ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.53

РАНЖИРОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ БЕСПРОВОДНОЙ СЕТИ ПО УРОВНЯМ ДОВЕРИЯ

И. Ю. ИВАЩУК

Санкт-Петербургский государственный университет информационных технологий, механики и оптики

e-mail: irina.ivashchukNi@cit.ifmo.ru

В статье рассматривается система уровней доверия к беспроводной сети, основанная на системе оценочных уровней доверия РД БИТ. Проводится анализ механизмов защиты подобных сетей в соответствии с критериями оценки защищенности и последующее их ранжирование по уровням доверия.

Ключевые слова: беспроводная сеть, уровень доверия, критерии оценки защищенности, механизмы защиты.

Введение

Беспроводные технологии с каждый годом становятся все более незаменимы в современной жизни человека. Увеличение доли информации, передаваемой по беспроводным каналам, увеличивает и долю атак на беспроводные сети (БС). Именно по этой причине столь важен вопрос защиты информации при ее передаче по радиоканалам.

Но зачастую, учитывая жесткую конкуренцию между компаниями на внутреннем и внешнем рынках нашей страны, одной защиты информации оказывается недостаточно. Необходимо еще подтвердить, что беспроводная сеть, по средствам которой осуществляется передача данных, на самом деле безопасна и отвечает предъявляемым к ней требованиям. Именно в этот момент возникает следующий вопрос: сертификация сети в соответствии с необходимым классом защищенности.

В общих чертах процесс сертификации состоит из аудита БС в целом и отдельно системы ее безопасности, анализа полученных данных в разрезе реализованных в сети механизмов защиты и присвоения сети соответствующего класса защищенности.

Уровни доверия к беспроводной сети

Для оценки реализованной системы защиты информации в беспроводной сети был разработан ряд уровней доверий (УД) к ней, основывающийся на оценочных уровнях доверия РД БИТ [1].

Цель введения данной системы УД заключается в оценке безопасности беспроводной сети на основе использующих в ней средств защиты информации. Причем рассматриваются только те средства, которые описаны непосредственно в семействе стандартов 802.11 [2], то есть мы исключаем механизмы защиты, направленные на предотвращение конкретных видов атак и включаемые в систему защиты беспроводной сети дополнительно в зависимости от ее специфики.

После проведения анализ защищенности беспроводной сети в соответствии с оценочными критериями защищенности БС[3], можно определить минимальный уровень доверия к данному объекту оценки (ОО), исходя из совокупности оценок средств защиты, которые используется для обеспечения безопасности в нем. Под объектом оценки понимается вся беспроводная сеть, а не отдельные рабочие станции с интегрированными беспроводными сетевыми адаптерами.

Уровень доверия к беспроводной сети определяется минимальным значением веса из полученной при анализе совокупности. Таким образом, если по всем критериям значение веса для данного ОО равно 4, а в то время как лишь по одному – 2, то общий УД тоже будет равен 2.

Если мы имеем только одно узкое место во всей сети, то мы сразу можем определить по какому параметру необходимо «подтянуть» защиту БС, либо в обратном случае, если защищенность сети является чрезмерной, снизить до требуемого уровня.

Для дальнейшего ранжирования механизмов защиты БС по УД характеризуем каждый из них (табл. 1):

