УДК.681.5.015

Маракова И.И., Сыропятов А.А.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЛЕКСНЫХ СИСТЕМ СВЯЗИ

Возросшие требования к информационным технологиям в различных областях деятельности современного общества, а также расширение возможностей сетевого построения информационных систем и внедрения методов распределенной обработки данных за счет реализации беспроводного доступа к вычислительным средствам обусловили широкое распространение на практике комплексных (комбинированных) систем связи (КСС). При этом одной из основных проблем является обеспечение информационной безопасности на участках беспроводных технологий связи. Существует мнение, что беспроводные сети предназначены исключительно для передачи открытой информации. При этом, однако, теряется смысл построения комплексных систем связи. Таким образом, проблема обеспечения информационной безопасности комплексных систем связи, т.е. включающих в свой состав беспроводные инфраструктуры, является весьма актуальной, требующей разрешения, как на концептуальном уровне, так и на уровне конкретного технического решения.

Наиболее широкое применение КСС нашли в так называемых сферах критических приложений, к которым относится деятельность институтов государственной власти, финансовых структур, учебных заведениях и т.д. Не умаляя общности рассуждений, при исключительном многообразии основные составляющие структур КСС традиционны (рис.1).

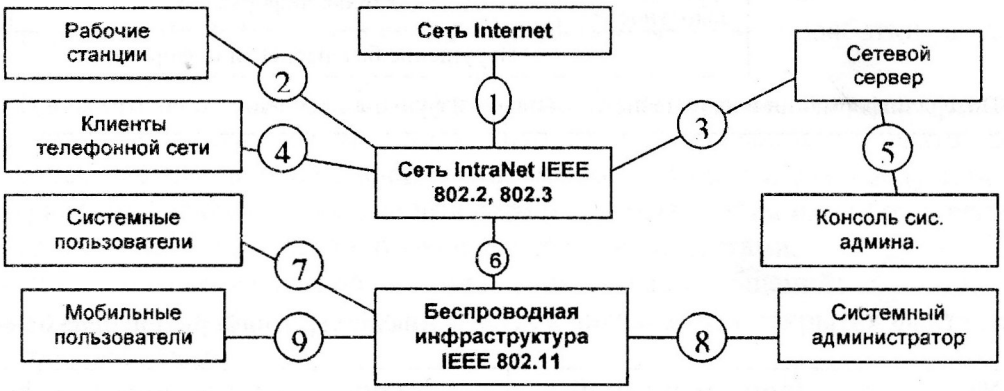

Рис. 1. Обобщенная структура комплексной системы связи

Выявление всех возможных каналов утечки конфиденциальной информации из системы связи является необходимым условием для определения путей и способов решения проблем ее защиты, а также конкретных мер по их реализации.

В табл. 2 показано, какие каналы взаимосвязи элементов КСС подвергаются угрозам информационной безопасности.

При решении задач, связанных с защитой информации КСС можно использовать подход, связанный с анализом уязвимостей эталонной модели взаимодействия открытых систем OSI (Open Systems Interconnection), рис. 2. В качестве обоснованных контрмер защиты от наиболее распространенных типовых сетевых атак (Port Scan, SYN-Flood, Denial of Service, TCP/IP Spoofing, Ping of Death, Man in the Middle), является использование специализированных программных средств. Которые, в свою очередь будут включать в себя: средства контроля защищенности, системы выявления атак, межсетевые экраны, средства шифрования и аутентификации, средства VPN, средства управления доступом и корпоративными ресурсами, средства анализа контекста, антивирусные средства.

Таблица 1.
Виды угроз, влияющие на безопасность информации и устойчивость функционирования КСС

