случаях. При этом изображение гражданина вообще практически не используется и необходимо лишь для обеспечения пропуска в случае отключения **СКУД**. И тогда изображение гражданина не несет самостоятельной идентифицирующей информации (т. е. опять не является биометрическими ПДн), а используется в комплексе идентифицирующих факторов.

3-й вариант может быть вообще без фото, но с использованием, например, дактилоскопической или иной биометрической идентификации: посетитель прикладывает к считывающему устройству палец (руку, глаз, др.) и на основании считанной и имеющейся в базе информации СКУД идентифицирует субъекта и пропускает/не пропускает посетителя. В этом случае мы имеем биометрическую систему идентификации.

Таким образом, такие простейшие данные, определяющие личность человека, как ФИО и фотография, — информация для точной идентификации личности, и это наиболее часто используемая информация в каждом организационном субъекте, хранимая в базах данных и наглядно представленная на пропуске на объект. Соответственно, требования приказа ФСТЭК России от 5.02.2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» распространяются и на такие ИСПДн, как СКУД.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ворона В. А., Тихонов В. А.* Системы контроля и управления доступом. М.: Горячая линия — Телеком, 2010. — 272 с.
2. *Лукацкий А. В.* Защита персональных данных и решения Cisco. URL: http://www.orbitacom.ru/images/conf5doc/ 11_Lukatskii.pdf.

Д. В. Калашникова

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К СИСТЕМАМ ПЛАТЕЖЕЙ НА ОСНОВЕ БЕСКОНТАКТНЫХ КАРТ PAYPASS

Бесконтактные платежи на основе карт MasterCard PayPass — это новая альтернатива безналичного расчета, которая позволяет существенно сократить время, нужное для совершения покупки. Применение такой технологии оплаты полезно в местах, где необходимо быстрое обслуживание клиентов. В основе платежей PayPass лежит радиочастотная технология Near Field Communication ближнего радиуса действия, которая позволяет мгновенно обмениваться данными на расстоянии не более 10 см.

Существенным отличием бесконтактных карт является наличие встроенного бесконтактного чипа, который хранит и обрабатывает данные расчетного счета, а также антенны [1]. Два важных составляющих компонента карты используются для передачи данных по воздуху в считыватель терминала и обратно — от считывателя терминала к карте. Антенна подключается к чипу и, как правило, проходит вблизи периметра карты.

Несмотря на принципиальное отличие в процессе оплаты, для бесконтактной банковской карты наряду с известными угрозами безопасности, характерными для контактных магнитных и микропроцессорных карт, существуют специальные угрозы, связанные с использованием радиоканала для обмена данными. Ниже представлены основные угрозы безопасности бесконтактного радиочастотного интерфейса [2]:

- «подслушивание» информации;
- искажение данных;
- модификация данных;
- вставка данных.

По отношению к системам платежей на основе бесконтактных карт PayPass рассмотрим трехуровневую концепцию требований безопасности. Каждый из трех уровней включает свои требования.

Административный уровень

К административному уровню относятся действия общего характера, направленные на создание программы работ в области защиты бесконтактных платежей, а также принятие стандартов, регламентирующих работу в сфере безопасности бесконтактных карт.

Основное требование данного уровня: создание и поддержание политики безопасности бесконтактных платежей на основе карт PayPass.

Организационный уровень

Организационный уровень ориентирован на людей и организации, которые задействованы в обработке платежей на основе бесконтактных карт PayPass. Именно на них направлены требования данного уровня, которые детально описаны в стандарте безопасности данных индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard).

Пользовательский уровень

Этот уровень относится непосредственно к держателю карты, самой карте и взаимодействию терминала и карты. Требования данного уровня связаны с угрозами безопасности бесконтактных карт [3].

1) Безопасное хранение пользователем карты и данных карты.

2) Использование динамического или комбинированного метода аутентификации (DDA – Dynamic Data Authentication, CDA – Combined Data Authentication).

3) Использование различных кодов проверки подлинности карты CVC (Card Verification Code) для бесконтактной транзакции и с использованием магнитной полосы.

