Эссе по Защите Информации

«Проблемы защиты информации в беспроводных сетях»

Аристов Н.В. группа 911

Информационная безопасность беспроводных цифровых сетей

Беспроводные цифровые сети, развитие которых является одним из наиболее перспективных направлений телекоммуникационной отрасли, в последнее время стали объектом пристального внимания разработчиков систем связи и информационного обмена, для которых проблема обеспечения защищенности таких сетей является одной из основных.

Проблемы обеспечения информационной безопасности

Повышение оперативности получения информации и обеспечение мобильности пользователей стали сегодня одними из важнейших требований к системам информационного обмена, вычислительным сетям и автоматизированным телекоммуникационным системам. Эти требования достаточно эффективно реализуются в цифровых сетях беспроводного доступа. Привлекательность применения этих сетей постоянно возрастает. В соответствии с прогнозами, в 2003 г. общий объем затрат на них превысит 2 млрд дол., а суммарное число пользователей составит несколько десятков миллионов. Однако темпы роста могут быть и более стремительны ми, если будет успешно решена задача по обеспечению защиты информации в беспроводных сетях.

Насколько защищены сети?

Быстрые темпы развития систем беспроводного доступа были достигнуты в основном благодаря небольшим фирмам и покупательской активности частных пользователей. Крупные корпоративные клиенты ведут себя осторожно и пока, как правило, только изучают возможность использования подобных технологий для решения своих задач, требующих обычно высокой степени информационной защищенности.

Анализ существующего положения показывает, что основной причиной нерешительности руководителей многих компаний является не столько нежелание расставаться с деньгами, которые нужно будет потратить при переходе на новые системы, сколько проблемы информационной безопасности, уровень которой как для отдельных линий, так и для системы в целом, пока не определен.

В первую очередь это связано с тем, что не установлена вероятность перехвата и дешифрования информации, передаваемой по эфиру, и организации несанкционированного доступа в информационную систему через радиоканал. Эта проблема типична для всех радиосистем, поскольку в них, в отличие от проводных (кабельных) систем, демаскирующие признаки доминируют не в топологической, а в информационно сигнальной области.

Кроме того, до сих пор не разработана детальная модель угроз, существующих в области цифровых сетей беспроводного доступа, и методов борьбы с ними, что также настораживает потенциальных потребителей.

Комбинированные решения вызывают сомнения

В настоящее время основным средством обеспечения мобильного компонента широкополосного доступа к цифровым сетям остается RadioEthernet беспроводной вариант технологии Ethernet, реализуемый на базе стандарта IEEE 802.1 Ib. Этот стандарт предусматривает передачу данных в диапазоне 2,4 ГГц со скоростью до 11 Мбит с. При этом для организации доступа мобильных пользователей к цифровым сетям применяются комбинированные решения: одна часть сети строится на кабельной основе, а в другой ее части задействуется беспроводная связь.

Администратор сети естественно за интересован в том, чтобы беспроводной участок был защищен так же надежно, как и кабельный. Однако трафик радиолинии доступен для прослушивания и анализа с помощью любого устройства, обеспечивающего прием и обработку сигнала стандартного протокола, в том числе и сигнала стандарта 802.1 Ib. Поэтому операторы связи неохотно идут на включение в свою сеть беспроводных сегментов.

Соотношение сигнального и информационного уровня

Недоверие к комбинированным решениям в немалой степени обусловлено также постоянными публикациями об обнаружении новых уязвимых программных и технических элементов в продуктах различных производителей. Наличие таких элементов на сигнальном уровне делает весьма проблематичной защиту информационного уровня, на котором должны быть предотвращены:

целенаправленное искажение пере даваемых и получаемых данных;

перехват информации, которая мо жет быть использована во вред поль зователю;

перехват управления системой связи или информационной системой.

Нужно отметить, что высокая степень защищенности канала на сигнальном уровне не является гарантией обеспечения столь же высокой информационной защищенности всей системы. Это обусловлено тем, что основным показателем успешного функционирования отдельного компонента системы является реализация его целевой функции. Сигнальный уровень является нижним и обеспечивает нейтрализацию конфликтного компонента или угрозы только на своем участке.

