Хоменко Сергей Александрович

Ордена трудового красного знамени

ФГБОУ ВО «Московский технический университет связи и информатики»

Студент

**История развития системы домашней автоматизации. Анализ существующих систем.**

**§ 1. История развития.**

Автоматизация — применение технических средств, экономико-математических методов и систем управления, освобождающих человека частично или полностью от непосредственного участия в процессах получения, преобразования, передачи и использования энергии, материалов или информации[[[1]](#footnote-1)].

Автоматизация позволяет повысить производительность труда, улучшить качество продукции, оптимизировать процессы управления, отстранить человека от производств, опасных для здоровья. Автоматизация, за исключением простейших случаев, требует комплексного, системного подхода к решению задачи.

Процесс автоматизации начался намного раньше, чем может казаться, автоматизация появилась практически сразу же с возникновением производства. К первым автоматизированными системами можно отнести самодействующие устройства. Они являютсяпрообразами современных автоматов и появились в глубокой древности.

Однако в условиях мелкого кустарного и полукустарного производства вплоть до 18 в. практического применения они не получили и, оставаясь занимательными "игрушками", свидетельствовали лишь о высоком искусстве древних мастеров. Совершенствование орудий и приемов труда, приспособление машин и механизмов для замены человека в производственных процессах вызвали в конце 18 в. начале   
19 в. резкий скачок уровня и масштабов производства, известный как промышленная революция 18-19 вв.

С появлением механических источников электрической энергии - электромашинных генераторов постоянного и переменного тока (динамомашин, альтернаторов) - и электродвигателей оказалась возможной централизованная выработка энергии, передача ее на значительные расстояния и дифференцированное использование на местах потребления. Тогда же возникла необходимость в автоматической стабилизации напряжения генераторов, без которой их промышленное применение было ограниченным. Лишь после изобретения регуляторов напряжения с начала 20 в. электроэнергия стала использоваться для привода производственного оборудования. Наряду с паровыми машинами, энергия которых распределялась трансмиссионными валами и ременными передачами по станкам, постепенно распространялся и электропривод, вначале вытеснивший паровые машины для вращения трансмиссий, а затем получивший и индивидуальное применение, то есть станки начали оснащать индивидуальными электродвигателями.

В 1936 г. Д.С.Хардер (США) определял автоматизацию как "автоматическое манипулирование деталями между отдельными стадиями производственного процесса". По-видимому, вначале этим термином обозначали связывание станков с автоматическим оборудованием передачи и подготовки материалов. Позднее Д.С.Хардер распространил значение этого термина на каждую операцию производственного процесса.

Высокая экономическая эффективность, технологическая целесообразность и часто эксплуатационная необходимость способствовали широкому распространению автоматизации в промышленности, на транспорте, в технике связи, в торговле и различных сферах обслуживания. Ее основные предпосылки - более эффективное использование экономических ресурсов: энергии, сырья, оборудования, рабочей силы и капиталовложений. При этом улучшается качество и обеспечивается однородность выпускаемой продукции, повышается надежность эксплуатации установок и сооружений.

Вторая половина 20 в. ознаменовалась дальнейшим совершенствованием технических средств автоматики и широким, хотя и неравномерным для разных отраслей народного хозяйства, распространением автоматических управляющих устройств с переходом к более сложным автоматическим системам, в частности в промышленности — от автоматизации отдельных агрегатов к комплексной автоматизации цехов и заводов. Существенной чертой является использование автоматики на объектах, территориально расположенных на больших расстояниях друг от друга, например крупные промышленные и энергетические комплексы, системы управления космическими летательными аппаратами и т.д. Для связи между отдельными устройствами в таких системах применяются средства телемеханики, которые совместно с устройствами управления и управляемыми объектами образуют телеавтоматические системы. Большое значение при этом приобретают технические (в том числе телемеханические) средства сбора и автоматической обработки информации, так как многие задачи в сложных системах автоматического управления могут быть решены только с помощью вычислительной техники. Наконец, теория автоматического регулирования уступает место обобщенной теории автоматического управления, объединяющей все теоретические аспекты автоматики и составляющей основу общей теории управления.