- УД1 включает в себя минимально возможный набор компонентов для удовлетворения минимальных требований безопасности сети. Подобная совокупность механизмов защиты использовались в основном в начале развития беспроводных технологий, когда пропускная способность сети оставляла желать много лучшего и мощные методики не могли быть реализованы в связи со значительными затратами на аппаратные ресурсы;
- УД2 характеризуется усилением применяемых механизмов на УД1, т.е. в основе лежат все те же малозащищенные протоколы и алгоритмы, на которые накладываются дополнительные «заплатки». Также к этому уровню можно отнести появившиеся средства защиты информации (СЗИ) с минимальным набором компонент;
- УД3 изначально использует новое поколение алгоритмов и механизмов, усиленных за счет возможностей, лежащих в их основе (например, увеличение длины ключа) либо введением дополнительных мер безопасности (использование цифровых сертификатов);
- УД4 представляет максимально возможный в рамках стандарта 802.11 уровень безопасности БС за счет использования механизмов защиты информации с максимально надежным набором компонент;
- УД5 внедряет дополнительные механизмы защиты информации, которые не описываются в рамках семейства стандартов 802.11 и в своем большинстве представляют защиту от конкретного вида атак или угроз [4]. (Данный уровень доверия не рассматривается в рамках данной статьи).

Ранжирование механизмов защиты беспроводной сети

В соответствии с оценочными критериями защищенности БС[3] все механизмы защиты в ней также можно разделить на две группы: криптографические механизмы защиты и механизмы защиты при аутентификации. Первоначально рассмотрим криптографическую группу.

При построении сети на базе беспроводных технологий могут быть использования лишь два стандарта шифрования: **WEP** и **AES**. При использовании алгоритма **WEP** для шифрования передаваемой по каналам связи информации ОО может принадлежать только к 1 либо 2 уровню. Это связано с общеизвестными уязвимостями данного стандарта. Остановимся на них, чтобы подкрепить фактами вышеизложенное предположение.

Таблица 1

Система уровней доверия к беспроводным сетям

УД	Признак
1	Минимально возможный уровень безопасности
2	Усиление «старых» механизмов и алгоритмов новыми компонентами
3	Использование более надежного нового поколения механизмов и алгоритмов
4	Максимально возможный уровень безопасности
5	Введение дополнительных СЗИ, выходящих за рамки стандартов 802.11

К очевидные недостаткам **WEP** можно отнести практически полное отсутствие первичной аутентификации. Аутентификация с помощью общего ключа немногим лучше открытой аутентификации. При использовании сетей на основе WEP, все пользователи должны пользоваться одинаковой конфигурации статических ключей (СК), следовательно, получение ключей WEP не представляет собой большой сложности. Отсутствие защищенного метода распределения динамических ключей делает невозможным функционирование любой статической схемы, используемой в WEP.

Теперь рассмотрим немного более подробно стандарт **AES**, который был принят в качестве государственного стандарта шифрования США взамен утратившего свои позиции **DES.**

Можно отметить следующие преимущества, относящиеся к аспектам реализации данного алгоритма:

- Алгоритм шифрования полностью "самоподдерживаемый". Он не использует других криптографических компонентов.
- Алгоритм не основывает свою безопасность или часть ее на неясностях или плохо понимаемых итерациях арифметических операций.
- Длины блоков от 192 до 256 бит позволяют создавать хэш-функции без коллизий, использующие **AES** в качестве функции сжатия. Длина блока 128 бит сегодня считается для этой цели недостаточной.
- Разработка позволяет специфицировать варианты длины блока и длины ключа в диапазоне от 128 до 256 бит с шагом в 32 бита.
- Хотя число раундов **AES** зафиксировано, в случае возникновения проблем с безопасностью он может модифицироваться и иметь число раундов в качестве параметра.

Недостатком же алгоритма можно считать лишь примененную в нем нетрадиционную схему – теоретически она может содержать скрытые уязвимости, обнаруживаемые только спустя достаточное количество времени после широкого использования данного алгоритма. Он появился совсем недавно и обладает хорошей криптостойкостью, а его симметрическая природа делает его достаточно быстрым. Таким образом, на сегодняшний день атаки на **AES** не увенчались успехом. Хотя недавно были открыты поразительные алгебраические особенности AES и родственных ему методов. Хотя до реальной атаки на AES еще очень далеко, однако теоретически добраться до нее можно

Использование в БС шифрования по средствам **AES** автоматически присваивает ей 3 либо 4 УД.

