Балуева А.В., Свинцов Ю.А.

**Управление событиями безопасности и построение защищенного протокола
передачи данных для системы Интернета вещей**

*Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
(Россия, Санкт-Петербург)*

doi:10.18411/lj-04-2018-130

idsp: 000001:lj-04-2018-130

Аннотация

В данной работе рассматриваются такие понятия как Интернет вещей, управление событиями безопасности, SIEM-система, инфракрасное дистанционное управление и его актуальность в настоящее время. В ходе работы рассмотрена реализация системы управления событиями безопасности, построен защищённый протокол передачи данных для ИК-канала связи.

Ключевые слова: Интернет вещей, SIEM-система, протокол передачи данных, ИК, умный дом, дистанционное управление.

I. Обзор литературы

При написании данной работы, были использованы статьи в периодических изданиях, статьи конференций и интернет-источники. Статьи [1] и [2] поясняют коммуникацию между устройствами в сфере Интернета вещей. В них подробно объясняются основные принципы коммуникации, а также предлагаются новые решения для системы умного дома. На основе статей [3], [4] и [5] были раскрыты основные принципы работы SIEM-систем. В статье [6] детально рассмотрено применение подхода управления событиями безопасности. Основным источником, раскрывающим теоретические основы инфракрасного излучения, явилась статья [7], где рассмотрено понятие инфракрасного излучения, его открытие и области применения. На основе работ [8], [9] и [10], в которых подробно рассказывается о взаимодействии ИК-передатчика и ИК-приёмника, а также варианты отправления кодированного сигнала, разработан собственный защищённый протокол передачи данных. В качестве защиты в протокол в процессе разработки была добавлена метка времени, информация по которой детально описана в статье [11].

II. Введение

В наше время происходит быстрое развитие информационных технологий. Современные мобильные устройства становятся всё более многофункциональными. Скорость и объем данных, которые они могут обрабатывать, быстро растут, и, в то же время, стоимость этих технологий снижается. Одной из областей развития информационных технологий является Интернет вещей, предназначенный для облегчения повседневных дел и устранения необходимости контроля человеком [1]. Большинство домашних приборов имеют свои процессоры, которые автоматизируют их работу. Это и является предпосылкой для создания единой системы управления с микроуправлением всех бытовых приборов. Основными преимуществами системы умного дома являются возможность автоматизировать работу различных устройств дома, таких как микроклимат, освещение, аварийные ситуации, функции безопасности и так далее. Это в свою очередь способствует повышению эффективности, надёжности, точности и скорости систем и, следовательно, ведёт к более комфортному существованию человека.

Однако, такое быстрое развитие информационных технологий в системе Интернета вещей, делает необходимым обеспечение надёжной системы безопасности. Классическим современным решением для управления безопасностью объектов являются системы управления информацией и событиями (SIEM), предназначенные для управления событиями безопасности в компьютерной системе.

Обе задачи, рассмотренные в данной статье направлены на решение различных проблем информационной безопасности в сфере IoT-систем. В пунктах III и IV описывается принцип работы SIEM-системы и её применение, в пунктах V-VIII описано проектирование защищённого протокола передачи информации по ИК-каналу связи.

III. Принцип работы SIEM-системы

Технология SIEM (security information and event management)-перспективная технология обеспечения безопасности в крупномасштабных системах. SIEM-система представляет собой централизованную консоль для просмотра, мониторинга и управления, связанных с безопасностью событий и журналов данных в масштабах предприятия. Поскольку SIEM-система обеспечивает анализ данных из нескольких источников, она позволяет быстро обнаруживать подозрительные модели поведения и реагировать на них, просматривая данные из отдельных систем. SIEM-системы также полезны для сбора и управления данными журналов в целях отчетности о соответствии.

SIEM собирают данные журнала с большого количества различных типов устройств. Транспортировка из журнала в SIEM должна быть конфиденциальной, аутентифицированной (для защиты от ложных журналов) и надежной.