Также в технике вводится понятие "автоматическое управление" — совокупность действий, направленных на поддержание или улучшение функционирования управляемого объекта без непосредственного участия человека в соответствии с заданной целью управления[[[2]](#footnote-2)]. Автоматическое управление широко применяется во многих технических и биотехнических системах для выполнения операций, не осуществимых человеком в связи с необходимостью переработки большого количества информации в ограниченное время, для повышения производительности труда, качества и точности регулирования, освобождения человека от управления системами, функционирующими в условиях относительной недоступности или опасных для здоровья.

Что же касается домашней автоматизации, то первым шагом на пути к домашней автоматизации стало изобретение первых бытовых приборов, которые использовали электричество для выполнения простых задач по приготовлению пищи и уборки: пылесос (1901 г.), тостер (1909 г.), домашний холодильник (1913 г.), посудомоечная машина (1913 г.), утюг с регулируемой температурой (1927 г.), диспоузер (1927 г.), стиральная машина (1935 г.), сушильная машина (1935 г.), микроволновая печь (1945 г.), электрическая кофеварка (1952 г.).

Первые единичные попытки домашней автоматизации в современном понимании появились в середине 20 в. Для своего времени они выглядели футуристическими экспериментами и причудами изобретателей и практического распространения не получили.

В 1950 г. в журнале "Popular Mechanics" вышла статья "Push-Button Manor"[[[3]](#footnote-3)]("кнопочный дом") американского инженера Эмиля Матиаса. Э.Матиас оборудовал свой дом множеством устройств и кнопками для их управления. Почти всеми процессами в доме можно управлять нажатием кнопки. Некоторые из нововведений Э.Матиаса включали в себя автоматически закрывающиеся с помощью переключателя шторы и окна, включение или выключение радио в определенное время, автоматическое включение света в гардеробе при выдвижении ящиков и многое другое. Кроме того система дома включала в себя автоматическую систему сигнализации, которая в том числе проверяла, закрыты ли все двери и окна в доме ночью, в случае их открытия загорались яркие огни, и в спальне звучал сигнал. Был даже интерфон, который поднимал звуки в гараже и, используя трубы, переносил их в спальню.

Хотя некоторые из вышеупомянутых предметов можно было купить в магазине в 1950-х годах, Э.Матиасу удалось построить собственный проект по автоматизации дома. Для реализации проекта Э.Матиас потратил более двух километров кабеля при этом все провода, моторы и другие использованные устройства были спрятаны в стенах и полу.

Следующим шагом в домашней автоматизации стал компьютер Echo IV американского инженера Джеймса Сазерленда, уже в 1966 г. компьютер мог регулировать работу домашней климатической техники, включать и выключать некоторые приборы и распечатывать списки покупок.

В 1975 г. шотландская Pico Electronics разработала первый специализированный стандарт управления домашними устройствами - X10. Новая система позволяла включать и выключать приборы и менять яркость света, а также получать данные о текущем состоянии приборов. Для управления X10 были разработаны специальные пульты и компьютерный интерфейс.

В наши дни стандарт все еще остается одним из самых популярных. Так как для связи модулей сети X10 используется обычная домашняя электрическая сеть. Закодированные цифровые данные передаются с помощью радиочастотного импульса вспышки частотой 120 кГц, длительностью 1мс и синхронизированы с моментом перехода переменного тока через нулевое значение. За один переход через нуль передается один бит информации. Приемник так же формирует окно ожидания вблизи перехода напряжения через 0. Размер окна — 200 мкс. Наличие импульса вспышки в окне — логическая "1", отсутствие — логический "0".

Относительно высокая несущая частота не позволяет сигналу распространяться через трансформаторы или между фазами в многофазных сетях и сетях с расщепленной фазой. Для сетей с расщепленной фазой для передачи сигнала с фазы на фазу может использоваться обычный конденсатор, но для многофазных сетей и тех сетей с расщепленной фазой, где простого конденсатора мало, необходимо использовать активный повторитель. Но при передаче сигнала с фазы на фазу необходимо учитывать вышеназванное условие — передача бита начинается при пересечении нуля. Именно по этой причине, при переходе с фазы на фазу, сигнал сдвигается на 1/6 цикла.

