УДК 004.7

И.И. Безукладников, А.А. Миронова

I.I. Bezukladnikov, A.A. Mironova

Пермский национальный исследовательский
политехнический университет

Perm National Research Polytechnic University

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ

INFORMATION SECURITY OF MODERN WIRELESS TECHNOLOGIES

Рассматривается тенденция последнего времени, связанная с переходом от централизованных клиент-серверных архитектур к частично и полностью распределенным. Проводится аналитический обзор наиболее популярных беспроводных протоколов: 6LoWPAN и Bluetooth 4.0 LE. Выявлены основные угрозы их информационной безопасности и уязвимости, а также описаны методы борьбы с ними, предлагаемые разработчиками.

Ключевые слова: беспроводные технологии, информационная безопасность, распределенные сети, технология 6LoWPAN, технология Bluetooth 4.0 LE.

This paper considers a recent trend in modern wireless technologies, associated with the transition from centralized (client-server) architectures to partially- and fully-distributed ones. Analytical review of the most popular wireless protocols and technologies such as 6LoWPAN, Bluetooth 4.0LE was carried out. Main security threats and vulnerabilities, as well as methods of dealing with them, offered by developers, were revealed and classified for all of the mentioned technologies.

Keywords: wireless technologies, information security, stratified architectures, 6LoWPAN technology, Bluetooth 4.0 LE technology.

В последнее время все большую популярность приобретают беспроводные технологии, они развиваются и повсеместно внедряются во многие области науки, промышленности, жизни, занимая место своих проводных аналогов – от компьютерных и периферийных интерфейсов до магистральных сетей. Основными преимуществами данного вида связи являются простота реализации и подключения пользователей, а также мобильность пользователей в зоне действия сети. Ведутся активные исследования в области беспроводных сетей, изучаются такие вопросы, как беспроводная передача энергии, контроль промышленных объектов и производственных процессов, внедрение беспроводных устройств мониторинга и управления, контроль состояния здоровья человека.

По прогнозам компании Cisco – одного из мировых лидеров в сфере телекоммуникационных технологий, к 2019 г. в сетях передачи данных будет существенно преобладать трафик, генерируемый беспроводными устройствами: он составит порядка 66 % от общего объема передаваемой информации [1].

Огромное разнообразие известных сегодня беспроводных технологий может быть условно разделено на следующие классы: персональные беспроводные сети, беспроводные локальные сети, беспроводные сети масштаба города, беспроводные глобальные сети.

К персональным беспроводным сетям относятся WPAN-сети (Wireless Personal Area Network). Наиболее распространенной технологией среди них являются сети Bluetooth, которые позволяют связать телекоммуникационные устройства на расстоянии до 10 м.

Беспроводные локальные сети – сети WLAN (Wireless Local Area Network), чаще их называют сетями Wi-Fi (Wireless Fidelity), так как технология Wi-Fi является самой известной среди них. Зона их действия может колебаться от 50 до 300 м.

К классу беспроводных сетей масштаба города относятся WMAN-сети (Wireless Metropolitan Area Networks). Наиболее популярным представителем среди них считаются WiMAX-сети, радиус их действия может достигать 10 км [2].

WWAN-сети (Wireless Wide Area Network) относятся к классу беспроводных глобальных сетей. Примерами таких сетей являются беспроводные технологии сотовой связи GPRS, расстояние действия которых превышает 10 км.

Однако с внедрением беспроводных технологий становится все более актуальной проблема обеспечения их информационной безопасности (ИБ), поскольку беспроводные сети обладают свойством открытости и их можно считать публичными [3]. При этом конечные цели, которые преследуют злоумышленники, могут быть различными, например похищение конфиденциальной информации или кража интернет-трафика.

Отдельно стоит отметить тенденцию последнего времени, связанную с переходом от централизованных клиент-серверных архитектур к частично и полностью распределенным (облачные сервисы, peer-to-peer, mesh-сети). По состоянию на текущий год в коммерческой эксплуатации насчитывается уже более десятка широко применяемых беспроводных технологий, имеющих опциональный mesh-режим либо для которых такой режим является основным/единственным.

При этом подавляющее множество существующих механизмов ИБ имеет централизованную архитектуру и основано на доверии между субъектами информационного обмена [4]. Так, например, типичная процедура защищенного общения состоит из обмена информацией с доверенным парт-

нером. Подобные механизмы крайне плохо применимы для распределенных сетей без серьезной переработки либо не применимы вообще.

