ПРОГРАММНАЯ РЕАЛИЗАЦИЯ НА ANDROID OS ОБНАРУЖИТЕЛЯ УТЕЧКИ ИНФОРМАЦИИ ПОСРЕДСТВОМ МОДУЛЯЦИИ ВИДИМОГО СВЕТА

Передача информации посредством модуляции интенсивности видимого света подтверждена работами многих авторов и существованием сети передачи данных Li-Fi. Повсеместное использование светодиодного освещения, управляемого контроллерами, потенциально формирует канал утечки акустической информации посредством модуляции видимого света. В работе авторы рассматривают структурную схему устройства обнаружения канала утечки информации. Авторы предлагают использовать современный смартфон под управлением Android OS для определения модуляции интенсивности освещения, регистрируемого датчиком освещенности смартфона.

Ключевые слова: модуляция видимого света, светодиод, фотодиод, датчик освещенности, обнаружение канала утечки информации.

Shvyrev B. A., Timonov D. A.

SOFTWARE IMPLEMENTATION ON ANDROID OS OF THE INFORMATION LEAK DETECTOR BY MEANS OF VISIBLE LIGHT MODULATION

The transmission of information by means of visible light intensity modulation is confirmed by the works of many authors and the existence of a Li-Fi data transmission network. The widespread use of led lighting controlled by controllers potentially creates a channel for acoustic

information leakage through visible light modulation. In this paper, the authors consider the block diagram of the device for detecting the channel of information leakage. The authors suggest using a modern smartphone running Android OS to determine the modulation of the refresh rate detected by the smartphone's light sensor.

Keywords: visible light modulation, led, photodiode, light sensor, information leakage channel detection.

Утечка акустической информации посредством модуляции видимого света рассмотрена в работах [1-3]. Очевидность существования такого канала утечки подтверждается существование сети передачи данных

видимого света представлена на рисунке 1. Рассмотрим схему основного автомата LTR-579ALS¹ (ALS) датчика освещенности смартфона под управлением Android OS на рис. 2.

Рис.1. Структурная схема устройства обнаружения утечки информации посредством модуляции видимого света

Li-Fi [4-6]. Существованию оптических скрытых каналов посвящена публикация [7]. Подробное описание оптической фильтрации простого оптического приемника, подключенного к параллельному порту старого компьютера, приводится в [8]. Известна работа [9] посвященная утечки информации и взлому компьютера, физически не соединённому ни с какой информационной сетью посредством перехвата видимого излучения от информационных светодиодов расположенных на системном блоке. В работе [10] рассматривается атака с использованием потребительских лампочек дневного освещения с функциями интернета вещей IoT для скрытой коммуникации через различные уровни интенсивности света.

Структура канала утечки посредством модуляции видимого света рассмотрена авторами в [11], а его характеристики в [12]. В настоящее время остается актуальным разработка устройства обнаружения утечки информации посредством модуляции видимого света от осветительных светодиодов. Перспективным направлением является использование для этих целей современные смартфоны под управление Android OS.

Структурная схема устройства обнаружения утечки информации посредством моду-

Во время работы ALS и датчика приближения (proximity sensor PS) измерения ALS можно активировать, установив бит ALS_Enable в 1 и PS измерение можно активировать, установив бит PS_Enable в 1. Как только датчики PS и / или ALS станут активироваться с помощью команды I2C, внутренние блоки поддержки становятся включены. После того, как напряжения и токи установлены (обычно через 5 мс), конечный автомат проверяет наличие событий запуска из планировщика измерений для запуска ALS или PS преобразования в соответствии с выбранными скоростями повторения измерений. После того, как PS_Enable или ALS_Enable будут изменен до 0, текущее преобразование на соответствующем канале будет завершено, и соответствующие АЦП и блоки поддержки станут отключены.

