Защита информации и беспроводные сети

Гончарук Роман Сергеевич,
старший специалист отдела технической защиты информации и противодействия технической разведке ЦИТСиЗИ УМВД России по Приморскому краю, старший лейтенант внутренней службы

Невероятно быстрые темпы внедрения в современных сетях беспроводных решений заставляют задуматься о надежности защиты данных. В статье рассматриваются старые и новые методы обеспечения безопасности.

В настоящее время устройства беспроводной связи на базе стандартов 802.11x продвигаются на рынке сетевого оборудования очень агрессивно. Количество всевозможного работающего оборудования стандартов 802.11x в мире впечатляет: по данным компании J`son & Partners, число хот-спотов в конце 2003 года превысило 43 тыс., а к концу 2004-го увеличилось более чем на 200%. Доля России в этих цифрах невелика, при том что количество сетей беспроводной связи неуклонно растет. Впечатляют не столько цифры, сколько те заблуждения, которые касаются обеспечения безопасной передачи данных в таких сетях.

802-11x — восприимчивость к угрозам извне

Сам принцип беспроводной передачи данных заключает в себе возможность несанкционированных подключений к точкам доступа. Взять хотя бы «непротокольные» угрозы, которые составляют основу проблемы. При разработке корпоративной сети администраторы в первую очередь заботятся о качественном покрытии территории офисов, забывая, что хакеры могут подключиться к сети прямо из автомобиля, припаркованного на улице. Бывают ситуации, когда просто нереально заблокировать саму возможность «слышать» передаваемый трафик.

Не менее опасная угроза — вероятность хищения оборудования. Если политика безопасности беспроводной сети построена на MAC-адресах, то сетевая карта или точка доступа, украденная злоумышленником, может открыть доступ к вашей сети.

Часто несанкционированное подключение точек доступа к ЛВС выполняется самими работниками предприятия. Защиту информации при подключении к сети таких устройств сотрудники обеспечивают тоже самостоятельно, не всегда задумываясь о последствиях.

Решением подобных проблем нужно заниматься комплексно. Организационные мероприятия в рамках данной статьи не рассматриваются — они чаще всего выбираются исходя из условий работы каждой конкретной сети. Что касается мероприятий технического характера, то весьма хороший результат достигается при использовании обязательной взаимной аутентификации устройств и внедрении активных (Obrserver 8.3, Airopeek NX 2.01, Wireless Sniffer 4.75) и пассивных (APTools 0.1.0, xprobe 0.0.2) средств контроля.

Уязвимость старых методов защиты

Защитой данных в беспроводных сетях комитет IEEE 802.11 занимался всегда. К сожалению, методы обеспечения безопасности сетей 803.11x на этапе их начального развития (1997–98 годы) использовались, мягко говоря, неудачные.

Классический протокол шифрации WEP, разработанный компанией RSA Data Security, использует 40-битный ключ, который складывается со сгенерированным вектором инициализации (IV, 24 бит). С помощью полученного ключа по алгоритму RC4 шифруются пользовательские данные и контрольная сумма. Вектор IV передается в открытом виде.

Первым минусом, безусловно, является 40-битный ключ, поскольку даже DES с его 56-битным ключом давно считается ненадежным. Вторым минусом можно считать неизменяемость ключа — применение статичного ключа упрощает проблему взлома. И, наконец, сам подход к шифрованию кажется весьма сомнительным. Размер IV — 24 бит, а значит, он повторится не позднее чем через 5 часов (длина пакета — 1500 байт, скорость — 11 Мбит/с), и это в самом крайнем случае.

В 2001 году появились первые реализации драйверов и программ, позволяющих справиться с шифрованием WEP. Документ, описывающий эту уязвимость, опубликован по адресу: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

Способы аутентификации тоже не внушают особого доверия. Например, ничего не стоит подслушать всю процедуру аутентификации по MAC-адресу, ведь MAC-адреса в кадре передаются незашифрованными. Самый удачный из перечисленных способов — PreShared Key. Но и он хорош только при надежной шифрации и регулярной замене качественных паролей.

