СПОСОБЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ

М.Л. Данилкович

Интеллектуальные карты (смарт-карты) являются самым молодым и перспективным представителем многочисленного семейства идентификационных карт, широко используемых в разнообразных прикладных информационных системах. В связи с широким внедрением технологий с использованием смарт-карт актуальным становится вопрос устойчивости интеллектуальных карт к атакам на их информационную безопасность.

Различают два вида атак на интеллектуальные карты: пассивные (passive) атаки и активные (active) атаки.

Примерами пассивных атак могут служить атака по времени выполнения (timing attack) и атака по потребляемой мощности (SPA).

В качестве защиты от атак по времени выполнения можно использовать следующие методы: обеспечить выполнение модулем шифрования операций строго за одно и то же количество тактов процессора независимо от значений операндов и маскировать время выполнения операций. В качестве противодействия SPA предлагаются различные методы зашумления — аналогично атакам по времени выполнения.

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. Независимо от вида воздействия на модуль шифрования, подобные атаки называются атаками на основе сбоев (fault attacks).

Заставить смарт-карту работать некорректно можно множеством различных способов. Наиболее эффективными воздействиями являются: изменение напряжения питания (spike attack), изменение тактовой частоты (glitch attack), высокоточное облучение (optical & radiation attacks), высокоточное наведение электромагнитного поля или локальный нагрев определенной области смарт-карты (electromagnetic & heating attacks) и внесение изменений в конструкцию смарт-карты.

К сожалению, какого-либо универсального средства защиты от активных атак на смарт-карты не существует. Однако, существенно усложнить проведение атак на основе сбоев можно следующими способами: внедрение детекторов различных воздействий, использование различного рода пассивного экранирования и 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.