Программный Темпест: скрытная передача данных с помощью электромагнитных излучений

Маркус Г. Кун и Росс Дж. Андерсон
(Компьютерная лаборатория университета Кембридж, Великобритания)

1. Введение

По крайней мере с начала 1960-х годов в военных организациях знают о том, что компьютеры порождают электромагнитные излучения, которые не только создают помехи для радиоприема, но также обеспечивают утечку информации об обрабатываемых данных. Обычно именуемое *компрометирующим излучением*, это явление стали называть также *Темпест*-излучением по кодовому названию секретной исследовательской программы правительства США. Электромагнитные утечки данных стали серьезной заботой при разработке чувствительных к сохранению тайны компьютерных приложений.

В своей книге "Ловец шпионов" [7] бывший ученый спецслужбы MI5 Питер Райт (Peter Wright) рассказывает о начале Темпест-атак на шифраппаратуру. В 1960 году Британия вела переговоры о присоединении к Европейскому экономическому сообществу, и премьер-министр беспокоился, что французский президент Де Голль заблокирует вхождение Англии. Поэтому он попросил разведывательное сообщество установить позицию Франции на переговорах. Разведка попыталась вскрыть французский дипломатический шифр, но без успеха. Однако, Райт и его ассистент Тони Сэйл (Tony Sale) обратили внимание, что шифрованный трафик нес слабый вторичный сигнал. Они сконструировали оборудование для восстановления этого сигнала. Оказалось, что это был открытый текст, который каким-то образом просачивался через шифратор.

Сегодня для защиты правительственных систем применяют дорогостоящее металлическое экранирование отдельных устройств, комнат, а иногда и зданий целиком [14]. Даже внутри экранированного помещения следуют принципу разделения на "красное/черное": "красное" оборудование, несущее секретные данные (например, компьютерные терминалы), должно быть отделено фильтрами и экранами от "черного" оборудования (такого, как, например, радиомодемы), обрабатывающего или передающего несекретную информацию. Оборудование, одновременно соединенное с "красными" и "черными" устройствами, такое как шифраппаратура или многоуровневые рабочие станции, требует особо тщательного тестирования. Американский стандарт NACSIM 5100A, формулирующий тестовые требования к Темпест-защищенному оборудованию, и его НАТОвский эквивалент AMSG 720B являются засекреченными документами [6]. В Германии держатся в секрете даже названия правительственных стандартов на компрометирующее излучение.

Поэтому можно только фантазировать об измерительных технологиях, применяемых в Темпест-тестах. Однако, данные в опубликованных патентах [12,13] дают основания полагать, что применяемый инструментарий на порядки более чувствителен, нежели при стандартных тестированиях на электромагнитную совместимость (EMC) и радиочастотную интерференцию (RFI). Некоторые тесты задействуют долговременные кросс-корреляционные измерения между сигналами, снятыми внутри изучаемой системы и шумовыми и искаженными сигналами, принятыми от внешних источников, включая не только антенны, но и линии питания, заземление, периферию и сетевые кабели.

Подходящими датчиками могут быть даже микрофоны, особенно при тестировании оборудования типа линейных принтеров. Усредняя корреляционные значения по миллионам образцов, можно выявлять даже очень слабые следы обрабатываемой информации в электрических, электромагнитных и даже акустических излучениях.

Аналогичную технику усреднения и корреляций можно использовать для атак и в том случае, когда сигнал является периодическим или в целом понята его структура. Контроллеры видеодисплеев периодически выдают на монитор содержимое буфера кадра и таким образом являются привлекательной мишенью атак, особенно когда видеосигнал усиливается до нескольких сотен вольт для катодно-лучевой трубки (КЛТ). Специальная закладка - программное обеспечение, которое атакующая сторона может имплантировать в систему, - способна также генерировать периодические или псевдопериодические сигналы, которые легко выявляются. Знание вида шрифтов, используемых в видеодисплеях и принтерах, позволяет на основе техники максимального правдоподобия получать более лучшее соотношение сигнал/шум для целых знаков, чем это возможно для отдельных пиксел знаков.

Похожую технику можно применять и при "прощупывании" ЦПУ, выполняющих известные алгоритмы. Даже если сигналы, порожденные отдельными инструкциями, затерялись в шуме, корреляционные методы позволяют выделить выполнение известного набора инструкций. В работе Бовенландера [8] описано, как для реализующей DES смарткарты криптографическая операция идентифицируется по потреблению питания, когда определенный паттерн повторяется шестнадцать раз. Известны также похожие атаки для случая, когда злоумышленник имеет возможность по потреблению питания выявлять намерение процессора произвести запись данных в ППЗУ. Например, можно ввести опробуемый PIN, по потреблению питания проследить, что он не подошел, и сделать перезагрузку перед тем, как счетчик попыток ввода обновит свое значение. Таким способом можно обходить порог опробований PIN.

Первая публикация о Темпест в открытой печати [1] появилась на шведском языке в 1983 году, но широкое внимание общественности к данной проблеме было привлечено статьей 1985 года [2], где Вим Ван Экк продемонстрировал на практике, что содержимое экрана дисплея можно восстанавливать на расстоянии с помощью дешевого непрофессионального оборудования - обычного телевизора, в котором генераторы синхроимпульсов заменены на управляемые вручную осцилляторы. Позднее его результаты были подтверждены М╠ллером, Бернштайном и Кольбергом, в работе которых обсуждаются также различные методы экранирования [5].

