УДК 004.7

ЗАЩИТА ИНФОРМАЦИИ В ИНТЕРНЕТЕ ВЕЩЕЙ IOT  
  
КАЗАНЦЕВА Л.В., КОНАКОВ П.О.

МИРЭА - Российский технологический университет 119454, Россия, г. Москва, проспект Вернадского, 78, konakov.po@yandex.ru

В данной статье рассказывается о потенциальных угрозах безопасности устройств интернета вещей (IoT – Internet of Things), а также о последствиях, которые влекут за собой недостаточное соблюдение мер предосторожности при использовании данной технологии.

Ключевые слова: безопасность, интернет вещей, шифрование, безопасная передача данных.

PROTECTION OF INFORMATION ON THE INTERNET IOT STUFF  
  
KAZANTSEVA L.V., KONAKS P.O.

MIREA - Russian Technological University 119454, Russia, Moscow, 78 Vernadsky Avenue, konakov.po@yandex.ru

This article describes the potential threats to the security of Internet of Things devices, as well as the consequences of not taking sufficient precautions when using this technology.

Keywords: security, internet of things, encryption, secure of data transfer.

**Развитие технологии**

В связи с большим развитием беспроводных технологий передачи данных, возникновением технологий облачных вычислений, а также постепенным переходом интернета на новый интернет-протокол IPv6 в последнее время получило развитие технология Интернета вещей (IoT – Internet of Things). Данная технология подразумевает взаимодействие устройств между собой, а также окружающей средой, исключая взаимодействие с человеком, которая позволяет решать некоторые вопросы автоматизации намного эффективнее и экономически выгоднее (с долгосрочной перспективой).

На 2018 год насчитывается около 22 миллиарда подключённых IoT-устройств, и это число постоянно растёт [1]. Однако повышением количества подключённых устройств растёт и угроза их безопасности, поскольку большинство из приборов уже после 5-ти минут подключения к сети подвергаются атаке [2]. В результате перехвата доступа к устройству злоумышленник может использовать его в своих корыстных целях.

В данной статье повествуется об основных аспектах безопасности при проектировании и конструировании IoT-систем, основных угрозах, с которыми можно столкнуться, а также последствиями, обусловленными пренебрежением к уровню безопасности устройств и передачи информации между ними.

**Фундаментальные аспекты безопасности в IoT**

Рассмотрим аспекты, которые надо учитывать при развёртывании системы, способную предотвратить пагубное воздействие от большинства угроз безопасности, возникающих при использовании интернета вещей. Среди них выделяют следующие: защита устройств, безопасность связи, контроль устройств и контроль взаимодействия сети [3]. Поговорим теперь о каждом по отдельности.

**Защита устройств** – обеспечение безопасности и целостности программного кода. В рамках устройства необходимо реализовывать криптографическое подписание сходного кода, необходимое для подтверждения правомерности запуска кода, чтобы исключить возможность внедрения вредоносного фрагмента злоумышленником во время его загрузки. Необходимо, чтобы все важные устройства, которые передаюn какие-то данные, были настроены на запуск только подписанного кода.

**Безопасность сети.** Помимо внутренней защиты устройств, надо гарантировать безопасную передачу данных через каналы связи. Для их защиты используют алгоритмы шифрования, а также технологии проверки подлинности доставленного пакета данных, чтобы устройства могли понять, могут ли они доверять данным, полученным от удалённой системы.

**Контроль устройств.** Вместе с развитием систем безопасности IoT-устройств также развиваются и методы их обхода. Ни одна система не является безопасной. Поэтому существует необходимость сопровождения этих систем обновлённым ПО даже после её передачи потребителю. Однако будет совсем не выгодно отправлять своих сотрудников на дом к клиентам, чтобы они могли установить новую версию прошивки. А если количество устройств рассчитывается десятками или сотнями тысяч? Поэтому необходимо позаботиться о том, чтобы на устройствах обеспечить “управляемость по воздуху” до того, как продукт попадёт к потребителям.