Существует распространенное заблуждение, что применение уникального Service Set ID (SSID) позволяет избежать несанкционированных подключений. Увы, SSID пригоден лишь для логического разбиения сетевых устройств на группы. Единственное, что вы можете сделать с помощью SSID — это смутить взломщиков использованием «непечатных» символов.

Рис. 1. Алгоритм анализа зашифрованных данных

WEP-атаки

Недостаточность длины ключа, отсутствие его ротаций и сам принцип шифрации RC4 — все это позволяет злоумышленнику организовать весьма эффективную пассивную атаку. Причем для этого ему не придется совершать никакие действий, которые помогли бы его обнаружить, — он будет просто слушать канал. Не требуется при этом и специального оборудования — хватит обычной WLAN-карточки, купленной долларов за 20–25, а также программы, которая

будет накапливать пакеты на жестком диске до совпадения значений вектора IV. Когда количество пакетов станет достаточным (чаще всего от 1 до 4 млн. пакетов), WEP-ключ легко вычисляется.

Неплохих результатов может достичь хакер, прибегающий к активным способам атаки. Например, посылая в локальную сеть известные данные (скажем, из Интернета) и одновременно анализируя, как их зашифровала точка доступа. Такой метод позволяет вычислить ключ и манипулировать данными.

Еще один метод активной атаки — Bit-Flip attack. Алгоритм действия здесь следующий. В перехваченном фрейме, зашифрованном WEP, произвольно меняется несколько битов в поле «Данные», пересчитывается контрольная сумма CRC-32 и посылается обратно на точку доступа. Точка доступа принимает фрейм на канальном уровне, поскольку контрольная сумма верна, пытается дешифровать данное и отвечает заранее известным текстом, например: «Ваш ключ шифрования неверен». Последующее сравнение текста в зашифрованном и незашифрованном виде может позволить вычислить ключ.

Атакам DOS, использующим способ широкополосной модуляции DSSS, могут быть подвержены устройства стандарта 802.11b и 802.11 g, работающие на низких скоростях.

Все вышесказанное позволяет говорить о ненадежности старых методов обеспечения безопасности в беспроводных сетях, поэтому в тех случаях, когда имеющееся оборудование не позволяет реализовать современные решения по защите информации, необходимо либо использовать строжайшую административную политику, либо применять технологию IPSec-ESP, которая даст возможность надежно защитить данные, однако заметно снизит производительность ЛС.

Современные требования к защите

Любой пользователь будет спокоен, если сможет обеспечить решение трех проблем для своего трафика: конфиденциальность (данные должны быть надежно зашифрованы), целостность (данные гарантированно не должны быть изменены третьим лицом) и аутентичность (надежная проверка того, что данные получены от правильного источника).

Аутентификация

В настоящее время в различном сетевом оборудовании, в том числе в беспроводных устройствах, широко применяется более современный по сравнению со стандартами 1997–1998 годов способ аутентификации, который определен в стандарте 802.1x. Принципиальное отличие его от прежних способов аутентификации заключается в следующем: пока не будет проведена взаимная проверка, пользователь не может ни принимать, ни передавать никаких данных. Стандарт предусматривает также динамическое управление ключами шифровании, что, естественно, затрудняет пассивную атаку на WEP.

Ряд разработчиков используют для аутентификации в своих устройствах протоколы EAP-TLS и PEAP, но более широко к проблеме подходит Cisco Systems, предлагая для своих беспроводных сетей, помимо упомянутых, следующие протоколы:

- EAP-TLS — стандарт IETF, обеспечивающий аутентичность путем двустороннего обмена цифровыми сертификатами;
- PEAP — пока предварительный стандарт (draft) IETF, предусматривающий обмен цифровыми сертификатами и дополнительную проверку имени и пароля по специально созданному шифрованному туннелю;
- LEAP — фирменный протокол Cisco Systems, представляющий собой «легкий» протокол взаимной аутентификации, похожий на двусторонний Challenge Authentification Protokol (CHAP). Использует разделяемый ключ, поэтому требует продуманной политики генерации паролей (в противном случае, как и любой другой способ Pre-Shared Keys, подвержен атакам по словарю);
- EAP-FAST — разработан Cisco на основании предварительного стандарта (draft) IETF для защиты от атак по словарю и имеет высокую надежность. Принцип работы схож с LEAP, но аутентификация производится по защищенному туннелю.

