Применение микроконтроллеров WIZnet для повышения безопасности IoT

Олег ИВАНОВ
oyi@efo.ru

Последнее время тема «Интернета вещей» становится все более популярной. И важно понимать, что практически все решения в этой области базируются на стеке протоколов TCP/IP, поскольку это основной протокол, используемый в Сети.

Вопросы безопасности таких устройств наряду с активным продвижением различными фирмами-производителями своих решений для IoT становятся все более актуальными. Если раньше системы управления для промышленности, как правило, не имели выхода в Интернет, то концепция IoT подразумевает использование в качестве канала связи именно интернет-соединение. Ввиду глобальной доступности такого конечного устройства риск подвергнуться хакерской атаке очень велик.

Как правило, для атак на подобные системы используются уязвимости компьютерных систем, работающих под управлением различных ОС. В области встраиваемых решений, для организации линий передачи через Интернет, обычно применяют либо системы на кристалле под управлением какого-либо дистрибутива Linux (но это подразумевает сравнительно высокую стоимость), либо используют программную реализацию стека протоколов в микроконтроллере (дешевое, но более ресурсоемкое решение). Оба варианта ввиду программной реализации стека TCP/IP подвержены различного вида атакам. Проблема особенно серьезна для встраиваемых устройств, ввиду ограниченности располагаемых вычислительных ресурсов, так как при разработке программы в первую очередь внимание уделяется функциональности устройства.

В качестве примера можно привести найденную в свое время уязвимость наиболее популярного и бесплатного программного стека lwIP. Специалист по безопасности Аллен Хаусхолдер (Allen D. Householder) сообщил о серьезной уязвимости в DNS-resolver одновременно в uIP и lwIP. Согласно бюллетеню Vulnerability Note VU#210620, DNS-resolver уязвим к атакам на «отравление кэш». Обеспокоенность вопросами безопасности IoT появляется в Интернете все чаще. Достаточно вспомнить недавний случай с найденной уязвимостью бортового компьютера автомобиля Jeep Cherokee.

На фоне этого оправданным решением для встраиваемых систем является применение микроконтроллеров с аппаратной реализацией стека протоколов TCP/IP. В течение нескольких десятилетий южнокорейская компания WIZnet развивает идею аппаратной реализации TCP/IP. Основным резоном применения чипов с аппаратной реализацией стека TCP/IP была возможность использования каналов связи Ethernet под управлением достаточно слабых микроконтроллеров, которые без применения дополнительных микросхем вообще не могли реализовать функции работы в сети или поддерживали очень ограниченную функциональность. В этих случаях микросхемы WIZnet обеспечивали не только необходимый функционал, но и высокую производительность обмена данными. В последнее время возросшие вычислительные ресурсы современных микроконтроллеров позволяют реализовать стек TCP/IP за счет их оснащения аппаратным блоком MAC-уровня и в редких случаях — аппаратным интерфейсом физического уровня (PHY) Ethernet.

Здесь необходимо отметить, что наличие MAC и PHY дополнительно потребует реализации самого TCP/IP, то есть применения программных библиотек. И хотя сама идея, заложенная в протокол, довольно проста, не факт, что, применяя стороннюю библиотеку, вы не столкнетесь с проблемами, для решения которых придется потратить много сил и драгоценного времени, чтобы найти ошибки и выполнить отладку.

Производительность канала передачи информации в случае программной реализации стека TCP/IP будет, несомненно, ниже, а ресурсы микроконтроллера потребуют дополнительного использования как программной флэш-памяти, так и некоторого количества оперативной памяти (по меркам микроконтроллеров достаточно значительной) и соответственно дополнительных вычислительных ресурсов ядра.