**Контроль взаимодействий в сети.** Некоторые угрозы в любом случае смогут преодолеть предпринятые меры по обеспечению безопасности в независимости от того, насколько хорошо вы занимались защитой. Именно поэтому лучше иметь возможность анализировать состояние систем в IoT. Системы для аналитики безопасности помогут заметить злонамеренные и подозрительные аномалии в работе устройств или передаваемых данных.

Это только основные аспекты, базовые рекомендации, которые подходят ко всем отраслям, в рамках которой можно развернуть данную систему. Также важно понимать, что в каждой сфере будут свои индивидуальные особенности, которые нужно учитывать при проектировании системы безопасности.

Поскольку проблема остро строит в сфере информационных технологий, специалисты в области кибер-безопасности. Международная организация OWASP (Open Web Application Security Project) была озабочена данной проблемой уже давно. И в 2018 году представила свой актуализированный топ-10 уязвимостей IoT-технологий [4], первая версия которого вышла ещё в далёком 2014 году. Этот проект был разработан в помощь разработчикам и компаниям, занимающихся использованием или разработкой IoT-систем.

**10 место – Недостаточная физическая безопасность**

Отсутствие мер по физической защите, позволяющее потенциальным злоумышленникам получить конфиденциальную информацию, которая в будущем может помочь реализовать удалённую атаку или получить локальный контроль над устройством

Компоненты экосистемы IoT расположены в обширном пространстве для большего контроля, и в большинстве своём устанавливаются в малозащищённых местах, к которым злоумышленник может легко добраться при должном желании. Скопировав себе настройки с устройства, он может спокойно проникнуть в систему управления для снижения эффективности работы системы или заражения системы вредоносным ПО.

**9 место – Небезопасные настройки по умолчанию**

Устройства или системы поставляются с небезопасными настройками по умолчанию или не имеют возможности сделать систему более безопасной, ограничивая пользователей в изменении конфигурации

Производитель хочет заработать больше, а работать меньше. В устройствах может быть много всяких функций, однако при этом в большинстве случаев упускается обеспечение оборудования требуемым уровнем защиты. Например, отсутствует проверка пароля на надёжность, настройка параметров шифрования данных или нет разграничения доступа по ролям (пользователь и администратор).

**8 место – Отсутствие возможности управлять устройством**

Отсутствие поддержки безопасности на устройствах, развёрнутых в производстве, включая управление активами, управление обновлениями, безопасный вывод из эксплуатации, мониторинг систем и реагирование.

Устройства IoT в основном представляют собой “чёрный ящик”, не предоставляя пользователям никакой информации о запущенных процессах и не давая возможности проверки на целостность загруженного ПО. Во время атаки прошивка устройства может быть так переконфигурирована, что восстановить функционал можно будет только при полной перепрошивке.

**7 место – Небезопасная передача и хранение данных**

Отсутствие шифрования или контроля доступа к конфиденциальным данным в любом месте экосистемы, в том числе при хранении, при передаче или во время обработки.

Устройства интернета вещей получают и хранят большие объёмы данных об окружающей среде, а также персональную информацию. Украденный пароль можно заменить, а вот данные о биометрии (глаз, отпечатки пальцев, лицо) – нет. Помимо этого, устройства могут и передавать данные по сети в незашифрованном виде. Если же рассматривать передачу данных в рамках локальной сети, то это ещё можно объяснить, то в случае беспроводной сети, то они могут стать достоянием всех и каждого.

**6 место – Недостаточная защита конфиденциальности**

Личная информация пользователя, хранящаяся на устройстве или в экосистеме, которая используется небезопасно, ненадлежащим образом или без разрешения.

Данная причина перекликается с предыдущей, однако здесь идёт речь о защите тайны личной жизни. Все данные, которые собирают устройства без ведома владельцев, в руках злоумышленника используются при шантаже.