Еще одним важным моментом является возможность блокирования сигналов за пределами действия сети, чтобы, например, модули одной сети X10 не влияли на сеть X10 в соседнем доме. В таких случаях для блокирования сигналов используется индуктивный фильтр.

Передаваемый по сети пакет состоит из адреса и команды, отправляемых контроллером управляемому модулю. Более сложные контроллеры также умеют опрашивать такие же управляемые модули об их статусе. Этот статус может быть достаточно простым ("включено" или "выключено"), указывать числовое значение (текущее значение яркости, температура или данные с других датчиков).

Вне зависимости от среды передачи (электрическая сеть или радиосигнал), пакеты X10 состоят из:

* 4 бита — код дома;
* 4 бита — код модуля (может быть задано несколько модулей);
* 4 бита — команда.

Во избежание путаницы и удобства пользователей код дома задается латинскими буквами от A до P, а код модуля — цифрами от 1 до 16.

Когда сеть X10 установлена, каждый модуль настраивается таким образом, чтобы откликаться на один из 256 возможных адресов (16 кодов домов × 16 кодов модулей = 256). Каждый модуль реагирует только на команды, отправленные непосредственно ему и на несколько широковещательных команд.

Например, по сети может прийти сообщение вида: "модуль A3" а за ним команда "включиться" (turn on), что заставляет модуль A3 включить подсоединенное к нему устройство. Управление несколькими модулями осуществляется сообщением вида: "модуль A3", "модуль A15" и "модуль A4", а затем команда "включиться". Результат — все вышеперечисленные модули должны включить подключенные к ним устройства.

Стоит отметить, что нет ограничения на использование более чем одного кода дома в случае перечисления, однако, широковещательные команды вида "включить весь свет" или "выключить все модули" влияет только на модули с одним кодом дома. Таким образом, коды домов могут быть использованы для разделения сети X10 на отдельные зоны.

Для обеспечения работы беспроводных пультов, переключателей и прочих устройств был разработан протокол использования радиоканала. Беспроводные устройства передают по радио пакеты данных, почти идентичные передаваемым по проводной сети. Для передачи используется частота 310 МГц в США и 433 МГц в Европе. Ресивер, подключенный к обычной электросети, транслирует полученные по радио команды в стандартную сеть X10.

Однако у Х10 существует ряд недостатков:

* Протокол X10 очень медленный. Около 3/4 секунды занимает передача адреса устройства и команды. Это может быть незаметным при использовании настольного контроллера, но может стать ощутимым при использовании двусторонней связи или при управлении через интеллектуальный контроллер (например, подключенный к компьютеру), особенно при использовании какого-либо сценария для управления несколькими устройствами.
* В сети X10 может передаваться только одна команда в конкретный момент времени. Если в одно и то же время будет вестись передача двух и более команд, это вызовет коллизии: команды не будут корректно приняты или же будут выполнены неверные действия.
* Устройства защитного отключения могут ослаблять сигнал настолько, что он не будет прочитан.
* Некоторые блоки питания, используемые в современной аппаратуре (компьютерах, телевизорах, ресиверах), могут "съедать" проходящие мимо команды сети X10. Это происходит из-за использования конденсаторов на входе блоков питания, которые создают низкое сопротивление для высокочастотного сигнала, сглаживая сигнал. Для подобных устройств существуют входные фильтры, которые позволяют пакетам X10 беспрепятственно проходить мимо подобных устройств.
* Некоторые модули X10 некорректно работают (или не работают вообще), если управляют устройством с низкой потребляемой энергией (менее 50 Ватт), например, флюоресцентными лампами.

В 1975 г. система Х10 была инновационной, позволяла включать и выключать приборы и менять яркость света, а также получать данные о текущем состоянии приборов. Кроме того широкому распространению систем на X10 способствовали простота их установки и низкая цена.