Алгоритмы шифрования

Стандартизацией технических решений в области защиты каналов передачи данных и обеспечением совместимости оборудования различных производителей занимается независимая организация WECA (Wireless Ethernet Compatibility Alliance). Продуктам, удовлетворяющим достаточно жестким требованиям WECA, присваивается марка Wi-Fi. Наиболее популярными методами защиты являются шифрование данных и их туннелирование (инкапсуляция).

Стандарт DES

Для реализации одного из основных методов обеспечения безопасности беспроводных сетей шифрования данных долгое время применялся стандарт DES (Data Encryption Standard) с 56-разрядными ключами. В соответствии с современными требованиями к инфраструктуре информационных систем следует использовать средства защиты, основанные на стандартных протоколах аутентификации и рассылки ключей, при этом длина последних должна быть не менее 128 бит. Этим требованиям удовлетворяет усовершенствованная версия стандарта DES - Triple DES. Однако реализация стандарта связана с большим расходом ресурсов питания процессора, поскольку данные передаются для шифрования не один раз, а три, что делает почти невозможным его применение в мобильных вы числительных устройствах.

Алгоритмы TKIP и AES

Рабочий комитет IEEE недавно одобрил спецификации стандарта 802.11i, который призван повысить информационную безопасность беспроводных сетей. Стандарт определяет алгоритм защиты, получивший название TKIP (Temporal Key Integrity Protocol), который предусматривает формирование новых ключей шифрования для каждых 10 кбайт передаваемых данных. Одним из основных достоинств этого метода

является то, что практически все известные аппаратно-программные комплексы беспроводных сетей передачи данных могут быть дополнены поддержкой TKIP.

В тоже время протокол TKIP рассматривается лишь как промежуточное решение проблемы безопасности и защиты информации на сигнальном уровне. Сейчас ведется подготовка спецификаций нового алгоритма, основанного на американском стандарте шифрования данных AES (Advanced Encryption Standard) со 128-разрядным ключом. Этот метод шифрования считается более надежным, чем TKIP, и должен заменить его в течение ближайших двух лет.

Длительность процесса обусловлена, главным образом, тем, что практическое внедрение AES потребует доработки не только программной, но и аппаратной части оборудования. Во многих случаях интеграция AES в уже используемые изделия для сетей 802.11 будет затруднена. Новые устройства с поддержкой AES смогут работать в рамках одной сети со старым оборудованием, но при этом эффективность защиты на сигнальном и, следовательно, на информационном уровнях будет не столь высока. Ожидается, что первые устройства на основе этого стандарта появятся на рынке в начале 2003 г.

AES

Устойчивость против известных видов атак

Дифференциальный криптоанализ

Дифференциальный криптоанализ возможен, если можно из всех возможных проходов выделить несколько(2 или 3) проходов, имеющих коэффициент распространения (относительное количество всех входящих пар, которые для данного входного различия дадут увеличение выходного) значительно превышает 2^{1-n}, где n – длина блока.

Для Rijndael не существует 4-раундовых дифференциальных проходов с предсказываемым коэффициентом распространения равным 2^{-150} (и ни одного 8-раундового с коэффициентом 2^{-300}). Для любой длины блоков в Rijndael это достаточно.

Линейный криптоанализ

Линейный криптоанализ возможен, если можно из всех возможных входных-выходных корреляций выделить несколько(2 или 3) значительно превышающих $2^{n/2}$, где n – длина блока. Входная-выходная корреляция состоит из линейных проходов, где эта корреляция является суммой коэффициентов корреляций всех линейных проходов, имеющих определённые начальные и конечные выбранные модели. Коэффициентам корреляций линейных проходов присвоены значения, которые зависят от величины Циклического (Round) ключа. Чтобы противостоять линейному криптоанализу, необходимо отсутствие прямых проходов с коэффициентом корреляции больше $2^{n/2}$.

Для Rijndael не существует 4-раундовых линейных проходов с предсказываемым коэффициентом распространения равным 2^{-75} (и ни одного 8-раундового с коэффициентом 2^{-150}). Для любой длины блоков в Rijndael это достаточно.

