Рынок беспроводных соединений

Наступает время стабильности

Подобно тому, как драматические произведения развиваются по заранее известной схеме «завязка–кульминация–финал», некоторые сегменты IT-рынка проходят в своем развитии те же стадии. Правда, называть их, как правило, надо «эйфория–разочарование–стабильность».

Парадокс ситуации

Эйфорию, которую испытало все IT-сообщество при появлении самого понятия «беспроводные коммуникации», можно сравнить с реакцией человечества на первый полет в космос. Компьютерные СМИ на стыке века прошлого и настоящего на разные голоса призывали резать провода и выходить на уровень нового тысячелетия.

Между тем люди опытные осторожно ждали того момента, когда эйфория сменится неизбежным разочарованием. Толчком к этому послужил тот факт, что, как оказалось, технологии беспроводной передачи так же уязвимы, как и обычные, а в некоторых случаях уровень безопасности последних гораздо выше в силу того, что опыт их эксплуатации неизмеримо богаче.

В феврале 2001 года только что вышедшего из тюрьмы Кевина Митника прямо-таки умиляла возможность «слушать» трафик любой беспроводной сети с помощью автомобиля и простейшей антенны. Причем автомобиль в этом случае требовался лишь для того, чтобы вас не догнали. Что же касается беспроводной передачи голоса, то даже у нас только ленивый не пытался собрать прибор, позволяющий вычислять частоту, на которой работает телефон соседа.

Но потенциал, заложенный в технологии беспроводной передачи, оказался настолько большим, что отсутствие безопасности не остановило ни разработчиков, ни пользователей. Более того, Wireless-сегмент IT-рынка — один из наиболее динамично развивающихся в России. »

» Есть решение проблемы, их даже много...

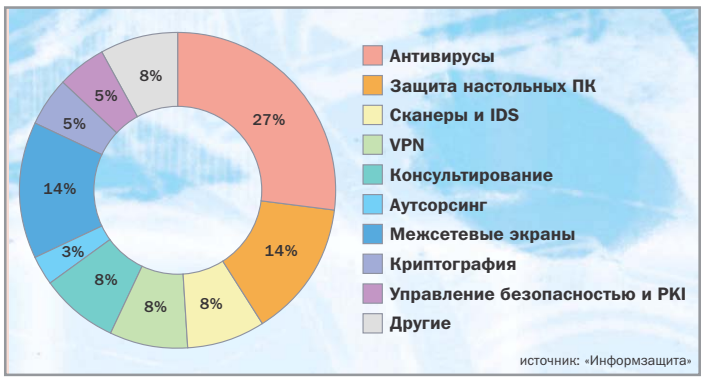
И все-таки беспроводную сеть безопасной сделать можно! Для этого разработчикам необходимо решить всего две проблемы.

Во-первых, очевидно, что передаваемый трафик надо шифровать. В выборе вариантов реализации и алгоритмов шифрования разработчики на данный момент достаточно свободны. Связано это с тем, что на сегодняшний день нет единого стандарта. Комитет IEEE 802.11 разрабатывает, конечно, рекомендации (подкомитеты 802.1i и 802.1X), но они и по сей день остаются рекомендациями. И во-вторых, для работы по «широкой полосе» необходимо обеспечить надежную аутентификацию пользователей.

К концу прошлого года существовало примерно пять-шесть компаний, получивших в свое распоряжение средства для разработки комплексных систем и средств защиты.

Самый большой грант (примерно $27,5 млн) использует компания Fiberlink Communications, которая создает комплексную систему удаленного доступа к корпоративной сети. $26 млн получила в свое распоряжение компания NTRU. В роли заказчиков в этом случае выступают Texas Instruments, Sony, Macrovision, Lehman Brothers. Примерно по $8 млн было вложено в компании Vernier и NetMotion, которые параллельно создают средства разработки программного обеспечения для корпоративных сетей независимо от способа организации каналов связи.

Между тем технологическая основа для решения проблемы безопасности Wireless-коммуникации существует уже сегодня. Технологии VLAN и VPN можно использовать вполне успешно, тем более что такие гиганты как IBM и Intel продвигают готовые решения, основанные на одной из них. Однако есть один аспект проблемы, который в последнее время выходит на первый план, — то, что в ушедшей в прошлое советской стране называлось «человеческий фактор».



На российском рынке основным средством защиты являются антивирусы

Решаем комплексно

Несмотря на всю красоту, технологии VLAN и VPN достаточно сложны для понимания. А тем более настройки. Рынок сегодня требует комплексных решений, ориентированных на конечного пользователя. То есть, конечно, для наших компаний это не так принципиально — российский пользователь свято верит в своего системного администратора. А для остального прогрессивного человечества становится важным наличие комплексного решения, которое требует минимальной настройки и неприхотливо в работе.

Кроме того, некоторые аналитики считают, что IT-сообщество находится сегодня на пороге появления новых стандартов и протоколов, ориентированных на беспроводные коммуникации. Это относится как к «базовым» алгоритмам шифрования (таковых сегодня насчитывается уже несколько десятков), так и к ПО.

В августе 2002 года компания Research In Motion Ltd. объявила о начале работ по оснащению Агентства национальной безопасности США новым ПО для обмена сообщениями по беспроводным коммуникациям с поддержкой протокола шифрования почтовых сообщений S/MIME (безопасный MIME).

Стабильность — признак мастерства

Абсолютная «прозрачность» беспроводных коммуникаций и полная беззащитность перед атаками взломщиков, похоже, остаются в прошлом. И это понятно. Привлекательность способов связи посредством беспроводных устройств настолько велика, что в рамках широкого внедрения этих технологий должно быть найдено решение любой проблемы. ■ ■ ■ Сергей Кондрашев

VPN и VLAN

Защищенная корпоративная сеть

Основной идеей VPN является то, что она абсолютно независима от типа канала связи, поверх которого организовывается. Для работы, как правило, используется механизм, известный как IP-туннелирование, когда в рамках одного IP-соединения организуется передача шифрованной информации. Механизм проверки пароля работает при входе в VPN, а механизм шифрации и дешифрации — при передаче трафика от узла к узлу. Кроме того, можно организовать защиту трафика при передаче его от одной сети к другой. При этом шифрация будет происходить на выходе одной сети, а дешифрация — на входе другой.

При работе VPN все данные в рамках одного и того же сегмента прозрачны для приложений, но недоступны компьютерам из другого сегмента. При инициализации сеанса каждый пользователь вместе с внутренним IP-адресом получает уникальный ключ для шифрования, действительный только на один сеанс.

Спецификация IEEE 802.1Q предусматривает наличие в кадрах Ethernet четырех дополнительных бит (тэгов). Используя эти биты, коммутаторы могут в соответствии с установками группировать свои порты и организовывать подсети, трафик (так называемый «тэгированный») которых не будет виден другим подсетям. Если коммутаторы разнесены географически, можно использовать транковые порты для объединения подсетей, имеющих один и тот же идентификатор.

Операционные системы, работающие на роутерах (Cisco OS, FreeBSD, Linux), имеют поддержку VLAN на уровне ядра. Windows-системы используют для работы по VLAN драйверы производителей сетевых карт.