Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
Vol. 4, Is. 2, pp. 68-74, 2015

DOI: 10.13187/vesp.2015.4.68
www.ejournal21.com

UDC 004.056

Automation Device Authentication at «Smart Home»

[1] Alexander V. Nasteka
[2] Catherine E. Bessonova

[1] National research university of information technologies, mechanics and optics, Russian Federation
197101, Saint Petersburg, Kronverkskiy prospekt, 49
E-mail: nasteka.av@gmail.com
[2] National research university of information technologies, mechanics and optics, Russian Federation
197101, Saint Petersburg, Kronverkskiy prospekt, 49
PhD in Engineering sciences, Assistant
E-mail: merom812@gmail.com

Abstract

This article brings to light features of modern system smart home. The author describes interconnection with private security firms. This work illustrates vulnerabilities smart home and methods for ensuring the confidentiality and integrity of transmitted data. The result of the research is software and hardware system that implements the model of mutual authentication

Keywords: information security, smart home, automation device, authentication, vulnerable information flow.

Введение

Для обеспечения безопасности квартир, коттеджей и других жилых помещений специальные правоохранительные органы и частные охранные предприятия используют специальное встраиваемое оборудование, которое позволяет отслеживать неразрешенную деятельность на контролируемой территории. В настоящее время активно развивается рынок решений для обустройства «умных» квартир и домов, что сказалось на возможностях систем охраны [7, 13]. Ранее они представляли собой лишь сильно изолированные комплексы с минимальным функционалом, то теперь они позволяют фиксировать движение; получать данные о разбитых окнах; фиксировать задымление, огонь, протечку воды; удаленно управлять помещением и другое.

Такое вычислительное средство можно приравнять к системам «умный дом», которые в свою очередь имеют серьезные проблемы по обеспечению безопасности передаваемых данных [8, 9]. Основным источником угроз подобных решений являются не аутентифицируемые конечные устройства автоматизации или датчики, которые общаются с управляющим центром по открытому каналу без возможности обеспечения конфиденциальности и целостности данных [1]. Задачей исследования является создание дополнительного программно-аппаратного комплекса поверх основного канала общения между элементами системы «умный дом».

Результаты

Общая схема системы "умный дом" представляет собой два основных потока данных, в которых циркулируют управляющие сигналы (см. рисунок 1) [3].

Рис. 1. Формальная модель системы «Умный дом»

Первый информационный поток находится между пользователем и управляющей системой. Здесь инициируется запрос на выполнение действия через какое-то устройство с графическим интерфейсом (выделенный терминал, мобильное устройство, web-приложение и т.д.). Основным потоком является второй, который находится между управляющей системой и устройством автоматизации [4]. Особенностью этого информационного потока являются конечные устройства автоматизации, их программно-аппаратная составляющая. Они редко представлены программируемыми устройствами, содержат ограниченный набор возможных команд, что делает невозможным обеспечение конфиденциальности и целостности данного информационного потока. Управляющая система вынуждена использовать команды в открытом, общедоступном виде.

Сам «умный дом» можно представить, как компьютерную сеть с двумя узлами и сетевым трафиком (запрос-ответ) между ними. В этом случае мы можем предположить возможные классы сетевых уязвимостей и применить основные сетевые атаки на такую модель. Наличие классов уязвимостей позволит определить последствия при нарушении конфиденциальности и целостности информации с учетом спецификации системы [6].

Основными классами уязвимостей на примере существующих коммерческих решений являются уязвимости на уровне проектирования и реализации [5]. Можно рассмотреть следующие основные сетевые атаки: подслушивание и Man-in-the-middle (MITM).

Не смотря на относительную простоту метода подслушивания (анализа), он будет являться основным для определения о применимости других способов воздействия на информационный поток. Если говорить о специфике системы, с помощью анализа возможно получить информацию о наличии в помещениях людей или какой-либо физической активности, без необходимости получения доступа к датчикам [10].

Применение MITM атаки позволяет злоумышленнику подменить запрос или ответ между управляющей системой и устройством автоматизации или датчиком. В случае анализа системы охраны или другой критичной для помещения технологии, данный способ воздействия будет одним из самых эффективных.

При правильном подходе к изучению информационных потоков в системах домашней автоматизации и охраны, можно не только получить доступ к конкретным элементам, но и в случае серьезных упущений при проектировании системы можно получить полный доступ над помещениями, включая систему охраны [11].

Таким образом, устройства автоматизации, управляющая система и информационный поток между ними – одни из самых уязвимых элементов в «умном доме». Рассмотрев уязвимости, приводящие к нарушению конфиденциальности и целостности, и возможные примеры атак, можно говорить о необходимости контроля циркулирующей информации в системе автоматизации. Для этого изучим и рассмотрим возможные пути и методы

обеспечения безопасности информационного потока между управляющей системой и устройствами автоматизации.