В 1980-х основным рынком X10 стали США, а в Европе устройства на X10 использовались значительно меньше, в первую очередь из-за особенностей государственного регулирования, не позволявшего применять весь функционал устройств. Одновременно европейские электротехнические компании готовили собственные аналоги X10. Чтобы эффективнее продвигать свои разработки, немецкие компании во главе с Siemens в итоге решили использовать единый стандарт, который назвали Европейской инсталляционной шиной (EIB, 1990). Группа компаний во главе с французской Electricité de France создала стандарт BatiBus. Голландская Philips, немецкая Daimler Benz, французская Thomson Consumer Electronics, British Telecom и ряд других создали Европейскую ассоциацию домашних систем (EHSA, 1991 г.) и третий европейский стандарт — EHS.

В 1984 г. американская Ассоциация жилищно-строительных компаний (National Association of Home Builders) изобрела для домов с использованием автоматизации термин "умный дом" (smart house), а в 1999 г. студия Disney выпустила фильм Smart House, представивший идею умного дома широкой публике.

В 1999 г. компании, производившие устройства на трех европейских стандартах, договорились об объединении и создании единого протокола KNX, который был представлен в 2002 г. и стал открытым.

Переворот в технологиях домашней автоматизации произошел в 2010-х, толчком к нему послужило появление iPhone (2007 г.) и других смартфонов. На рынке домашней автоматизации появились сразу несколько прорывных разработок, за которыми последовали сотни новых устройств. В 2010 г. Dropcam представила недорогую (200 долларов) камеру видеонаблюдения с современным дизайном, онлайн-доступом к видео со смартфона и возможностью хранить записи в облаке. В 2011 г. компания Nest представила программируемый термостат, призванный решить проблемы предыдущих: они были слишком сложными, и пользователи были не в состоянии настраивать их так, как хотели, и экономить энергию. В отличие от них, термостат Nest был самообучаемым, а кроме того давал возможность управления со смартфона.

В 2012 г. еще одна компания из Кремниевой долины SmartThings представила прорывную систему домашней автоматизации, стоившую в сотни раз меньше существовавших до сих пор аналогов: хаб за 100 долларов, датчики по 30-40 долларов, розетки и выключатели по 50 долларов и ряд других устройств. Вдобавок SmartThings поддерживала более 100 тысяч сторонних устройств и приложения 8 тысяч сторонних разработчиков. В 2014 г. компанию купила Samsung.

В 2014 г. появилась первая "умная колонка" Amazon Echo — небольшое устройство со встроенным умный помощником Alexa с голосовым управлением. Она позволяла получать ответы на бытовые вопросы и управлять домашними устройствами. В 2016 г. появился аналог Google Home на основе собственного умного помощника Google Assistant. Компания Apple выпустила умную колонку Apple HomePod на базе голосового помощника Siri.

Рост популярности автоматизированных домашних систем обусловлено желанием человека жить в комфорте и удобстве. В настоящее время с помощью автоматизированных домашних систем можно осуществить многие идеи изобретателей прошлого поколения, упростив быт человека начиная от автоматизации цветов и контроля освещения заканчивая обеспечением безопасности жилища — контроль протечек или задымления, системы безопасности с удаленным оповещением.

Именно многогранность домашней автоматизации делает ее актуальной для изучения, а быстрый рост развития новых технологий позволяет совершенствовать систему автоматизации делая ее не только проще и удобней, но и более доступной с финансовой точки зрения.

**§ 2. Анализ безопасности домашних автоматизированных систем.**

Домашняя автоматизация в наше время возможна либо путем покупки "готовой" системы, либо путем самостоятельной сборки отдельных ее элементов.

Огромным минусом готовых систем домашней автоматизации является их уязвимость. Основная идея автоматизированных домашних систем заключается не только в стремление к тому, чтобы все бытовые устройства могли дистанционно контролироваться и настраиваться, а также в том, что все эти действия можно произвести находясь в удалении от дома. Однако все компоненты, которые могут получить доступ к домашней сети, а следовательно, могут иметь доступ к Интернету, потенциально уязвимы.

