Возрастание рисков информационной безопасности при использовании M2M технологий

Владимир ВОРОТНИКОВ,
руководитель отдела перспективных исследований и проектов, ЗАО «С-Терра СиЭсПи»

Взаимодействие с различными устройствами уже прочно вошло в нашу жизнь. Тем не менее обмен данными происходит не только между человеком и техникой. Довольно часто устройства общаются непосредственно между собой. Такие технологии носят название «межмашинное взаимодействие» (M2M – «от машины к машине»). M2M-технологии давно применяются в промышленности и уже созрели для перехода на массовый пользовательский рынок. Да и наступающее высокотехнологическое будущее немыслимо без повсеместного распространения M2M-технологий. Однако если не озаботиться вопросами защиты M2M, последствия будут катастрофическими в прямом смысле этого слова. Но обо всем по порядку.

Существует несколько классификаций межмашинного взаимодействия. В рамках данной статьи рассмотрим две из них:

– по способу взаимодействия: по собственным протоколам; внутри локальной сети с использованием существующих протоколов (например, Ethernet); через глобальные сети, с использованием существующих протоколов; – по областям применения: финансовый сектор, транспорт и логистика, здравоохранение и др.

В контексте разговора о безопасности M2M-технологий первая классификация важна для выявления и понимания потенциальных угроз, вторая – для оценки последствий от реализации этих угроз.

История развивается по спирали. При разработке первых сетевых протоколов вопросам безопасности уделялось мало внимания. Позднее пришло осознание, насколько это важно. Как результат – мы получили целую серию функционально сходных протоколов, которые различались в первую очередь уровнем защищенности (например, изначально разработанный HTTP и расширение к нему – HTTPs). Вот и в области разработки M2M-технологий сейчас происходят похожие процессы. Далеко не все разрабатываемые технологии проектируются с учетом требований безопасности. Справедливости ради отметим, что это не касается отраслей, где M2M-взаимодействие уже стало привычным, а потенциальные убытки от инцидентов безопасности высоки (например, в банковском секторе). В подобных сферах M2M-технологии активно пользуются технологиями безопасности. Однако не везде и не всегда M2M-взаимодействие защищено должным образом. Рассмотрим два примера, подтверждающих это утверждение.

Классическая иллюстрация проблемы безопасности M2M-технологий – наделавший много шума в 2010–2011 гг. «червь» stuxnet. Его ключевой особенностью стало то, что он проник в промышленные системы и мог воздействовать на автоматизированные производственные процессы. По сути, был открыт Ящик Пандоры, напрямую связавший виртуальный и физический миры: компьютерный вирус мог нанести не только экономический вред, но и вполне ощутимые физические разрушения. Представьте, насколько опасным становится такая вредоносная программа, когда речь идет о химических производствах и атомных станциях.

Другим пугающим примером являются исследования, показавшие на практике возможность взлома некоторых кардиостимуляторов. Последствия такого злонамеренного вторжения вне пределов исследовательских лабораторий легко предсказать.

Вместе с тем существуют области, в которых вопрос защиты M2M-взаимодействия менее серьезен и решается более простыми способами. В качестве примера можно привести устройство, сочетающее в себе спортивные часы с шагомером, GPS-трекером, пульсометром и оснащенное Bluetooth-связью со смартфоном или компьютером. Подобного рода устройства позволяют записывать и анализировать физическую активность, делиться достижениями с друзьями, получать рекомендации от специалистов. Взлом подобного прибора несомненно доставит некоторую неприятность хозяину (может быть, например, уничтожена еще не синхронизированная история или подложены неверные данные), но катастрофических последствий не вызовет. Для предотвращения вмешательства злоумышленника в данном случае достаточно базовой защиты: например простейшей аутентификации и шифрования передаваемых данных. К тому же мало кому придет в голову взламывать то, что и так обычно напрямую попадает в социальные сети.