Люкс Формула. Lux_Calc - это рассчитанное значение в люксах, а ALS DATA - цифровое представление (выходной АЦП) окружающей среды. Уровень освещенности сохраняется в регистрах (Адрес: 0x0D-0x0F) независимо от источников света

$$Lux_{calc} = \frac{0.8 * ALS_{DATA}}{(GAIN * INT)}$$

Если датчик располагается под тони-

Optical SensorProduct Data SheetLTR-579ALS-01. https://optoelectronics.liteon.com/upload/download/DS86-2015-0005/LTR-579ALS-01_FINAL_DS_V1.1.PDF

Рис. 2. Схема функционирования конечного автомата датчика освещенности смартфона приемника оптического сигнала

ванным стеклом необходимо воспользоваться соотношением

$$Lux_{calc} = \frac{0.8 * ALS_{DATA}}{(GAIN * INT)}$$

вается, когда данные выбранного источника прерывания выше верхнего или ниже нижнего порога для заданного количества последовательных измерений, установленных в ALS Persist в регистре INT_PST (0x1A). Сигнал прерывания также сохраняется в регистре MAIN_STATUS (0x07) как бит флага в бите 4 (состояние ALS INT). Это бит флага состояния очищается чтением регистра MAIN_STATUS. Сброшенный флаг также очистит сигнал прерывания на контакте INT. Прерывание PS активируется битом 0 (разрешение контакта прерывания PS). Оно срабатывает, когда результат преобразования PS выше верхнего или нижнего порога PS для заданного количества последовательных измерений, установленных в PS Persist в INT_PST регистр (0x1A). Логический сигнал PS, бит 2 регистра MAIN_STATUS (0x07), устанавливается в 0, когда данные PS ниже нижнего PS порога, и он установлен в 1, если данные PS выше верхнего порога PS.

Таблица 1

ALS Gain	GAIN
X1	1
X2	3
X3	6
X4	9
X5	18

Resolution (bit) / Integration Time (ms)	INT
16-bit, 25ms	0.25
17-bit, 50ms	0.5
18-bit, 100ms	1
19-bit, 200ms	2
20-bit, 400ms	4

Особенности прерывания датчика освещенности. Это устройство генерирует независимые сигналы прерывания ALS и PS, которые можно мультиплексировать и выводить на выход INT (см. табл. 1). Условия прерывания всегда оцениваются после завершения нового преобразования каналов ALS и PS. Режим логики PS имеет приоритет над любым другим сигналом прерывания. Если выбрано (PS Logic Mode = 1), прерывание ALS не может сигнализировать на выходе INT. ALS и PS прерывания, а также режим PS Logic активны на низком уровне на выходе INT. Прерывание ALS активируется битом 2 (контакт ALS INT включен) регистра INT_CFG (0x19). Прерывание ALS Источник - канал ALS. INT устанавли-

вается, когда данные выбранного источника прерывания выше верхнего или ниже нижнего порога для заданного количества последовательных измерений, установленных в ALS Persist в регистре INT_PST (0x1A). Сигнал прерывания также сохраняется в регистре MAIN_STATUS (0x07) как бит флага в бите 4 (состояние ALS INT). Это бит флага состояния очищается чтением регистра MAIN_STATUS. Сброшенный флаг также очистит сигнал прерывания на контакте INT. Прерывание PS активируется битом 0 (разрешение контакта прерывания PS). Оно срабатывает, когда результат преобразования PS выше верхнего или нижнего порога PS для заданного количества последовательных измерений, установленных в PS Persist в INT_PST регистр (0x1A). Логический сигнал PS, бит 2 регистра MAIN_STATUS (0x07), устанавливается в 0, когда данные PS ниже нижнего PS порога, и он установлен в 1, если данные PS выше верхнего порога PS.

Существует два варианта указания сигнала прерывания PS на выводе INT: в виде непрерывного логического сигнала или в виде, иницируемом фронтом сигнал прерывания, который очищается при следующем считывании из регистра MAIN-STATUS. Сигнал прерывания PS также сохраняется в регистре MAIN-STATUS (0x07) как бит флага в бите 1 (состояние PS INT). Это бит флага состояния очищается чтением регистра MAIN-STATUS.

