УДК 004.457
МРНТИ 81.93.29

АКУСТИЧЕСКИЙ КРИПТОАНАЛИЗ ЖИДКОКРИСТАЛЛИЧЕСКИХ МОНИТОРОВ

Денисюк А.В.[1]
[1]*СКГУ им. М. Козыбаева, Петропавловск, Казахстан*

Аннотация

Данная работа посвящена изучению возможностей применения методов акустического криптоанализа для распознания изображения на жидкокристаллическом мониторе. В частности, проверяется возможность обнаружения акустической утечки монитора вне студийных условий, при помощи смартфона. Для этого мы вели одновременную запись звуков, издаваемых монитором при открытом на весь экран окне с автоматически генерируемым содержимым одновременно со студийного микрофона и со смартфона. Записи были преобразованы в спектрограммы, на основании графического анализа которых был сделан вывод о том, что ЖК-мониторы действительно производят зависимый от изображаемого на них контента звук, который может быть записан в бытовых условиях без помощи специального оборудования, и для этого возможно использование даже простого типичного микрофона в мобильном устройстве. Также было разработано программное обеспечение, генерирующее изображения, наиболее ярко демонстрирующие наличие акустической утечки в мониторе, вне зависимости от его разрешения, а также ускоряющее процесс сбора образцов этой акустической утечки для их анализа.

Ключевые слова: криптоанализ, жидкокристаллический монитор, побочные каналы, акустическая утечка, электромагнитная утечка, оптическая утечка, спектрограмма.

СҰЙЫҚ КРИСТАЛДЫ МОНИТОРЛАРДЫҢ АКУСТИКАЛЫҚ КРИПТОАНАЛИЗІ

А.В. Денисюк.[1]
[1]*М. Қозыбаев атындағы СҚМУ, Петропавл, Қазақстан*

Аңдатпа

Бұл жұмыс сұйық кристалды мониторда кескінді тану үшін акустикалық криптанализ әдістерін қолдану мүмкіндіктерін зерттеуге арналған. Атап айтқанда, ол смартфонды қолдана отырып, студиядан тыс жерде монитордың акустикалық ағуын анықтау мүмкіндігін тексереді. Ол үшін біз бір уақытта студия микрофонынан және смартфоннан автоматты түрде шығарылатын мазмұны бар бүкіл экранға терезе ашылған кезде монитор жасаған дыбыстарды жаздық. Жазбалар спектрограммаларға айналдырылды, оның негізінде графикалық талдау негізінде LCD мониторлар үйде арнайы жабдықтың көмегінсіз жазыла алатын және оларда қарапайым жазылатын, оларда көрсетілген мазмұнға байланысты дыбыс шығарады деген қорытындыға келді. ұялы құрылғыдағы әдеттегі микрофон. Сондай-ақ, мониторда оның шешілуіне қарамастан, акустикалық ағудың болуын неғұрлым айқын көрсететін, сонымен қатар талдау үшін осы акустикалық ағып кетудің үлгілерін жинауды суреттейтін бағдарламалық жасақтама жасалды.

Түйінді сөздер: криптоанализ, сұйық кристалды монитор, жанама арналар, акустикалық кему, электромагниттік кему, оптикалық кему, спектрограмма.

ACOUSTIC CRYPTANALYSIS OF LIQUID CRYSTAL MONITORS

A. Denissyuk[1]
[1]*NKSU named after M. Kozybayev, Petropavlovsk, Kazakhstan*

Abstract

This work is devoted to studying the possibilities of using acoustic cryptanalysis methods for image recognition on a liquid crystal monitor. In particular, it checks the possibility of detecting acoustic leakage of the

monitor outside the studio environment using a smartphone. To do this, we simultaneously recorded sounds made by the monitor when a window was opened on the entire screen with automatically generated content simultaneously from the studio microphone and from the smartphone. The recordings were converted into spectrograms, based on a graphic analysis of which it was concluded that the LCD monitors do indeed produce a sound dependent on the content displayed on them, which can be recorded in the home environment, without the help of special equipment, and even with just a simple and typical microphone in a mobile device. Also, software was developed to generate images that most clearly demonstrate the presence of acoustic leakage in the monitor, regardless of its resolution, and also speeds up the process of collecting samples of this acoustic leak for further analysis.

