Раздел VI. Безопасность

УДК 004.056.53

И.Ю. Иващук

ИССЛЕДОВАНИЕ ЛОГИЧЕСКИХ СВЯЗЕЙ В СТРУКТУРЕ МЕХАНИЗМОВ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ

Анализируется взаимосвязь между механизмами защиты информации в беспроводных сетях. Приведены результаты исследований в области оценки защищенности беспроводных сетей: критерии оценки защищенности и уровни доверия к ним.

Беспроводная сеть; уровень доверия; алгоритм шифрования; протокол аутентификации.

I.Y. Ivashchuk

RESEARCH OF LOGICAL LINKS IN STRUCTURE OF PROTECTION MECHANISMS OF WIRELESS NETWORKS

In work the interrelation between protection mechanisms of the information in wireless networks is analyzed. The results of studies in the assessment of an estimation of wireless network security are demonstrated: estimation criteria of security and trust levels to them.

Wireless network; trust level; algorithm of enciphering; authentication protocol.

В настоящее время день проблема защиты беспроводных сетей (БС) стоит как никогда остро. Это связано в первую очередь с ускоряющимся темпом жизни в современном мире, который требует от человека полной мобильности и мгновенного принятия решений. К сожалению, проводные сети не всегда могут удовлетворить данным условиям. Именно поэтому за последние 5 лет столь возросла популярность и распространенность беспроводных сетей. Но увеличение доли передаваемой информации по средствам беспроводных технологий прямо пропорционально увеличивает долю угроз и атак по отношению к ним.

Для правильного построения системы защиты нужно определить ценность информации, циркулирующей в сети, и в соответствии с полученными результатами выбрать подходящий уровень доверия (УД) к ней [1].

УД к БС основаны на средствах защиты информации (сзи), которые реализованы в ней согласно семейству стандартов 802.11 [2].

Установление взаимосвязи между различными сзи БС и дальнейшее их ранжирование по УД значительно упростит процедуру сертификации данного вида сетей.

Для исследования логических связей в структуре механизмов защиты беспроводной сети необходимо проанализировать семейство стандартов 802.11 по критериям защищенности [3].

Криптографические критерии:

1) криптографические алгоритмы;
2) длина используемого ключа;
3) использование динамических или статических ключей;
4) технология проверки целостности сообщений.

Критерии аутентификации:

1) протокол;
2) наличие сервера аутентификации;
3) взаимная аутентификация;
4) использование цифровых сертификатов.

В результате анализа предполагается получить полный структурированный набор механизмов защиты, которые описываются в стандартах для БС.

Первоначально исследуем механизмы защиты, призванные обезопасить сеть с точки зрения защиты передаваемых данных. Для этих целей проанализируем семейство стандартов при помощи криптографических критериев.

Основополагающим механизмом в этой сфере является криптографический алгоритм, используемый для шифрования передаваемого трафика.

На заре становления беспроводных технологий этим целям удовлетворял алгоритм WEP, используемый совместно с 40-битным разделяемым ключом. Позже для усиления его криптостойкости стали использовать уже 128-битный ключ, в то время как сам алгоритм остался прежним.

В стандарте 802.11i вводится новый алгоритм AES, который обладает значительно большей криптостойкостью по сравнению с предшественником. Но усиление защитных свойств алгоритма приводит к значительному увеличению ресурсоемкости оборудования для развертывания беспроводной сети. Именно поэтому на первых этапах внедрения алгоритм AES также применяется со 128-битным ключом. Но в стандарте сразу же закладывается возможность последующего расширения и алгоритм AES можно использовать как со 192-битным ключом, так и с 256-битным.

Возможность изменения ключа на протяжении сеанса связи тоже была введена не сразу. Когда БС только начали появляться на рынке сетевых технологий, статистический ключ вполне удовлетворял поставленным целям. Но пропорционально росту популярности беспроводной связи увеличиваются и требования конечных пользователей к уровню безопасности, который могут обеспечить подобные соединения. Наравне с увеличением длины ключа применяется методика его периодической смены, ключ становится динамическим.

Для проверки целостности передаваемых сообщений в стандартах семейства 802.11 описываются два протокола: MIC и CCMP.

Впервые протокол проверки целостности вводится во временном стандарте WPA (Wireless Protected Access). Он появился в 1999 году и является результатом договоренности производителей оборудования. К такой мере пришлось прибегнуть вследствие того, что ратификация 802.11i заняла больше времени, чем предполагалось.