Для управления датчиком освещенности разработана программа позволяющая регистрировать изменения интенсивности освещения. Для обработки полученных данных освещенности и обнаружения в них передачи информации в работе использовалось выявление коррелированных данных в потоке, для этого рассчитывалась автокорреляционная функция.

Рассмотрим реализация автокорреляционной функции. Поток данных представляет собой дискретные значения освещенности. Запишем автокорреляционную функцию дискретного сигнала как:

$$B_u(n) = \sum_{j=-\infty}^{\infty} u_j u_{j-n}$$

где u_j – отсчеты дискретного сигнала освещенности,

n – задержка сигнала (целочисленный аргумент, указывающий, на сколько позиций сдвинута копия сигнала относительно оригинала).

При $n = 0, B_u(n)$ она максимальна и равна энергии сигнала, однако функция в общем случае не является четной функцией и необязательно достигает максимума при $n = 0$. При передачи дискретных сообщений с неизвестной фиксированной частотой дискретизации максимум автокорреляционной функции $B_u(n)$ соответствует временной задержке равной интервалу дискретизации исследуемого процесса. Такой подход позволяет определить наличие связанных данных в изменениях интенсивности освещения.

Решающим устройством является программный компаратор. Выносящий суждение при значительном превышении текущих значений $B_u(n)$. Что сигнализирует о возникновении канала утечки в контролируемом помещении посредством модуляции видимого света.

Разработанная программное средство позволяет обнаружить передачу информации в оптическом диапазоне посредством модуляции видимого света, излучаемого осветительными светодиодами.

Литература

1. Канал утечки акустической информации посредством модуляции видимого света // Швырев Б.А., Тимонов Д.А. / Вестник УрФО. Безопасность информационной сфере. 2019. № 1 (31). С. 11-16.
2. Occurrence channel of leakage of the acoustic due to the modulation of the visible light // Shvyrev B.A., Vlasenko A.V., Makaryan A.S., Timanov D.A./ Industry 4.0. 2019. Т. 4. № 4. С. 161-163.
3. Mathematical model of the leakage channel of acoustic information by modulating the light flux // Shvyrev B.A., Vlasenko A.V., Timanov D.A./Mathematical Modeling. 2019. Т. 3. № 1. С. 30-31.
4. «Comprehensive Summary of Modulation Techniques for LiFi. LiFi Research». www.lifi.eng.ed.ac.uk. Retrieved 2018-01-16.
5. Harald Haas. «Harald Haas: Wireless data from every light bulb». ted.com. Archived from the original on 8 June 2017.
6. H. Haas, L. Yin, Y. Wang, C. Chen, What is LiFi?, J. Light. Technol. 34 (6) (2016). PP. 1533-1544
7. Information leakage from optical emanations. J Loughry, DA Umphress. ACM Transactions on Information and System Security (TISSEC) 5 (3), 20021, p.262-289. http://www.applied-math.org/optical_tempest.pdf
8. Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. April 15, 2005. by Michal Zalewski. <https://www.amazon.com/Silence-Wire-Passive-Reconnaissance-Indirect/dp/1593270461>
9. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. Mordechai Guri ; Boris Zadov ; Andrey Daidakulov ; Yuval Elovici. 2018 16th Annual Conference on Privacy, Security and Trust (PST). DOI: 10.1109/PST.2018.8514196. <https://arxiv.org/ftp/arxiv/papers/1706/1706.01140.pdf>.
10. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. Eyal Ronen, Adi Shamir. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). DOI:10.1109/EuroSP.2016.13. Corpus ID: 206649455. <http://www.wisdom.weizmann.ac.il/~eyalro/EyalShamirLed.pdf>
11. Параметры канала утечки акустической информации за счет модуляции видимого света//Власенко А.В., Швырев Б.А., Тимонов Д.А./ Прикаспийский журнал: управление и высокие технологии. 2019. № 1 (45). С. 188-192.