Смулдерсом показано, что часто можно перехватывать даже сигналы от экранированных кабелей RS-232 [4]. Соединительные кабели образуют резонансные цепи, состоящие из индуктивности кабеля и емкости между устройством и землей; эти цепи возбуждаются высокочастотными компонентами сигнала данных, и результирующие короткие ВЧ-колебания испускают электромагнитные волны.

Предполагают, что злоумышленник, вооружившись довольно простым радиооборудованием и встав возле банкомата, может регистрировать как сигналы от магнитной полоски, так и PIN-данные пользователей, поскольку считыватель карты и клавиатура как правило соединяются с ЦПУ по последовательным линиям. Похожая опасность возникает при взаимном обмене сигналами между параллельно идущими кабелями. Например, продемонстрировано восстановление сетевых данных от телефонной линии, причем телефонный кабель проходил рядом с кабелем компьютерной

сети всего на протяжении двух метров [15]. Еще одна опасность исходит от "активных" атак: злоумышленник, знающий резонансную частоту, скажем, кабеля клавиатуры персонального компьютера, может облучать его на этой частоте, а затем регистрировать коды нажатия клавиш в ретранслируемом резонансном сигнале благодаря вызванным ими изменениям импеданса [16].

Принимая во внимание то возбуждение, что породила публикация открытий Ван Экка [3], и те огромные затраты на экранирование, что характерны для дипломатической и военной областей, можно считать удивительным, что практически никаких дальнейших исследований о Темпест-атаках и соответствующей защите в исследовательской литературе не появилось. Однако, лабораторные радиоисследования - вещь дорогостоящая, а получать чисто теоретические результаты сложно ввиду отсутствия опубликованных данных об излучениях современной аппаратуры.

Коммерческое использование Темпест-технологий - дело малорентабельное. Британским и германским правительствами делались попытки заинтересовать коммерческие фирмы темой Темпест, когда искали применение разработкам, накопленным за годы Холодной войны. Но к успеху это не привело: Темпест-экранированные ПК и рабочие станции в несколько раз дороже стандартных моделей и, кроме того, их продажа на экспорт как правило строго контролируется. Поэтому нет ничего удивительного в том, что экранированное оборудование практически никогда не используется за пределами дипломатического и военного сообществ.

Но эта ситуация может измениться. В данной статье мы описываем несколько несложных экспериментов, проведенных нами с Темпест-приемником и дешевым радиоаппаратом. На эту работу авторов подвигло любопытство и она никем не финансировалась. У нас не было доступа к дорогостоящему оборудованию, которое можно найти в радиоразведывательных спецслужбах; даже наш устаревший Темпест-приемник ненамного сложнее обычного модифицированного телевизора. Таким образом, наши эксперименты демонстрируют, какого рода атаки являются практичными в 1998 году для творчески мыслящего любителя-перехватчика. Кроме того, нами разработаны некоторые чрезвычайно дешевые защитные меры.

2. Коротковолновые аудиопередачи

Если мы хотим внедрить компьютерный вирус в банк или службу сертификации, где вирус будет извлекать ключевой материал и передавать его нам по импровизированному радиоканалу, то важным критерием конструкции является стоимость приемника. Сложное оборудование, типа фазированных антенн, может применяться спецслужбами, но пока оно не стало общедоступным. Поэтому наиболее естественным решением для любительского Темпест-прибора стал радиоприемник бытовой магнитолы ценой около 100 долларов.

Для того, чтобы заставить видеомонитор компьютера вырабатывать аудиосигналы для нашего радиоприемника, нам пришлось разработать экран, вызывающий такой ток видеолуча, который аппроксимирует передачу радиосигнала. Если последний имеет несущую частоту f_c, то звуковой тон с частотой f_t может быть представлен как

$$s(t) = A \cdot \sin(2\pi f_c t) \cdot [1 - B \cdot \sin(2\pi f_t t)]$$

Временные показатели системы цифрового видеодисплея прежде всего характеризуются тактовой частотой пиксел f_p, которая обратна времени, за которое электронный луч в КЛТ

проходит от центра одного пиксела до центра его правого соседа. Тактовая частота пиксел - это целое кратное частот горизонтального и вертикального отклонения, то есть скорости $f_h = f_p/x_t$, с которой рисуются строки, и скорости $f_v = f_p/y_t$, с которой на экране выстраиваются полные кадры. Здесь x_t и y_t - это суммарные ширина и высота поля пиксел, с которым мы имеем дело, если электронному лучу не требуется время для перескока к началу строки или кадра. Однако, высвечиваемый на экране образ имеет лишь x_d пиксел в ширину и y_d пиксел в высоту, поскольку время, остающееся для остальных ($x_t y_t - x_d y_d$) виртуальных пиксел используется для возврата электронного луча к противоположной стороне экрана.

Программа-закладка может считывать эти параметры непосредственно из чипа видеоконтроллера либо отыскивать их в файлах конфигурации. Например в Linux-станции, с которой работали авторы, строка вида

```
ModeLine "1152x900"  95  1152 1152 1192 1472 900 900 931 939
```

в конфигурационном файле сервера X Window System под названием /usr/lib/X11/XF86Config обозначает, что в данной системе используются параметры f_p = 0.95 МГц, x_d = 1152, y_d = 900, x_t = 1472 и y_t = 939. Откуда устанавливается, что частоты отклонения f_h = 64.5 КГц и f_v = 68.7 Гц.