Все современные способы аутентификации (см. таблицу) подразумевают поддержку динамических ключей. Однако если сравнивать эти стандарты и по остальным параметрам, то способы EAP-TLS и PEAP оказываются более тяжеловесными. Они больше подходят для применения в сетях, настроенных на базе оборудования различных производителей.

Способы аутентификации, разработанные Cisco, выглядят привлекательнее. Особую прелесть им придает поддержка технологии Fast Secure Roaming, позволяющей переключаться между различными точками доступа (время переключений составляет примерно 100 мс), что особенно важно при передаче голосового трафика. При работе с EAP-TLS и PEAP повторная аутентификация займет существенно больше времени и, как следствие, разговор прервется. Главный недостаток LEAP и EAP-FAST очевиден — эти протоколы поддерживаются в основном в оборудовании Cisco Systems.

Рис. 2. Структура пакета 802.11x при использовании TKIP-PPK, MIC и шифрации по WEP

Шифрование и целостность

На основании рекомендаций 802.11i Cisco Systems реализован протокол TKIP (Temporal Integrity Protocol), обеспечивающий смену ключа шифрования PPK (Per Packet Keying) в каждом пакете и контроль целостности сообщений MIC (Message Integrity Check).

Процедура PPK предусматривает изменение вектора инициализации IV в каждом пакете. Причем шифрация осуществляется значением хэш-функции от IV и самого WEP-ключа. С учетом того, что WEP-ключи динамически меняются, надежность шифрации оказывается довольно высокой.

Обеспечение целостности возложено на проMIC. В формирующийся фрейм добавляются поля MIC и SEQuence number, в поле SEQ указывается порядковый номер пакета, что позволяет защититься от атак, основанных на повторах и нарушениях очередности. Пакет с неверным порядковым номером просто игнорируется. В 32-битном поле MIC располагается значение хэш-функции, вычисленной исходя из значений самого заголовка пакета 802.11, поля SEQ, пользовательских данных.

Другой перспективный протокол шифрования и обеспечения целостности, уже зарекомендовавший себя в проводных решениях, — AES (Advanced Encryption Standart). Он обладает лучшей криптостойкостью по сравнению с DES и ГОСТ 28147–89. Длина ключа AES — 128,192 или 256 бит. Как уже отмечалось, он обеспечивает и шифрацию, и целостность.

Заметим, что используемый в нем алгоритм (Rijndael) не требует больших ресурсов ни при реализации, ни при работе, что очень важно для уменьшения времени задержки данных и нагрузки на процессор.

Особенности способов аутентификации

Показатель	Способ			
	LEAP	EAP-FAST	PEAP	EAP-TLS
Поддержка современных ОС	Да	Да	Не все	Не все
Сложность ПО и ресурсоёмкость аутентификации	Низкая	Низкая	Средняя	Высокая
Сложность управления	Низкая	Низкая	Средняя	Средняя
Single Sign	Да	Да	Нет	Да
Динамические ключи	Да	Да	Да	Да
Одноразовые пароли	Нет	Да	Да	Нет
Поддержка баз пользователей не в формате MS Windows	Нет	Да	Да	Да
Fast Secure Роуминг	Да	Да	Нет	Нет
Возможность локальной аутентификации	Да	Да	Нет	Нет
Сложность управления низкая, но необходима продуманная политика генерации паролей, что усложняет управление.				

Стандарт 802.11i ратифицирован

Институт инженеров по электротехнике и радиоэлектронике (IEEE) 25 июня 2005 года ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях — 802.11i.

Задолго до его принятия, еще в 2002 году, отраслевой консорциум Wi-Fi Alliance предложил использовать в качестве промежуточного варианта протокол WPA (Wi-Fi Protected Access), в который входили некоторые механизмы 802-11i, в том числе шифрование по протоколу TKIP (Temporal Key Integrity Protokol), и возможность применения системы аутентификации пользователей 802.1x, базирующейся на протоколе RADIUS. Протокол WPA существует в двух модификациях: облегченной модификации (для домашних пользователей) и модификации, включающей стандарт аутентификации 802.1x (для корпоративных пользователей).