Все последующие криптографические критерии находятся в прямой зависимости от используемого стандарта шифрования (**WEP** или **AES**), поэтому, целесообразно все дальнейшие возможно варианты конфигурации сети рассматривать, отталкиваясь от этого.

При использовании **WEP** УД к сети не может превышать второго, это связано с его низкой криптостойкостью и наличием большого числа уязвимостей. При шифровании передаваемой информации по средствам **RC-4** используют длину ключа равную либо 40 либо 128 битам.

Самым незащищенным считается соединение, при установке которого используется **WEP-40**, так как подобные схемы использовали еще на заре развития беспроводных технологий, то при такой длине ключа возможен лишь один неизменяющийся ключ на протяжении всего сеанса связи (статистический). Также в то время еще никакой и речи не было о проверки целостности передаваемой информации. Таким образом при использовании **WEP-40** возможна только одна конфигурация сети, причем явно видно, что УД к ней будет минимальным, т.е. равным первому.

С развитием стандарта 802.11 разработчики стали искать пути увеличения информационной безопасности сети, в связи с этим было введено использование более длинного ключа в 128 бит (**WEP-128**). При его использовании стало возможным применение динамических ключей (ДК). Также было внедрено использование протокола **MIC** для проверки целостности (ПЦ) сообщений.

Эти варианты являются однозначно более защищенным и ОО, в которых реализованы подобные механизмы защиты, уже можно отнести ко второму УД.

Но здесь хотелось бы отметить тот факт, что хотя с появлением **WEP-128** взамен **WEP-40** уровень безопасности возрос, в то же время использование статистического ключа без проверки целостности сообщений не дает нам полной уверенности, что данная сеть может принадлежать к УД-2, поэтому данная конфигурация используемых СЗИ относится также к УД-1 (табл. 2).

Таблица 2

Ранжирование совокупностей криптографических механизмов защиты при использовании алгоритма WEP

Ключи	Проверка целостности	WEP-40	WEP-128
Статистический ключ	Есть проверка целостности		2
	Нет проверки целостности	1	1
Динамический ключ	Есть проверка целостности		2
	Нет проверки целостности		2

Теперь в свою очередь рассмотрим стандарт шифрования **AES**. Он оперирует длиной ключа 128, 192 или 256 бит – название стандарта соответственно **AES-128**, **AES-192** либо **AES-256**.

При шифровании информации в сети по средствам **AES** мы имеем 12 возможных вариантов реализации СЗИ в БС.

При использовании **AES-256** сеть «автоматически» можно отнести к четвертом УД, так как этот алгоритм является на сегодняшний день наиболее криптостойким из тех, которые применяются в БС. Использование же **AES-128** либо **AES-192** относит исследуемый ОО на третий либо четвертый уровни соответственно, за исключением тех случаев, когда ключ на протяжении сеанса связи остается неизменным и отсутствует проверка целостности сообщений (**CCMP**). В таком случае ОО можно отнести только либо на второй либо на третий уровни соответственно (табл. 3).

Теперь перейдем ко второй группе – механизмам защиты при аутентификации.

Открытая аутентификация не позволяет точке радиодоступа определить, является ли абонент легитимным или нет. Это становится серьезной брешью в системе безопасности в том случае, если в беспроводной ЛВС не используется шифрование WEP. В итоге получаем, что при реализации в сети только аутентификации с открытым ключом УД к ней не может быть больше первого.

Таблица 3

Ранжирование совокупностей криптографических механизмов защиты при использовании алгоритма AES

Ключи	Проверка целостности	AES-128	AES-192	AES-256
Статистический ключ	Есть проверка целостности	3	4	4
	Нет проверки целостности	2	3	4
Динамический ключ	Есть проверка целостности	3	4	4
	Нет проверки целостности	3	4	4

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Она требует настройки у абонента статического ключа шифрования WEP.

