УДК 004.356.056.55

АКУСТИЧЕСКИЙ КРИПТОАНАЛИЗ

Дедюрин А.Б., студент группы ИТб-121,
Научный руководитель: Алексеева Г.А., старший преподаватель.

Кузбасский государственный технический университет
имени Т.Ф.Горбачева
г. Кемерово.

Актуальность защиты информации от утечки по акустическим, вибрационным, электромагнитным каналам несомненна и занимает важное место в вопросах обеспечения информационной безопасности. Злоумышленниками придумано уже множество методов получения информации по сторонним каналам утечки. Одним из вариантов воздействия по сторонним каналам можно считать акустический криптоанализ.

Акустический криптоанализ представляет собой тип пассивной атаки по сторонним каналам, который использует звуки, испускаемые компьютерами, или иными шифрующими устройствами. Современный акустический криптоанализ в основном фокусируется на звуках, производимых компьютерными клавиатурами, или внутренними компонентами компьютера.

Метод акустического криптоанализа компьютерных процессоров разработан и реализован большим коллективом израильских ученых из нескольких университетов страны. Три основных деятеля группы (в порядке возраста и известности) – это Ади Шамир (Adi Shamir, буква S в знаменитом шифре RSA) из Вейцмановского научного института, Эран Тромер (Eran Tromer) из Тель-Авивского университета и Даниэль Генкин (Daniel Genkin) из университета Технион.

Главным же итогом исследования можно считать следующий факт. Разработанная авторами атака примерно за час времени позволяет успешно вскрывать алгоритм шифрования – RSA с длиной ключа 4096 битов.

Особо следует подчеркнуть, что с технической точки зрения эта атака весьма проста в реализации, так что может быть проведена с помощью недорогой и общедоступной аппаратуры. По сути дела, секретный криптографический ключ вскрывается в результате прослушивания с помощью обычного

микрофона работы компьютерного процессора в тот период, когда он занят расшифровкой неких зашифрованных данных.

В ходе исследований было обнаружено, что операция шифрования RSA (пакета GnuPG) обладает характерным частотным спектром. Более того, спектр во многих случаях проявляет зависимость по ключу, то есть, различные ключи издают различные звуки.

В основе процесса извлечения ключа лежит атака на основе адаптивно подобранного шифротекста. Благодаря особенностям реализации алгоритма шифрования, в цикле алгоритма появляется серия нулей. Один проход по циклу выполняется слишком быстро для улавливания микрофоном. Но при повторении этого события в течение нескольких тысяч проходов утечка по акустическому каналу становится значительной, позволяя побитово получать информацию о ключе.

Тот же самый тип электрических компрометирующих данных от ЦПУ можно выделять далеко не только акустически, но и от многих других источников побочных утечек: от электророзетки в стене; от удаленных концов сетевого кабеля Ethernet или видеокабеля VGA.

Акустическое поле генерируется с помощью электромагнитных (закон Ампера) и электростатических сил (закон Лоренца) которые существуют в открытом пространстве. При наличии в конструкции ферромагнитных материалов дополнительно проявляется эффект магнитострикции, а при наличии керамических конденсаторов диэлектрики которых обладают пьезоэффектом — пьезоэлектрический эффект. Последние многократно увеличивают преобразование электромагнитного поля в акустическое.

Сила Ампера создаваемая импульсным током протекающим по свободным виткам катушек индуктивности (и токонесущим проводникам) побуждает их к вибрациям, которые многократно усиливаются при их (и окружающих их элементах) механическом резонансе. В компьютере таковыми являются индуктивности системы питания, ток через которые промодулирован током питающим процессор. Он так же усиливается если ферритовый сердечник такой катушки обладает эффектом магнитострикции.

Но основным источником акустического излучения в компьютерах (процессорах) являются SMD керамические конденсаторы, которые во множестве расположены на самом процессоре и материнской плате и включенные в цепь питания процессора. Они предназначены как раз для фильтрации напряжения питания от широкополосных помех генерируемых процессором в шинах питания.

Эти конденсаторы для получения их высокой емкости (0,1 — 100 мкФ) выполнены многослойными и из диэлектриков классов II и III имеют значительно более высокую диэлектрическую проницаемость и, следовательно, ёмкость. Они являются пьезоэлектриками, поэтому механическое воздействие на них производит напряжение, то есть они подвержены микрофонному эф-

фекту. И наоборот при подаче на них переменного напряжения они склонны к преобразованию его в вибрации и соответственно акустическую волну. И чем больше слоев (чем больше емкость) такого конденсатора, тем больше амплитуда акустической волны. На работе большинства источников питания эти эффекты не сказывается, за исключением случаев, когда рабочая частота находится в звуковом диапазоне.

Фильтруемое ими напряжение прикладывается к обкладкам многослойных керамических SMD конденсаторов, где переменная составляющая напряжения и создает акустическую волну.

Снизить мощность генерируемого акустического поля и, как следствие, снизить вероятность извлечения ключей шифрования можно:

- Программно, рандомизировать элементы алгоритма RSA.
- С помощью грамотного проектирования корпуса компьютера, с применением звукопоглощающих материалов.
- Добавление шума, добавлением случайных вычислений, параллельных работе алгоритма.
- Добавление устройств, генерирующих специфический шум, схожий с работой алгоритмов шифрования.

Исследования проводились в условиях, далеких от реальной жизни, не были изучены возможности появления резонансных явлений, а так же и другие недостатки в проведенном эксперименте. Но даже с учетом неоднозначности полученных результатов сам факт развития подобных технологий означает что угроза утечки информации по акустическим каналам существует, развивается и мы можем столкнуться с ней в ближайшем будущем. Поэтому необходимо создавать дополнительные средства защиты. Методы подобной защиты разрабатываются, как программные, так и технические, но на сегодняшний день большого распространения не имеют.

Список использованной литературы:

1. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis[Электронный ресурс] URL: http://cs.tau.ac.il/~tromer/acoustic/
2. GPGPU[Электронный ресурс] URL: https://www.pgpru.com/forum/kriptografija/akusticheskijjkriptoanaliztehnicheskijjkanalute?show_comments=1&p=1#Comment1899
3. Хабрахабр[Электронный ресурс] URL: https://habrahabr.ru/
4. Хорев А.А. Защита информаци от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436с.