Key words: cryptanalysis, liquid crystal monitor, side channels, acoustic leak, electromagnetic leak, optical leak, spectrogram.

Введение

В данный момент хорошо изучены акустические утечки, исходящие от клавиатур и принтеров, однако наблюдается недостаточное количество исследований данного типа утечки в жидкокристаллических (ЖК) мониторах. ЖК-мониторы используются повсеместно в течение уже второго десятка лет, и потому представляется необходимым изучение уязвимостей для безопасности информации, которые данные устройства могут в себе нести. Электронные устройства являются одними из самых личных объектов в жизни многих людей. Мы используем их для хранения и управления конфиденциальной и приватной информацией, такой как фотографии, пароли и сообщения. Защита таких конфиденциальных данных с помощью шифрования является распространенным подходом для предотвращения несанкционированного доступа и разглашения. Однако защита от утечки данных до шифрования отсутствует. Фактически прослушивание физических сигналов, таких как акустические или электромагнитные излучения, является одним из способов восстановления либо текстовых данных перед шифрованием, например, во время их ввода или визуализации, либо ключей шифрования, например, во время шифрования и дешифрования данных.

Методы исследования

В нашем исследовании мы проверяли следующую гипотезу: ЖК-мониторы производят зависимый от изображаемого на них контента звук.

Для этого использовался графический метод анализа данных: агрегированные звуковые данные по ЖК-мониторам были преобразованы в спектрограммы для выявления частот аудио утечки и степени ее выраженности.

Результаты исследования

История подслушивания физических сигналов восходит к 1943 году, когда инженер компании Bell Telephone обнаружил, что осциллограф может извлекать обычный текст из электромагнитных излучений модели звонящего телефона модели Bell Telephone 131-B2 – устройства микширования, используемого армией США для защищенной связи. «Когда один из микшеров тестировался в лаборатории Bell, исследователь совершенно случайно заметил, что каждый раз, когда машина выполняла действия, на осциллографе в отдаленной части лаборатории появляется шип. После более тщательного изучения этих всплесков он обнаружил, что он может прочитать чистый текст сообщения, зашифрованного машиной!» [1]. Позже, в 1951 году, ЦРУ обнаружило, что чистый текст можно восстановить с помощью этого явления на расстоянии до четверти мили. Связанные методы использовались для шпионажа обеими сторонами во время холодной войны. Лишь в 1985 году, когда голландский ученый Вим ван Эйк опубликовал свою статью, демонстрирующую, что

излучения компьютерных мониторов можно собирать и отображать на телевизоре в соседнем здании [2], знания о таком типе подслушивания стали доступны за пределами военных кругов [3].

Обычной целью для физических атак перехвата являются периферийные устройства ввода/вывода, такие как клавиатуры, мыши, сенсорные экраны и принтеры. Примерами изученных физических атак подслушивания являются: электромагнитное (ЭМ) излучение периферийных устройств, видео пользователей, печатающих на клавиатуре или сенсорном экране, акустические утечки клавиатур и принтеров, оптическая утечка мониторов, и, наконец, акустическая утечка мониторов.

ЭМ утечка является побочным каналом с длинной историей слухов и утечек, связанных с его использованием для шпионажа. Хорошо известно, что оборонные организации во всем мире параноидально относятся к ограничению электромагнитных излучений от своего оборудования и проводят исследования по электромагнитным атакам и обороне в условиях полной секретности.

В открытом доступе значение побочного канала ЭМ впервые было продемонстрировано Вим ван Эйком в 1985 году [2]. Он показал, что электромагнитные излучения от компьютерных мониторов могут быть получены на расстоянии и использованы для восстановления отображаемой информации.

Из новейших исследований в данной области можно вынести анализ информационных утечек в лазерных принтерах посредством ЭМ излучения. Излучения лазерного принтера, который может обрабатывать секретную информацию, исследуются в среде электромагнитного излучения, проводников линии электропередач и проводников сигнальных линий.

Контрмеры ЭМ анализа включают в себя перепроектирование микросхемы для уменьшения непреднамеренных излучений, методы для уменьшения отношения сигнал/шум, наблюдаемого противникоми контрмеры на основе рандомизации излучаемых сигналов.