Подобная методика аутентификации не может значительно увеличить защищенность беспроводного соединения, поэтому УД тоже будет равен первому, как и в случае с аутентификацией по открытому ключу.

Следующим шагом для усиления механизмов аутентификации в беспроводной сети стало внедрение протокола **EAP**. Различные производители создали свои реализации протокола EAP для обеспечения безопасности беспроводных сетей. Сразу хотелось бы отметить, что при использовании протокола **EAP** в сети всегда используется сервер аутентификации.

EAP-MD5 подтверждает подлинность пользователя путем проверки пароля, являясь процедурой односторонней аутентификации саппликанта сервером аутентификации, основанной на применении хеш-суммы **MD5** имени пользователя и пароля как подтверждения для сервера **RADIUS**. Вопрос использования шифрования трафика отдан на откуп администратору сети. Данный метод не поддерживает ни управления ключами, ни создания динамических ключей. Слабость EAP-MD5 заключается в отсутствии обязательного использования шифрования. По сравнению с предыдущими механизмами применение данного протокола увеличивает эффективность СЗИ и соответственно УД уже будет равен второму.

Протокол «легковесный EAP» (Lightweight EAP, LEAP), который создала компания Cisco, предусматривает не только шифрование данных, но и ротацию ключей. LEAP не требует наличия ключей у клиента, поскольку они безопасно пересылаются после того, как пользователь прошел аутентификацию. Это позволяет пользователям легко подключаться к сети, используя учетную запись и пароль.

Ранние реализации LEAP обеспечивали только одностороннюю аутентификацию пользователей. Позднее Cisco добавила возможность взаимной аутентификации (ВА). Однако выяснилось, что протокол LEAP уязвим к атакам по словарю. LEAP безопасен в той мере, насколько стоек пароль к попыткам подбора. В связи с выявленными уязвимостями УД к сети при реализации **LEAP** также не может превышать второго уровня.

Более сильный вариант реализации EAP — **EAP**-TLS, который использует предустановленные цифровые сертификаты (ЦС) X.509 на клиенте и сервере, был разработан компанией Microsoft. Этот метод обеспечивает взаимную аутентификацию и полагается не только на пароль пользователя, но также поддерживает ротацию и динамическое распределение ключей. Неудобство EAP-TLS заключается в необходимости установки сертификата на каждом клиенте, что может оказаться достаточно трудоемкой и дорогостоящей операцией. К тому же этот метод непрактично использовать в сети, где наблюдается частая смена сотрудников. Использование цифровых сертификатов сразу дает нам возможность причислить сети, где используется протокол **EAP-TLS** к третьему УД.

Производители беспроводных сетей продвигают решения упрощения процедуры подключения к беспроводным сетям авторизированных пользователей. Эта идея вполне осуществима, если включить LEAP и раздать имена пользователей и пароли. Но если возникает необходимость использования цифрового сертификата или ввода длинного WEP-ключа, процесс может стать утомительным.

Компании Microsoft, Cisco и RSA совместными усилиями разработали новый протокол — PEAP, объединивший простоту использования LEAP и безопасность EAP-TLS. PEAP использует сертификат, установленный на сервере, и аутентификацию по паролю для клиентов.

Tunneled TLS (TTLS) – EAP, разработанный компаниями Funk Software и Certicom и расширяющий возможности EAP-**TLS. EAP**-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между сапликантом и сервером аутентификации. В результате дальнейший процесс может производиться с помощью других протоколов аутентификации, например таких, как: PAP, CHAP, MS-CHAP или MS-CHAP-V2. Сильной стороной этого протокола является простота применения и довольно высокий уровень обеспечиваемой безопасности.

Применение этих протоколов дает возможность присвоить сети 3 либо 4 УД соответственно. Но отдельно бы хотелось оговорить вариант, когда используется протокол **PEAP** с взаимной аутентификацией и цифровыми сертификатами. Подобная совокупность СЗИ является довольно-таки стойкой и ее в полной мере можно отнести к 4 УД (табл. 4).