Усеченные Дифференциалы. (Truncated Differentials)

Этот вид атаки использует тот факт, что в некоторых шифрах дифференциальные проходы группируются. Группировка имеет место, если для определённого набора входных и выходных дифференциальных рисунков (pattern) количество дифференциальных проходов очень велико. Ожидаемая вероятность того, что

дифференциальный проход останется внутри кластера (группы), может быть подсчитана независимо от коэффициентов распространения для дифференциальных проходов. Шифры, в которых все преобразования имеют вид ровных блоков, являются восприимчивыми к этому виду атак. Так как Rijndael оперирует с байтами, а не с одиночными битами, то была установлена его устойчивость к этому виду атак.

Ожидаемая устойчивость

Для любой определённой стандартом длины блоков и любых ключей ожидается, что Rijndael ведёт себя на столько хорошо, на сколько можно это ожидать от шифра с заданной длиной и ключом. Это подразумевает следующее: наиболее эффективным видом атак против Rijndael является взлом ключа путем обыкновенного перебора. Количество переборов зависит от дины ключа (для 16-байтного, например, 2^{127}).

Преимущества и ограничения

Преимущества

- аспекты применения:

скорость выполнения Rijndael необычайно высока для блочных шифров

Rijndael может быть применен на Смарт-картах, требуя малого кода, использующего малое количество RAM и имеющего малое количество циклов

- простота разработки:

шифр является полностью «самоподдерживаемым», то есть не использует других криптографических компонент

шифр не базирует свою защищенность на полном или частичном сокрытии взаимосвязей между арифметическими операциями

- переменная длина блока

длины ключа и блока могут варьироваться от 128 до 256 бит с шагом 32 бита

Ограничения

Ограничения шифра связаны с обратным(inverse) шифром:

Обратный шифр менее пригоден для Смарт-карт(требует больше места и циклов)

в программном обеспечении прямой и обратный шифры используют различный код и (или) таблицы

Как работает протокол WEP

WEP в настоящее время использует два варианта для шифрования — 64 и 128 бит. Ключ образуется из 24-битного вектора инициализации (initialization vector — IV) и действующего секретного ключа из 40 или 104 бит. Указанное 40-битное шифрование эквивалентно 64-битному кодированию. В стандарте ничего не упоминается об управлении ключом; единственным требованием является то, чтобы карта беспроводного соединения с сетью и точка доступа использовали один и тот же алгоритм. Обычно каждый пользователь в локальной сети использует один и тот же ключ секретности. Алгоритм RC4 использует этот ключ для генерации неопределенной,

псевдослучайной последовательности ключей. Однако пользователи беспроводных ЛВС используют различные IV для предотвращения того, чтобы пакеты данных всегда использовали одинаковые ключи RC4, «случайно» генерируемые на основе идентичного ключа WEP.

До передачи пакетов данных, процедура integrity check (IC) вычисляет контрольную сумму. Цель этого — предотвратить попытки хакеров изменить данные во время их передачи. RC4 тогда генерирует последовательность ключей из ключа секретности и IV. Затем WEP связывает данные и IC с последовательностью ключей, используя функцию «исключающего ИЛИ» (XOR). Сначала передается IV в простом тексте, затем зашифрованные данные. Восстановив RC4 последовательность ключей из IV и известного ключа, получатель данных сможет, наконец, дешифровать данные путем XOR.

Слабина: вектор инициализации

Слабость шифрования WEP проистекает из плохого применения IV. Если, например, хакер использует функцию XOR для того, чтобы математически связать два пакета в сессии, обрабатываемых одними и теми же IV, являющимися идентичными ключами RC4, тогда он сможет вычислить ключ.

Поскольку вектор инициализации имеет длину в 24 бита, он повторится в используемой точке доступа (при отсылке пакетов по 1500 байт на скорости 11 Мб/с) не более чем через 5 часов. За это время можно передать максимум 24 ГБ. Поэтому вполне реально записать передаваемые данные, используя ноутбук, и получить пакеты с идентичными IV и, следовательно, идентичными ключами RC4.

Поскольку в стандартах ничего не сказано о генерации IV, не все производители используют целое поле в 24 бита под IV. Поэтому IV может дублировать себя даже быстрее, и в этом случае записывать придется меньше. Карты для организации беспроводных сетей производства компании Lucent, например, обнуляют IV каждый раз при их инициализации, и затем продолжают подсчет. Записывая потоки данных от нескольких пользователей в беспроводной ЛВС, хакер быстрее насчитает пакеты с продублированными IV.