<table>
<tr><td colspan="14">Угрозы</td></tr>
<tr><td colspan="9">1.Внешние</td><td colspan="5">2.Внутренние</td></tr>
<tr><td colspan="5" rowspan="2">1.1.Природные</td><td colspan="9">Искусственные</td></tr>
<tr><td colspan="9">1.2.Преднамеренные</td><td colspan="5">2.1.Непреднамеренные</td></tr>
<tr><td>Землятресения</td><td>Наводнения</td><td>Пожары</td><td>Ураганы</td><td>Электромагнитные бури</td><td>1.2.3. Электромагнитное излучение</td><td>1.2.2. Вирусы или вложенные дефекты</td><td colspan="5">1.2.1. Программные и аппаратно-технические средства</td><td>2.1.4. Потеря или утрата</td><td>2.1.3. Неправомерные действия</td><td>2.1.2. Ошибки в работе</td><td>2.1.1. Нарушение доступа законных пользователей</td></tr>
<tr><td colspan="6" rowspan="5"></td><td rowspan="2">Разру-шение</td><td rowspan="2">Искаже-ние</td><td colspan="3" rowspan="2">Раскрытие</td><td colspan="5" rowspan="3"></td><td colspan="2" rowspan="4">Нарушение доступности</td></tr>
<tr><td colspan="5">Подделка</td><td>Рассекречивание</td><td>Дешифрация</td><td>Декодирование</td><td>Перехват или кража</td></tr>
<tr><td colspan="10">Несанкционированный доступ</td></tr>
<tr><td colspan="2">Нарушение целостности</td><td colspan="8">Утечка информации</td></tr>
<tr><td colspan="12">Нарушение безопасности информации</td></tr>
<tr><td colspan="14">Потеря информации и нарушение устойчивости функционирования сетей передачи данных</td></tr>
</table>

Таблица 2.
Анализ угроз информационной безопасности КСС

№ взаимосвязи	Используемый протокол	Угрозы безопасности информации (табл. 1)
1	TCP/IP, UDP	1.1., 2.1., 1.2.1., 1.2.2.
2	IEEE 802.2, 802.3	1.1., 1.2., 2.1.
3	IEEE 802.2, 802.3	1.1., 1.2.3., 2.1.2., 2.1.4
4	Zmodem	1.1., 1.2.2., 2.1.2., 2.1.4.
5	-	1.1., 2.1.
6	IEEE 802.2, 802.3	1.1., 1.2.1., 2.1.
7	IEEE 802.11	2.1.2., 2.1.3
8	-	2.1.
9	IEEE 802.11	2.1.2., 2.1.3, 1.2.2.

Одним из основных каналов утечки информации в комплексных системах связи являются каналы радиосвязи, обеспечивающие привязку мобильных станций к базовым. Основным недостатком каналов радиосвязи является доступность передаваемых сигналов к

перехвату с целью прочтения, разрушения и модификации передаваемой информации. С другой стороны, надёжность системы определяется надёжностью самого слабого звена. Это позволяет делать вывод о уязвимости системы связи (рис.1), даже при применении новейшего оборудования и мощных криптоалгоритмов из-за лёгкости перехвата данных в среде передачи (радиоэфир) беспроводной связи. Если в Intranet, имеется возможность ограничить среду передачи зданием, в котором развёрнута беспроводная сеть, тем самым существенно усложнив доступ к физическому каналу передачи данных, то при соединении нескольких Intranet беспроводной связью, между собой или с Интернет, ничто не помешает получить доступ к физическому каналу передачи данных.

Источник		Приемник
Уровень 7, прикладной	⟷	Уровень 7, прикладной
Уровень 6, уровень представления	⟷	Уровень 6, уровень представления
Уровень 5, сеансовый	⟷	Уровень 5, сеансовый
Уровень 4, транспортный	⟷	Уровень 4, транспортный
Уровень 3, сетевой	⟷	Уровень 3, сетевой
Уровень 2, канальный	⟷	Уровень 2, канальный
Уровень 1, физический	⟷	Уровень 1, физический

Рис. 2. Модель OSI

Названная особенность канала связи обуславливает необходимость применения в интересах информационной безопасности специальных методов обработки и передачи информации.

Меры обеспечения безопасности информации в беспроводных системах связи имеют цель сокрытия содержания передаваемой информации (а по возможности и факта передачи) и недопущение навязывание ложной информации. Отнесем к таким мерам следующие:

аутентификация беспроводных станций сети и идентификация их оборудования – для обеспечения работы только с санкционированными корреспондентами;

шифрование – для сокрытия содержания передаваемых сообщений;

программная перестройка рабочих параметров сигнала для сокрытия факта передачи сообщения и его содержания

Безусловно, применение двухключевых (асимметричных) криптографических подходов позволит существенно улучшить практическую реализацию вышеперечисленных пунктов. Однако при этом для поставщика услуг возникает задача организации соответствующей инфраструктуры (табл. 3).