Таблица 4

Ранжирование совокупностей механизмов защиты на этапе аутентификации

№	Конфигурация	УД
1	Аутентификация с открытым ключом	1
2	Аутентификация с общим ключом	1
3	EAP-MD5-ВА-ЦС	2
4	LEAP-ВА	2
5	LEAP+ВА	2
6	EAP-TLS-ВА+ЦС	3
7	EAP-TLS+ВА+ЦС	3
8	PEAP-ВА-ЦС	3
9	PEAP-ВА+ЦС	3
10	PEAP+ВА-ЦС	3
11	PEAP+ВА+ЦС	4
12	EAP-TTLS-ВА-ЦС	4
13	EAP-TTLS-ВА+ЦС	4
14	EAP-TTLS+ВА-ЦС	4
15	EAP-TTLS+ВА+ЦС	4

Выводы

В ходе проведенного исследования была построена система уровней доверия к беспроводной сети. Также был проведен анализ семейства стандартов 802.11 и в соответствии с критериями оценки защищенности БС выявлены описанные в нем механизмы защиты. В дальнейшем полученные совокупности механизмов были проранжированы по уровням доверия. Логическим итогом работы является следующая сводная табл. 5.

Таблица 5

Ранжирование механизмов защиты беспроводной сети по уровням доверия

УД	Группа	Совокупность механизмы защиты
1	Критографические	WEP-40
		WEP-128 + СК – ПЦ
	Аутентификации	Аутентификация с открытым ключом
		Аутенификация с общим ключом
2	Критографические	WEP-128 + СК + ПЦ
		WEP-128 + ДК – ПЦ
		WEP-128 + ДК+ ПЦ
		AES-128 + СК – ПЦ
	Аутентификации	EAP-MD5-ВА-ЦС
		LEAP-ВА
		LEAP+ВА
3	Критографические	AES-128 + СК + ПЦ
		AES-128 + ДК – ПЦ
		AES-128 + ДК + ПЦ
		AES-192 + СК – ПЦ
	Аутентификации	EAP-TLS-ВА+ЦС
		EAP-TLS+ВА+ЦС
		PEAP-ВА-ЦС
		PEAP-ВА+ЦС
		PEAP+ВА-ЦС
4	Критографические	AES-192 + СК + ПЦ
		AES-192 + ДК – ПЦ
		AES-192 + ДК + ПЦ
		AES-256 + СК – ПЦ
		AES-256 + СК + ПЦ
		AES-256 + ДК – ПЦ
		AES-256 + ДК + ПЦ
	Аутентификации	PEAP+ВА+ЦС
		EAP-TTLS-ВА-ЦС
		EAP-TTLS-ВА+ЦС
		EAP-TTLS+ВА-ЦС
		EAP-TTLS+ВА+ЦС

Полученные результаты значительно облегчат работу аудиторов в разрезе реализованной системы безопасности БС и упростят процесс ее дальнейшей сертификации в соответствии с необходимым классом защищенности.

Литература

1. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. – М.: Гостехкомиссия России, 2002.

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.). – Санкт-Петербург, 2007. – С. 76-80.

4. 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.). – Санкт-Петербург, 2009. – С. 31-33.

RANKING OF WIRELESS NETWORK'S PROTECTION MECHANISMS ON ASSURANCE LEVEL

I. Y. IVASHCHUK

Saint-Petersburg state university of information technologies, mechanics and optics

e-mail: irina.ivashchukNi@cit.ifmo.ru

The article considers the system of assurance levels to the wireless network, based on system of estimated assurance levels of Common Criteria. The analysis of protection mechanisms of similar networks according to estimation criteria of security and their subsequent ranking on assurance levels are carried out.

Key words: wireless network, assurance level, estimation criteria of security, protection mechanism.