**5 место – Использование небезопасных или устаревших компонентов**

Использование устаревших или небезопасных программных компонентов или библиотек, которые могут позволить скомпрометировать устройство. Это включает небезопасную настройку платформ операционной системы и использование сторонних программных или аппаратных компонентов из скомпрометированной цепочки поставок.

**4 место – Отсутствие безопасных механизмов обновления**

Отсутствие возможности безопасного обновления устройства. Это включает в себя отсутствие валидации прошивки на устройстве, отсутствие безопасной доставки (без шифрования при передаче), отсутствие механизмов предотвращения отката и отсутствие уведомлений об изменениях безопасности из-за обновлений.

Отсутствие возможности обновить прошивку устройства само по себе является слабым местом безопасности. Отсутствие обновления означает, что устройство будет уязвимо к угрозам неопределённый промежуток времени. Однако и само обновление ПО может быть не безопасно. Возможно, отсутствует шифрование обновления или проверка данного кода на целостность и наличия сертифицированных ключей, возможно также отсутствует система оповещения об изменениях в системе после обновлений.

**3 место – Небезопасные интерфейсы экосистемы**

Небезопасный веб-интерфейс, API, облачные или мобильные интерфейсы в экосистеме вне устройства, что позволяет компрометировать устройство или связанные с ним компоненты. Общие проблемы включают в себя отсутствие аутентификации или авторизации, отсутствие или слабое шифрование, а также отсутствие фильтрации ввода и вывода.

Использование небезопасных API и веб-интерфейсов позволяет скомпрометировать устройство или связанные с ним компоненты без подключения к нему.

В основном это связано с тем, что веб-интерфейс может быть подвержен межсайтовому скриптингу и SQL-инъекциям. Поэтому в данных системах рекомендуется реализация системы авторизации с восстановлением пароля.

**2 место – Небезопасные сетевые сервисы**

Ненужные или небезопасные сетевые службы, запущенные на самом устройстве, особенно открытые для внешней сети, ставящие под угрозу конфиденциальность, целостность, подлинность, доступность информации или допускающие несанкционированное удаленное управление.

Небезопасные сетевые службы ставят под угрозу безопасность устройства, особенно если они имеют доступ к интернету. Он могут быть подвержены DDoS-атакам. Открытые сетевые порты могут быть просканированы на наличие уязвимостей и небезопасных служб для подключения.

**1 место – Слабый, угаданный или жёстко заданный пароль**

Использование легко взламываемых, общедоступных или неизменяемых учетных данных, включая бэкдоры во встроенном программном обеспечении или клиентском программном обеспечении, которое предоставляет несанкционированный доступ к развернутым системам. В результате такой не бдительности о смене пароля, в июне 2019 года воспользовалось вредоносное ПО Silex, которое в течение часа сломало около 2000 устройств интернета вещей, используя базовые комбинации логин-пароля для всех устройств [5].

Когда потребители приобретают устройства технологии Интернета вещей, в большинстве они задумываются лишь о комфорте их использования, пренебрегая в большинстве случаев вообще какими-либо мерами безопасности. В результате чего злоумышленникам открывается доступ к тысячам устройств, действиями которых они могут пользоваться как хотят. Самое очевидное – использование взломанных IoT-устройств в целях DDoS-атак, спам-атак, а также скрытый майнинг криптовалюты[6]. В последние 2 года проводилось расследование по источникам DDoS-атак. На первом месте находится протокол Telnet, который широко использовался устройствами интернета вещей. Количество девайсов, которые под контролем протокола производили атаки на сервера, исчисляется сотнями миллионов (Рис. 1)[7][8]. Однако на данный момент существуют проекты, которые разрабатывают свои системы безопасного управления IoT-устройствами, например, Центр Интернета вещей Azure, проект от компании Microsoft.