Механизмы безопасного распространения ключей и сертификатов между различными элементами КСС поддерживают выполнение следующих операций:

- распространение открытых ключей;
- эмиссия сертификата;
- отзыв сертификата;
- запрос сертификата;
- запрос списка отозванных сертификатов.

Таблица 3.

Элементы инфраструктуры КСС при использовании двухключевых криптографических методов

Орган регистрации	Орган регистрации обеспечивает глобальную координацию всех действий по управлению безопасностью, полное и целостностное представление конфигурации режима безопасности. В части управления ключами он регистрирует пользователей при получении ключей и сертификатов, собирает информацию, необходимую для подачи запросов на выдачу или отзыв сертификатов, и обеспечивает взаимодействие между органами сертификации.
Орган сертификации	Орган сертификации выпускает и отзывает сертификаты в соответствии с политикой сертификации. Является специализированным компонентом, работающим в режиме оффлайн, которым управляет оператор сертификации в соответствии с политикой сертификации.
Агент органа сертификации	Агент органа сертификации является точкой взаимодействия внешнего мира в оперативном режиме с органом сертификации.
Пользователь	Пользователем может быть обладатель сертификата, могущий использовать его для подписи цифровых документов, либо пользователь, запрашивающий подтверждение подлинности цифровых подписей и их цепочку сертификации через доверенные органы сертификации.
Реестр	В реестре хранятся и из него извлекаются по мере необходимости сертификаты и списки отзывов

Обмен запросами и сертификатами между пользователями, должен происходить в соответствии с разработанными пятнадцатью стандартами Public Key Cryptography Standards (PKCS).

Распространение открытых ключей и сертификатов может происходить в открытом виде. Пользователь при их получении вычисляет “отпечаток“ (односторонний хэш) и по другим каналам (телефон, электронная почта, т.д.) сравнивает с “отпечатком“, имеющимся у оператора. После получения аутентичных открытых ключей пользователь обращается за своим сертификатом, инициируя механизм эмиссии сертификата. Пользователь получает сертификат для представления его другой стороне, с которой будет вступать в безопасную связь. Эмиссия сертификата может быть организована т следующим образом :

1. Пользователь генерирует свою пару секретный ключ–открытый ключ.
2. Пользователь заполняет запрос на эмиссию сертификата, добавляет к нему парольную фразу, шифрует открытым ключом и отправляет в адрес Парольная фраза является дополнительным методом аутентификации при эмиссии сертификата и проверке действий пользователя по другим каналам.
3. Адресат зашифровывает запрос на эмиссию своим секретным ключом, затем автоматически или вручную с участием оператора одобряет или отклоняет запрос на эмиссию сертификата.
4. После одобрения подписывает запрос на эмиссию сертификата, используя свой секретный ключ, и возвращает пользователю полностью готовый сертификат.
5. Получив сертификат, пользователь сохраняет его для последующего предъявления по требованию.

Отзыв сертификата происходит в случае компрометации секретного ключа пользователя, или в иных случаях, когда дальнейшее использование сертификата невозможно или нежелательно. Для отзыва сертификата пользователь связывается с оператором и сообщает свою парольную фразу, которая известна обеим сторонам, поскольку была передан на этапе эмиссии сертификата. Убедившись в корректности парольной фразы, оператор следует процедуре по отзыву пользовательского сертификата, после чего отозванный сертификат будет опубликован в списке отозванных сертификатов. При отсутствии у пользователя возможности по хранению собственного сертификата он может использовать функцию запроса сертификата для его получения.

Архитектура двухключевых криптосистем допускает наличие иерархии, вследствие чего эмиссию сертификатов может производить как главный орган сертификации, так и подчиненный ему.. В инфраструктуре возможно существование дополнительных компонентов органов регистрации для обработки запросов на выдачу сертификатов и снижения нагрузки на сервисный центр в рамках системы, обрабатывающей значительное количество транзакций, либо для поддержания работоспособности инфраструктуры в случае временной недоступности сервисного центра.

Орган сертификации–центральная "точка доверия" в инфраструктуре двухключевой системы. Все субъекты организации доверяют сервисному центру как авторитетному источнику информации об аутентичности субъектов. Когда сервисный центр эмитирует сертификат, его цифровая подпись служит признаком того, что обладатель является частью инфраструктуры двухключевой системы.