12. Акустические аспекты модели угроз утечки информации по средствам модуляции видимого света// Швырев Б.А., Тимонов Д.А./Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 3. С. 120-124.

References

1. Kanal utechki akusticheskoy informacii posredstvom modulyacii vidimogo sveta [Channel leakage of acoustic information by modulating the visible light] // SHvyrev B.A., Timonov D.A. / Vestnik UrFO. Bezopasnost' v informacionnojsfere. 2019. № 1 (31). S. 11-16.
2. Occurrence channel of leakage of the acoustic due to the modulation of the visible light // Shvyrev B.A., Vlasenko A.V., Makaryan A.S., Timanov D.A./ Industry 4.0. 2019. T. 4. № 4. C. 161-163.
3. Mathematical model of the leakage channel of acoustic information by modulating the light flux // Shvyrev B.A., Vlasenko A.V., Timanov D.A./Mathematical Modeling. 2019. T. 3. № 1. C. 30-31.
4. «Comprehensive Summary of Modulation Techniques for LiFi. LiFi Research». www.lifi.eng.ed.ac.uk. Retrieved 2018-01-16.
5. Harald Haas. «Harald Haas: Wireless data from every light bulb». ted.com. Archived from the original on 8 June 2017.
6. H. Haas, L. Yin, Y. Wang, C. Chen, What is LiFi?, J. Light. Technol. 34 (6) (2016). PP. 1533-1544
7. Information leakage from optical emanations. J Loughry, DA Umphress. ACM Transactions on Information and System Security (TISSEC) 5 (3), 20021, p.262-289. http://www.applied-math.org/optical_tempest.pdf
8. Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. April 15, 2005. by Michal Zalewski. <https://www.amazon.com/Silence-Wire-Passive-Reconnaissance-Indirect/dp/1593270461>
9. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. Mordechai Guri ; Boris Zadov ; Andrey Daidakulov ; Yuval Elovici. 2018 16th Annual Conference on Privacy, Security and Trust (PST). DOI: 10.1109/PST.2018.8514196. <https://arxiv.org/ftp/arxiv/papers/1706/1706.01140.pdf>.
10. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. Eyal Ronen, Adi Shamir. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). DOI:10.1109/EuroSP.2016.13. Corpus ID: 206649455. <http://www.wisdom.weizmann.ac.il/~eyalro/EyalShamirLed.pdf>
11. Parametry kanala utechki akusticheskoy informacii za schet modulyacii vidimogo sveta [Parameters of the acoustic information leakage channel due to visible light modulation]//Vlasenko A.V., SHvyrev B.A., Timonov D.A./Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. 2019. № 1 (45). S. 188-192.
12. Akusticheskie aspekty modeli ugroz utechki informacii po sredstvam modulyacii vidimogo sveta [Acoustic aspects of the threat model of information leakage by means of visible light modulation]// SHvyrev B.A., Timonov D.A./Sovremennaya nauka: aktual'nye problem teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki. 2019. № 3. S. 120-124.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, главный научный сотрудник ФКУ Научно-исследовательский институт ФСИН России. 125130, г. Москва, ул. Нарвская, д. 15а, стр. 1. E-mail: bor2275@yandex.ru

ТИМОНОВ Дмитрий Александрович, начальник лаборатории Научно-исследовательского центра Краснодарского высшего военного училища имени генерала армии С.М. Штеменко. 350063, г. Краснодар, ул. Красина, дом 4. E-mail: dmitrii-timonov@bk.ru

SHVYREV Boris, Candidate of Physical and Mathematical Sciences, Chief Researcher, PKU Research Institute of the Federal Penitentiary Service of Russia. Bld. 15a, p. 1, Narvskaya Str., Moscow, 125130. E-mail: bor2275@yandex.ru

TIMONOV Dmitry, the head of laboratory of the research center of Krasnodar higher military school named after Army General S.M. Shtemenk. Bld. 4, Krasina Str., Krasnodar, 350063. E-mail: dmitrii-timonov@bk.ru