Для обеспечения безопасности второго информационного потока было разработано устройство, в основе которого лежит модель взаимной аутентификации:

1) $System \rightarrow \{msg,S\}_k \rightarrow Device$
2) $Device \rightarrow \{(S)_{skey},D\}_k \rightarrow System$
3) $System \rightarrow \{msg,(D)_{dkey}\}_k \rightarrow Device$,где:

$System$ – управляющая система;
$Device$ – устройство автоматизации;
msg – команда устройству автоматизации на выполнение;
S, D – метки управляющей системы и устройства автоматизации;
$skey, dkey$ – открытые ключи управляющей системы и устройства автоматизации;
k – сеансовый ключ.

Она состоит из 3 зашифрованных сообщений типа запрос-ответ, их содержимое может варьироваться, но обязательно использование меток устройств, которые участвуют в сеансе связи.

Рассмотрим каждый этап подробнее:

На 1 шаге управляющая система *System* отправляет свою метку *S*, зашифрованную сеансовым ключом *k*, и команду для выполнения *msg* устройству автоматизации *Device*.

На 2 шаге Устройство автоматизации шифрует метку *S* открытым ключом *skey* и отправляет управляющей системе *System* сообщение, зашифрованное сеансовым ключом *k* вместе со своей меткой.

После расшифровки сообщения, убедившись, что с другой стороны находится устройство автоматизации *Device,* управляющая система *System* на 3 шаге формирует сообщение, в котором повторяется команда *msg* и содержится зашифрованная метка *D* открытым ключом *dkey*.

На последнем этапе данная схема показывает корректность обеих сторон и подтверждает выполнение команды, которая была инициирована в первом сообщении.

После встраивания подобного устройства в действующую сеть, она не повлияет на функциональные возможности основной системы домашней автоматизации, однако оно позволит обеспечить конфиденциальность и целостность данных между управляющим центром и устройствами автоматизации.

Проверка результатов

Для проверки результатов был создан опытный образец программно-аппаратного решения, который реализует представленный метод взаимной аутентификации управляющей системы и устройства автоматизации.

На рисунке 2 представлена общая схема программно-аппаратного решения:

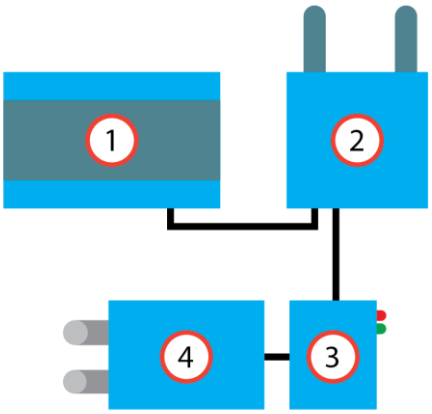

Рис. 2. Схема технической реализации механизма аутентификации управляющей системы и устройства автоматизации

В качестве управляющей системы (см. 1 на рисунке 2) выступает управляющая система SmartHome v 3.5 отечественного производителя Contactless.ru с дополнительным аутентифицирующим модулем на языке python. Устройство представляет собой компактный контроллер в защитном пластмассовом корпусе, имеет множество интерфейсов для взаимодействия с различными устройствами автоматизации, как проводных, так и беспроводных [2, 12]. Имеет возможность автономной работы, в отсутствии основного источника питания. Взаимодействие осуществляется через набор стандартных компонентов, установленных на Debian Linux 7.0. Для реализации механизма взаимной аутентификации на данном уровне, дополнительно создан исполняемый модуль на языке python, выполняющий запросы и ответы согласно описанной ранее модели взаимной аутентификации управляющей системы и устройства автоматизации.

Устройство автоматизации имитирует дверной замок, представлено в виде сервопривода постоянного вращения (см. 4 на рисунке 2), которым можно управлять только через внешние импульсы.

Для реализации аутентификации на стороне устройства автоматизации (также для управления устройством автоматизации в данном случае) используется программно-аппаратное решение (см. 3 на рисунке 2) на базе Arduino Uno с подключенным Ethernet контроллером enc28j60. Данный микроконтроллер поддерживает огромное количество внешних устройств, что позволяет сделать его практически универсальным для взаимодействия с различными элементами автоматизации. Ethernet контроллер, в общем случае, будет обязательным элементом для работы с сетью, второй интерфейс взаимодействия может быть подобран индивидуально к устройству управления.

Для связи управляющей системы и устройства автоматизации используется маршрутизатор Tp-link (см. 2 на рисунке 2).

