сурс] / Журнал «Хакер». – Режим доступа: https://xakep.ru/2011/03/09/54790, свободный.

6. Чернов, А. В. Об одном методе маскировки программ [Текст] /А.В. Чернов // Труды Института Системного программирования РАН. – 2003. – С. 85-119. – ISSN 2079-8156.

7. Christian Collberg. A taxonomy of obfuscating transformations. [Текст] / Christian Collberg, Clark Thomborson, Douglas Low. – 1997.

В.А. Кардаков

БЕЗОПАСНОСТЬ ТЕХНОЛОГИИ IoT

(Казанский национальный исследовательский технический университет
им. А.Н.Туполева-КАИ)

Технология IoT (интернет вещей) набирает с каждым годом всё больше интереса и популярности. Выходят большинство новостей о «умных» бытовых приборах (чайник, холодильник, кофеварка и т.п.). Например, имеется статья про создание интернет-розетки, при помощи которой можно управлять чайником через интернет. Появляются компании, которые предлагают управлять холодильниками, кофеварками и даже автомобильными парковками. Так что же это такое IoT (интернет вещей)?

IoT – концепция вычислительной сети физических предметов, оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека [1].

IoT использует те же протоколы, которые используем мы для передачи информации с одного персонального устройства (ПК, ноутбук, смартфон и т.п.) на другой при помощи сети интернет. Только в качестве исходящих или принимающих устройств выступают бытовые приборы, двери, окна и т.п. Благодаря технологии IoT имеется возможность создания полноценных «умных» домов, когда удаленно при помощи смартфона и интернета мы можем открывать или закрывать окна, выключать и включать электричество, запустить кофемашину, включить телевизор и т.п.

Также IoT предусматривает автономную работу обмена данными между устройствами без участия человека. Благодаря этим двум факторам, бытовые предметы могут превратиться в интернет-узлы. И уже имеются экспертные исследования проблем безопасности IoT. Уже в 2008 г. (в этом году IoT появилось как явление) IoT фигурирует в отчете Национального разведывательного совета США в качестве одной из шести потенциально разрушительных технологий.

В 2015 году, компания OpenDNS представила собственные результаты исследования, проведенного в корпоративных сетях, которые используют технологию IoT. Бренд OpenDNS принадлежит компании Cisco, одному из лидеров

в области IT, с которым связаны общепринятая формулировка термина «IoT» и популяризация этой технологии.

Компания OpenDNS, исходя из результатов исследования, заявила: безопасного IoT не существует. Инфраструктура, которая используется для подключения устройств в корпоративные сети, не контролируется ни пользователями, ни IT-специалистами. Вот лишь некоторые выкладки из экспертного отчета [2]:

- только 35% компаний используют отдельную Wi-Fi сеть для потенциально небезопасных «интернет-вещей»;
- видеокамеры, медицинские гаджеты, фитнес-браслеты и другое оборудование передают данные за пределы корпоративной сети;
- большинство телевизоров, интегрированных в IoT, не имеют сертификатов безопасности;
- жесткие диски используют для хранения данных небезопасные облачные серверы.

Также к этим уязвимостям можно добавить возможные преднамеренные электромагнитные воздействия на используемые корпоративные сети, сети электропитания и перехваты информативных электромагнитных излучений [3, 4, 5, 6].

Собственное исследование провела компания HP, в потребительском секторе. Результаты оказались аналогичными. В этом случае также были выявлены множества уязвимостей, начиная от применения дефолтных паролей и заканчивая незащищенным веб-интерфейсом, который используют большинство устройств, подключенных к IoT. Было выявлено, что исследуемые девайсы собирают личную информацию пользователей, которые могут быть успешно перехвачены злоумышленником [7].

В данный момент, системы безопасности IoT не очень эффективны. Для совершения некоторых киберпреступлений злоумышленникам будет легче взломать приборы, подключенные к IoT, нежели личные устройства пользователей. Парк «умных» устройств стремительно пополняется. Сегодня к сети подключается около 6 000 000 «умных» приборов ежедневно. Зная, что почти каждый девайс имеет не одну проблему в безопасности, а несколько, то ситуация складывается плачевной.

Вот некоторые киберпреступления, которые могут совершить злоумышленники, используя IoT:

- кража пользовательских данных. Для бесперебойной работы большинство «умных» приборов собирают пароли и личную информацию, начиная от имени пользователя и заканчивая фактами из биографии. Для хранения пользовательских данных нужна надежная защита, которой похвастаться IoT не может в данный момент;
- быстрое создание мощного ботнета из множества устройств, используемых IoT. Так как пользователи используют дефолтные пароли и небезопасные сети, то легче взломать и получить удаленный доступ к IoT – устройствам, нежели к персональным устройствам (ПК, смартфоны и т.п.).