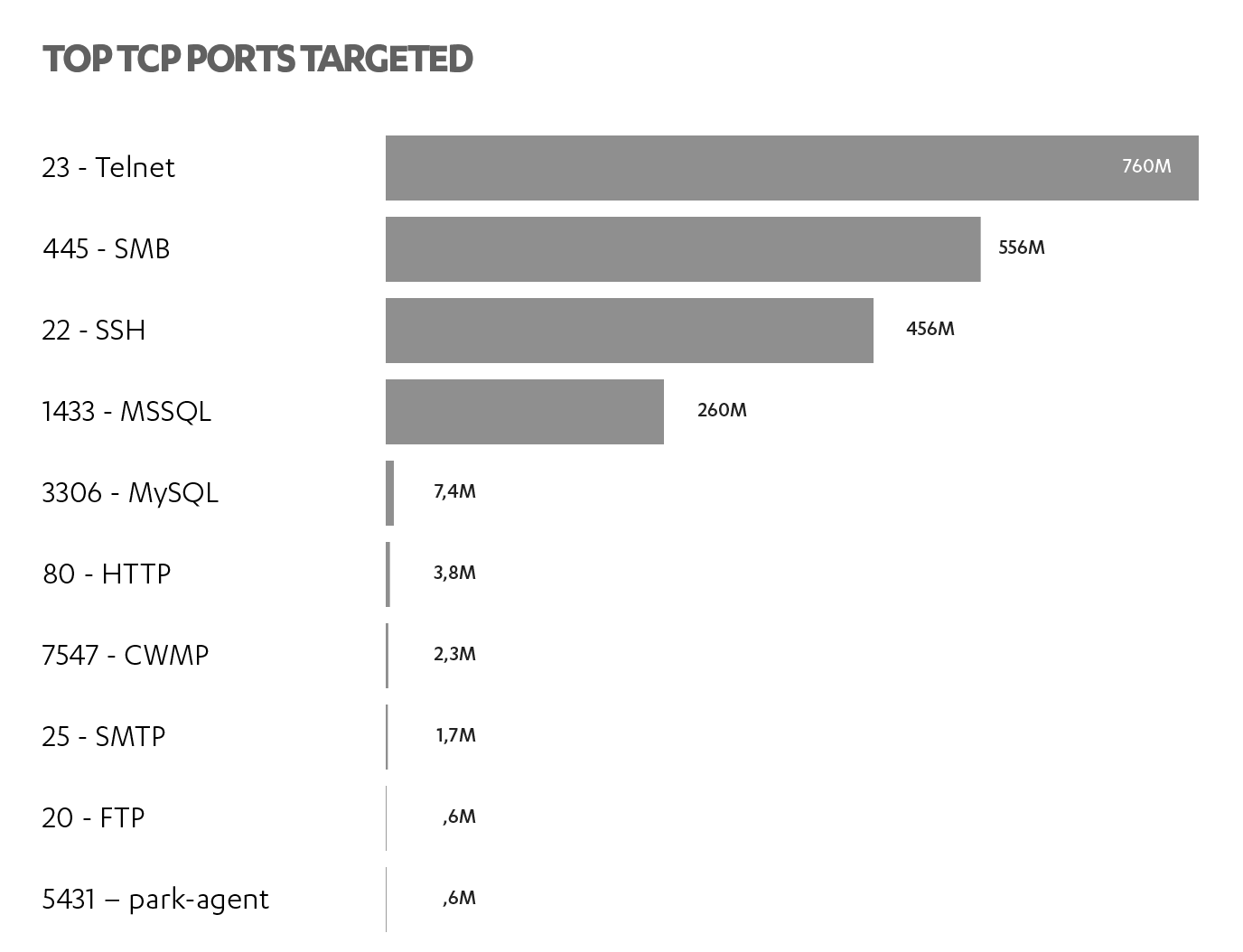


Рис. 1 – Топ протоколов, по которым происходили атаки

Он позволяет серверной части решения, расположенной в облаке, виртуально подключаться к любому устройству. Помимо этого, работу системы можно обеспечит как на облаке, так и на пограничных устройствах с помощью системы аутентификации каждого устройства, что также значительно повышает уровень безопасности системы за счёт конфиденциальных сообщений между облаком и устройствами [9].