Исследователи Fluhrer, Martin и Shamir также обнаружили существование слабых векторов инициализации, которые создают следы от байтов ключа с вероятностью в 5 %. После записи от четырех до шести миллионов пакетов (порядка 8,5 ГБ), хакер получает достаточное количество слабых IV для определения целого ключа WEP.

Эта процедура может быть еще проще, если ключ WEP будет затребован ПО беспроводной ЛВС не в формате Hex, а в виде последовательности ASCII-символов. Поскольку ввести можно только нормальные символы и числа, количество возможных комбинаций уменьшается. Таким образом, увеличивается степень определенности, о которой говорилось выше, и для определения ключа потребуется запись не более одного или двух миллионов пакетов.

Инструментарий хакера в Интернет

В то время как Adam Stubblefield в своей статье подробно описал практическую попытку, не публикуя при этом само хакерское ПО, на Web-сайтах в Интернет таких инструментов навалом. Эти программы используют карты для создания беспроводной ЛВС с чипсетом Prism-2. Это, например, модели Compaq WL100, D-Link DWL-650, Linksys WPC11 и SMC 2632W, не говоря уже о продукции менее известных производителей. Все это легко купить. Этот чипсет выбран из-за того, что для него существует драйвер под ОС Linux (WLAN-NG), что позволяет производить запись пакетов без регистрации в сети. Программы ищут слабые векторы инициализации, и,

после записи от пяти до десяти миллионов пакетов, предоставляют ключ WEP за секунду.

Возможны активные атаки

Поскольку описанные выше пассивные атаки (запись пакетов) хорошо срабатывают, активные атаки не столь важны. Однако их также могут использовать, например, для кражи информации из заинтересовавшей ЛВС. Допустим, что хакер знает оригинальные данные и зашифрованный результат. В этом случае он сможет заменить данные своими собственными, даже не зная ключа. Получатель будет рассматривать информацию как правильную. Это опять-таки базируется на математической функции XOR.

Хакер может также попытаться манипулировать не собственно данными как таковыми, а адресами IP. Поскольку большинство ЛВС, как правило, подсоединены к Интернет, хакер может изменить целевые адреса таким образом, что данные, посланные со станции в беспроводной ЛВС, дешифруются на точке доступа и посылаются хакеру в виде простого текста по Интернет.

Эффективные лекарства

Для улучшения безопасности WEP, организация RSA Security — создатель шифрования RC4, и калифорнийская компания Hifn (http://www.hifn.com), поработали над улучшением алгоритмов шифрования. Они анонсировали новое шифрующее решение RC4 Fast Packet Keying. Различные ключи RC4 генерируются в быстрой последовательности для каждого передаваемого пакета данных. Обе стороны используют RC4 128-битный ключ, так называемый Temporal Key (TK). Каждая отсылающая сторона использует различные последовательности ключей в качестве TK, связанного с адресами отсылающих сторон. К ним добавляется 16-битный IV, что опять-таки отражается в 128-битном ключе RC4. RC4 Fast Packet Keying создан таким образом, чтобы у существующих беспроводных ЛВС могли быть модернизированы как firmware, так и программные драйверы.

Cisco идет своим путем

Компания Cisco разработала ряд усовершенствований для серии своей продукции Aironet, которые, однако, можно использовать только в сетях, где нет компонентов не от Cisco. Протокол LEAP (Lightweight Extensible Authentication Protocol), разработанный специалистами Cisco, обеспечивает аутентификацию для Cisco Radius Server (Access Control Server 2000 V2.6).
В продукции Cisco используется метод разделяемых ключей для генерации ответов на обоюдные запросы. Ключи, симметричные и несимметричные, делают атаки посредством производимых паролей невозможными.

В продукции Cisco используются динамические, основанные на пользователе и сессии WEP ключи, которые могут быть сгенерированы системой без каких-либо дополнительных административных усилий. Каждый пользователь в каждую сессию получает уникальные ключи для сессии, которые не используются совместно ни с каким другим пользователем. Передаваемые по сети ключи WEP шифруются посредством аутентификации LEAP до того, как отсылаются. Только пользователь с соответствующим ключом сессии может работать с ключом WEP.