Различные типы форматов журнала большинство SIEM-систем нормализуют к собственному формату. После нормализации начинается процесс агрегации. Его цель состоит в том, чтобы объединить различные события, имеющие общий тип. Это похоже на корреляцию, которая, однако, объединяет разные части (разные типы событий) одной атаки.

Существует несколько сообщений, которые могут указывать на попытки вторжения и/или другие проблемы безопасности. Например, можно отслеживать логины, которые входят в систему рано утром или поздно вечером, или по выходным. Кроме того, совокупность сообщений может показывать события, которые не заметны в отдельных сообщениях. Например, злоумышленник, пытающийся войти в учетную запись определенного пользователя, может попытаться угадать пароль. Так как неудачный вход в систему не является чем-то ненормальным (неправильное написание пароля может происходить, т.к. хорошие пароли, обычно, содержат много специальных символов), отдельного сообщения недостаточно. Но множество неудачных попыток входа в систему за малый промежуток времени скорее всего попытка вторжения.

Далее идёт процесс корреляции. Различные события журнала (различных типов) объединяются, чтобы сформировать атаку или инцидент безопасности. Этот процесс является довольно продвинутым и требует интенсивной обработки, поскольку он должен понимать, что принимать за атаку. Это достигается путем загрузки информации об угрозах из онлайн баз данных и использования контекстной информации (базы знаний).

SIEM информирует администраторов о том, что происходят/имели место атаки или странное поведение, тремя способами. Либо SIEM отправляет предупреждение, как только он понимает, что что-то не так, либо отправляет отчет в заданное время. Третий вариант, конечно, заключается в том, что администратор активно отслеживает SIEM в режиме реального времени (обычно через веб-интерфейс, поддерживающий различные роли учетных записей пользователей). Оповещения должны содержать необходимую информацию для дальнейших действий.

Некоторые продукты SIEM могут даже выполнять защитные (реактивные) действия (например, удалять вредоносные программы, закрывать порты) через подключенные устройства (сравнить IP-адреса). Конечно, это требует, чтобы SIEM контролировал устройства, а не просто пассивно прослушивал. Это означает, что это не только продукт безопасности, но и продукт управления сетью.

Отчеты, как правило, генерируются регулярно, но также могут выполняться «на лету». Обычно существуют сотни шаблонов отчетов для стандартных нужд, которые значительно ускоряют развертывание SIEM. Большинство продуктов SIEM предоставляют визуализацию общей статистики. Такие отчеты идеально подходит для быстрого обзора состояния администратором.

В процессе анализа данные обычно хранятся в сети, после чего архивируются. Данные могут храниться нормализованными (и агрегированными), чтобы ускорить доступ при повторном использовании. Обычно данные хранятся в сжатом и зашифрованном виде.

IV. Применение подхода

Рассмотрим реализацию системы на примере использования микроконтроллера Raspberry pi и сенсоров. Для этого был разработан программный компонент на платформе Android Things, который собирает данные с различных сенсоров. Для примера, в качестве сенсоров были использованы кнопка, фоторезистор, и программно-смоделированные сенсоры. При взаимодействии с данными сенсорами, производится сбор (регистрация) событий физической безопасности. После сбора, все данные передаются компоненту предобработки, который отфильтровывает их и нормализует (приводит к единообразному представлению). На этом этапе можно выявить сообщения, сигнализирующие о проблемах безопасности. Например, ненормальным поведением будет множество срабатываний одного сенсора за малый промежуток времени.

Далее идёт процесс корреляции, который объединяет события различных типов. Корреляция инцидентов безопасности производится на основе специализированных правил. Например, на данном этапе ненормальным событием будет являться одновременное срабатывание всех сенсоров, и такое событие послужит сигналом, что необходимо выполнить защитные действия.

После мониторинга и проверки событий, все отчёты об инцидентах безопасности сохраняются для возможности для возможности обзора состояния системы.