Особенно остро эта проблема стоит для компаний, занимающихся разработкой соответствующих протоколов и технологий, поскольку даже в условиях существования утвержденных стандартов, описывающих реализацию базовых механизмов ИБ, в распределенной сети они практически не применимы. Зачастую при данных обстоятельствах каждая из компаний-разработчиков вынуждена решать вопросы безопасности в своих продуктах по мере возможности и бессистемно.

Настоящая работа посвящена аналитическому обзору наиболее популярных беспроводных протоколов и выявлению основных угроз ИБ и уязвимостей, а также методов борьбы с ними, которые предлагают разработчики. Конечной целью работы являются систематизация имеющихся наработок и попытка создания обобщенной модели угроз, характерных для распределенных беспроводных технологий, а также оценка глубины и системности подхода к безопасности среди этих технологий.

Ниже (табл. 1, 2) представлен фрагмент проведенного анализа для двух наиболее популярных беспроводных технологий, имеющих mesh-организацию: Bluetooth 4.0 LE и 6LoWPAN.

Таблица 1

Технология 6LoWPAN

№ п/п	Угрозы	Предлагаемые меры противодействия
1	Физические атаки	Угрозы безопасности следует четко понимать и документировать. Начальная загрузка устройств должна рассматриваться с учетом местоположения. Существующие технологии IP-безопасности должны быть упрощены для реализации в 6LoWPAN
2	Отказ в обслуживании (DoS-атаки)	
3	“sleepdeprivationtorture”	
4	Нарушение доступности сети	
5	Атака на ключевой процесс распределения идентификаторов	
6	Изменение информации при маршрутизации	
7	Выборочное продвижение данных (Selective for Warding) – злоумышленник отбрасывает определенные сообщения, гарантируя, что они не будут распространены дальше	
8	Атака воронки (Sinkhole Attack) – препятствует получению базовой станцией полных и корректных данных	
9	Атаки Сибиллы – злоумышленник создает узел, тождественный другим узлам сети	
10	Wormhole-атаки – атаки, действующие по принципу червя	
11	Атаки Neighbor Discovery	

Таблица 2

Технология Bluetooth 4.0 LE

№ п/п	Угрозы	Предлагаемые меры противодействия
1	BlueSnarfing – атака, позволяющая подключиться к устройству Bluetooth, тем самым получив доступ к данным, хранящимся на устройстве, в том числе международный идентификатор мобильного оборудования (IMEI)	Отключать возможности Bluetooth, когда они не используются. Устройства Bluetooth должны быть настроены по умолчанию как неопознаваемые и оставаться неопознаваемыми, за исключением необходимости спаривания
2	BlueJacking – злоумышленник может инициировать BlueJacking, отправив нежелательные сообщения пользователю Bluetooth. BlueJacking может причинить вред, когда пользователь инициирует ответ на отправленное сообщение BlueJacking с отрицательными намерениями	Требовать авторизацию для всех входящих запросов на соединение. Не принимать передачи любого вида из неизвестных или подозрительных устройств. Эти типы передач включают в себя сообщения, файлы и изображения
3	BlueBugging – эта атака использует команды устройства без уведомления пользователя, что позволяет атакующему получить доступ к данным, прослушивать телефонные звонки, отправлять сообщения и использовать другие услуги или функции, предлагаемые устройством	Устройства Bluetooth должны быть настроены по умолчанию как неопознаваемые и оставаться неопознаваемыми, за исключением необходимости спаривания
4	CarWhisperer – это программный инструмент, которые эксплуатирует интерфейс Bluetooth, установленный в автомобилях. Программное обеспечение автомобилей позволяет злоумышленнику отправить или получить звук от автомобильного комплекта	Отключать возможности Bluetooth, когда они не используются. Выполнять сопряжение как можно реже, в идеале в безопасной зоне. Установить уровень мощности устройств Bluetooth минимально возможным, когда устройства будут обеспечивать функциональность
5	FuzzingAttacks – атаки Fuzzing состоят из посылки искаженного или нестандартного пакета данных для Bluetooth-радиоустройства и «наблюдают», как устройство реагирует	Установить антивирусное программное обеспечение
6	PairingEavesdropping – сопряжение устройств Bluetooth 2.0 и ранее, а также Bluetooth LE (4.0) с использованием PIN-кода подвержено данному типу атак. Позволяет определить секретный ключ и сделать расшифровку данных	Необходимо отслеживать, чтобы не использовались настройки и пароли по умолчанию. Выбирать PIN-коды, которые являются случайными. Избегать статических и слабых PIN, таких как нули. Использовать предельно допустимые размеры ключа, тем самым обеспечивая защиту от атак перебором. Пароли должны быть действительны в течение ограниченного срока
7	SecureSimplePairingAttacks – ряд методов, которые могут заставить устройство работать дистанционно	Установить антивирусное программное обеспечение