MIC представляет собой достаточно сложный математический алгоритм, который позволяет сверять отправленные в одной точке и полученные в другой данные. Благодаря применению функции MIC программное обеспечение устройств беспроводной связи будет извещать получателя обо всех случаях изменения содержимого кадров в процессе передачи. Отправитель и получатель независимо друг от друга вычисляют значения MIC. Если получатель генерирует значение MIC, отличное от значения, вложенного в кадр, то программное обеспечение устройств беспроводной связи считает этот кадр измененным и отвергает его. В итоге получается, что каждый передаваемый по сети пакет данных имеет собственный уникальный ключ, а каждое устройство беспроводной сети наделяется динамически изменяемым ключом.

С выходом в свет стандарта 802.11i алгоритм MIC заменяется на более современный алгоритм CCMP, состоящий из связки алгоритма шифрования AES и

кода CBC-MAC(Cipher-Block Chaining (CBC) with Message Authentication Code (MAC) Protocol). CCMP вычисляет код целостности сообщения, прибегая к хорошо известному и проверенному методу CBC-MAC. Изменение даже одного бита в сообщении приводит к совершенно другому результату. CCMP призван обеспечить конфиденциальность, аутентификацию, целостность и защиту от атак воспроизведения. Данный алгоритм основан на методе CCM алгоритма шифрования AES, который определен в спецификации FIPS PUB 197. Все AES-процессы, применяемые в CCMP, используют AES со 128-битовым ключом и 128-битовым размером блока. Алгоритм CCM описан в IETF RFC 3610.

Таким образом, был получен полный набор механизмов защиты БС в соответствии с криптографическими критериями. Представим его в наглядном виде с учетом существующих логических связей (рис. 1). Причем сплошная линия указывает на обязательность использования механизмов защиты совместно, в то время как пунктирная – на возможность их совместного применения.

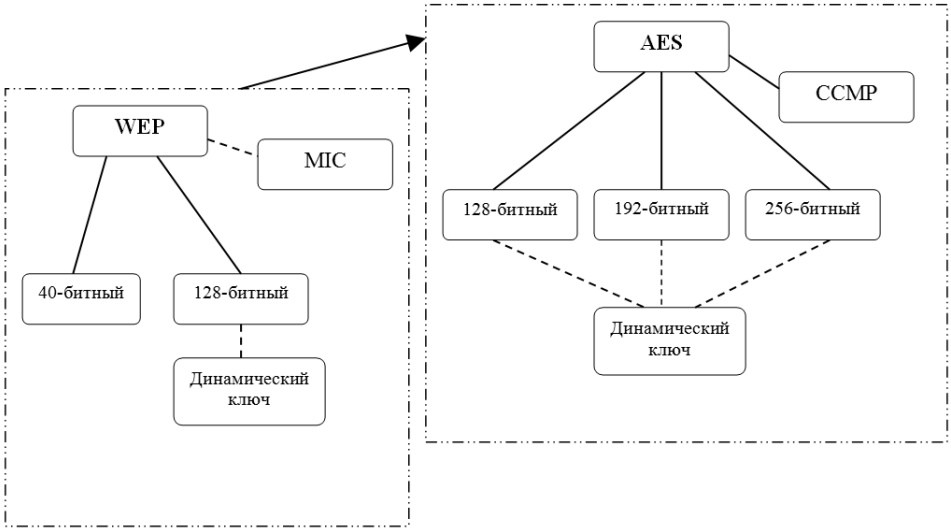

Рис. 1. Логическая структура криптографических механизмов защиты беспроводной сети

Обобщив данные по всем возможным реализациям криптографических механизмов защиты в БС, составляем табл. 1 и 2.

Таблица 1

Возможные сочетания криптографических механизмов защиты при использовании алгоритма WEP

		WEP-40	WEP-128
Статистический ключ	Есть проверка целостности		+
	Нет проверки целостности	+	+
Динамический ключ	Есть проверка целостности		+
	Нет проверки целостности		+

В табл. 2 получаем 5 возможных вариантов.

Таблица 2

Возможные сочетания криптографических механизмов защиты при использовании алгоритма AES

		AES-128	AES-192	AES-256
Статистический ключ	Есть проверка целостности	+	+	+
	Нет проверки целостности	+	+	+
Динамический ключ	Есть проверка целостности	+	+	+
	Нет проверки целостности	+	+	+

В табл. 2 получаем 12 возможных вариантов.