Исследовательское сообщество вложило много усилий в изучение *акустических утечек клавиатуры* и продемонстрировало, что это очень серьезная проблема конфиденциальности. Успешная акустическая атака по побочному каналу позволяет противнику узнать, что печатает жертва, на основе звука, производимого нажатием клавиш. Как правило, звуки записываются либо напрямую, с использованием микрофонов, либо с использованием различных датчиков (например, акселерометров), чтобы восстановить ту же акустическую информацию. После сбора аудиопоток обычно анализируется с использованием методов, таких как контролируемое и неконтролируемое машинное обучение или триангуляция. Конечный результат - полная или частичная реконструкция данных жертвы.

Исследование акустического перехвата клавиатуры началось с оригинальной статьи Асонова и Агравала [4], которая показала, что при обучении нейронной сети на определенной клавиатуре можно добиться хорошей производительности при прослушивании ввода на той же клавиатуре или на других клавиатурах той же модели. Эта работа также исследовала причины возможности проведения данной атаки и обнаружила, что плита под клавиатурой (где клавиши ударяются о датчики) ведет себя как барабан. Это приводит к тому, что звук, производимый разными клавишами, немного различается.

Принтеры также используются в качестве устройств вывода для компьютерных систем. *Акустические эманации принтеров* были изучены в 1991 году, и буквы «W» и

«J» были успешно различены [5]. Был представлен метод атаки, основанный на записи звука матричного принтера, обрабатывающего текст на английском языке [6]. Атака состоит в восстановлении того, что печатает текстовый принтер, обрабатывающий английский текст, на основе записи звука, который он издает, если микрофон находится достаточно близко к принтеру. В экспериментах атака восстанавливает до 72% напечатанных слов и до 95%, если предположить контекстные знания о тексте, с микрофоном на расстоянии 10 см от принтера. После начального этапа обучения атака полностью автоматизирована и использует сочетание методов машинного обучения, обработки звука и распознавания речи, включая функции спектра, скрытые марковские модели и линейную классификацию; кроме того, он учитывает инкрементальное обучение на основе обратной связи. Было описано успешное применение атаки в полевых условиях (с соответствующими средствами защиты конфиденциальности) на практику врача с целью восстановления содержания медицинских рецептов.

Также была дана оценка эффективности контрмер: идея, лежащая в основе всех контрмер, состоит в том, чтобы подавлять акустические излучения настолько, чтобы реконструкция становилась трудной в практических сценариях.

В 2008 году была представлена техника наблюдения за данными, отображаемыми на произвольном экране компьютера, включая широко распространенные в ЖК-мониторы. Методика использует отражения *оптических излучений экрана* в различных объектах, которые обычно обнаруживаются в непосредственной близости от экрана, и использует эти отражения для восстановления исходного содержимого экрана. К таким предметам относятся очки, чайники, ложки, пластиковые бутылки и даже глаза пользователя. Было продемонстрировано, что эта атака может быть успешно проведена, чтобы шпионить даже за маленькими шрифтами, используя готовое оборудование стоимостью менее 1500 долларов с расстояния до 10 метров. Опора на более дорогое оборудование позволяет проведение этой атаки с расстояния более 30 метров, демонстрируя, что подобные атаки возможны с другой стороны улицы или из близлежащего здания [7].

В августе 2018 был обнаружен новый физический побочный канал: зависящая от содержимого экрана *акустическая утечка с ЖК-экранов* [8]. Эта утечка может быть обнаружена расположенными поблизости микрофонами, такими как микрофоны, встроенные в веб-камеры и некоторые компьютерные экраны. Пользователи обычно обмениваются звуком, записанным этими микрофонами, например, во время голосовой связи по IP и звонкам в режиме видеоконференции. Более того, соответствующие звуки настолько слабые и высокие, что они почти не слышны человеческому уху, и поэтому (в отличие от механических периферийных устройств) у пользователей нет оснований подозревать, что эти излучения существуют и что информация об их содержимом экрана доступна любому, кто получает аудиопоток или запись. Фактически, пользователи часто пытаются разместить свою веб-камеру (и, следовательно, микрофон) в непосредственной близости от экрана, чтобы поддерживать зрительный контакт во время видеоконференции, предлагая тем самым высококачественные измерения для потенциальных злоумышленников.

Кратковременное потребление энергии, вызванное цифровыми цепями монитора, изменяется в зависимости от содержимого экрана, обрабатываемого в растровом порядке. Это, в свою очередь, влияет на электрическую нагрузку на компоненты блока питания, которые обеспечивают питание цифровой платы монитора, заставляя их вибрировать и издавать звук.