Если мы зададим, что t = 0 - это момент времени, когда луч находится в центре пиксела верхнего левого угла (x = 0 , y = 0), тогда электронный луч будет в центре пиксела (x, y) в момент времени

$$t = \frac{x}{f_p} + \frac{y}{f_h} + \frac{n}{f_v},$$

для всех 0 <= $x < x_d$, 0 <= $y < y_d$, n=0,1,2,3,... . Используя данную формулу со счетчиком кадров n = 0, мы можем теперь вычислить время t для каждого пиксела (x, y) и выставить этот пиксел в 8-битное значение $\lfloor 128 + s(t) \rfloor$ по шкале оттенков серого с амплитудами A = 64 и B = 1. На рисунке 1 представлены экранные изображения, генерируемые таким образом для передачи звуковых тонов методом амплитудной модуляции (AM).

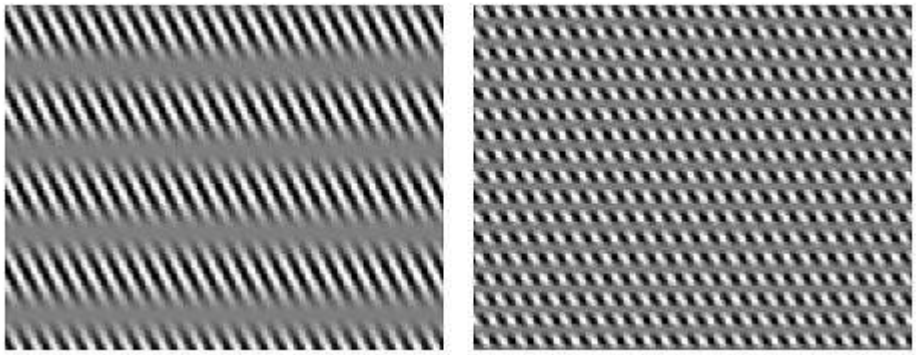

Рисунок 1. Примеры экранов, вызывающих излучение монитором тонов ft =300 Гц (слева) и 1200Гц (справа) на несущей частоте fc = 2.0 МГц с амплитудной модуляцией.

В принципе, нет необходимости заполнять весь экран данным паттерном, но энергия передаваемого сигнала пропорциональна количеству пиксел, его высвечивающих. В

идеальном случае как f_c, так и f_t должны быть целыми кратными частоты f_v , чтобы избежать фазовых скачков при переходе от одного кадра к другому.

У нас не возникло никаких проблем при приеме дешевым переносным радиоаппаратом тестовой мелодии, передаваемой нашим ПК. Система работала повсюду в нашей лаборатории и в соседних комнатах, в то время как прием на более значительных расстояниях был хорошим лишь когда приемная антенна располагалась близко к линиям электропитания. Насколько можно судить по задействованным длинам волн, линии питания распространяют больше энергии радиочастот, нежели это делают паразитные антенны в ПК. Мы думаем, что если бы мы подсоединили радио через подходящий ВЧ-мост непосредственно к нужной фазе сети питания, то смогли бы принимать сигнал и из соседних зданий. Кроме того, в нашем простеньком радиоприемнике была лишь обычная неподстраиваемая дипольная антенна, так что с более серьезной антенной можно ожидать и вполне приемлемую регистрацию на расстоянии в несколько сотен метров.

Для такого рода атак наилучшей представляется коротковолновая радиополоса в диапазоне 1-30 МГц. Уровень приема существенно зависит от того, насколько зашумлен радиоспектр поблизости от несущей частоты f_c, так что ее надо выбирать в стороне от радиовещательных станций.

В случае типичной недорогой атаки перехватчик размещает радиоприемник с магнитофоном поблизости от цели и внедряет в компьютер программу-закладку, используя стандартную технику вирусов или троянских коней. Поскольку излучаемые паттерны видимы для глаза, атака должна проводиться во внерабочее время. Многие ПК не выключаются на ночь, это стало обычной практикой благодаря распространению современных энергосберегающих технологий эксплуатации.

Программа-закладка для передачи информации может использовать сдвиг частоты тона, когда 0 и 1 представляются картинками типа показанных на рис.1. Они загружаются в два видеобуфера, которые переключаются со скоростью частоты кадров f_c. Сам же битовый сигнал, перед тем как его использовать для управления сменой передаваемых тонов, предварительно кодируется для обеспечения исправления возможных ошибок.

В нашем дешевом перехватывающем оборудовании содержимое магнитофонной кассеты с записанной передачей затем перекачивается в ПК и оцифровывается с помощью звуковой карты. Завершающие шаги - распознавание символов, синхронизация и декодирование - описаны в любом учебнике по цифровой связи [19]. Типичная скорость передачи для данной ситуации невелика - около 50 бит/сек, так что программа-закладка должна уметь отбирать информацию для трансляции. Очевидными целями являются файлы паролей, ключевой материал и документы, отобранные текстовым поиском на жестком диске.