В последнее время все больше компаний и групп ученых занялись проблемой безопасности "готовых" домашних автоматизированных систем и "Интернет вещей" ( IoT - Internet of Things), то есть бытовых приборов имеющих функцию подключения к интернету.

Hewlett-Packard (США) провела исследование рынка интеллектуальных систем в ходе которого выяснила, что практически все системы имеют проблемы с безопасностью. Исследования же компания Synack (США) показали, что из 16 "готовых" автоматизированных систем 15 имеют серьезные уязвимости и только одна система имеет достойную систему защиты.

Так, например, в эксперименте группы исследователей из Принстонского университета (США) в 2017 г. был произведен анализ интенсивности трафика четырех IoT гаджетов, используемых в готовых домашних автоматизированных системах (мониторинг потребления электроэнергии Sense, домашние видеокамеры Nest Cam, "умная" розетка We-Mo и смарт-колонка Amazon Echo)[[[4]](#footnote-4)].

На основании этого исследования, ученые сделали вывод, что разделить записанный трафик на потоки и ассоциировать каждый из них с определенным устройством не так сложно. На основе полученной информации злоумышленник может определить режим сна пользователя, когда он бывает дома или как часто использует виртуальный ассистент Amazon Alexa.

Как показали исследования, некоторые пользователи системы игнорируют основные правила безопасной реализации, сетевые подключения просто не зашифрованный и происходят в режиме "пароли по умолчанию", так что любой человек, у кого есть доступ к локальной сети, может методом подбора контролировать работу Интернет вещей.

Даже без перехвата трафика, наблюдатели могут использовать для анализа внешние запросы DNS (англ. Domain Name System "система доменных имен") с целью идентифицировать интеллектуальные домашние устройства с потенциальными уязвимости для получения конфиденциальной информации потребителей. Многие производители пытаются решить данные проблемы шифрованием.

Однако использование одного лишь шифрования нельзя считать адекватной мерой защиты конфиденциальности владельцев "умных" домов, да и зачастую, вычислительная мощность некоторых устройства слишком низка, чтобы обеспечить лучшее или даже асимметричное шифрование. "Систематическое решение для защиты неприкосновенности частной жизни потребителей потребует обфускации или формирования всего трафика умного дома для маскировки вариаций, по которым можно определить настоящее поведение", - отметили ученые, добавив, что такое решение не должно негативно влиять на производительность IoT-устройства и не требовать модификации его программного обеспечения.

По причине того, что большинство систем домашней автоматизации для обратной связи с клиентом (мобильное приложение, личный кабинет на сайте производителя) используют свои сервера, при анализе внешнего трафика владельца данной системы несложно получить информацию о производителе IoT-устройства.

Имея эту информацию можно совершить ряд атак. По направлениям, данные атаки можно разделить согласно таблице 1.1.

Таблица 1.1. - Виды атак на информацию о производителе IoT-устройства.

|  |  |
| --- | --- |
| Вид атаки | Последствия |
| Атака на центральный узел, либо сервер, осуществляющий сбор и обработку информации, оповещение об инцидентах | Нарушение работы, вывод из строя, а следовательно и всей системы, Нарушение конфиденциальности, целостности и доступности информации. |
| Вирусные и троянские программы | Сбой программного обеспечения системы. Нарушение работы либо вывод из строя элементов системы. Использование компонентов системы для DDoS-атак. |
| Перехват информации передаваемой по проводным и беспроводным каналам связи. | Нарушение конфиденциальности, целостности и доступности информации. Вывод из строя компонентов системы, возможность захвата управления системой. |
| Доступ злоумышленника с правами администратора на центральный сервер в случае утраты, хищения, сброса или подбора пароля. | Нарушение конфиденциальности, целостности и доступности информации. Возможность управления уведомлениями в случае наступления события. |

Помимо сбора конфиденциальной информации у "готовых" систем есть ряд других недостатков:

- у разных производителей таких систем отсутствует единая политика безопасности.

- полное отключение "готовой" системы в случае прекращения подачи электроэнергии (отсутствие аварийного источника питания для сигнализации о состоянии системы).