Теперь исследуем механизмы защиты, направленные на контроль доступа к БС. При анализе семейства стандартов 802.11 воспользуемся полученными критериями аутентификации.

Если с точки зрения криптографической защиты данных алгоритм шифрования является основополагающим критерием, то с точки зрения защиты доступа к сетевым ресурсам основным критерием для оценки является протокол аутентификации. В данной сфере тоже довольно-таки ярко прослеживается поступательная динамика усиления защитных свойств протокола с развитием беспроводных технологий.

На ранних этапах использовались примитивные схемы аутентификации, как то: аутентификация с открытым либо общим ключом. Первая, по сути, не является как таковым алгоритмом аутентификации, а вторая – лишь незначительно усиливает первую за счет шифрования передаваемой служебной информации.

Полноценные протоколы аутентификации появляются позднее, после того как было найдено и обосновано несоответствие возможностей WEP постоянно расширяющемуся кругу задач БС.

Разрабатывается семейство протоколов EAP. Его многообразие объясняется тем, что производители беспроводного оборудования внедряли свою версию протокола в зависимости от своего видения будущего развития беспроводных технологий. На сегодняшний день используется 5 основных протоколов данного семейства, каждый из которых усиливает свойства предыдущего: EAP-MD5, LEAP, EAP-TLS, PEAP, EAP-TTLS [4].

Но защита беспроводной связи не ограничивается лишь схемой аутентификации пользователя в сети. Для достижения более высоких показателей в этой области вводятся дополнительные механизмы защиты.

Начиная с реализации протокола LEAP, в структуру решения по обеспечению защиты от НСД вводят сервер аутентификации, который обеспечивает дополнительные возможности разграничения прав пользователя при работе в сети. Причем возможны 2 варианта его применения: с односторонней и взаимной аутентификацией.

Также в качестве дополнительных механизмов защиты можно рассматривать и использование цифровых сертификатов (начиная с реализации протокола EAP-TLS) для верификации предоставленной пользователем информации. Стоит отметить, что при реализации протокола EAP-TLS использование цифровых сертификатов является обязательным условием, в то время как в последующих протоколах семейства EAP – лишь дополнительной опцией.

Объединив полученные механизмы защиты БС в области контроля доступа, представим в наглядном виде логические связи между ними (рис. 2). Так же, как и при построении логической структуры криптографических механизмов защиты, сплошная линия обозначает обязательность совместного применения механизмов, в то время как пунктирная – лишь возможность.

По аналогии с криптографическими СЗИ составим сводную таблицу всех возможных наборов механизмов защиты, направленных на контроль доступа к сети (табл. 3). Получается 15 возможных вариантов реализации.

Подводя итог всему вышесказанному, получаем, что в части криптографической оценки защищенности сети мы имеем 17 возможных вариантов реализации СЗИ, в то время как в части аутентификации – 15. Наиболее рациональной представляется оценка объекта исследования отдельно по каждой группе критериев. А впоследствии в результате аппроксимации полученных результатов можно определить уровень доверия к исследуемой беспроводной сети.