V. Инфракрасное излучение

Инфракрасное дистанционное управление (ИКДУ) является неотъемлемой частью Интернета вещей и применяется практически во всей бытовой электронной аппаратуре[2]. ИКДУ было выбрано для массового использования по понятным причинам – на то время (1970-е годы) ИК было самым надёжным и самым дешёвым видом беспроводной односторонней связи на короткие расстояния. Что же представляет из себя тепловое излучение? По сути это свет небольшой мощности и невидимый человеческому глазу (но видимый для камер)[7]. ИК-излучение не огибает предметы и не проходит сквозь них и распространяется по прямой, а его интенсивность уменьшается с расстоянием. Интенсивность излучения зависит так же и от типа источника, и режима его работы, поэтому расстояние, на котором можно уверенно принимать сигнал зависит от мощности источника и чувствительности ИК-приёмника (помимо побочных факторов). Для излучения инфракрасного света используются инфракрасные светодиоды, работающие в импульсном режиме, а для приёма – фотодиоды с усилителями. Фотодиоды в аппаратуре закрываются ИК-фильтрами (красным или дымчатым пластиком) для снижения чувствительности к солнечному или электрическому свету[8]. Фильтры как правило частично задерживают полезное ИК-излучение, поэтому от фильтра в том числе зависит дальность работы инфракрасного дистанционного управления.

VI. Использование ИК-канала связи

Прежде всего ИКДУ использовалось в бытовых телевизорах. И так как каждая фирма разрабатывала свой собственный ИКДУ протокол, на данный момент существует уже несколько десятков протоколов на разных частотах модуляции. Самые первые ИК-системы работали по принципу «есть излучение/нет излучения», т.е. передавалась одна команда – «включить» или «выключить». Такой вариант не обладал приемлемой помехозащищённостью и был совершенно не функционален. Требовалась разработка специальных последовательных протоколов, а также использование модуляции. Грубо говоря, ток светодиода модулируется дважды, сначала несущей частотой (30-60кГц), которая модулируется последовательностью битов команд. Но также существовали ИКДУ-системы и без модуляции, например, протокол ИТТ. Как правило, когда сигнал передаётся, это называют «Pulse», когда передача отсутствует – «Space». Во время Pulse подаётся несущая частота, светодиод вспыхивает с частотой 30-60кГц, а во время «Space»

ток на светодиоде отсутствует[9]. На приёмнике сигнал усиливается, демодулируется и на выходе получаем исходную последовательность импульсов.

VII. Кодирование импульсов и создание протокола

Итак, для осуществления отправки битов информации можно использовать два способа: «1» и «0» различаются либо длиной импульсного сигнала «Pulse», либо длиной паузы «Space»[10]. В данной работе для реализации кодирования битов информации будет использован первый вариант. Используя различную длину сигнала «Pulse», отправление битов будет выглядеть следующим образом:

Рисунок 1. Отправление сигнала

Чтобы отправить бит на приёмник, светодиод включается на определённое время, то есть на приёмник поступает импульс. «1» – сигнал длительностью 20мс, «0» – длительностью 150мс. После отправления нуля или единицы берётся «пауза» в 200мс, питание на светодиод не поступает и происходит разделение пришедших битов данных. Таким образом, приёмник получает импульсы разной длительности и записывает их как набор нулей и единиц.

VIII. Реализация защищённого протокола передачи данных

Выше было описано, как можно реализовать отставку «1» и «0», теперь рассмотрим создание самой структуры пакета данных. Предлагается пакет данных вида:

Рисунок 2. Предлагаемая структура пакета данных

В каждом секторе пакета находится определенное количество семизначных двоичных чисел. S и E – стартовая и конечная комбинации, они состоят из одного символа (двоичного представления ascii-кодировки) – «s» и «e» соответственно. Идентификатор пакета i состоит из одного массива длиной 7 бит и содержит длину сообщения для дальнейшей обработки. Поле payload содержит полезную нагрузку (сообщение) и может быть длиной от 1 до 127 символов (так как поле идентификатора не может иметь значение больше 127). Timestamp – последовательность символов, показывающая точное время создания пакета[11]. Так как при переводе из integer в binary получается большое двоичное число длиной в 31 бит, то удобнее разбить это число на пять «наборов» семизначных двоичных чисел с добавлением в первый набор четырех нулей во избежание искажения значения. Затем поля payload и timestamp складываются и хэшируются 128-битным алгоритмом md5 – так создаётся поле H длиной 32 символа. Итоговая длина пакета составляет от 287 до 1169 бит в зависимости от передаваемого сообщения. Обработка пакета на приёмнике собирает все единицы и нули. Затем все биты делятся на определённое количество семизначных двоичных чисел и декодируются в символы. В итоге в пакете будет находиться от 41 до 167 символов.

