УДК 004.087.5

А.И. Шемаров

ПРИМЕНЕНИЕ ГИБРИДНЫХ МЕТОДОВ ЗАЩИТЫ ОТ ПОДДЕЛКИ ИДЕНТИФИКАЦИОННЫХ УСТРОЙСТВ, ВЫПОЛНЕННЫХ НА БАЗЕ МИКРОКОНТРОЛЛЕРОВ

Дальнейшее развитие информационных технологий, и в частности технологий электронного правительства, предполагает широкое использование электронных идентификационных устройств. Выполнение множества операций, таких как электронные платежи, доступ к транспортным средствам, использование электронных замков, может быть выполнено с применением идентификационных устройств различного типа. Кроме наличия самой идентификационной карты, предназначенной для идентификации пользователя в системе электронного доступа, часто требуется ввод пароля или простого цифрового кода (pin-кода).

Большинство людей, особенно среднего и пожилого возраста, чей род деятельности напрямую не связан с информационными технологиями, не всегда представляют себе возможные опасности при использовании электронных идентификационных карт. Использование банковских платежных карт с магнитной полосой в ближайшем будущем станет нецелесообразным. В средствах массовой информации и специальной литературе регулярно появляется информация о разнообразных способах мошенничества, связанных с использованием таких карт. При массовом использовании банковских платежных карт постоянно приходится решать оптимизационную задачу между стоимостью карты и ее защищенностью. Обычно это приводит к ослаблению защиты вследствие стремления банка уменьшить стоимость карты массового использования. Считывание кодов, записанных на карте, с последующей их эмуляцией и получение кодов доступа, как правило, не вызывает значительных технических трудностей. С электронными замками дела обстоят еще проще, особенно при применении широко распространенных электронных идентификационных устройств простейших типов, например таких, как младшие модели электронных идентификационных ключей фирмы Dallas. Использование идентификационных карт на базе микроконтроллеров существенно усложняет задачу злоумышленников, но не защищает от использования инсайдерской информации для дезавуации алгоритмов работы идентификационных устройств такого типа.

Глобально проблема может быть решена с использованием гибридных методов защиты идентификационных устройств, использующих

иные средства, чем цифровой код, записанный в идентификационной карте и являющийся главной целью атаки злоумышленников. Это связано в первую очередь с доминированием цифровых технологий и математических криптографических алгоритмов. В качестве гибридной технологии целесообразно использовать объединение цифровых и аналоговых методов защиты информации.

Исторически использование цифрового кодирования и цифровых методов обработки сигналов вытеснило использование аналоговых методов благодаря своей точности, достоверности и повторяемости. Использование иных (аналоговых) методов кодирования данных обычно проигрывает цифровым методам кодирования и в настоящее время практически не применяется. Однако современное состояние электронных технологий позволяет работать с аналоговыми сигналами (генерировать и анализировать) любой степени точности. Стоимость таких систем незначительна, и обычно они могут быть выполнены в виде подсистем широко распространенных современных микроконтроллеров, выпускаемых массовыми тиражами.

Суть гибридного метода заключается в использовании дополнительного канала передачи кодированных аналоговых данных на базе физического интерфейса, применяемого для передачи цифрового кода идентификационной карты. При этом передача аналогового кодированного сообщения сопровождается нарушением стационарных вероятностных характеристик аналоговых сигналов интерфейса. Реально сгенерированный аналоговый сигнал несет цифровой код, интересующий злоумышленника, в пределах допустимых отклонений физических параметров для конкретного интерфейса. Этот код он и получает с помощью сканера. На артефакты и фантомы злоумышленник обычно не обращает внимание. Учитывая многообразие параметров физического сигнала и их вероятностные отклонения, такая задача становится весьма затруднительной. Гибридный метод позволяет отличить оригинальную идентификационную карту от ее эмуляции, выполненной с помощью специальных технических средств.

При распознавании идентификационной карты-эмулятора, например, банковский терминал может защитить счет клиента, сообщая злоумышленнику о минимальном количестве средств на нем. Получение терминалом сигнала о применении идентификационной карты-эмулятора должно вызвать ряд действий со стороны службы безопасности.

Метод может быть реализован путем идентификации с помощью различных физических параметров электрических и оптических интерфейсов. Использование физических параметров интерфейсов, применя-

емых для передачи кода идентификационной карты, позволяет получать дополнительные каналы для передачи данных. Отсутствие «физически нереализуемых» артефактов позволяет легко выявить идентификационную карту-эмулятор.

Сохранение секретности используемого физического параметра для создания дополнительного канала передачи данных и отсутствие явной реакции при распознавании идентификационной карты-эмулятора значительно осложняют подделку идентификационной карты.

При разработке алгоритмов, используемых идентификационными устройствами, появляется возможность разделения методов защиты между различными группами разработчиков и программистов.

УДК 004

В.А. Щекин, А.С. Кольцов, А.А. Загуменнов

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ НА УДАЛЕННОМ ОБЛАЧНОМ СЕРВЕРЕ

В современных условиях с каждым днем увеличивается количество видов информации и процессов, производимых с ней широким кругом лиц. Совершенствуются методы получения несанкционированного доступа. Таким образом, защита данных является одной из приоритетных задач при проектировании любой информационной системы. В большинстве случаев несанкционированный доступ заключается в удаленном управлении информационной системой, контроле за пользователем и получении его данных. В силовых и ведомственных структурах потеря такой информации повлечет за собой колоссальные проблемы, для устранения которых потребуются огромные силовые и материальные ресурсы.

При несанкционированном доступе лицо, вторгающееся в информационную среду пользователя, делает это так, что часто пользователь не в силах обнаружить вмешательство, а тем более его ликвидировать. Если информационной средой является удаленный облачный сервер, необходимо предпринимать разумные и эффективные средства обеспечения защиты информации. Для решения этой проблемы применяется система обнаружения вторжений, которая является программным или аппаратным средством, предназначенным для выявления фактов и предотвращения последствий доступа неавторизованных пользователей в