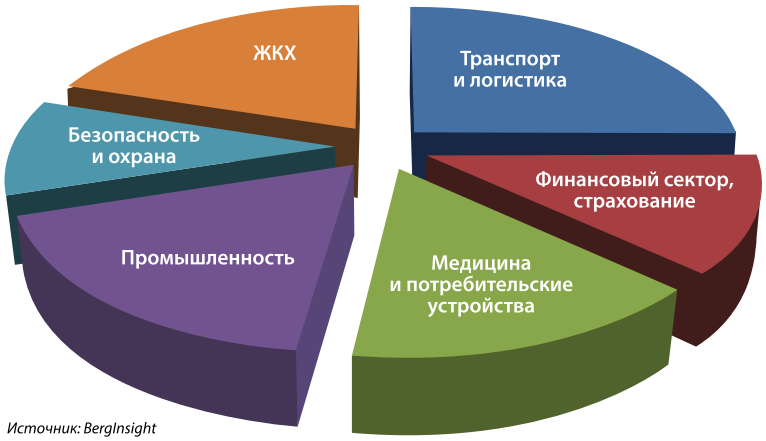
Теперь, когда масштаб проблемы понятен, выделим несколько основных факторов, которые осложняют обеспечение защиты межмашинного взаимодействия.

Ключевой проблемной точкой является отсутствие общепринятых стандартов обеспечения ИБ для M2M-систем. В области межмашинного взаимодействия существует острый дефицит не только стандартов обеспечения безопасности, но и стандартов самих M2M-технологий. Чем больше различных протоколов межмашинного взаимодействия, тем сложнее защитить их все и тем меньше вероятность, что для каждого из них будет создана система защиты. Разработка стандартов – длительный и трудоемкий процесс, который требует привлечения широкой группы экспертов из соответствующих предметных областей. Однако в результате завершения такой работы M2M-технологии получат мощнейший толчок к развитию. Кроме того, это упростит вход на рынок относительно небольшим игрокам, которые на данный момент просто не рискуют разрабатывать свой M2M-продукт, опасаясь, что в дальнейшем он окажется несовместим с продуктами вендоров – лидеров области.

Говоря о M2M-технологиях, невозможно не коснуться такого понятия, как «Интернет вещей». Наше общество становится все более технологичным. Мир будущего будет пронизан всевозможными системами автоматизации. А это значит, что в большинство устройств будут внедрены системы связи, исполнительные механизмы и датчики различного рода. Чайник, который получает информацию от будильника и включается к тому моменту, как вы просыпаетесь. Холодильник, который отслеживает срок годности и количество оставшихся продуктов и заказывает заканчивающиеся. Обогреватели, кондиционеры и увлажнители воздуха, которые заблаговременно меняют свое поведение в зависимости от краткосрочного прогноза погоды, чтобы у вас в квартире всегда был идеальный микроклимат. Автомобили, которые получают данные от светофора о рекомендуемой скорости для попадания в «зеленую волну». Медицинские браслеты, которые собирают информацию о вас и на основе экспертизы компьютера дают постоянные рекомендации по питанию и физическим нагрузкам. Все это уже не фантастика, а реальные проекты в той или иной стадии готовности. Но для того чтобы подобные системы могли работать массово, они должны войти в глобальную сеть. Датчикам нужно передавать информацию центральному серверу или локальному устройству агрегации информации, а управляющим серверам – сигналы исполняющим устройствам. И главным прототипом-кандидатом является существующий Интернет. Рано или поздно количество устройств без пользователя, подключенных к Интернету, значительно превзойдет количество пользовательских устройств. И мы получим «Интернет вещей».