Во многих случаях применение чипов WIZnet способно обеспечить преимущество в стоимостном отношении, поскольку поддерживает более высокую производительность, даже используя микроконтроллеры с ядром Cortex-M0. Обычно она зависит от возможностей основной программы подготавливать данные для передачи или от скорости обработки принимаемой информации, тогда как для решения той же задачи с программной реализацией стека потребуются уже микроконтроллеры с ядром Cortex-M3 или более мощные. Решение в данном случае все равно получается двухчиповое — микроконтроллер + микросхема, реализующая физический уровень Ethernet. Надо к тому же учитывать, что в случае программной реализации стека практически каждый пакет обрабатывается ядром микроконтроллера и большое количество ресурсов может быть затрачено на обработку широковещательных пакетов или пакетов, посылаемых в результате хакерской атаки. Кроме того, свободно распространяемый lwIP не имеет технической поддержки со стороны разработчика. Поэтому в случае появления каких-либо проблем можно надеяться только на помощь коллег на различных форумах. Конечно, существуют коммерческие стеки TCP/IP от различных фирм, но такие библиотеки имеют значительную стоимость, и приобретение их оправдано, когда планируется массовый выпуск продукции.

Исследуя вопросы устойчивости к различным типам интернет-атак, специалисты компании WIZnet провели сравнительное тестирование решений на основе программной реализации стека TCP/IP и функционально аналогичного устройства с применением стека, выполненного аппаратно (с помощью нового чипа W7500).

Платформы и их краткие технические характеристики, использованные для сравнительного тестирования решений с микроконтроллерами LPC1768 и W7500, приведены в таблице. Результаты сравнения можно посмотреть на рис. 1.

С помощью утилит *iperf.exe* и scapy были построены графики достигнутой произво-

Таблица. Платформы для сравнительного сетевого соединения под воздействием сетевой атаки

	Программный стек TCP/IP	Аппаратный стек TCP/IP
Микроконтроллер	LPC1768	W7500 EVB
Ядро контроллера	Cortex-M3	Cortex-M0
FLASH/RAM, кбайт	512/64	128/16
Рабочая частота, МГц	96	48
Режим DMA	Не используется	
Программа	RTOS + lwIP	OS — нет, только firmware
Размер кода ПЗУ/ОЗУ, кбит	64,5/35,2	9,09/8,99
Компилятор	mbed.org	keil

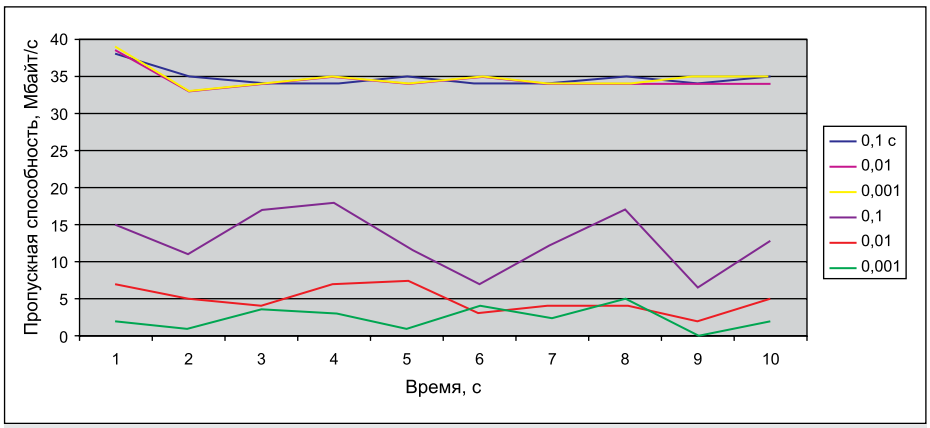

Рис. 1. Сравнительные результаты тестирования пропускной способности в зависимости от варианта реализации стека (три верхние кривые на диаграмме для W7500) под воздействием syn-flood-атаки, нижние — программный стек lwIP

дительности (измерения выполнялись для различных интервалов опроса) под воздействием syn-flood-атаки (DDoS).

На диаграмме видно, что аппаратный стек TCP/IP препятствует передаче атакующих запросов работающей программе. В случае реализации программного стека эти запросы отнимают процессорное время, соответственно понижают производительность сетевого соединения и к тому же загружают ядро микроконтроллера дополнительной работой, что может привести к недостатку ресурсов, необходимых для выполнения основной программы, и даже к частичной потере функциональности всего устройства. Аналогичная картина, соответствующая малому влиянию сетевой атаки на производительность сетевого соединения, будет получена для всех решений на основе чипов WIZnet.