Приемник для перехвата видеодисплея

Дальнейшие эксперименты проводились с приемником для Темпест-мониторинга ESL model 400 фирмы DataSafe Ltd. (Челтнэм, Англия), см. Рис.2. Это устройство не предназначено для решения радиоразведывательных задач; его создали в конце 1980-х годов как тестовый и демонстрационный инструмент для работы с видеодисплейными технологиями того периода [9]. По сути своей, это обычный черно-белый телевизор с некоторыми модификациями, наиболее важная из которых та, что схемы восстановления сигнала синхронизации заменены двумя вручную настраиваемыми осцилляторами.

Частота горизонтального отклонения или частота строк может выбираться в пределах 10-20 Кгц с почти миллигерцовым разрешением, а частота вертикального отклонения или частота кадров может выбираться в пределах 40.0-99.9 Гц с разрешением 0.1 Гц. В отличие от обычного телевизора, этот аппарат легко можно настроить на четыре полосы в диапазоне 20-860 МГц, а его чувствительность изменяется от 60 V при 20 МГц до 5 V при 860 МГц.

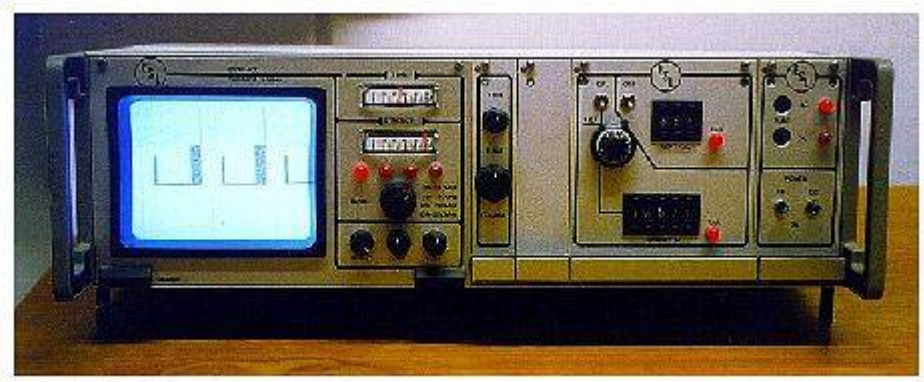

Рисунок 2. DataSafe/ESL Model 400 - монитор Темпест-излучений

С помощью складной 4-метровой дипольной антенны мы получали наилучшее качество изображения в диапазоне 100-200 МГц. Данная антенна далеко не самая оптимальная; эксперименты с позаимствованной логарифмически-спиральной конической антенной с номинальным диапазоном 200-2000 МГц дали намного лучшие результаты даже на частотах 140-200 Мгц. Похоже, что такая более дорогая антенна лучше подходит для эллиптически поляризованных излучений от типичного видеомонитора.

Использованный в наших экспериментах монитор - это обычный 43-см Super-VGA ПК-монитор со 160-МГц полосой видеосигнала, удовлетворяющий требованиям малых излучений MPR II.

Требования к излучениям стандартов MPR и TCO задают только измерения в диапазонах до 400 Кгц. Поля, излучаемые в этих полосах порождаются главным образом катушками отклонения и не несут существенной информации о содержимом экрана. Излучения, связанные с содержимым экрана находятся главным образом на частотах, много превышающих 30 МГц, в ОВЧ и УВЧ диапазонах (если не брать в расчет патологические картинки, транслируемые в описанном ранее эксперименте предыдущего раздела). Стандарты MPR и TCO, введенные в целях охраны здоровья, не требуют экранирования УВЧ и ОВЧ диапазонов, и по сути дела не имеют отношения к Темпест-проблемам. Не следует думать, что так называемые малоизлучающие мониторы или даже жидкокристаллические дисплеи обеспечивают какую-то защиту. Мы установили, что некоторые современные ноутбуки с TFT-LCD дисплеями дают на приеме даже более четкий сигнал, чем многие катодно-лучевые трубки.

Наш ПК-монитор, с его 64 Кгц частотой строк и 95 МГц частотой пиксел, оказался далеко за пределами диапазона тех дисплеев, для которых предназначался аппарат ESL 400. Нам пришлось установить горизонтальный синхрогенератор на 16.1 Кгц, то есть на одну четверть действительной частоты ПК. Вследствие этого содержимое экрана на мониторе приемника выдавалось в четыре колонки; так как последовательные пикселы строк теперь разбивались по модулю 4, то знаки обычного текста хотя и остались видимыми, но стали нечитаемыми.

Скрытие информации в паттернах дрожания

Мы заметили, что наш Темпест-приемник главным образом высвечивает высокочастотную часть видеосигнала. Самые сильные полезные спектральные компоненты находятся на частотах, близких к частоте пиксел и ее гармоникам. Однако, за последнее десятилетие технология мониторов претерпела серьезнейшие изменения. Терминалы начала 80-х годов, изучавшиеся Ван Экком в [2], включали и выключали электронный луч для каждого отдельного пиксела. Это повышало качество изображения в узкополосных КЛТ того времени, поскольку все пикселы в строке выглядели одинаковыми. Без такой пульсации пиксел получалось, что пикселы в середине горизонтальной строки казались ярче тех, что находились по краям, так как в ранней электронике переключение между подъемом и падением напряжения происходило медленно.