Для проверки возможности распознания данной утечки вне студийных условий, а также определения различий между использованием профессионального микрофона (BM 800) и смартфоном (Xiaomi Redmi Note 3), была написана программа на языке C++ (Рисунок 1), генерирующая полноэкранные окна с «зебрами» – чередующимися черными и белыми полосами одинаковой толщины, вне зависимости от разрешения используемого монитора. Толщина каждой из полос составляет 8 пикселей первые три секунды, затем каждые три последующие секунды толщина увеличивается на 2 пикселя, до конечной толщины в 20 пикселей.

```
LRESULT CALLBACK WindowProcedure (HWND hwnd, UINT message, WPARAM wParam, LPARAM lParam)
{
    HDC hdc;
    PAINTSTRUCT ps;
    RECT rt;
    COLORREF color = RGB(0, 0, 0);
    double x,y;

    switch (message)                  /* handle the messages */
    {
        case WM_PAINT:
            //std::cout << width << " " << height << std::endl;
            hdc = BeginPaint(hwnd, &ps);
            GetClientRect(hwnd, &rt);
            RECT rect;
            HBRUSH brush;
            rect.left = 0;
            rect.right = width;
            for (int i=8; i<22; i+=2){
                clr = 0;
                rect.top = 0;
                rect.bottom = i;
                brush = CreateSolidBrush(RGB(255,255,255));
                FillRect(hdc, &rect, brush);
                for (int j=i; j<height-i; j+=i){
                    rect.top=j;
                    rect.bottom=j+i;
                    if (clr==0){
                        brush = CreateSolidBrush(RGB(0,0,0));
                        FillRect(hdc, &rect, brush);
                        //std::cout << j << " " << clr << std::endl;
                        clr = 1;
                    } else if (clr==1){
                        brush = CreateSolidBrush(RGB(255,255,255));
                        FillRect(hdc, &rect, brush);
                        //std::cout << j << " " << clr << std::endl;;
                        clr = 0;
                    }
                }
                Sleep(3000);
            }
            DeleteObject(brush);
            EndPaint(hwnd,&ps);
            break;
        case WM_DESTROY:
            PostQuitMessage (0);       /* send a WM_QUIT to the message queue */
            break;
        default:                      /* for messages that we don't deal with */
            return DefWindowProc (hwnd, message, wParam, lParam);
    }

    return 0;
}
```

Рисунок 1 Основная часть программы рисования «зебр»

Во время генерации окна с «зебрами» осуществлялась запись звука монитора с использованием одновременно и студийного микрофона, и смартфона (Рисунок 2). Запись проходила в жилой квартире, с типичным для данных условий сопровождающим шумом.