Второй аргумент в пользу применения микроконтроллеров компании WIZnet — простота управления и высокая производительность реализуемого Ethernet-соединения. Стоимость чипов WIZnet сравнима с микросхемами физического уровня, поэтому по цене оба варианта — с программной реализацией стека и применением чипа от WIZnet — будут соизмеримы. Но программный стек TCP/IP потребует больше ресурсов микроконтроллера, и вместо Cortex-M0 придется применить значительно более дорогой Cortex-M3 (4).

В последнее время фирма WIZnet разработала три новые микросхемы — W5500, W7500 и W7500P. Микросхема W5500 уже успешно применяется многими производителями в различных проектах, а массовые поставки W7500 и W7500P начнутся в ближайшее время. Микросхема W7500 в части, касающейся TCP/IP, повторяет идеологию предыдущих микроконтроллеров, но вместо физического уровня Ethernet оснащена интерфейсом управления MII (Media Independent Interface). В отличие от большинства микросхем WIZnet — это полноценный микроконтроллер Cortex-M0 с встроенным аппаратным стеком TCP/IP и ресурсами, доступными для собственного программного обеспечения. Такое решение позволяет подключать к нему различные микросхемы физического уровня не только для витой пары, но и для оптики.

Основные технические характеристики W7500:

- Ядро Cortex-M0 с частотой 48 МГц.
- Аппаратный стек TCP/IP с поддержкой 8 сокетов одновременно и буфером пакетов 32 кбит.
- Объем встроенной памяти:
  - FLASH — 128 кбит;
  - RAM 16 кбит (+32 кбит для TCP/IP), возможно использование буфера сокетов в качестве RAM, максимально 48 кбит;
  - ROM для загрузочного кода — 6 кбит.
- АЦП — 8 каналов 12 бит (до 1 Msps).
- DMA — 6 каналов.
- Порты ввода/вывода: 3×16-разрядных и 1×5-разрядный (максимально 53 линии ввода/вывода).
- Таймеры:
  - 1×Watchdog (32 бит);
  - 4×32-бит (могут использоваться как пары 16-бит);
  - 8-канальный ШИМ с предделителем 6 бит.
- Последовательные интерфейсы:
  - 3×UART (один простой, два с буферами FIFO и возможностями управления потоком);
  - 2×SPI;
  - 2×I²C (fast mode 400 кГц, master и slave).
- Генератор случайных чисел (32 бит).
- Встроенный *RC*-генератор 8 МГц (обеспечивает тактовые частоты до 48 МГц).
- Напряжение питания 1,5–3,3 В.
- Корпус TQFP-64.

В общем, по современным меркам, без аппаратного стека TCP/IP — это хороший микроконтроллер семейства Cortex-M0 (причем довольно мощный), но с возможностью использования 48 кбит ОЗУ в случае, если подключение Ethernet не планируется.

Данный чип особенно интересен в таких приложениях, как системы сбора информации. В сетях на основе 10/100Base-TX используется топология «звезда» и требуется применение сетевых устройств коммутации пакетов (хабы и т. п.).

Подобная топология требует от хаба (или другого типа коммутатора) наличия отдельного кабеля 5-й категории к каждому устройству (то есть минимум две витые пары). Но учитывая, что пропускная способность 100-мегабитного канала зачастую во много раз превышает необходимую для работы одного устройства, возможно использовать данный микроконтроллер совместно с микросхемами, реализующими функцию хаба (свитча и т. п.). Такое решение позволяет подсоединять несколько устройств в цепочку с последовательным включением устройств через одну витую пару, разделить домены коллизий, использовать дополнительные возможности микросхемы, реализующей хаб (с управлением через MII), и, кроме этого, преодолеть ограничение на длину сегмента в локальной сети.