В официальном стандарте 802.11i к возможностям протокола WPA добавилось требование использовать стандарт шифрования AES (Advanced Encryption Standard), обеспечивающий уровень защиты, соответствующий требованиям класса 140–2 стандарта FIPS (Federal Information Processing Standard), применяемого в правительственных структурах США.

Кроме того, новый стандарт приобрел и несколько малоизвестных свойств. Одно из них — key-caching: незаметно для пользователя информация о нем записывается, что позволяет при выходе из зоны действия беспроводной сети и последующем возвращении в нее не вводить всю информацию о себе заново.

Второе нововведение — преаутентификация, суть которой заключается в следующем: из точки доступа, к которой в настоящее время подключен пользователь, пакет преаутентификации направляется в другую точку доступа, обеспечивая этому пользователю предварительную аутентификацию еще до его регистрации на новой точке, тем самым сокращая время авторизации при перемещении между точками доступа.

Wi-Fi Alliance приступил к тестированию устройств на соответствие новому стандарту (его еще называют WPA2). По заявлению представителей Wi-Fi, повсеместной замены оборудования не понадобится. И если устройства с поддержкой WPA1 могут работать там, где не требуется продвинутое шифрование и RADIUS-аутентификация, то продукты стандарта 802.11i можно рассматривать как WPA-оборудование, поддерживающее AES.

Wi-Fi Protected Access

Стандарт Wi-Fi Protected Access (WPA) — это набор правил, обеспечивающих реализацию защиты данных в сетях 802.11x. Начиная с августа 2003 года соответствие стандартам WPA является обязательным требованием к оборудованию, сертифицируемому на высокое звание Wi-Fi Certified (http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf).

В спецификацию WPA входит немного измененный протокол TKOP-PPK. Шифрование производится на сочетании нескольких ключей — текущего и последующего. При этом длина IV увеличена до 48 бит. Это дает возможность реализовать дополнительные меры по защите информации, к примеру ужесточить требования к реассоциациям, реаутентификациям.

Спецификации предусматривают и поддержку 802.1x/EAP, и аутентификацию с разделяемым ключом, и, несомненно, управление ключами.

WPA-устройства готовы к работе как с клиентами, работающими с оборудованием, поддерживающим современные стандарты, так и с клиентами, совершенно не заботящимися о своей безопасности. Категорически рекомендуется распределять пользователей с разной степенью защищенности по разным виртуальным ЛС и в соответствии с этим реализовывать свою политику безопасности.

Выводы и рекомендации

При условии использования современного оборудования и ПО в настоящее время вполне возможно построить на базе стандартов серии 802.11x защищенную и устойчивую к атакам беспроводную сеть, для чего необходимо реализовать в ней лишь несколько разумных постулатов.

Нужно помнить, что почти всегда беспроводная сеть связана с проводной, а это, помимо необходимости защищать беспроводные каналы, является побудительным мотивом к внедрению новых методов защиты в беспроводных сетях. В противном случае сеть будет иметь фрагментарную защиту, что, по сути, является угрозой безопасности. Желательно использовать оборудование, имеющее сертификат Wi-Fi Certified, то есть подтверждающий соответствие WPA.

Многие администраторы, устанавливая в ЛС устройства, оставляют настройки производителя по умолчанию, что категорически недопустимо в серьезных беспроводных сетях.

Несомненно, нужно внедрять 802.11x/EAP/TKIP/MIC и динамическое управление ключами. В случае смешанной сети следует использовать виртуальные локальные сети; при наличии внешних антенн применяется технология виртуальных частных сетей VPN.

Необходимо сочетать как протокольные и программные способы защиты, так и административные. Имеет смысл подумать и о внедрении технологии Intrusion Detection Systems (IDS) или специальных программных пакетов для обнаружения возможных вторжений.

При планировании защищенной беспроводной сети нужно помнить, что любое шифрование или другие манипуляции с данными неизбежно приводят к дополнительным задержкам, увеличивают объем служебного трафика и нагрузку на процессоры сетевых устройств. Безопасность, безусловно, важный фактор в современных сетях, но он теряет всякий смысл, если трафик пользователя не получает должной полосы пропускания. Сети создаются в конечном счете не для администраторов, а для пользователей.