УСТРОЙСТВО МОНИТОРИНГА ЛОКАЛЬНОЙ СЕТИ С ФУНКЦИЯМИ ОПОВЕЩЕНИЙ О НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ

LOCAL NETWORK MONITORING DEVICE WITH FUNCTIONS OF UNAUTHORIZED ACCESS ALERT FUNCTIONS

A. Andryukhin
N. Grachev
V. Smirnov

Summary. The paper presents the results of studies on the protection of small LANs, in particular its wireless segment, solved using network encryption, corporate encryption methods. It is shown that these methods and tools are rarely used, they require additional equipment, maintenance and are difficult to configure. Custom encryption methods are used more often — they are easy to set up, do not require additional equipment and maintenance, but almost always can be cracked in a relatively short period of time. According to the results of the analysis, the work examines and studies the principle of construction of the principle and the device based on it, which allows to increase the security of networks using custom encryption methods. The principle developed in the work and the device monitors and notifies about network events of the channel and network level, as a result of which all network activity becomes transparent, which significantly increases the network security.

Keywords: Design, Device, Software, Information Security.

Андрюхин Александр Гавриилович
К.т.н., доцент, МИРЭА — Российский технологический университет (г. Москва)
pr1110@list.ru
Грачев Николай Николаевич
К.т.н., профессор, МИРЭА — Российский технологический университет (г. Москва)
nngrachev@mail.ru
Смирнов Валентин Сергеевич
МИРЭА — Российский технологический университет, г. Москва
cmp18@ya.ru

Аннотация. В работе представлены результаты исследований вопросов защиты малых ЛВС, в частности ее беспроводного сегмента, решаемых с помощью шифрования сети, корпоративных методов шифрования. Показано, что эти методы и средства используются редко, они требуют дополнительного оборудования, обслуживания и сложны в настройке. Пользовательские методы шифрования используются чаще — они просты в настройке, не требуют дополнительного оборудования и обслуживания, но практически всегда поддаются взлому за относительно небольшой промежуток времени. По результатам проведенного анализа, в работе рассматривается и исследуется принцип построения принципа и устройства на его основе, позволяющее повысить безопасность сетей использующие пользовательские методы шифрования. Разработанный в работе принцип и устройство отслеживает и оповещает о сетевых событиях канального и сетевого уровня, вследствие чего вся сетевая активность становится прозрачной, что значительно повышает безопасность сети.

Ключевые слова: Проектирование, Устройство, Программные средства, Защита информации.

В 80-е годы персональные компьютеры начинают вторгаться в жизнь обычных людей, в 90-е в пользовательском окружении начинают появляться компьютерные сети, в 2000-е на пользовательском рынке появляются беспроводные сетевые решения. В те годы локальные сети не были массовым явлением и использовались продвинутыми пользователями для специфичных целей [1,2]

Но сегодня ситуация изменилась — локальная сеть на основе роутера стала общим достоянием, имеется почти в каждой квартире, и большинство пользователей — технически неграмотны в вопросах безопасности сетей. Риски несанкционированного доступа к локальной сети серьезны: совершение незаконных действий в интернете от имени пользователя, перехват и расшифровка вводимых пользователем данных на посещаемых сайтах (в т.ч. паролей и данных банковских карт), получение полного доступа к компьютерам домашней сети и информации на них (путем взлома операционной системы). Поэтому даже малые пользовательские сети требует защиты.

Что представляет собой сетевая безопасность? Локальная сеть на основе роутера чаще всего состоит из объединенных проводных и беспроводных сегментов. Для получения доступа к такой сети достаточно получить доступ к любому сегменту сети. С безопасностью проводного сегмента проблем нет — для взаимодействия с ним потребуется физический доступ к кабелю, но беспроводной сегмент уязвимее, так как эфиром является радиоканал. Для попыток несанкционированно-

го взаимодействия с сетью требуется просто находиться в зоне вещания сети. Следовательно, беспроводной сегмент требует серьезной защиты.