В более сложных реализациях орган регистрации может выполнять операции по установлению подлинности личности пользователя и паролей для транзакций по управления сертификатами, размещению запросов на эмиссию в орган сертификации, а также другие разнообразные операции, напр. отзыв сертификатов и проч.

Орган регистрации обладает лишь полномочиями по приёму запросов эмиссии и передаче их органу сертификации. Орган регистрации не имеет права эмиссии сертификатов или публикации реестра отозванных сертификатов–за эти функции также отвечает орган сертификации .

Порядок взаимодействия может быть следующий.

Шаг 1. Субъект представляет запрос на эмиссию сертификата в орган регистрации.

Шаг 2. Орган регистрации дополняет запрос специфической информацией, запрос одобряется в соответствии с политикой организации и передаётся в орган сертификации .

Шаг 3.Орган сертификации подписывает сертификат и возвращает его субъекту.

Таким образом, простейшая инфрастуктура двухключевой криптосистемы может состоять из одного органа сертификации, объединяющего функциональность регистрации и сервера, обслуживающего функции центра распространения списков отозванных сертификатов. Подобная простейшая инфраструктура имеет ограниченные возможности по масштабированию, не обладает отказоустойчивостью и сложна в управлении в рамках организации с множеством самостоятельных административных единиц (подразделений). К решению этих проблем традиционно подходят путём распределения инфраструктуры внутри организации по географическому и/или функциональному признакам.

На крупном предприятии, подразделения которого нуждаются в чётком контроле за безопасностью на основе "личности" субъекта, может быть развёрнута иерархическая инфраструктура, состоящая из нескольких органов сертификации и аутентификации. В этом случае пользователю А будет эмитирован сертификат органом регистрации в соответствующем подразделении. При установлении защищённой связи с пользователем В, сертификат которого эмитирован органом сертификации В в рамках той же инфраструктуры, пользователь А проверит, подписывает ли его сертификационный центр сертификаты других центров. Если нет, то пользователь переходит на следующий уровень иерархии до тех пор,

пока не будет найден общий сертификат для обеих ветвей системы, вплоть то главного органа сертификации

После того как субъектам эмитированы сертификаты, они готовы для вступления в безопасную связь друг с другом. В большинстве случаев участники обмена вначале контактируют друг с другом посредством протокола прикладного уровня, напр. ISAKMP для IPSec или HTTP для SSL. В конце концов участники обмениваются своими сертификатами для взаимной аутентификации.

Субъекты проводят проверку сертификатов на предмет того, что:

- Срок действия представленного сертификата не истёк;
- Орган сертификации, подписавший сертификат, является частью соответствующей инфраструктуры системы;
- Сертификат отсутствует в реестре отозванных сертификатов.

Если сертификат соответствует всем перечисленным критериям годности, субъекты могут использовать открытые ключи. Все данные шифруются открытым ключом получателя, и расшифровываются на принимающей стороне секретным ключом. Разумно использовать периодическую смену ключей по прошествию наперёд заданного интервала времени или по завершению передачи определённого интервала времени.

Аутентификация в такой системе может происходить посредством организации протокола квитирования:

1. SSL-клиент устанавливает соединение с сервером и посылает запрос аутентификации.
2. Сервер посылает клиенту свой цифровой сертификат.
3. Клиент проверяет действительность сертификата и его цифровую подпись.
4. Сервер запрашивает аутентификацию клиента.
5. Клиент посылает серверу свой цифровой сертификат.
6. Сервер проверяет действительность сертификата клиента и его цифровую подпись.
7. Сервер и клиент согласуют алгоритмы шифрования и контроля целостности сообщения.

После этого происходит обмен пользовательскими данными через шифрованный туннель посредством протокола обмена данными.

Описанный метод аутентификации опирается на архитектуру 802.1x/EAP, подразумевающую наличие следующих компонентов: клиента (компонент операционной системы абонентского оборудования), аутентификатора (точка радиодоступа) и сервера аутентификации (RADIUS (Remote Authentication Dial-In User Service) сервер). Клиент и RADIUS-сервер должны поддерживать метод аутентификации EAP-TLS. Точка радиодоступа должна поддерживать процесс аутентификации в рамках 802.1x/EAP, хотя может и не знать деталей конкретного метода аутентификации.