В качестве защиты, на приёмнике сначала проверяется структура пакета – считывание первого и последнего символа. Так же важна и метка времени, вложенная в

пакет. Она позволяет, в том числе, отражать атаки повторного воспроизведения – это атаки на систему аутентификации путём записи и последующего воспроизведения ранее посланных сообщений. Для этого считываются поля *payload* и *timestamp*, вычисляется хэш-сумма полученного сложения и сравнивается с тем, что находится внутри пакета. При любом несовпадении обработка пакета прерывается, и обработчик переходит к следующему пакету. Таким образом создан защищённый протокол передачи данных для ИК-интерфейса.

IX. Заключение

Мы живем в век быстрого развития технологий. Технология Интернета вещей включает в себя использования множества современной техники. В статье представлен общий подход к анализу событий безопасности и его реализация. Использование ИК-канала, а также множество различных датчиков позволяет реализовать автоматизацию и дистанционное управление между различными системами в доме, что повышает комфорт жильцов умного дома. Протокол, разработанный в ходе данной работы, имеет довольно небольшую скорость, но при наличии более продвинутого оборудования можно увеличить скорость отправления и объем информации.

1. Himadri Nath Saha, Supratim Auddy, Avimita Chatterjee and others – «IoT Solutions for Smart Cities». Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual, pp. 74-80.
2. Olena Starkova, Kostiantyn Herasymenko, Yekaterina Babailova – «Remote Control Systems of Household Appliances». 2017 4th International Scientific-Practical Conference, Kharkiv, Ukraine, 2017, pp. 585-588.
3. Henrik Karlzen – «An Analysis of Security Information and Event Management Systems». 2009 Department of Computer Science and Engineering CHALMERS UNIVERSITY OF TECHNOLOGY UNIVERSITY OF GOTHENBURG Göteborg, Sweden
4. Zegzhda D. P., Lavrova D. S – «Approach to Internet of Things Detection of Security Incidents Using SIEM Technology». 2017 Peter the Great St. Petersburg Polytechnic University St. Petersburg, Russia
5. «SIEM systems: Basic concepts and glossary», <https://learn.techbeacon.com/units/siem-systems-basic-concepts-glossary>
6. Десницкий В.А., Котенко И.В., Копчак Я.М. – «Анализ событий для управления инцидентами безопасности на примере системы контроля и управления доступом». 2016 Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)
7. «What is infrared?», <https://www.livescience.com/50260-infrared-radiation.html>
8. «Infrared remote control technology», <http://www.epanorama.net/links/irremote.html>
9. «IR Communication», <https://learn.sparkfun.com/tutorials/ir-communication>
10. «NEC протокол инфракрасного управления», https://led-displays.ru/ir/nec_protocol.html
11. Yuxiang Feng, Yukai Weng and others, «A Replay-Attack Resistant Authentication Scheme for the Internet of Things». 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), pp.541-547.

Димитриев А.П., Лавина Т.А.

О некоторых предпосылках для автоматизированной обработки данных

*Чувашский государственный университет имени И.Н. Ульянова
(Россия, Чебоксары)*

doi:10.18411/lj-04-2018-131

idsp: 000001:lj-04-2018-131

Аннотация

Возможность реализации алгоритмов обработки данных в среде разработки Turbo Delphi основана на ряде технических предпосылок. В статье рассмотрены элементы пользовательского интерфейса для работы с файлами, функции, реализующие операции над файлами и каталогами, а также вопросы организации параллельной обработки информации. Для иллюстрации рассмотрено применение этих предпосылок в программных комплексах.