Беспроводные сети стали поддерживать шифрование сразу после своего рождения. Первым методом шифрования стал WEP, но существовал он недолго — метод взломали через несколько лет после выхода на рынок [1,2].

В дальнейшем появились методы WPA, WPA2, WPA3. Методы подразделяются на корпоративные и пользовательские реализации. Корпоративных реализаций имеется достаточное количество. Самые надежные из них практически не поддаются взлому, так как для авторизации устройств используют комбинации смарт-карт, двухсторонних сертификатов и уникальных логинов с динамическими ключами. Но такие методы сложны в настройке, так как требуют дополнительного оборудования и обслуживания.

Пользовательские реализации методов просты в настройке и не требуют дополнительного оборудования или обслуживания. Для доступа к сети используется общий ключ — парольная фраза. Ключевое отличие между пользовательскими методами заключается в разрядности ключа, но все они бессильны против «брутфоса» (перебора): злоумышленник похищает необходимые данные из эфира и выполняет оффлайн перебор пароля. Учитывая мощности современной техники, злоумышленник не затратит много времени — максимальный ключ (63 символа) самого популярного пользовательского метода (WPA2-PSK) на массиве современных видеокарт перебирается за несколько дней (покупать видеокарты необязательно, можно заказать услугу перебора через интернет). Но иногда необходимости нет и в этом: уязвимая технология WPS (включена по умолчанию на многих роутерах) позволяет получить пароль без оффлайн перебора менее, чем за сутки. Черные и белые списки физических адресов устройств на роутере ситуацию не спасают — злоумышленник может просканировать физические адреса сети, даже не зная от нее пароля.

Множество хакерских программ для осуществления вышеописанной деятельности (с руководствами) находятся в открытом доступе, их осилит даже новичок. Следовательно, взлом пользовательских методов шифрования — всего лишь вопрос желания. Следовательно, взлом локальной сети с такой защитой — тоже всего лишь вопрос желания.

Логичным шагом от производителей роутеров было бы создание системы оповещений о подключаемых к сети устройствах, но внешний вид роутеров в данном аспекте не информативен — на роутере присутствуют только светодиоды активности сетевых интерфейсов. В web интерфейсе управления роутера можно наблюдать за подключенными устройствами, но на постоянной основе этого делать никто не будет (а начинающие пользователи и вовсе не подозревают о такой возможности). Авторы статьи видят два решения этой проблемы.

Первое решение подразумевает установку на уже существующий роутер свободной операционной системы (например, OpenWRT) с необходимыми драйверами для специального оборудования и разработанным прикладным ПО. В качестве специального оборудования выступает USB звуковая карта динамиком, в качестве разработанного прикладного ПО выступают программы для мониторинга сети. Данное решение было разработано и опробовано [4] но из-за привязки прикладного ПО мониторинг к конкретной модели роутера, пришлось не останавливаться на достигнутом и развивать идею дальше.

Второе решение проблемы — разработка собственного устройства, выполняющего мониторинг. Первым разработанным устройством стало простое устройство на кристалле SoC AR9331 [5]. Разработка была не сложной, ведь в интернете уже есть принципиальные схемы устройств на этой же SoC (например, одноплатный компьютер Onion Omega1). Но устройство не было лишено недостатков по нескольким причинам. Первая причина — цена: стоимость устройства получалась более 20$ за экземпляр, что дороговато для такого класса устройств. Вторая причина — нестандартная реализация ПО: устройство работало на ОС OpenWRT и должно было быть шлюзом сети, что в свою очередь ограничивало пропускную способность сети и вносило коррективы в топологию существующей сети.

Учитывая прошлые ошибки, авторы разработали новое устройство: на одной плате 50*50 мм удалось разместить все необходимые компоненты для его работы. Рассмотрим главные компоненты устройства.