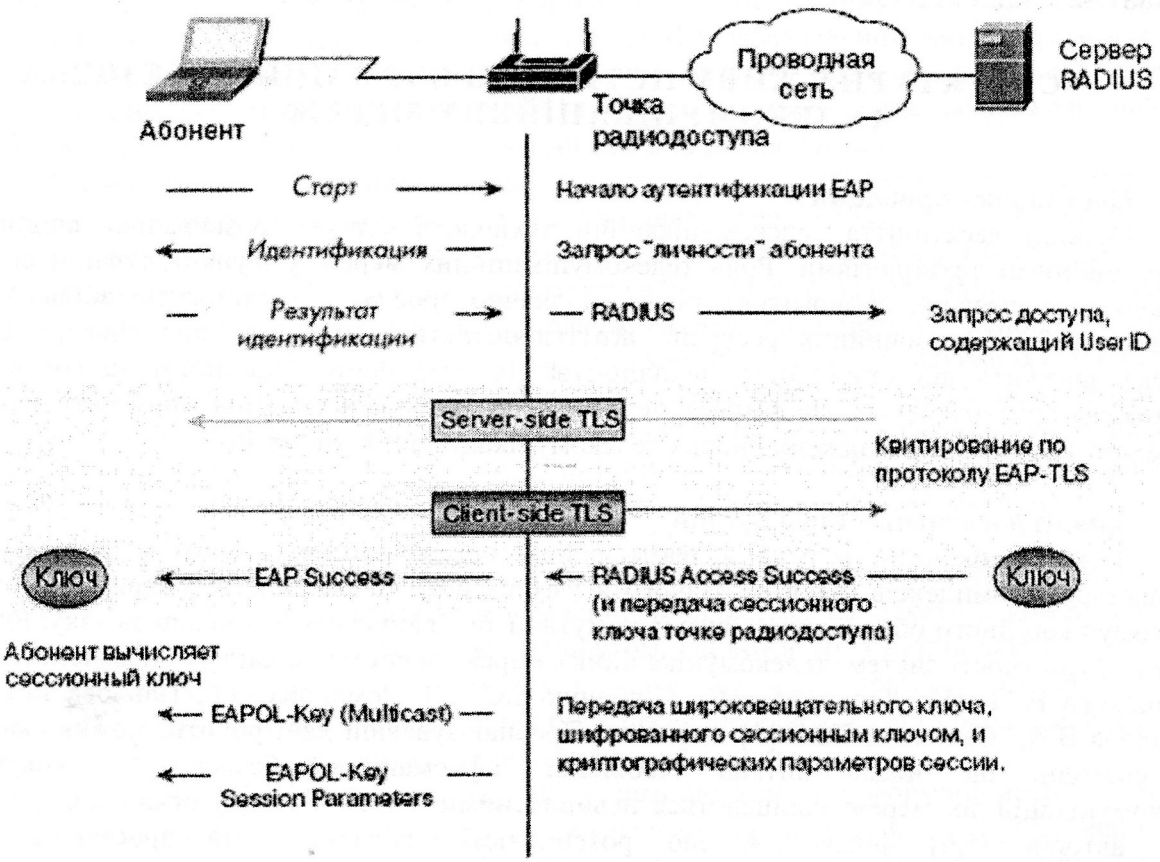

Рис. 3. Структура процедуры аутентификации

Таким образом, если среди основных ограничений обеспечения информационной безопасности беспроводных систем КСС выделить физическую среду передачи, оборудование и протоколы передачи данных, то последний фактор не является критическим, как было показано.

Повышение безопасности КСС возможно также не при помощи усложнения доступа к самим данным, а на основе отслеживания и последующего привлечения к ответственности злоумышленника, путём добавления по некоторому алгоритму в передаваемые данные особых меток, позволяющих в последствии наказать нарушителя. Однако, данное направление будет рассмотрено в отдельной публикации

Список литературы

1. Закон України «Про Захист інформації в автоматизованих системах» від 05.07.94 // Відомості Верховної Ради України.— № 31— 1994.— С. 286.

2. . *Schneir B.* Applied Cryptography. Protocols, Algorithms and Source Code in C. N.Y.: J.Wiley&Sons. — 1993. — 619 p.

Поступила 11.09.2006