МЕТОДЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ ОТ АКТИВНЫХ АТАК

М.Л. Данилкович

Государственное предприятие "НИИ ТЗИ", Минск, Беларусь

В настоящее время основными областями применения интеллектуальных карт (смарт-карт) являются: финансы, безопасность, социальные программы, транспорт, применение цифровой подписи и электронные паспорта. В связи с широким внедрением технологий с использованием смарт-карт актуальным становится вопрос устойчивости интеллектуальных карт к атакам на их информационную безопасность.

Рассмотрим более детально активные атаки и методы защиты от них.

Активные атаки подразумевают различные специфические воздействия на смарт-карту с целью нарушения ее нормального функционирования, в результате чего она может давать

сбои в процессе своей работы. Такие наведенные криптоаналитиком ошибки в работе модуля шифрования смарт-карты могут предоставить ему существенно больше по сравнению с уже описанными методами информации, полезной для дальнейшего анализа. Независимо от вида воздействия на модуль шифрования, подобные атаки называются атаками на основе сбоев (fault attacks) [1].

Заставить смарт-карту работать некорректно можно множеством различных способов. Наиболее эффективными воздействиями являются [2]:

а) изменение напряжения питания, существенно превосходящее допустимые пределы (spike attack);

б) изменение тактовой частоты, выходящее за допустимые рамки (glitch attack);

в) высокоточное облучение с помощью лазера, источника ультрафиолетового или рентгеновского излучения (optical & radiation attacks);

г) высокоточное наведение электромагнитного поля или локальный нагрев определенной области смарт-карты (electromagnetic & heating attacks);

д) внесение изменений в конструкцию смарт-карты, например, нарушение определенных электрических контактов.

Кроме того, атаки на основе сбоев классифицируются также по тому признаку, насколько атакующий может контролировать следующие факторы [2]:

а) местоположение сбоя (например, конкретный бит обрабатываемых данных);

б) время возникновения сбоя (например, номер итерации алгоритма шифрования, при выполнении которого происходит сбой);

в) количество бит, подверженных сбою;

г) вид сбоя: инверсия значения бита или его сброс (в 0 или 1 в зависимости от технологических особенностей смарт-карты и вида воздействия).

Очевидно, что чем больший контроль над данными факторами атаки имеет криптоаналитик, тем более действенной является атака. Считается, что наибольший контроль перечисленных факторов атакующему дает наведение сбоев с помощью высокоточного облучения или электромагнитного поля.

К сожалению, какого-либо универсального средства защиты от описанных методов воздействия на смарт-карты не существует. Однако, существенно усложнить проведение атак на основе сбоев можно следующими способами [3]:

а) внедрение детекторов различных воздействий (например, детекторов изменения напряжения, частоты питания и/или синхронизации, освещенности и т.д.), которые, при обнаружении воздействия выполняли бы блокировку смарт-карты;

б) различного рода пассивное экранирование, устранение которого приводило бы к выходу из строя смарт-карты;

в) различные виды дублирования вычислений со сравнением результатов.

Подобные методы в свою очередь приводят к удорожанию устройств и/или снижению их быстродействия и должны выбираться с учетом рисков нарушения безопасности смарт-карт.

Литература

1. *Hagai B.-E.* Known Attacks Against Smartcards // http://discretix.com/PDF/Known%20Attacks%20Against%20Smartcards.pdf

2. *Панасенко С.В.* Атаки на алгоритмы шифрования. Часть2. http://www.cio-world.ru/bsolutions/e-safety/308455/ — 5 марта 2007.

3. *Дшхунян В.Л., Шаньгин В.Ф.* Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты // М.: ООО "Издательство АСТ": Издательство "НТ Пресс", 2004. 695 с.