Работа представленной схемы происходит по следующему алгоритму:

1. Извне приходит команда от пользователя на некоторое действие в управляющую систему (1), там определяется необходимое действие и через программный аутентифицирующий модуль формируется шифрованный запрос.
2. Шифрованный запрос отправляется через маршрутизатор (2) на программно-аппаратное решение (3).
3. Программно-аппаратное решение (3), согласно описанной ранее модели взаимной аутентификации управляющей системы и устройства автоматизации, посредством запросов и ответов принимает решение о корректности запроса и целесообразности его выполнения. В случае успешной аутентификации необходимая команда отправляется устройству автоматизации (4).
4. В случае получения команды от программно-аппаратного решения (3) устройство автоматизации выполняет предписанное действие, в случае провала процедуры взаимной аутентификации устройство остается в текущем состоянии.

Были проверены основные типы сетевых атак до и после встраивания представленного устройства защиты, результаты представлены в таблице.

Таблица. Проверка применимости атак

Название атаки	Возможность применения атаки	
	Без использования защиты	С использованием защиты (модель взаимной аутентификации)
Анализ трафика	Возможна в полной мере	Частично возможна
Модификация данных	Возможна в полной мере	Не применима
IP Address Spoofing	Возможна в полной мере	Не применима
Отказ в обслуживании	Возможна в полной мере	Возможна в полной мере
MITM атака	Возможна в полной мере	Не применима
Анализ сети	Частично возможна	Частично возможна
Replay атака	Возможна в полной мере	Не применима

Очевидно, что после аутентификации отдельных устройств автоматизации системы «умный дом» через устройство защиты, основные типы сетевых атак становится не применимы к данному информационному потоку.

Заключение

Таким образом, можно говорить о комплексном изучении сфера системы «умный дом», ее текущее состояние в мире информационных технологий, а также приоритет данного направления для вневедомственных подразделений и частных охранных предприятий. Рассмотрена формальная схема работы системы «умный дом», которая в упрощенном виде позволяет объединить различные решения и понять специфику работы. На последнем шаге, после исследования и объединения всех полученных в ходе исследования данных, был создан программно-аппаратный комплекс, реализующий представленную модель взаимной аутентификации, что позволило обеспечить конфиденциальность и целостность информационного потока между управляющей системой и устройствами автоматизации или датчиками.

Примечания:

1. Бессонова Е.Е., Ефремов А.А., Настека А.В., Овсяникова В.В., Салахутдинова К.И., Трофимов А.А. Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ «УМНЫЙ ДОМ» // Региональная информатика «РИ-2014» Материалы конференции 2014. (124). [Электронный ресурс] – URL: http://spoisu.ru /files/ri/ri2014/ ri2014_materials.pdf

2. Гололобов В.Н. «Умный дом» своими руками. М.: НТ Пресс, 2007. 9-12 с., ISBN 5-477-00484-3

3. Настека А.В., Ефремов А.А, Овсяникова В.В., Салахутдинова К. И., Трофимов А. А. Защита системы «Умный дом» от программных сбоев // Сборник тезисов докладов конгресса молодых ученых. [Электронное издание] – URL: http://kmu.ifmo.ru/ collections_article/1011/ zaschita_sistemy_%C2%ABumnyy_ dom%C2% BB_ot_ programmnyh_sboev.htm

4. Настека А.В., Ефремов А.А, Овсяникова В.В., Салахутдинова К. И., Трофимов А. А. Защита управляющих сигналов в системе «Умный дом» // Сборник тезисов докладов конгресса молодых ученых. [Электронное издание] – URL: http://kmu.ifmo.ru/ collections_article/1013/ zaschita_upravlyayuschih_ signalov_v_ sisteme_ «umnyy _dom».htm

5. Стариковский А.В. Исследование уязвимостей систем умного дома [Текст] / А.В. Стариковский, И.Ю. Жуков, Д.М. Михайлов, А.М. Толстая, Ф.В. Жорин, В.В. Макаров, А.Б. Вавренюк // Спецтехника и связь. 2012. №2. С. 55-57.

6. Безопасность АСУЗ. Можно ли взломать Умный дом? [Электронный ресурс] – URL: http://www.cnews.ru/reviews/?2011/01/24/424494

7. "Умный дом" - маркетинговый исследование российского рынка: текущее состояние и прогноз развития. [Электронный ресурс] – URL: http://www.directinfo. net/index.php?option=com_content&view=article&id=139%3A2010-07-06-13-57-09

8. СТО НП "АВОК" 8.1.2-2008 Стандарт АВОК. Автоматизированные системы управления зданиями. Часть 2. Технические средства.

9. СТО НП "АВОК" 8.1.3-2007 Стандарт АВОК. Автоматизированные системы управления зданиями. Часть 3. Функции.

10. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. P. 9-14.