Современные дисплеи имеют намного более широкую видеполосу и поэтому не нуждаются в пульсации пиксел. Вследствие этого, все, что перехватчик может принять от горизонтальной строки экрана современного монитора - это два коротких импульса, излучаемых в те моменты, когда луч включается на левом конце и выключается на правом. В действительности, Темпест-сигнал - это грубо говоря амплитуда производной видеосигнала. С текстом это обычно не составляет проблемы, поскольку знаки (в большинстве языков) идентифицируются по их вертикальным компонентам; но это мешает приему экранных изображений типа фотографий, которые не удается легко восстанавливать лишь по четким вертикальным краям.

Человеческий глаз менее чувствителен к высоким, нежели к низким частотам колебаний. "Дрожание" (dithering) - это техника, использующая данное свойство глаза для увеличения цветовых оттенков на дисплеях с небольшим размером таблицы цветности. На современных мониторах с высоким разрешением пользователь не может легко отличить средне-серый цвет от паттерна шахматной доски из черных и белых пиксел, особенно когда расстояние между пикселами меньше диаметра фокуса электронного луча. Для перехватчика же, с другой стороны, высокочастотный черно-белый паттерн порождает максимально возможный по силе сигнал, в то время как постоянный цвет приводит к наислабейшему сигналу.

Мы можем использовать эту разницу в спектральной чувствительности пользователя и перехватчика для того, чтобы они видели различную информацию. На Рис.3 представлены: слева - тестовый сигнал на мониторе рабочей станции авторов; справа - экран, получающийся на Темпест-приемнике.

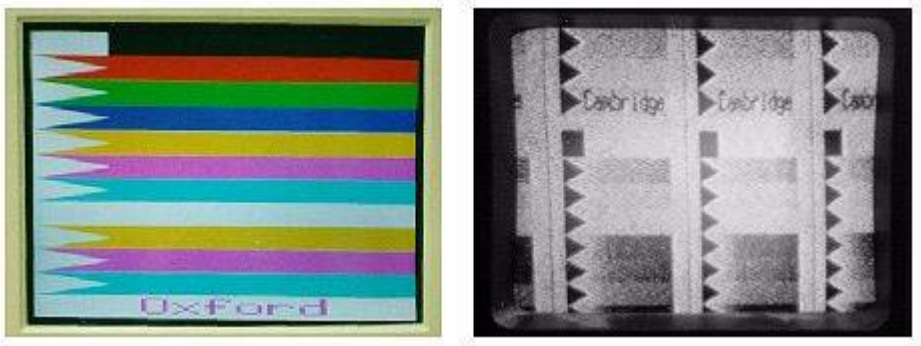

Рисунок 3. Тестовая картинка на мониторе компьютера (слева) и перехваченный сигнал (справа). Три копии на мониторе перехватчика - результат более низкой частоты вертикального отклонения (16.1 кГц вместо 64 кГц, четвертая копия теряется в процессе отката луча).

Тестовая картинка имеет на левой стороне один прямоугольный и несколько треугольных маркеров, нарисованных дрожащим паттерном из вертикальных черных и белых линий. Эти маркеры помогают проследить другие свойства картинки, и даже с нашей простой дипольной антенной их очень ясно видно на мониторе приемника, даже из других комнат на расстоянии свыше 20 метров. Справа от каждого маркера - цветная полоса, кажущаяся равномерной на мониторе компьютера, но постепенно исчезающая к левому краю полосы на Тмпест-картинке. Эти полосы вслед за семью треугольниками были нарисованы равномерными цветами (темно-красный, темно-зеленый, темно-синий, желтый, розовы, голубой и серый) с левого края и постепенно оттенялись дрожащими паттернами вправо (красный/черный, зеленый/черный, синий/черный, желтый/черный, розовый/черный, голубой/черный, белый/черный). Идущие ниже три полосы (На Темпест-приемнике это верхние полосы) - снова желтая, розовая и голубая с левого края, но в этот раз дрожащий паттерн дает фазовый сдвиг между первичными цветами, так что этот паттерн к правому краю становится красно/зеленый, красно/синий и сине/зеленый. Между левым и правым краями полос амплитуда паттерна дрожания нарастает линейно. Эта тестовая картинка сразу позволяет увидеть, какая из трех электронных пушек порождает пригодный Темпест-сигнал и начиная с какого порога. (Одно из наблюдений: сигналы, генерируемые идентичными напряжениями видеовхода для трех основных цветов - красного, зеленого и синего - демонстрируют различные Темпест-амплитуды.)

Впечатляющее приложение чувствительности перехватчика к амплитудам дрожания дано в цветной полосе справа от одиннадцатого треугольника В то время как компьютерный монитор явно высвечивает здесь большими буквами "Оксфорд", перехватчик вместо этого видит на своем экране "Кембридж". На Рис.4 изображено увеличение поля пиксел вокруг букв "Ох", излучающих как "Са". В то время как "Oxford" нарисован розовым вместо серого путем простого выключения зеленой компоненты, "Cambridge" вставлен в картинку наращиванием амплитуды дрожания.

Изменение амплитуда дрожания должно быть сглаженным, чтобы не возбуждать очень чувствительные детекторы в сетчатке человеческого глаза. Для того, чтобы изменение было невидимым, надо учитывать несколько физических эффектов мониторов. Значение цветового компонента, выбираемого дисплейной программой, обычно линейно отображается в напряжение видеовхода, подаваемого на монитор. Но соотношение между видеонапряжением V и светимостью L экрана нелинейно и может быть аппроксимировано как $L = \text{const} \cdot V^{\gamma}$, где γ - зависящая от аппаратуры экспонента, обычно имеющая значение в пределах 1.5-3, в зависимости от конструкции катодно-лучевой трубки. Программисту следует помнить, что общая светимость двух цветовых дрожащих паттернов зависит от среднего арифметического их светимостей, а не от напряжений.