Несмотря на то что «Интернет вещей» как апофеоз M2M-взаимодействия сулит нам немало преимуществ, он имеет и очевидные проблемы, в том числе в области безопасности. Устройства, которые будут обеспечивать подключение к общей сети всего и вся, потребуются в огромном количестве, превышающем количество живущих людей минимум на порядок (т. е. десятки, а то и сотни миллиардов экземпляров). Это значит, что каждое удорожание себестоимости производства или обслуживания таких устройств лишь на несколько центов обойдется в миллиарды долларов. Усложнят ли встроенные системы защиты такие устройства? Вероятно, да. В попытках войти в новый огромный рынок не будет ли слишком велик соблазн у вендоров

Доля сегментов по количеству M2M-подключений, 2011 год в мире



Источник: BergInsight

мнение специалиста

Игорь КОРЧАГИН,
руководитель группы обеспечения безопасности информации, компания ИВК

Растущая с каждым годом информатизация общества приводит к тому, что все чаще начинают обсуждаться вопросы информационной безопасности как неотъемлемой части данного процесса. Ассимиляция информационных технологий с образом жизни каждого человека интенсивно возрастает, что ведет к повышению рисков, связанных с ИБ. Не являются исключением и M2M-технологии. Как верно отмечено автором, эти технологии проникают в нашу жизнь уже на бытовом уровне.

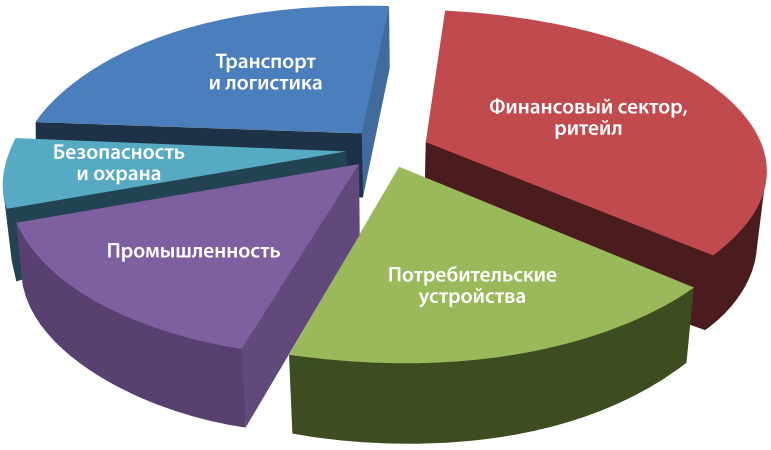
С одной стороны, использование таких технологий исключает целый пласт угроз ИБ, связанных с человеческим фактором. Однако касается это в основном стадии функционирования средств межмашинного взаимодействия, но не этапов их разработки и внедрения.

Развитие функциональности информационных технологий и их стандартизация всегда были впереди решения вопросов ИБ. Из этого следует одна из первоочередных проблем развития M2M-технологий – отсутствие соответствующих стандартов по ИБ в данной области.

Наиболее широкое распространение M2M-технологии получили в таких областях, как медицина, логистика, АСУ ТП, банковский сектор. Активно используются они и в средствах беспроводной передачи данных. Поэтому к наиболее важным задачам ИБ M2M относятся:

- подтверждение функционирования устройства в безопасном состоянии до подключения к сети;
- обеспечение аутентичности устройств и передаваемых ими данных;
- обеспечение целостности и конфиденциальности данных.

Доля сегментов по количеству M2M-подключений, 2011 год в России



Источник: J'son § Partners Consulting, консолидированные оценки опрошенных экспертов

снизить себестоимость устройств за счет систем безопасности? Надеюсь, что нет, но исключать этого нельзя.

Еще одной очевидной проблемой безопасности M2M-технологий в эру «Интернета вещей» является сложность первичной настройки механизмов безопасности, централизованного управления и мониторинга систем с таким количеством устройств. Но эта проблема имеет хорошо очерченные границы, решения-прототипы для меньшего количества устройств, носит преимущественно технический характер и, уверен, будет решена.