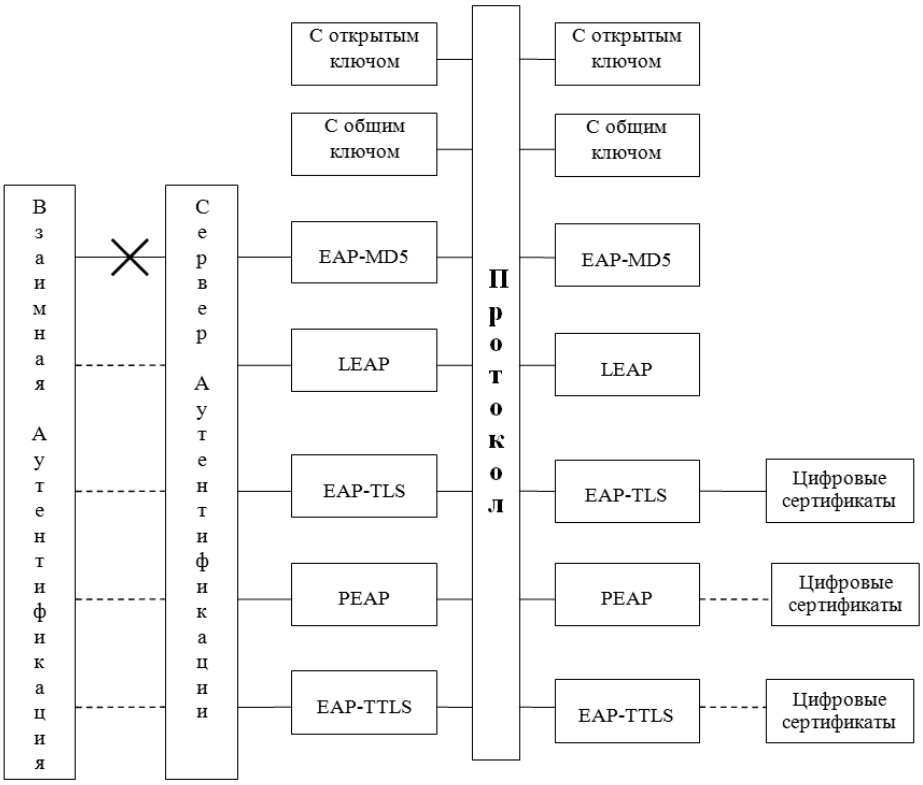

Рис. 2. Логическая структура механизмов аутентификации беспроводной сети

Таблица 3

Возможные сочетания механизмов защиты на этапе аутентификации

Протокол аутентификации	Сервер аутентификации		Цифровые сертификаты
	Отсутствует	Взаимная аутентификация	
С открытым ключом	-		-
С общим ключом	-		-
EAP-MD5		-	-
LEAP		+/-	-
EAP-TLS		+/-	+
PEAP		+/-	+/-
EAP-TTLS		+/-	+/-

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Иващук И.Ю.* Система уровней доверия к беспроводной сети на основе реализованных в ней механизмов защиты // Теория и технология программирования и защиты информации: Сб. трудов XIV Междунар. научно-практ. конф. (Санкт-Петербург, 20 мая 2009 г.). – СПб., 2009. – С. 31-33.
2. IEEE Standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area nerworks – Specific requirements. Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – IEEE Std. 802.11. – 2007 Edition.
3. *Иващук И.Ю.* Критерии оценки безопасности беспроводных сетей // Теория и технология программирования и защиты информации: Сб. трудов XI Междунар. научно-практ. конф. (Санкт-Петербург, 18 мая 2007 г.). – СПб., 2007. – С. 76-80.
4. *Гордейчик С.В., Дубровин В.В.* Безопасность беспроводных сетей. – М.: Горячая линия – Телеком, 2008. – 288 с.

Иващук Ирина Юрьевна
Санкт-Петербургский Государственный университет информационных технологий, механики и мптики (СПбГУ ИТМО).
E-mail: irina.ivashchuk@gmail.com.
197101, г. Санкт-Петербург, ул. Саблинская, 14.
Тел.: 88122338651.

Ivashchuk Irina Yurievna
Saint-Petersburg State University of Information Technologies, Mechanics and Optics (SPbSU ITMO).
E-mail: irina.ivashchuk@gmail.com.
14, Sablinskaya, Saint-Petersburg, 197101, Russia.
Phone: 88122338651.

УДК 656.7.08

Ján Piľa, František Adamčík

SAFETY RISK AND SAFETY HAZARD IN AVIATION AND SLOVAK WORKPLACE HEALTH AND SAFETY LEGISLATION

The topic of the article is to explain some peculiarities in definitions according to ICAO Safety Management System, USA FAA and Slovak legislation. Misunderstandings with terms "risk" and "hazard" following International Civil Aviation Organization (ICAO), USA Federal Aviation Authority (FAA) definitions and Slovak Workplace health and safety legislation it could make a problem in aviation risk management and hazard identification according to ICAO Safety Management System (SMS). In Slovak administrative law the term a hazard is missing. Instead of term hazard terms danger, thread or dangerousness are used.

Aviation safety; hazard; risk; danger; threat; aviation legislation; administrative law

Ján Piľa, František Adamčík

РИСК И ОПАСНОСТЬ В АВИАЦИИ И ИХ ПОНИМАНИЕ В СЛОВАЦКОМ ЗАКОНОДАТЕЛЬСТВЕ ОБ ОХРАНА ТРУДА

Объясняются понятия риск и азарт по ICAO, FAR и в словацком законодательстве. Неправильное толкование понятий «риск» (англ. risk) и «азарт» (англ. hazard), которые применяются в терминологии ICAO, FAR и законодательства Словацкой республики в связи с безопасностью и охраной здоровья во время труда, могут стать причиной проблем в системе управления безопасностью воздушного движения. В словацком административ-