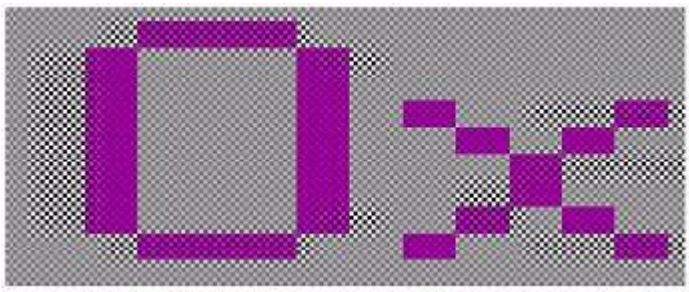

Рисунок 4. Увеличение фрагмента экрана, где пользователь читает "Ох", а на экране перехватчика этот же участок читается как "Са".

Окончательные вычисления известны специалистам в области ТВ и компьютерной графики как "*гамма-коррекция*". Текст, который видит перехватчик, - это гамма-скорректированная амплитудная модуляция паттерна фона, а собственно сообщение для пользователя - просто низкочастотный сигнал.

В случаях, когда передаваемый образ должно быть очень трудно увидеть, параметры дрожания должны вручную калиброваться под конкретный монитор. Такая калибровка зависит не только от типа монитора, но и от яркости, контрастности и других параметров, которые пользователь может изменять. Поэтому осторожный шпион будет пытаться спрятать читаемый текст не в равномерно окрашенные области, а в структурно-богатое экранное содержание, типа фоновых фотографий или анимации, демонстрируемой программами-заставками (скрин-сэйверами). Такие программы, как и любое другое программное обеспечение с доступом к дисплею, - это часть "доверяемой" (trusted) вычислительной базы, коль скоро не имеется эффективного физического экранирования.

5. Широкополосные передачи

Наш метод модуляции амплитуд дрожания для больших читаемых знаков был разработан как средство простой и дешевой трансляции скрытой информации. Профессиональный же разведчик, скорее всего, выберет метод, который воздействует лишь на небольшой участок экранной картинки и будет оптимизирован для максимально надежного приема с помощью сложного оборудования. В данном разделе мы дадим примерный набросок того, как может выглядеть подобная система.

Прием излучений монитора с помощью модифицированного телевизора требует либо точного знания частот горизонтального и вертикального отклонения, либо наличия достаточно сильного сигнала для ручной подстройки генераторов синхроимпульсов. При больших расстояниях и низких уровнях сигнала излучаемую информацию можно отделить от шума только усреднением периодического сигнала за определенный период времени, а ручная подстройка синхронизации довольно сложна.

В случае профессиональной атаки для преодоления глушения сигнала можно использовать технику размазанного спектра. Программа-закладка будет раскладывать дрожанием один или несколько цветов в нескольких строках экранной картинки, используя псевдослучайную битовую последовательность (ПСБП). "Троянская" программа, к примеру, может встроить такое дрожание в строку меню окна. Кросс-коррелятор в приемнике получает один вход с антенны и ищет на других своих входах ту же самую последовательность псевдослучайных бит, выдаваемую с предполагаемой частотой пиксел монитора. Кросс-коррелятор сгенерирует выходной пик, дающий разность фаз между приемником и мишенью. Затем цикл с запертой фазой может управлять осциллятором приемника таким образом, чтобы стало возможным стабильное

и долговременное усреднение экранного содержимого. Информацию можно транслировать инвертированием ПСБП, в зависимости от того, должен ли передаваться бит 0 или 1. Читателям, знакомым с техникой непосредственной модуляции размазанного спектра, известны подобные идеи, и в данной ситуации можно применять множество иных технологий из этой области коммуникаций.

Если же ПСБП, кодируемая как ряд черных и белых пиксел, слишком отличается от обычно серой инструментальной линейки меню, привычной пользователю, то вместо этого можно использовать фазовую модуляцию. Амплитуду паттерна дрожания можно изменять постепенно для нескольких пиксел вблизи фазовых скачков, чтобы избежать видимых перемен яркости на линейке меню. Можно также использовать лишь небольшое количество строк - может быть, только одну неиспользуемую строку по верху линейки (или даже за видимым краем экрана).

Преимущества техники размазанного спектра следующие:

- нужно выбирать только тактовую частоту пиксел и (возможно) несущую частоту. Это обеспечивает быстрое запирание фазы и полностью автоматическую работу;
- возможно достижение более высоких уровней приема, поскольку шум подавляется кросс-корреляцией и усреднением;
- могут достигаться более высокие скорости передачи, и упрощается задача автоматического декодирования принятых данных.