Мозгом устройства является контроллер ESP8285 (Рис. 1) От обычных контроллеров отличается высокой производительностью (80 МГц в штатном режиме, 160 МГц в переходном режиме), наличием 1 МБ ПЗУ (SPI в режиме dual) и наличием встроенного WI-FI (N-150) модуля.

В соответствии с алгоритмом, контроллер осуществляет мониторинг события в сети и каждые 30 секунд проверяет наличие изменений.

Аудио контроллером устройства является микросхема YX5200–24SS. Аудио контроллер общается с главным контроллером через интерфейс UART. При получении команды на воспроизведение оповещения о каком-либо событии, аудиоконтроллер считывает необходимые

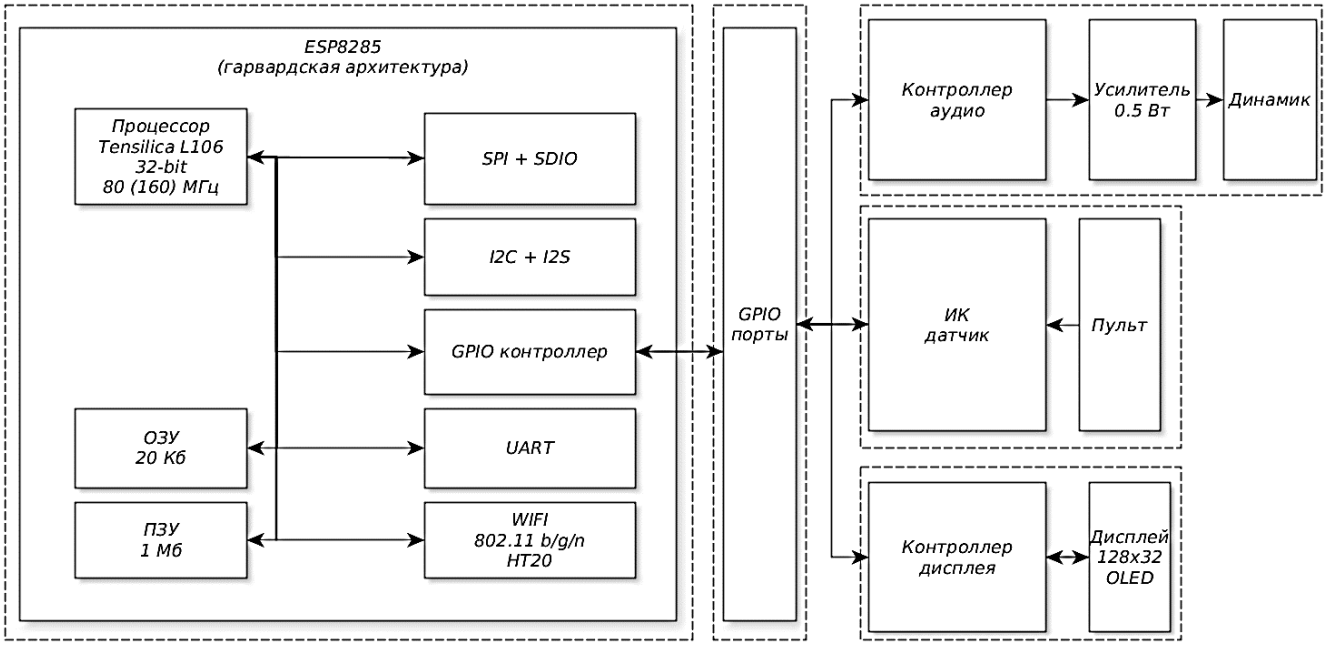

Рис. 1. Структурная схема устройства.

аудиоданные из подключенного к нему ПЗУ (SPI, 16 МБ), и выводит аудиопоток на маломощный (0.5 W) усилитель, к которому подключен динамик. Если уровня громкости не будет достаточно, на плате реализован вывод под внешние активные колонки.