11. Michael S., Ulf L., 7 Smart-Home-Starter-Kits im Sicherheits-Test // AV-TEST-Studie. 2014. P. 16-41.

12. Othmar K., How to Smart Home // 2013. P. 23-28. ISBN 978-3-944980-00-3

13. Smart Homes Market. [Электронный ресурс] –URL: http://www.prweb.com /releases/smart-homes-market-2020/analysis-and-forecasts /prweb11302579.htm

References:

1. Bessonova E.E., Efremov A.A., Nasteka A.V., Ovsyanikova V.V., Salakhutdinova K.I., Trofimov A.A. Rossiya, Sankt-Peterburg, Sankt-Peterburgskii natsional'nyi issledovatel'skii universitet informatsionnykh tekhnologii, mekhaniki i optiki ANALIZ ZAShchISHchENNOSTI SISTEM «UMNYI DOM» // Regional'naya informatika «RI-2014» Materialy konferentsii 2014. (124). [Elektronnyi resurs] – URL: http://spoisu.ru/files/ri/ri2014/ ri2014_materials.pdf
2. Gololobov V.N. «Umnyi dom» svoimi rukami. – M.:NT Press, 2007. – 9-12 s., ISBN 5-477-00484-3
3. Nasteka A.V., Efremov A.A, Ovsyanikova V.V., Salakhutdinova K. I., Trofimov A. A. Zashchita sistemy «Umnyi dom» ot programmnykh sboev // Sbornik tezisov dokladov kongressa molodykh uchenykh. [Elektronnoe izdanie] – URL: http://kmu.ifmo.ru/collections_article/1011/ zaschita_sistemy_%C2%ABumnyy_dom%C2%BB_ot_programmnyh_sboev.htm
4. Nasteka A.V., Efremov A.A, Ovsyanikova V.V., Salakhutdinova K. I., Trofimov A. A. Zashchita upravlyayushchikh signalov v sisteme «Umnyi dom» // Sbornik tezisov dokladov kongressa molodykh uchenykh. [Elektronnoe izdanie] – URL: http://kmu.ifmo.ru /collections_article/1013/ zaschita_upravlyayuschih_signalov_v_sisteme_«umnyy_dom».htm
5. Starikovskii A.V. Issledovanie uyazvimostei sistem umnogo doma [Tekst] / A.V. Starikovskii, I.Yu. Zhukov, D.M. Mikhailov, A.M. Tolstaya, F.V. Zhorin, V.V. Makarov, A.B. Vavrenyuk // Spetstekhnika i svyaz'. – 2012. –№2. S. 55-57.
6. Bezopasnost' ASUZ. Mozhno li vzlomat' Umnyi dom? [Elektronnyi resurs] – URL: http://www.cnews.ru/reviews/?2011/01/24/424494
7. "Umnyi dom" - marketingovyi issledovanie rossiiskogo rynka: tekushchee sostoyanie i prognoz razvitiya. [Elektronnyi resurs] – URL: http://www.directinfo.net /index.php?option =com_content&view=article&id=139%3A2010-07-06-13-57-09
8. STO NP "AVOK" 8.1.2-2008 Standart AVOK. Avtomatizirovannye sistemy upravleniya zdaniyami. Chast' 2. Tekhnicheskie sredstva.
9. STO NP "AVOK" 8.1.3-2007 Standart AVOK. Avtomatizirovannye sistemy upravleniya zdaniyami. Chast' 3. Funktsii.
10. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. P. 9-14.
11. Michael S., Ulf L., 7 Smart-Home-Starter-Kits im Sicherheits-Test // AV-TEST-Studie. 2014. P. 16-41.
12. Othmar K., How to Smart Home // 2013. P. 23-28. ISBN 978-3-944980-00-3
13. Smart Homes Market. [Elektronnyi resurs]. URL: http://www.prweb. com/releases/smart-homes-market-2020/analysis-and-forecasts/prweb11302579.htm

УДК 004.056

Аутентификация устройств автоматизации в системе «умный дом»

[1] Александр Владимирович Настека
[2] Екатерина Евгеньевна Бессонова

[1] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101, Санкт-Петербург, Кронверкский проспект, 49
E-mail: nasteka.av@gmail.com
[2] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101, Санкт-Петербург, Кронверкский проспект, 49
Кандидат технических наук, ассистент
E-mail: merom812@gmail.com

Аннотация. Данная статья раскрывает особенности существующих систем домашней автоматизации, их взаимосвязь со штатными системами охраны правоохранительных органов. Подробно рассмотрены уязвимости «умных домов», способы обеспечения конфиденциальности и целостности передаваемых данных, а также описывается программно-аппаратный комплекс, реализующий модель взаимной аутентификации устройств.

Ключевые слова: информационная безопасность; домашняя автоматизация; устройства автоматизации; аутентификация; уязвимый информационный поток.