Интересным коммерческим приложением данной технологии может быть контроль использования лицензированного программного обеспечения. Большинство лицензий позволяет использовать продукт лишь на одном компьютере за раз, но это условие очень часто нарушается. Нами предложено, чтобы фирменное программное обеспечение включало в картинку экрана несколько строк с ПСБП-сигналом, кодирующим серийный номер лицензии плюс некоторое случайное значение [20]. Подобно тому, как автофургоны с "ТВ-детектором" ездят в странах с обязательным лицензированием ТВ-приемников (в частности, в Британии), чтобы выявлять нелицензированные телевизоры по их излучениям, так и фургоны с "детектором программ" можно использовать для патрулирования деловых районов и других мест, где есть подозрение на программное пиратство. Если фургон принимает двадцать сигналов одной и той же копии программы Word от компании, имеющей лицензии лишь на пять копий, то есть основания для начала расследования.

Случайное значение, кодируемое в ПСБП, помогает отличать эхо-сигналы сообщений, принимаемых от различных компьютеров. Наконец, если бы ПСБП выдавалась операционной системой, то этим можно было бы транслировать идентификаторы и лицензионные номера всех активных в данное время программ.

7. Новая мера защиты: Темпест-шрифты

Как мы отмечали ранее, перехватчику доступны только высокочастотные компоненты видеосигнала. Слева на Рисунке 5 представлена тестовая картинка, помогающая определить, какая часть спектра изображения действительно порождает Темпест-сигнал. Такого рода "зонная" картинка используется ТВ-специалистами и генерируется на основе функции $\cos(x^2+y^2)$, когда начало системы координат располагается в центре экрана. В каждой точке этого тестового сигнала локальный спектр имеет единственный пик по горизонтальной и вертикальной частоте, пропорциональный горизонтальной и

вертикальной координатам данной точки. Этот частотный пик достигает частоты Нюквиста f_p / 2 для точек на границе "зонной картинки".

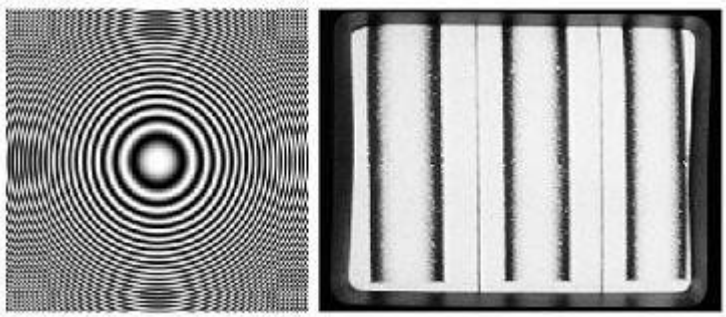

Рисунок 5. Тестовый сигнал "зонной картинки" (слева) и перехватываемый сигнал (справа).

Справа на Рис.5 представлен Темпест-сигнал, перехваченный от монитора с "зонной картинкой" (для этого и других экспериментов, описанных в данном разделе, мы располагали антенну как можно ближе к монитору для достижения наилучших условий приема). Как и следовало ожидать, только горизонтальная частота сигнала задает то, что принимается. Более же интересно то, что только внешние 30% "зонной картинки" выглядят темными на экране монитора приемника. Это означает, что если посмотреть на преобразование Фурье горизонтальной частоты пиксел, то оказывается, что в нашей установке может приниматься лишь информация, представляемая в спектре Фурье частотами из диапазона $0.7 \cdot f_{\mathrm{p}}/2 < f \leq f_{\mathrm{p}}/2$. Конкретное значение 0.7 явно зависит от используемого оборудования, но похоже, что такая его величина не является нетипичной.

Нам стало интересно, а нельзя ли использовать это для потенциально очень дешевой, основанной на программном обеспечении техники защиты от перехвата. На Рисунке 6 слева представлено увеличенное поле пиксел, высвечивающее некоторый текст. Справа показано то же самое поле пиксел после того, как мы удалили верхние 30% преобразования Фурье сигнала, сворачивая его подходящим НЧ-фильтром sin(x)/x.

Отфильтрованный текст выглядит довольно расплывчатым и неприятным на этой увеличенной картинке, но как ни удивительно, потери в качестве текста почти незаметны пользователю на экране компьютера. Ограниченный фокус электронного луча, ограниченное разрешение глаза, а также эффекты, порождаемые маской и электроникой монитора, всячески фильтруют этот сигнал.

Рисунок 6. Слева - увеличенный текст обычным шрифтом, справа - отфильтрованный текст с удаленными верхними 30% спектра горизонтальной частоты.

Хотя для пользователя видимые изменения незначительны, фильтрация текста вызывает эффект, когда ранее легко принимавшаяся информация полностью исчезает с Темпест-монитора, даже если антенна расположена вплотную к видеодисплею.

Перехват текста, высвечиваемого на мониторе - это лишь один тип Темпест-угроз,

связанных с персональными компьютерами. Тем не менее, мы считаем его наиболее серьезной угрозой. Как правило, видеодисплей - сильнейший источник излучений, и, благодаря своей периодической природе, видеосигнал легко выделяется из других периодическим усреднением.

Мы обнаружили еще два потенциальных источника периодических сигналов в каждом ПК, и оба из них можно исправить с помощью дешевого программного обеспечения либо небольшими изменениями конструкции. Во-первых, контроллеры клавиатуры выполняют бесконечный цикл сканирования матрицы клавиш, когда последовательность инструкций выполняется в зависимости от нажимаемой в данное время клавиши. Короткая подпрограмма случайного ожидания внутри данного цикла может предотвратить периодическое усреднение, проводимое перехватчиком. Во-вторых, многие дисководы считывают последний обрабатывавшийся трак непрерывно до тех пор, пока не предпринимается очередной доступ к диску. Поскольку атакующая сторона может попытаться восстановить этот трак периодическим усреднением, мы предлагаем, чтобы после доступа к секретным данным головка диска смещалась к траку с несекретными данными до следующего запроса на считывание.

