko I.V., Doynikova E.V. Selection of countermeasures against network attacks based on dynamical calculation of security metrics // The Journal of Defense Modeling and Simulation. – 2017. – P. 1-23. DOI: 10.1177/1548512917690278.
11. Buchmann A., Koldehofe B. Complex event processing // IT-Information Technology Methoden und innovative Anwendungen der Informatik und Informationstechnik. – 2009. – T. 51. – No. 5. – P.241-242.
12. Sadoddin R., Ghorbani A. Alert correlation survey: framework and techniques // Proceedings of the 2006 international conference on privacy, security and trust: bridge the gap between PST technologies and business services. Article No. 37. – ACM, 2006. – 15 p.

10 Igor Kotenko, Dr.Sc., Professor, Head of Laboratory of Computer Security Problems at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. E-mail: ivkote@comsec.spb.ru

11 Dmitry Levshun, Junior Research fellow at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, E-mail: levshun@comsec.spb.ru

12 Andrey Chechulin, Ph.D, Leading Research fellow at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. E-mail: chechulin@comsec.spb.ru

13 Igor Ushakov, Senior Lecturer at Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, Russia. E-mail:, ushakovia@gmail.com

14 Andrey Krasov, Ph.D, Associate Professor, Head of Secure Communication Systems department, Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, Russia. E-mail: krasov@inbox.ru

13. Müller A. Event correlation engine // Department of Information Technology and Electrical Engineering-Master's Thesis, Eidgenössische Technische Hochschule Zürich. – 2009.
14. Tiffany M. A survey of event correlation techniques and related topics // Research paper, Georgia Institute of Technology. – 2002.
15. Denise W. Guerer, Khan I., Ogler R., Keffer R. An artificial intelligence approach to network fault management. Sri international. – 1996. – Vol. 86.
16. Levshun D.S., Chechulin A.A., Kotenko I.V. Design lifecycle for secure cyber-physical systems based on embedded devices //Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 9th IEEE International Conference on. – IEEE, 2017. – Vol. 1. – P. 277-282.