В комбинации с Access Control Server 2000 2.6 можно установить направления для повторения аутентификации. Пользователи должны регулярно аутентифицировать себя и приписывать новый ключ для сессии при каждой регистрации. Вектор инициализации модифицируется для каждой сессии, не давая возможности хакерам использовать предопределенные последовательности и создавать таблицы дешифровки, проистекающие из этих последовательностей.

Тем не менее, все эти предосторожности не дают абсолютной защиты, потому что применение IV и механизма шифрования ключей WEP остается неизменным. Постоянные изменения ключей, однако, значительно снижают уязвимость перед хакерскими атаками. Любые атаки, основанные на таблицах дешифровки, обречены на неуспех. Если ключи меняются столь часто, что длины записанных пакетов будет недостаточно для оценки, шансы на удачную атаку станут практически равны нулю.

В рамках организации IEEE в настоящее время разрабатывается модернизированная версия WEP. В этом стандарте RC4 будет заменен новым протоколом шифрования.

Заключение

Таким образом, не все так плохо с безопасностью беспроводных сетей. При правильном построении радиосети наиболее вероятную угрозу безопасности представляет нарушение физической целостности, нехарактерное для проводных сетей. Что делать. За преимущества радиосетей, связанные с отсутствием кабельной инфраструктуры, приходится платить.

Следует иметь в виду, что в радиосетях без каких-либо ограничений могут применяться средства обеспечения безопасности, предоставляемые операционными системами и программно-аппаратными средствами мониторинга сетей.

Литература:

Wired Equivalent Privacy Vulnerability Princy C. Mehta April 4, 2001

[BO1] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Intercepting Mobile Communications: The Insecurity of 802.11*. January 2001.

[BO2] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Security of the WEP Algorithm*. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, University of California at Berkeley, February 2001.

[BOW] Bowman, Lisa M. *Wireless Networks Leave Holes for Hackers*. http://news.cnet.com/, CNET News.com, February 5, 2001.

[FIS] Fisher, Dennis and Nobel, Carmen. *Wireless LAN Holes*. http://www.zdnet.com/eweek/stories/general/0,11011,2684337,00.html, eWeek, February 11, 2001.

[GAR] Garcia, Andrew. WEP Remains Vulnerable. http://www.zdnet.com/eweek/stories/general/0,11011,2700806,00.html, eWeek, March 26, 2001.

[GRO] Grogans, Candance; Bethea, Jackie; and Hamdan, Issam. *RC4 Encryption Algorithm*. http://www.ncat.edu/~grogans/main.htm, North Carolina Agricultural and Technical State University , March 5, 2000.

[HOL] *Holes in Wireless Nets*. http://www.zdnet.com/eweek/stories/general/0,11011,2687518,00.html, eWeek, February 26, 2001.

[MCM] McMurry, Mike. *Wireless Security*. http://www.sans.org/infosecFAQ/wireless/wireless_sec.htm, January 22, 2001.

[PES] Pescatore, John. *Commentary: An Object Lesson in Managing Security Risks of New Technologies*. http://www.techrepublic.com/article.jhtml?src=search&id=r00120010207ggp10.htm, TechRepublic, Inc. February 7, 2001.

[SAN] Sandberg, Jared. *Hackers poised to land at wireless AirPort*. http://www.zdnet.com/enterprise/stories/main/0,10228,2681947,00.html, ZDNet, February 5, 2001.

[SHI] Shim, Richard. *How to Fill Wi-Fi's Security Holes*. http://www.zdnet.com/enterprise/stories/main/0,10228,2693864,00.html, ZDNet, March 8, 2001.

[USK] Uskela, Sami. *Security in Wireless Local Area Networks*. http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html, Helsinki University of Technology, 1997.

[ZUR] Zurko, Ellen. *Listwatch: Items from Security-Related Mailing Lists*. http://www.ieee-security.org/Cipher/Newsbriefs/2001/022001.ListWatch.html, IEEE, February 16, 2001.

[ZYR] Zyren, Jim and Petrick, Al. *IEEE 802.11 Tutorial*. http://www.wirelessethernet.org/whitepapers.asp.