Управление и настройка устройством осуществляется с помощью ИК пульта (посредством ИК приемника, подключенного к GPIO выводам контроллера). Базовая информация о состоянии сети отображается на миниатюрном OLED128x32 экране, подключенного к главному контроллеру по интерфейсу I2C.

В устройстве установлен аккумулятор на 500 mAh (с платой защиты и контроллером заряда MCP78831), что позволяет работать устройству при отключении внешнего питания как минимум в течении 2 часов.

Использование вышеперечисленных компонентов позволило снизить итоговую стоимость устройства более, чем в 2 раза по сравнению со стоимостью предыдущего устройства.

Рассмотрим алгоритм работы устройства. Прошивка устройства переработана, поэтому устройству теперь не требуется быть шлюзом сети и иметь физический контакт с сетью — устройство просто должно находиться в зоне вещания сети (такая концепция не мешает контролировать устройству и проводной сегмент сети). После включения устройства производится начальная диагностика и начальный анализ сетевого эфира. После этого предлагается выбрать сеть, для которой осуществляется мониторинг. После выбора сети устройство запросит от нее пароль. Его можно не водить — в этом случае будут доступны только оповещения о событиях канального уровня (что не рекомендуется). Дальнейшая настройка устройства не требуется — устройство будет работать в самостоятельном режиме и будет сообщать: о фактах подключения (отключения) неизвестных устройств и устройств из белого списка (сообщается MAC адрес, IP адрес, имя узла), о попытках подключения устройств из черного списка (сообщается MAC адрес), о пропаже (появления) доступа в интернет (сообщается выданный шлюзу IP адрес и маска сети), о смене IP адреса устройств (при отличии адреса от предыдущего), о задании устройствами статического IP адреса.

Также реализован контроль подозрительного служебного трафика для борьбы с атаками деаутентификации и подмены точки доступа, поэтому, в большинстве случаев, устройство сообщает об атаке на сеть еще до того, как злоумышленник получает полноценный доступ к сети.

Аналогов подобных устройств авторами статьи найдено не было, за исключением программных аналогов (программ сетевого мониторинга). Но программные аналоги требуют выделенного компьютера, знаний и внимания персонала, в то время как разработанное устройство лишено таких недостатков — даже технически неграмотный пользователь сможет его настроить и всегда быть в курсе вторжений в свою сеть.

ЛИТЕРАТУРА

1. Олифер В. Г., Олифер Н. А., Безопасность компьютерных сетей — М: Горячая линия — Телеком, 2017. — 644 с.
2. Бондарев В. В., Анализ защищенности и мониторинг компьютерных сетей. Методы и средства — М: МГТУ им. Н. Э. Баумана, 2017. — 228 с.
3. Олифер В. Г., Олифер Н. А., Компьютерные сети. Принципы, технологии, протоколы — СПб: Издательский Дом ПИТЕР, 2019. — 992 с.
4. Львов Н. С., Смирнов В. С. Разработка программного обеспечения для сетевого оборудования, предназначенного для оповещения пользователей о вторжениях в ЛВС / Искусственный интеллект: философия, методология, инновации. Сборник трудов IX всероссийской конференции студентов, аспирантов и молодых ученых. г. Москва, МИРЭА, 10–11 декабря 2015 г. — М: МИРЭА, 2015. — С 74–79.
5. Андрюхин А. Г., Смирнов В. С. Разработка устройства мониторинга локальной вычислительной сети с голосовым оповещением о несанкционированном доступе / Электронный журнал: наука, техника и образование. Выпуск 3/2018 (21) [Электронный ресурс] — Калуга: Изд-во ООО «Манускрипт», 2018. — С 81–88. — Режим доступа: [http://nto-journal.ru/uploads/articles/4ce290710858889e64ce6db22e3a1597.pdf]

© Андрюхин Александр Гавриилович (pr1110@list.ru),
Грачев Николай Николаевич (nngrachev@mail.ru), Смирнов Валентин Сергеевич (cmp18@ya.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»

МИРЭА — Российский технологический университет