БЕЗОПАСНОЕ ПРИМЕНЕНИЕ ТЕХНОЛОГИИ «МОБИЛЬНОГО WIMAX»

Середницкий Виктор Сергеевич
ГОУ ВПО «Уральский государственный технический университет –УПИ имения первого Президента России Б.Н.Ельцина».
Екатеринбург, Россиия.

Технология WiMAX (Worldwide Interoperability for Microwave Access) признана одной из самых перспективных технологий беспроводной широкополосной связи на сегодня, т.к. способна предоставить высокоскоростную широкополосную связь – как фиксированную, так и мобильную в соответствии со всеми требованиями сетей 4-го поколения. Технологию WiMAX можно использовать для создания широкополосных соединений "последней мили", развертывания точек беспроводного доступа, организации сети между филиалами компаний и решения других задач, которые ранее были ограничены традиционными технологиями. Но, как показала практика, при внедрение новых телекоммуникационных технологий мало внимания уделяется вопросам информационной безопасности.

В настоящее время в нашей стране применяется технология WiMAX для фиксированного доступа - стандарт IEEE 802.16-2004, а также новая технология WiMAX – технология беспроводной связи мобильного доступа – стандарт IEEE 802.16e («мобильный WiMAX»). Наиболее защищенной с точки зрения информационной безопасности является технология WiMAX стандарта IEEE 802.16e.

Данная статья посвящена описанию одного из методов безопасного применения технологии «мобильного WiMAX».

В основе функционирования технологии WiMAX лежит взаимодействие базовой станции (БС) и абонентских станций (АС). Взаимодействие станций заключается в обмене информацией следующего характера: данные для установлении сеанса связи, данные для обеспечения аутентификации, собственно полезная информация, различные служебные сообщения.

Одним из существенных недостатков стандарта IEEE 802.16-2004 является отсутствие взаимной аутентификации БС и АС. Разработчики IEEE 802.16e постарались исправить этот недостаток, поэтому спецификация «мобильного WiMAX» позволяет применять схему аутентификации станций с использованием сервера аутентификации [1].

Наиболее надежной является схема аутентификации на основе протокола RADIUS (Remote Authentication Dial-In User Service), роль сервера аутентификации выполняет так называемый RADIUS-сервер. Не будем заострять внимание на пояснение процедуры аутентификации – по этому вопросу много документации, остановимся на одной из важных проблем информационной безопасности.

При обмене сервера RADIUS и АС используются пакет, содержащий поле *Response Authenticator*. Это поле используется для проверки достоверности сторон, участвующих в обмене информацией. Для вычисления этого поля инициатор сообщения должен знать секретный код сервера RADIUS. Значение *Response Authenticator* формируется алгоритмом шифрования MD5 (MD5-свертка), на вход которого поступает информация, содержащая требуемые аутентификационные данные и секретный код сервера RADIUS [2].

Важно то, что в отличие от другой информации сервера RADIUS, только в поле *Response Authenticator* используется секретный код сервера RADIUS.

Таким образом, злоумышленник, перехвативший пакет с полем *Response Authenticator*, используя средства подбора парольной информации может вычислить значение секретного кода сервера RADIUS. Нужно заметить, что по умолчанию один и тот же секретный код сервера RADIUS может использоваться в течении месяца, причем для многих АС. Значит, злоумышленник имеет шансы на дальнейшее проведение атаки.

Негативным моментом, с точки зрения информационной безопасности, является то, что секретный код сервера RADIUS используется для генерации ключей шифрования информации АС и БС, например PMK (Pairwise Master key – основной парный ключ) [3]. PMK - обновляемый симметричный ключ, владение которым означает разрешение на доступ к среде передачи данных в течении сессии. Для каждого сеанса связи между АС и БС создается новый PMK. В свою очередь, ключ PMK используется для генерации других ключей, которые применяются непосредственного для шифрования трафика межу станциями в данной сессии.

Таким образом, злоумышленник зная секретный код сервера RADIUS, может вычислить PMK, а затем может получить доступ к информации, передаваемой между станциями.

Для обеспечения безопасного применения данной технологии, необходимо предпринять ряд мер: исключить или затруднить возможность перехвата трафика в корпоративной беспроводной сети; передавать трафик сервера RADIUS по туннелю на основе протокола IPsec (к сожалению, немногие продукты поддерживают такую возможность); административными мерами сформировать сложный секретный код сервера RADIUS для каждого беспроводного клиента и регулярно обновлять его.

Библиографический список

1. Trung Nguyen. A survey of WiMAX security threats. 2009.
2. Вишневский В.М. Энциклопедия WiMAX. Путь к 4G. М., 2009.
3. IEEE Std 802.16e™-2005 and IEEE Std 802.16™-2004/Cor1-2005. NY., 2006