Bluetooth 4.0 LE – беспроводная технология Bluetooth с низким энергопотреблением. Устройства, использующие данную спецификацию, будут потреблять меньше энергии, таким образом, увеличится время связи данных устройств в пределах персональных сетей. Технология Bluetooth 4.0 LE позволяет использовать большое количество приложений и дает возможность уменьшать размеры конечных устройств.

6LoWPAN (IPv6 overLow-Power Wireless Personal Area Networks) – стандарт взаимодействия по протоколу IPv6 поверх маломощных беспроводных персональных сетей стандарта IEEE 802.15.4.6LoWPAN – позволяет маломощным беспроводным устройствам использовать протокол IPv6, а также обеспечивает доступ к этим устройствам через глобальную сеть по уникальному IP-адресу. Область применения данного протокола обширна и включает автоматизацию зданий, учет потребляемых ресурсов, управление уличным и домашним освещением, технологию «Умный дом», промышленные системы распределенного управления и др. [5].

В ходе анализа рассмотрены предложения в области безопасности от ведущих организаций: рекомендации Национального института стандартов и технологий, интернет-проект Samsung Electronics по анализу безопасности 6LoWPAN и др.

По итогам проведенного анализа были сделаны следующие основные выводы:

1. Системный подход к анализу угроз ИБ, основанный на использовании обобщенных моделей, подходов и методов в обеих технологиях отсутствует. При этом разработчики конкретных технологий ведут независимую проработку вопросов ИБ. Это приводит к тому, что более ранняя технология Bluetooth имеет значительно более проработанные элементы ИБ, а более современная 6LowPAN, по существу, снова начинает «исследование вопроса ИБ» практически с нуля. Переноса имеющихся наработок практически не выявлено.

2. Основная масса механизмов безопасности направлена против конкретных атак, которые не переносимы на другие технологии, что требует некоторой переработки. В рекомендациях также отсутствуют методы противодействия нетрадиционным атакам (посредством стеганографических методов, при помощи скрытых каналов и т.д.).

3. Недостаточно внимания уделяется специфическим распределенным атакам и инсайдерским угрозам. Механизмы безопасности 6LoWPAN, в сравнении с механизмами Bluetooth 4.0 LE, являются архитектурными и не несут в себе конкретных способов противодействия угрозам. Многие механизмы безопасности определены по остаточному принципу, в связи с этим отсутствует комплексный подход к безопасности информации.

Список литературы

1. Гущина О. Беспроводное будущее: геологические исследования по Wi-Fi и авиадвигатель с Bluetooth [Электронный ресурс]. – URL: http: // rosnauka.ru/publication/782 (дата обращения: 18.08.2016).

2. Маркелов К.С., Нейман А.Б. Безопасность беспроводных сетей // Молодой ученый. – 2012. – № 4. – С. 63–66.

3. Шабуров А.С., Миронова А.А. О повышении эффективности защиты персональных данных в информационных системах открытого типа // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2015. – № 6. – С. 106–117.

4. Шабуров А.С., Рашевский Р.Б. Реализация отказоустойчивого распределенного межсетевого экрана // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2014. – № 11. – С. 129–136.

5. Олссон Дж. Раскрываем тайны 6LoWPAN // Новости электроники. – 2015. – № 11.

Получено 02.09.2016

Безукладников Игорь Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика», электротехнический факультет, Пермский национальный исследовательский политехнический университет, e-mail: fantomtk@yandex.ru.

Миронова Анна Алексеевна – студентка кафедры «Автоматика и телемеханика», электротехнический факультет, Пермский национальный исследовательский политехнический университет, e-mail: mir550@yandex.ru.