При разработке такого решения появляется дополнительная задача обеспечения питанием указанных устройств. В данном случае отличным решением станет применение технологии Power-over-Ethernet (PoE). Кроме использования централизованного источника питания для всех устройств, обеспечивается полная (до 1500 В) гальваническая развязка между устройствами.

Нередко дешевые устройства, предлагающие питание устройств через Ethernet, выполнены с отклонениями от стандарта PoE. Такие решения допустимы в локальной сети, которая обслуживается одним пользователем. Но когда рассматриваются промышленные системы, то возникает потребность в устройствах, полностью соответствующих стандарту и имеющих промышленный температурный диапазон работы, что избавит от необходимости дополнительной сертификации и обеспечит совместимость с промышленными системами PoE. И здесь оправдано применение готовых модулей PoE (их легко использовать как опцию, предусмотрев применение на плате подходящего для PoE MagJack или комбинации RJ-45 с соответствующим трансформатором и дополнительным разъемом).

Для примера можно рассмотреть модули от тайваньской компании Befact

Рис. 2. Модуль PoE PDI-12

(www.befact.com.tw). Хотя на рынке присутствует большое количество аналогичных решений, тем не менее многие устройства имеют либо коммерческий температурный диапазон, либо чрезмерную стоимость. Поэтому серия сплиттеров PDI компании Befact является золотой серединой, так как сертифицирована для промышленного температурного диапазона, полностью совместима со стандартами PoE и оптимальна по цене. Внешний вид модуля PDI-12 представлен на рис. 2.

Модули имеют габаритную мощность 12 Вт и выпускаются на выходное напряжение 5 и 12 В, оснащены защитой от короткого замыкания, превышения тока и температуры. Особенностью модулей является применение керамических конденсаторов для обеспечения надежной работы в широком температурном диапазоне. Размеры модулей составляют 16×60×17 мм.

Дальнейшее логическое развитие W7500 представляет W7500P. Это также полнофункциональный микроконтроллер, но уже снабженный физическим уровнем 10/100Base-TX. Микросхема имеет аналогичное ядро Cortex-M0 и схожие характеристики.

Для начала работы с микроконтроллерами W7500 и W7500P компанией WIZnet были созданы оценочные платы (рис. 3, 4), выполненные в популярном конструктиве Arduino.

Для программной и аппаратной поддержки новых микросхем компанией WIZnet был запущен сервер с адресом www.wizwiki.net. На страницах этого сайта также размещается форум, посвященный продуктам компании и поддерживаемый техническими специалистами WIZnet.

Совокупность описанных решений позволяет создавать конечные устройства с подключением через витую пару или оптическую среду, обеспечить простоту реализации сетевых приложений и высокую устойчивость к различным атакам из Интернета.

Литература

1. www.wiznet.co.kr
2. www.wizwiki.net
3. www.github.com/Wiznet
4. www.securitylab.ru/analytics/470706.php
5. Безмалый В. Сможем ли мы защитить «Интернет вещей»? // PC Week. 24 июля 2015.

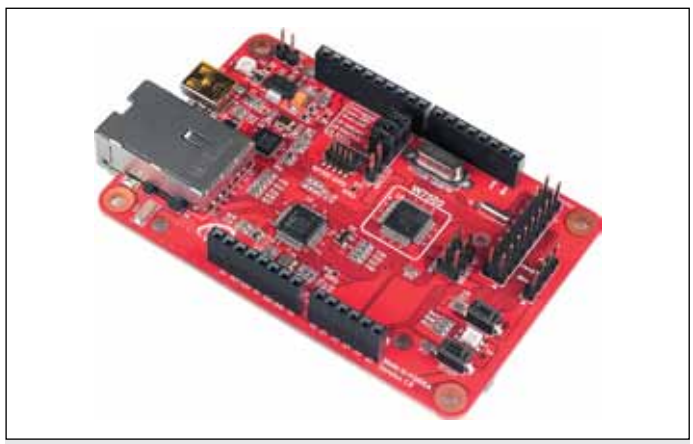

Рис. 3. Оценочная плата WizWiki-W7500

Рис. 4. Оценочная плата WizWiki-W7500P