4) Использование отдельных диапазонов номеров карт, не поддерживающих операции без присутствия карты.

5) Использование различных номеров для PayPass чипа и магнитной полосы, которые относятся к одной карте.

6) Проверка кода подлинности карты CVC2 (Card Verification Code), пин-кода и некоторой секретной информации при интернет-платежах или платежах при заказе по телефону или почте.

7) В данных первой дорожки бесконтактной карты имя держателя карты указываться не должно.

8) Данные бесконтактного чипа должны отличаться от карт с магнитной полосой.

9) Использование защищенного канала передачи данных от карты к считывателю терминала.

10) Использование ограничений на размер транзакций.

11) Использование ограничений на количество неавторизованных транзакций.

12) Использование специального устройства, которое создает имитацию наличия большого числа радиочастотных RFID (Radio Frequency IDentification) устройств.

13) Хранение карты в металлическом футляре или непрозрачной для радиочастот упаковке.

14) Использование кнопки активации бесконтактного интерфейса.

Разработанные требования безопасности могут быть в дальнейшем использованы для проектирования системы защиты бесконтактных платежей, включающей основные технические

средства обработки защищаемой информации, и для разработки безопасных алгоритмов передачи данных от карты к ридеру терминала.

СПИСОК ЛИТЕРАТУРЫ:

1. MasterCard PayPass Mag Stripe Acquirer Implementation Requirements. Официальный сайт Mastercard PayPass. Version 1.0. October 2008. URL: http://www.paypass.com/documentation.html#.
2. Security in Near Field Communication (NFC): printed handout of Workshop on RFID / Ernst Haselsteiner, Klemens Breitfub. 06.07.2006. URL: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf.
3. MasterCard PayPass Security: largest community for sharing presentations. 2011. URL: http://www.slideshare.net/szalaydaniel/pay-pass-security-fact-sheet-2010-final.

С. Д. Кулик, И. А. Лукьянов

ЗАЩИТА .NET-СБОРОК ОТ ОБРАТНОЙ ИНЖЕНЕРИИ И ИНЪЕКЦИЙ КОДА С ПРИМЕНЕНИЕМ МЕТОДОВ КРИПТОГРАФИИ

При распространении различного рода систем достаточно остро встает проблема их защиты от обратной инженерии. Другими словами, от декомпиляции и дизассемблирования. Для программ, разработанных на платформе .NET или любой другой, использующей промежуточный код, выполнить эти операции несколько проще, чем для программ, компилируемых непосредственно в машинный код. Как правило, промежуточный код представляет собой ассемблер высокого уровня, не зависящий от архитектуры процессора, что в совокупности упрощает его анализ.

В большинстве случаев применяются подходы к защите от обратной инженерии трех типов: обфускация, статическое и динамическое шифрование. Перечисленные подходы обладают как достоинствами, так и недостатками, однако не обеспечивают полной защиты от декомпиляции.

Обфускация заключается в запутывании кода, например через присвоение классам, полям, методам и т. п. бессмысленных случайно сгенерированных имен, добавление логически незначимых команд, разложение математических операций, добавление условных переходов и т. д. Для платформы .NET разработано достаточно большое число обфускаторов, однако ни один из них не дает гарантированной сложности декомпиляции. Злоумышленники применяют программы-дезобфускаторы для преодоления этого типа защиты. Данные программы создаются путем анализа соответствующих обфускаторов и основаны на выполнении обратного преобразования (из обфусцированного кода в исходный).

Подходы, основанные на шифровании, подразумевают шифрацию сборок одним из криптографических алгоритмов и поставку в зашифрованном виде. Недостатком этих подходов является внесение дополнительной сложности в разрабатываемую программу.

При статическом шифровании расшифровка происходит один раз во время инициализации программы, после чего расшифрованный код выполняется. Данный подход достаточно прост в реализации, однако для его преодоления злоумышленнику достаточно снять дамп памяти выполняемого процесса, проанализировав который он может дизассемблировать расшифрованный код. Чтобы предотвратить такой вид вмешательства, применяют различные механизмы защиты памяти, выходящие за рамки рассмотрения данной работы.