- производители, зачастую, с целью минимизации стоимости продукции не уделяют безопасности должного внимания.

Кроме того, не стоит опускать тот момент, что для установки "готовой" системы домашней автоматизации чаще всего необходимо полностью заменить всю электропроводку, переделать систему водопроводных труб и кранов, систему отопления, кондиционирования и вентиляции, так же возможны траты на замену окон и дверей, что влечет дополнительные расходы пользователя.

Однако основным недостатком "готовых" систем умного дома является, на мой взгляд, проприетарное программное обеспечение, используемое для управления данными системами. Нежелание производителей делиться кодом делает невозможным модернизацию функций системы, оптимизацию кода и оперативный выпуск патчей для устранения выявленных уязвимостей системы безопасности.

При видимости достаточно большого количества производителей систем домашней автоматизации на мировом рынке выбор невелик: это либо огромные корпорации, либо небольшие компании, пытающиеся выйти на рынок.

Небольшие компании, зачастую с действительно инновационными идеями, не могут пробиться дальше проекта на kickstarter и вынуждены распрощаться со своей идеей (ярким примером служит отечественная команда проекта "Black Swift" с их одноименным одноплаточным встраиваемым компьютером).

Именно отсутствие честной конкуренции ведет к торможению развития систем домашней автоматизации и высокой рыночной стоимости.

Но самой большой опасностью для системы домашней автоматизации является сам пользователь. Зачастую, получив долгожданное устройство пользователь спешит поскорее насладиться работой нового устройства, в лучшем случае дочитав инструкцию до раздела "подключение устройства к wifi". Подавляющее число производителей не требуют смену пароля пользователем, как следствие, мы имеем огромное количество устройств как в приветных сетях, так и в глобальной компьютерной сети Интернет с реквизитами доступа типа admin/admin, admin/1234 и тому подобных.

Немаловажным условием поддержания безопасности является своевременное обновление программного обеспечения на устройстве. Но тут тоже все не так оптимистично: автоматическое обновление, как правило, отключено, а пользователь, зайдя на устройство первый раз для подключения его к своему домашнему маршрутизатору, не заходит на него никогда. Ярким примером здесь служит огромное количество wifi-роутеров до сих пор подверженных атаке средствами Reaver и подобного ПО (перебор ключа WPS).

С целю подтвердить свою позицию по вопросу преимущества открытых систем домашней автоматизации перед систем с закрытым кодом, хочу рассмотреть пример со сплит-системой кондиционирования.

Имеется две сплит-системы с возможностью управления через мобильное приложение производителя (для подключения к сети интернет в каждой системе имеется wifi модуль):

1) Аналогичные модели без возможности управления через интернет стоят примерно на 10% дешевле (при стоимости wifi модуля порядка 1% относительно самой сплит-системы (ESP-8266)).

2) Мобильное приложение не позволяет настраивать ни тригеры, ни календари.

То есть проприетарное программное обеспечение мало того, что не дает возможности пользователю производить гибкую настройку сплит-системы, но и управлять этой системой кроме как с авторизованного мобильного устройства.

3) С целью анализа данных мною была использована утилита tcpdump.

Исходя из вывода данной утилиты следует:

root@ubnt:~# tcpdump -i switch0 host 192.168.99.11 -nn -v

tcpdump: listening on switch0, link-type EN10MB (Ethernet), capture size 262144 bytes

19:45:20.833884 IP (tos 0x0, ttl 64, id 19184, offset 0, flags [none], proto TCP (6), length 253)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0x2baf (correct), seq 1821266:1821479, ack 89614934

19:45:20.837823 IP (tos 0x0, ttl 64, id 19185, offset 0, flags [none], proto TCP (6), length 40)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [.], cksum 0x017d (correct), ack 214, win 7260, length 0

19:45:25.841828 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.99.11 is-at a0:6f:aa:aa:79:bc, length 42

19:46:04.132270 IP (tos 0x0, ttl 64, id 19186, offset 0, flags [none], proto TCP (6), length 40)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [.], cksum 0x0088 (correct), ack 459, win 7260, length 0