Исходя из проблем безопасности IoT и возможностей использования злоумышленниками данной технологии, можно предложить некоторые решения для повышения безопасности IoT:

• единая стандартизация для установки регламента для каждой области IoT. В 2016 году Еврокомиссии предоставила планы по обязательной сертификации предметов, интегрированных в IoT. Один из вариантов сертификации является необходимость внедрение чипов в приборы, подключенные к глобальной сети. Но речь идет о тех устройствах, которые сами по себе не представляют ценности для преступников, но могут быть использованы для создания ботнетов – холодильниках, телевизорах, видеокамерах, принтерах и т.п.;

• каждая категория устройств, встроенных в IoT, должна использовать не более двух-трех платформ. Например, все холодильниками должны быть оснащены с типичными микроконтроллерами, прошивками, и, например, видеокарты должны использовать одинаковые драйверы;

• улучшенная производительность самого ПО. Улучшение безопасности в плане проникновения и масштабируемости, так как IoT – приборов становится с каждым днём всё больше.

IoT находится только в начале своего развития, как когда-то и компьютеры. Компьютеры тоже были уязвимы, были совершены множества хакерских атак, глобальных распространений вирусов. И проблемы в плане безопасности имеют место быть в технологии IoT. В данный момент персональные устройства, например, компьютеры, имеют хорошую безопасность от хакерских атак и вирусов. Вместе с развитием IoT будет развиваться и их безопасность, как развивалась безопасность персональных устройств.

Литература

1. Из чего состоит IoT // Хабрахабр. - 2019. - 19 января [Электронный ресурс]. URL: https://habr.com/ru/post/436708/ (дата обращения: 20.04.2019).

2. Интернет вещей: обзор проблем безопасности // Блог о разном: тренды, идеи, развитие. - 2017. - 19 сентября [Электронный ресурс]. URL: https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti/ (дата обращения: 22.04.2019).

3. Гизатуллин З.М., Набиев И.И., Шкиндеров М.С. Помехоустойчивость локальных вычислительных сетей при внешних электромагнитных воздействиях // Телекоммуникации. 2017. – №2. – С. 41-47.

4. Гизатуллин З.М., Гизатуллин Р.М., Шкиндеров М.С., Нуриев М.Г., Салимов Р.И. Моделирование электромагнитных помех в неэкранированной витой паре при внешних электромагнитных воздействиях // Журнал радиоэлектроники. – 2016. – №12. – С. 1.

5. Гизатуллин Р.М., Гизатуллин З.М. Помехоустойчивость и информационная безопасность вычислительной техники при электромагнитных воздействиях по сети электропитания: монография. – Казань: Изд-во Казан. гос. техн. ун-та, 2014. – 142 с.

6. Гизатуллин З.М., Нуриев М.Г., Шкиндеров М.С., Назметдинов Ф.Р. Простая методика исследования электромагнитного излучения от электронных средств // Журнал радиоэлектроники. – 2016. – №9. – С. 7.

7. 7 причин, почему Интернет вещей должно вас пугать [Электронный ресурс]. URL: https://alfa-service42.com/tehnologii/internet-veschey-obzor-problem-bezopasnosti.html (дата обращения: 12.05.2019).

Т.А. Курзенева

NFC-МЕТКИ КАК ЭЛЕМЕНТ «УМНОГО ДОМА» И ОБЕСПЕЧЕНИЕ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

В настоящее время экономия времени на выполнении бытовых задач и соответствующая адаптация устройств является актуальным направлением в информационных технологиях. Обеспечение дома или любого другого помещения с использованием элементов и устройств вычислительных систем, позволяющих выполнять повседневные задачи или иные пожелания владельца относится к системам «Умного дома». Данные системы разрабатываются на основе различных технологий: от высокотехнологичных систем, позволяющих объединить множество устройств и отдать их под управление искусственного интеллекта до небольших элементов, обеспечивающих работу таких систем.

Near field communication, NFC («коммуникация ближнего поля», «ближняя бесконтактная связь») – технология беспроводной высокочастотной связи малого радиуса действия. Такая технология позволяет обмениваться данными между устройствами, расположенными на близком расстоянии (не более 10 сантиметров). Разработано 2 вида устройств на основе NFC технологии: активные (создают поля, позволяющее считывать) и пассивные (не создают полей, с них можно только считать).

NFC-метки представляют собой антенну минимальных размеров (обычно толщиной с бумажный лист и диаметром 1,5-2 сантиметра), осуществляющую пассивную передачу данных. NFC-метки можно запрограммировать для выполнения различных задач, облегчающих жизнь современного человека.

В настоящее время привычным стало использование NFC технологий в телефонах для оплаты. Однако возможности применения такой технологии гораздо шире. Например, можно установить NFC-метку на зарядное устройство в машине и обеспечить тем самым беспроводную зарядку или можно запрограммировать девайс на автоматическое подключение к точке доступа. Наклеив чип на поверхность прикроватной тумбы и задав правильную команду, можно установить будильник, изменить мелодию или отрегулировать яркость экрана на ночную. NFC-метку можно наклеить на лобовое стекло машины вместо номера, тогда если ваша машина будет мешать проезду, используя одно