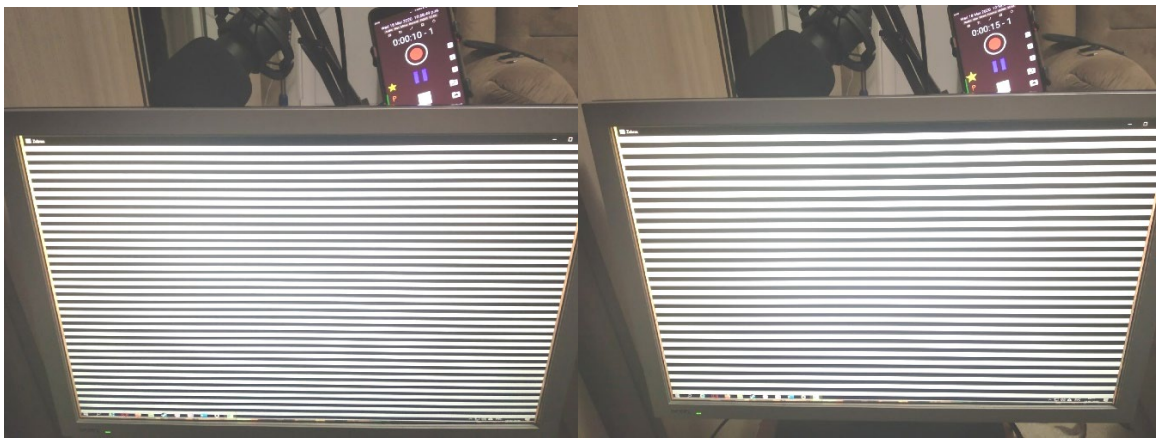
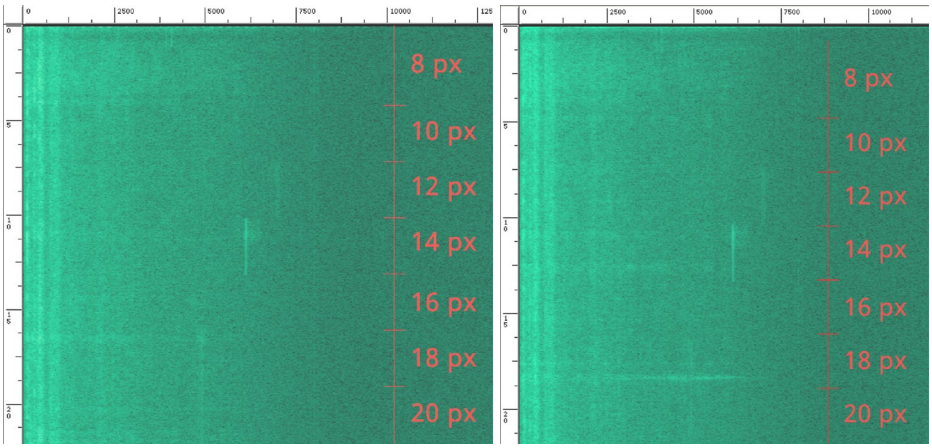


Рисунок 2 Запись звука «зебр» на мониторе BenQ FP222W

Для того, чтобы проверить наличие различий и схожестей между акустической утечкой монитора при отображении различных изображений, было использовано программное обеспечение «Baudline», которое преобразовало полученные записи с микрофона и с телефона в спектрограммы (Рисунок 3).



а) б)

Рисунок 3 Запись звука зебр с микрофона (а) и с мобильного телефона (б)

Спектрограммы наглядно иллюстрируют несколько фактов:

1) ЖК-мониторы действительно производят акустическую утечку;
2) акустическая утечка зависима от изображаемого на мониторе контента;
3) степень выраженности утечки также зависит от изображения;
4) обнаружение утечки возможно вне студийных условий;
5) обнаружение утечки возможно с помощью мобильного телефона;
6) мобильный телефон подбирает больше шума.

Заключение

Таким образом, выдвинутая нами гипотеза подтвердилась: ЖК-мониторы производят зависимый от изображаемого на них контента звук, который может быть записан в бытовых условиях без помощи специального оборудования, и для этого возможно даже использование типичного микрофона в мобильном устройстве.

Литература:

1. Джеффри Фридман. Буря: проблема сигнала // Криптологический Спектр Национального Агенства Безопасности, 35:76, 1972.
2. Вин ван Эйк. Электромагнитное излучение от видеоэкранов: риск подслушивания? // Компьютеры и безопасность, 4, 1985. – С. 269-286.
3. Райан Сингел. Рассекреченный документ Национального Агенства Безопасности раскрывает секретную историю бури // Журнал «Wired», 29, 2008.
4. Дмитрий Асонов, Ракеш Агравал. Акустические излучения клавиатуры // Симпозиум Института инженеров по электротехнике и электронике по безопасности и конфиденциальности, 2004. – 30 с.
5. Роланд Бриоль. Эманация: как сохранить конфиденциальность ваших данных // Симпозиум по электромагнитной безопасности для защиты информации, 1991.
6. Майкл Бэкс, Маркус Дюрмут, Себастьян Герлинг, Манфред Пинкал и Кэролайн Спорледер. Акустические побочные атаки на принтеры // Симпозиум по безопасности USENIX, 2010. – 16 с.
7. Майкл Бэкс, Маркус Дюрмут, Доминик Унру. Компрометирующие отражения-или-как читать ЖК-мониторы за углом // Симпозиум Института инженеров по электротехнике и электронике по безопасности и конфиденциальности, 2008. – 12 с.
8. Даниэль Генкин, Михир Паттани, Рой Шустер, Эран Тромер. Синестезия: обнаружение содержимого экрана через удаленные акустические боковые каналы // Санта-Барбара: конференция CRYPTO, 2018. – 31 с.