Интересный момент, который следует отметить, касается социальной инженерии. Этот инструмент всегда являлся одним из самых мощных и часто используемых при взломах различных систем. Его трудоемкость зачастую существенно ниже, а эффективность выше, чем у других инструментов для взлома. Тем не менее есть надежда, что в M2M-технологиях социальная инженерия будет работать не так хорошо, как это происходит сейчас в компьютерных системах. И происходить это будет по той причине, что такое звено, как человек, будет практически полностью исключено из некоторых цепей взаимодействий. Впрочем, на полное исчезновение социальной инженерии надеяться наивно. Думаю, она все равно останется одним из основных инструментов работы злоумышленников.

Немаловажным является вопрос об архитектуре глобальной сети будущего. Современный Интернет строится на базе стека протоколов TCP/IP. Создание протоколов IPv4, TCP, UDP и ряда других привело к появлению компьютерных сетей (в частности, Интернета) в том виде, в котором они сегодня существуют. Однако никакая, даже столь хорошая архитектура не может существовать вечно. И сейчас уже понятно, что в «Интернете вещей» не будет главенствовать протокол IPv4. Его время безвозвратно уходит, наступает время нового протокола – IPv6. Он решает многие проблемы с масштабированием и обслуживанием, которые были у IPv4. Особенно важно, что IPv6 обладает встроенными механизмами обеспечения безопасности: например, всем нам знакомый IPsec является уже органично встроенным в IPv6.

Несколько слов о том, в каких сферах M2M-технологии наиболее распространены. В мире традиционно наиболее широкое распространение M2M-технологии имеют в области транспорта. Немалую долю рынка занимают сферы промышленности, медицины и ЖКХ. При этом наибольший рост M2M ожидается в медицине и на потребительском рынке. Очень перспективными выглядят технологии «умных» домов и городов. Но их трудно отнести к какой-либо из вышеперечисленных категорий, поскольку они включают в себя и транспорт, и медицину, и потребительские устройства.

Российский рынок во многом повторяет мировой с некоторым запаздыванием, однако существуют и свои особенности. Как и в остальном мире, первопроходцами M2M в России стали транспорт и логистика. Однако в отличие от западных стран в России M2M-технологии получили наиболее широкое распространение не в области медицины и ЖКХ, а в сфере платежных систем и ритейла. Главным драйвером M2M-технологий в России являются крупные корпорации, хотя, как и по всему миру, ожидается существенное повышение спроса со стороны частных заказчиков.

В качестве примера крупного внедрения защищенных M2M-технологий в России можно привести недавно реализованный проект по оснащению коммерческого транспорта тахографами, в состав которых входит навигационно-криптографический модуль. На всех этапах работы такого тахографа обеспечена защита информации специальными продуктами российских компаний («Атлас-карт», «Крафтвей», «С-Терра СиЭсПи»). Устройство обеспечивает строгую аутентификацию, конфиденциальность, целостность и достоверность информации при работе с данными тахографа и карт водителей. В мастерских, обслуживающих тахографы и карты водителей, также стоит специальное оборудование, позволяющее создать доверенный канал по протоколу IPsec до центрального сервера для передачи данных и активации тахографа.

Еще одно знакомое каждому из нас устройство, в котором применяются M2M-технологии, – банкомат. Сегодня уже никого не нужно убеждать в необходимости защищать сведения, которыми банкомат обменивается с центром обработки данных. Практически все российские вендоры средств сетевой защиты производят устройства, предназначенные специально для банкоматов, – компактные, надежные, с высоким быстродействием и недорогие.

Приведенные примеры еще раз показывают актуальность и практическую пользу от применения M2M-технологий, а также то, что и вендоры-производители, и интеграторы решений понимают необходимость построения защищенных решений.

M2M-технологии – это новый огромный рынок, который может кардинально поменять наш привычный образ жизни. На пути разработки и внедрения решений будет немало трудностей. Но несомненно, что опыт, накопленный российскими производителями в области ИТ, позволит создавать безопасные, надежные и удобные M2M-технологии. ■