19:46:04.148869 IP (tos 0x0, ttl 64, id 19187, offset 0, flags [none], proto TCP (6), length 1492)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [.], cksum 0x63af (correct), seq 213:1665, ack 459, win 8192, l

19:46:04.204767 IP (tos 0x0, ttl 64, id 19188, offset 0, flags [none], proto TCP (6), length 113)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0x3316 (correct), seq 1665:1738, ack 459, win 7260,

19:46:06.014854 IP (tos 0x0, ttl 64, id 19189, offset 0, flags [none], proto TCP (6), length 40)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [.], cksum 0xf9ad (correct), ack 688, win 7260, length 0

19:46:06.214731 IP (tos 0x0, ttl 64, id 19190, offset 0, flags [none], proto TCP (6), length 40)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [.], cksum 0xf8c8 (correct), ack 917, win 7260, length 0

19:46:09.036387 IP (tos 0x0, ttl 64, id 19191, offset 0, flags [none], proto TCP (6), length 1421)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0xaa6a (correct), seq 1738:3119, ack 917, win 8192,

19:46:09.141435 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.99.11 is-at a0:6f:aa:aa:79:bc, length 42

19:46:12.038304 IP (tos 0x0, ttl 64, id 19192, offset 0, flags [none], proto TCP (6), length 1421)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0x8075 (correct), seq 3119:4500, ack 917, win 8192,

19:46:15.049739 IP (tos 0x0, ttl 64, id 19193, offset 0, flags [none], proto TCP (6), length 1421)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0xcfac (correct), seq 4500:5881, ack 917, win 8192,

19:46:18.037221 IP (tos 0x0, ttl 64, id 19194, offset 0, flags [none], proto TCP (6), length 1421)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0x6581 (correct), seq 5881:7262, ack 917, win 8192,

19:46:20.829971 IP (tos 0x0, ttl 64, id 19195, offset 0, flags [none], proto TCP (6), length 253)

192.168.99.11.59181 > 158.255.4.47.47878: Flags [P.], cksum 0xda84 (correct), seq 7262:7475, ack 917, win 8192,

19:46:20.837075 IP (tos 0x0, ttl 64, id 19196, offset 0, flags [none], proto TCP (6), length 40)

Можно сделать вывод, что сплит-система непрерывно передает некие данные удаленному серверу. Так как целю данной работы не является анализ трафика, передаваемый IoT-устройствами, мы не будем осуществлять разбор данного дампа.

Хочу лишь сказать, что при реализации атаки Man in the middle (MITM) на сплит систему и использовании прокси-сервера с понижением https запросов до http, ни мобильное приложение, ни сплит система не сочла это вмешательство подозрительным.

Смоделируем ситуацию:

Проанализировав внешний трафик и найдя обращения к IP адресу 158.255.4.47 становится ясно, что в квартире установлена сплит-система определенного производителя. Применив атаку с целью подмены целевого ресурса (например hijacking bgp, атаки на DNS) можно получить доступ к сплит-системе. Так же, можно подменить файл прошивки на файл с модифицированным ПО и инициировать обновление. Так же, модифицированную сплит-систему злоумышленник может использовать для организации DDoS атаки, а в случае, если на первом этапе была использована атака hijacking bgp, то количество зараженных систем будет исчисляться тысячами.

1. Большой энциклопедический словарь / гл. ред. А. М. Прохоров. Изд-е 2-е, перераб. и доп. М.-СПб.: Большая рос. энцикл.; Норинт, 2000. - 1434 с. [↑](#footnote-ref-1)
2. Новиков В.П. Автоматизация литейного производства. Часть 1. Управление литейными процессами. Учебное пособие. - М.:МГИУ, 2008. -292 с. [↑](#footnote-ref-2)
3. URL: http://blog.modernmechanix.com/push-button-manor/ [↑](#footnote-ref-3)
4. N.Apthorpe, D.Reisman, and N.Feamster, “A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,” 2016. [↑](#footnote-ref-4)