Наша работа показывает, что разработанная техника "Программный Темпест", и в частности Темпест-шрифты, позволяет существенно повысить безопасность за счет очень небольших затрат. Существует масса приложений, где их будет вполне достаточно: в приложениях среднего уровня секретности многие правительственные органы используют "схему зон", когда компьютеры с секретными данными не экранируются, а располагаются в комнатах, далеко расположенных от областей возможного доступа. Здесь 10-20 dB защиты, предоставляемых Темпест-шрифтом играет весьма важную роль. Существуют также приложения, где Темпест-шрифты являются лишь дополнительной опцией в ситуациях, когда стране приходится неожиданно закупать большие количества обычных коммерческих компьютеров и задействовать их в какой-нибудь серьезной операции типа "Буря в пустыне". Наконец, в таких приложениях как дипломатия, требующих высочайшего уровня защиты, пользователи могут устанавливать Темпест-программы наряду с Темпест-аппаратурой: аппаратное экранирование часто не срабатывает из-за грязных прокладок или организационных проблем, вроде тех, когда в жару послы наотрез отказываются держать двери закрытыми.

8. Выводы

Компрометирующие излучения продолжают оставаться интереснейшей областью исследований, хотя по большому счету они не изучены в научной литературе. Высокая стоимость физического экранирования и постоянно растущие тактовые частоты современных компьютеров гарантируют, что данную проблему быстро не преодолеть. Одновременно, появление мощных программных радиоприемников на любительском рынке способно лишь ухудшить ситуацию.

Однако, нами показано, что Темпест - это не только исследование радиочастот. Программные методы могут существенно изменить картину: их можно применять для новых атак, конструировать новые средства защиты и изобретать совершенно новые приложения. Мы полагаем, что наша технология "Программный Темпест" может существенно развить данную область исследований.

Библиография

1. Kristian Beckman: Laekande Datorer. (Цитируется в [3])
2. Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eaves-dropping Risk? Computers & Security 4 (1985) 269-286
3. Harold Joseph Highland: Electromagnetic Radiation Revisited. Computers & Security 5 (1986) 85-93 and 181-184.
4. Peter Smulders: The Threat of Information Theft by Reception of Electromagnetic Radiation from RS232 Cables. Computers & Security 9 (1990) 53-58
5. Erhard Moeller, Lutz Bernstein, Ferdinand Kolberg: Schutzmassnahmen gegen kompromittierende elektromagnetische Emissionen von Bildschirmsichtgerten. Labor fr Nachrichtentechnik, Fachhochschule Aachen, Aachen, Germany
6. Deborah Russell, G. T. Gangemi Sr.: Computer Security Basics. Chapter 10: TEMPEST, O'Reilly & Associates, 1991, ISBN 0937175714
7. Peter Wright: Spycatcher - The Candid Autobiography of a Senior Intelligence Officer. William Heinemann Australia, 1987, ISBN 0855610980
8. Ernst Bovenlander, invited talk on smartcard security, Eurocrypt 97
9. Operating Manual for DataSafe/ESL Model 400B/400B1 Emission Monitors. DataSafe Limited, 33 King Street, Cheltenham, Goucestershire GL50 4AU, United Kingdom, June 1991
10. Lars Hoivik: System for Protecting Digital Equipment Against Remote Access. United States Patent 5165098, November 17, 1992
11. John H. Dunlavy: System for Preventing Remote Detection of Computer Data from TEMPEST Signal Emissions. United States Patent 5297201, March 22, 1994
12. Joachim Opfer, Reinhart Engelbart: Verfahren zum Nachweis von verzerrten und stark gestoerten Digitalsignalen und Schaltungsanordnung zur Durchfuehrung des Verfahrens. German Patent DE 4301701 C1, Deutsches Patentamt, May 5, 1994
13. Wolfgang Bitzer, Joachim Opfer: Schaltungsanordnung zum Messen der Korrelationsfunktion zwischen zwei vorgegebenen Signalen. German Patent DE 3911155 C2, Deutsches Patentamt, November 11, 1993
14. Electromagnetic Pulse (EMP) and Tempest Protection for Facilities. Engineer Pamphlet EP 111032, 469 pages, U.S. Army Corps of Engineers, Publications Depot, Hyattsville, December 31, 1990
15. Ueberkoppeln auf Leitungen, Faltblaetter des BSI 4, German Information Security Agency, Bonn, 1997.
16. Schutzmassnahmen gegen Lauschangriffe, Faltblaetter des BSI 5, German Information Security Agency, Bonn, 1997.
17. Blosstellende Abstrahlung, Faltblaetter des BSI 12, German Information Security Agency, Bonn, 1996.
18. RJ Lackey, DW Upmal, Speakeasy: The Military Software Radio. IEEE Communications Magazine v 33 no 5 (May 95) pp 56-61
19. John G. Proakis: Digital Communications. 3rd ed., McGrawHill, New York, 1995, ISBN 0070517266
20. Ross J Anderson, Markus G Kuhn, Software Piracy Detector Sensing Electromagnetic Computer Emanations. UK Patent application no GB 9722799.5, 28th November 1997