Исходя из выше сказанного, можно сделать вывод, что на данный момент существует множество уязвимых мест в сфере технологии интернета вещей, в основном связанные с неграмотностью пользователей в данной области и безответственным отношением к потенциальным угрозам безопасности. Вопреки этому, всё же существуют сервисы автоматизированного сопровождения таких систем, которые ориентированы в большинстве своём именно на потребителя, а не на разработчика и проектировщика.

Список литературы

1. Evgeniy Bryndin. Development of sensitivity and active behavior of cognitive robot by means artificial intelligence. International Journal of Robotics Research and Development. VOL - 10, ISSUE - 1; 2020. Pages: 1-11.

2. Брындин Е.Г. Роботы с искусственным интеллектом и спектроскопическим зрением на высокотехнологичном рынке труда. Журнал "Мягкие вычисления и измерения". № 9. 2019. С. 49-56.

3. Evgeniy Bryndin. Program Hierarchical Realization of Adaptation Behavior of the Cognitive Mobile Robot with Imitative Thinking. International Journal of Engineering Management. Volume 1, Issue 4. 2017, pp. 74-79

4. Evgeniy Bryndin. Cognitive Robots with Imitative Thinking for Digital Libraries, Banks, Universities and Smart Factories. International Journal of Management and Fuzzy Systems. V.3, N.5, 2017, pp 57- 66.

5. Evgeniy Bryndin. Communicative Associative Logic of Cognitive Professional Robot with Imitative Thinking. Journal Engineering Mathematics, Volume 2, Issue 2. 2018. Pages: 79-85.

6. Е.Г. Брындин. Когнитивные профессиональные роботы с переобучением навыков. Материалы III международной конференции «Когнитивная робототехника». Издательский Дом ТГУ. 2018. С. 3-6.

7. Evgeniy Bryndin. System retraining to professional competences of cognitive robots on basis of communicative associative logic of technological thinking. International Robotics Automation Journal. 2019; 5(3.):112‒119

8. Evgeniy Bryndin. Collaboration of Intelligent Interoperable Agents via Smart Interface. International Journal on Data Science and Technology, Vol. 5, Issue 2. 2019

References

1. Evgeniy Bryndin. Development of and active behaviour of cognitive robot by means of artificial intelligence. International Journal of Robotics Research and Development. VOL - 10, ISSUE - 1; 2020. Pages: 1-11.

2. E.G. Bryndin Robots with Artificial Intelligence and Spectroscopic Vision in the High Technology Labour Market. Magazine "Soft Computing and Measurement". № 9. 2019. С. 49-56.

3. Evgeniy Bryndin. Program Hierarchical Realization of Adaptation Behavior of the Cognitive Mobile Robot with Imitative Thinking. International Journal of Engineering Management. Volume 1, Issue 4. 2017, pp. 74-79

4. Evgeniy Bryndin. Cognitive Robots with Imitative Thinking for Digital Libraries, Banks, Universities and Smart Factories. International Journal of Management and Fuzzy Systems. V.3, N.5, 2017, pp 57- 66.

5. Evgeniy Bryndin. Communicative Associative Logic of Cognitive Professional Robot with Imitative Thinking. Journal Engineering Mathematics, Volume 2, Issue 2. 2018. Pages: 79-85.

6. E.G. Bryndin. Cognitive professional robots with retraining of skills. Materials of the III International Conference "Cognitive Robotics". Publishing House of TSU. 2018. С. 3-6.

7. Evgeniy Bryndin. System retraining to professional competences of cognitive robots on the basis of communicative associative logic of technological thinking. International Robotics Automation Journal. 2019; 5(3.):112‒119

8. Evgeniy Bryndin. Collaboration of Intelligent Interoperable Agents via Smart Interface. International Journal on Data Science and Technology, Vol. 5, Issue 2. 2019