ВОПРОСЫ ПРИМЕНЕНИЯ ИДЕНТИФИКАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ДОСТУПЕ К РЕСУРСАМ СИСТЕМ МНОГОПРОГРАММНОГО ВЕЩАНИЯ

Зелевич Е.П., Дорохин В.И.
Московский технический университет связи и информатики
111024, Россия, Москва, Авиамоторная, 8а

Реферат. Рассмотрены особенности применения идентификаторов для доступа к ресурсам систем многопрограммного телерадиовещания. Особое внимание уделено защите идентификаторов от несанкционированного доступа к хранящимся в них секретным алгоритмам и ключевой базе.

Обмен данными между терминалом и смарт-картой происходит через канал I/O.

Перед выполнением процедуры защиты данных обе связывающиеся стороны должны согласовать используемые криптографический алгоритм и секретный ключ. При расшифровке информации секретного ключа вся система защиты сообщений превратилась бы в вычисление дополнительной контрольной суммы, снижающей скорость передачи информации.

Требования обеспечения критерия прозрачности по отношению к командам и к двум принципиально различным протоколам информационного обмена привели к созданию гибкого, достаточно сложного метода защиты сообщений, стандартизированного ISO/IEC 7816-4. Он основан на вложении всех пользовательских данных в TLV-кодированные объекты.

Можно выделить три различных типа таких объектов:

- для открытого текста, содержащие данные в открытом тексте (например, секция данных APDU);
- для механизмов защиты, содержащих выходы механизмов защиты (например, MAC);
- для дополнительных функций, содержащих данные управления для защиты сообщений (например, метод дополнения незначащей информацией).

Байт класса применяется для индикации наличия процедуры защиты по ISO/IEC 7816-4.

Объекты данных открытого текста. По стандарту данные, не кодированные как BER-TLV, должны быть вложены в объекты данных. Для указания включения объекта данных в вычисление криптографической контрольной суммы существуют различные идентификационные символы.

Объекты данных для механизмов защиты. Объекты данных, используемые в механизмах защиты, подразделяются на используемые для опознавания и конфиденциальности. Опознавание касается объектов данных, связанных с криптографическими контрольными суммами и цифровыми подписями. Кодирование данных и идентификация, необходимые для обеспечения защиты сообщений, проходят под заголовком конфиденциальности ID.

Объекты данных для дополнительных функций используются для определения общих условий во время защиты сообщений. Обе стороны информационного обмена используют их для обмена данными об используемых криптографическом алгоритме, ключах и другой информации. На практике объекты данных используются редко, так как все условия защиты сообщений задаются неявно и их не надо определять во время информационного обмена.

Используя варианты, предлагаемые процедурой защиты сообщений, стандартизированной ISO/IEC 7816-4, рассмотрим две фундаментальные процедуры.

Процедура опознавания защищает пользовательские данные, т.е. APDU, с помощью криптографической контрольной суммы (CCS, MAC) от манипуляций во время сессии информационного обмена. В противоположность этому, комбинированная процедура используется для полного кодирования пользовательских данных с тем, чтобы атакующий не мог воспользоваться данными, содержащимися в передаваемых командах и ответах. Счётчик последовательностей сеансов передачи работает только в комбинации с одной из этих двух процедур. Исходным значением счетчика является случайное число, увеличивающееся после прихода и получения каждой команды и с каждым ответом. Это позволяет обеим сторонам обнаружить утерянную или искусственно введённую информацию. При совместном использовании с комбинированной процедурой счётчик последовательностей передачи может также обеспечить режим работы, при котором аналогичные APDU отличаются одна от другой. Такая процедура известна как “разнесение данных”.

Процедура опознавания гарантирует передачу подлинного информационного блока APDU. Получатель данных APDU может определить, были ли они изменены во время информационного обмена. Это делает невозможным для атакующего изменение данных APDU незаметно для получателя.

Реализация этой процедуры индицируется битом в байте класса таким образом, чтобы получатель мог проверить поступающий информационный блок APDU на подлинность. Информация APDU передаётся открыто и не кодируется, т.е. передаваемые данные могут быть приняты и оценены атакующим при возможности подключения к каналу связи.

Для вычисления криптографической контрольной суммы может использоваться любой алгоритм кодирования. По практическим соображениям, как правило, используется алгоритм DEA с блоком фиксированной длины 8 байт. Поэтому объекты индивидуальных данных должны быть кратны 8 байтам, что обеспечивается путём дополнения незначащей информацией. Объекты данных, информация которых кратна 8 байтам, также расширяются на один блок. После этого вычисляется CCS (Cryptographic Check Sum,

Криптографическая Контрольная Сумма) APDU с помощью алгоритма DES в режиме CBC. Полученная 8-байтная контрольная сумма, за исключением четырех наименее значащих байтов, объединяется с APDU как TLV-кодированный объект данных с исключением четырёх наименее значащих байтов. Все дополняющие байты после вычисления контрольной суммы удаляются. Переформатированный блок APDU после вышеописанной процедуры посылается через интерфейс к получателю. Эта процедура незначительно снижает скорость передачи. Исходный формат данных APDU трансформируется в TLV-кодированные данные с дополнением объектов данных до кратности 8 бит, затем вычисляется CCS. Данные информационного блока APDU дополняются TLV-кодированным объектом, содержащим CCS, с дополнением объектов данных до кратности 8 бит.

Объекты данных для структур управления могут однозначно индицировать, какие алгоритм и метод дополнения незначащей информацией использовались. Для простоты примем, что смарт-карте и терминалу в неявном виде известны параметры используемой системы защиты данных.

Когда защищённый блок данных APDU достигает получателя, тот вновь расширяет его до объёма, кратного 8 байтам, и, в свою очередь, вычисляет MAC APDU. Сравнивая вычисленные значения с принятым MAC, вычисленным отправителем, получатель может определить, модифицировалась ли информация APDU в процессе сеанса связи.

Обязательным условием для вычисления криптографической контрольной суммы является наличие секретного ключа DEA у обоих участников сеанса связи.

Дополнительные меры, необходимые для передачи и приёма защищенных APDU, снижают эффективную скорость передачи. При этом допустимо двукратное снижение скорости передачи основной информации.

Литература

1. Зверев Б.В., Зелевич Е.П. Анализ тенденций развития технологий смарт-карт. – М., Вестник связи, 2004.- № 8.- С.66-70.

2. Зелевич Е.П., Пластиковые карты в связи.- М.: Радио и связь, 2004.- 288с.