НИЧТО ТАК НЕ ГОВОРИТ О ИБ, КАК СОТНИ ИБ-ПРОДУКТОВ И БИОМЕТРИЧЕСКИЙ СКАНЕР

ХРОНИКИ БЕЗОПАСНИКА

ДАЙДЖЕСТ. 2024 / 05

Добро пожаловать в очередной выпуск ежемесячного сборника материалов, который является вашим универсальным ресурсом для получения информации о самых последних разработках, аналитических материалах и лучших практиках в постоянно развивающейся области безопасности. В этом выпуске мы подготовили разнообразную подборку статей, новостей и результатов исследований, рассчитанных как на профессионалов, так и на обычных любителей. Цель нашего дайджеста - сделать наш контент интересным и доступным. Приятного чтения!

Больше контента:

BOOSTY.TO

SPONSR.RU

TELEGRAM

Рубрика: Новичок

Для новичков в мире ИБ или для тех, кто предпочитает работать с контентом без финансовых обязательств.

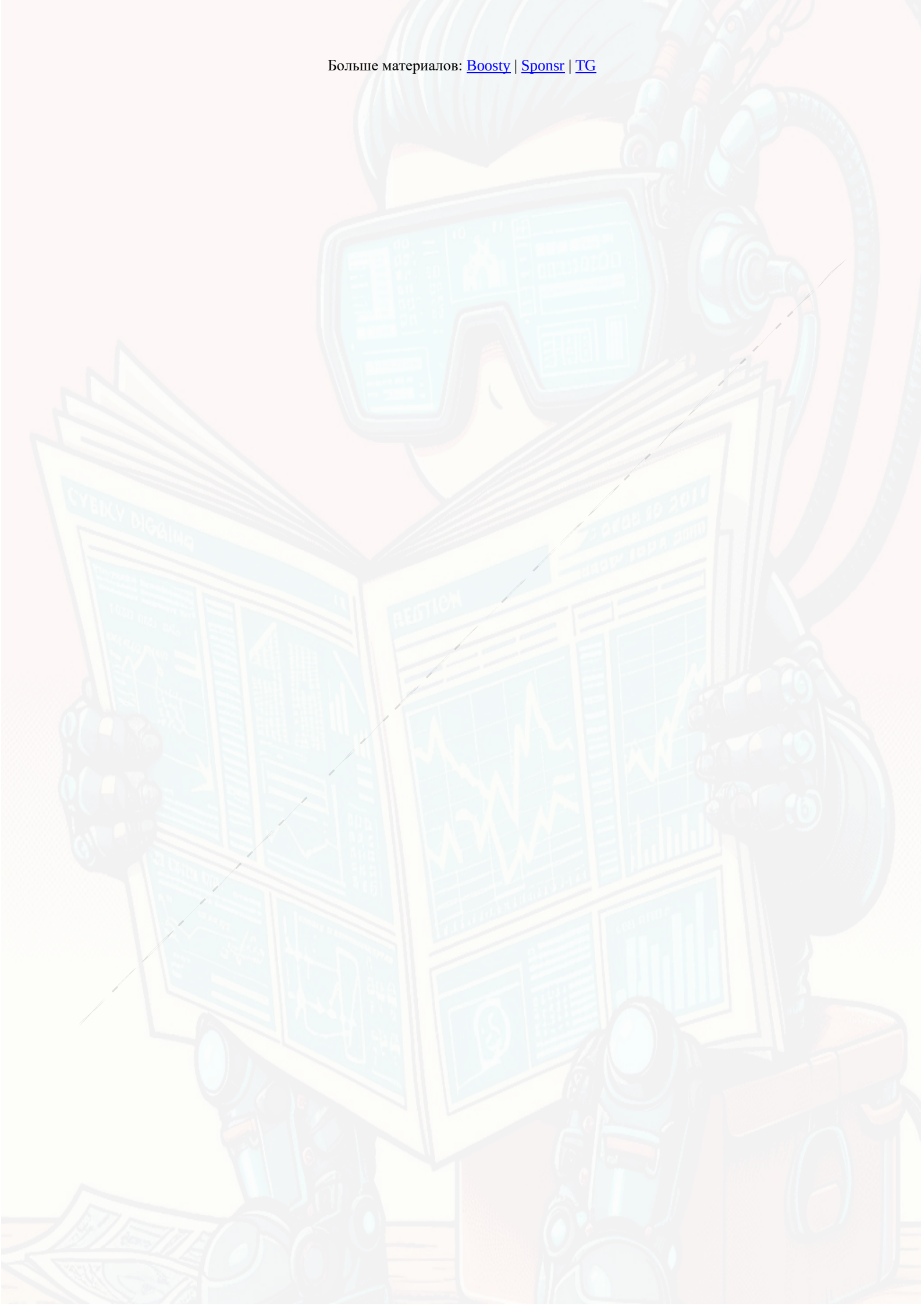
Рубрика: Специалист

Для постоянных читателей, которые заинтересованы быть в курсе последних тенденций в мире кибербезопасности

Рубрика: Профессионал

Для ИТ-специалистов, экспертов, и энтузиастов, которые готовы погрузится в сложный мир ИБ.

Больше материалов: Boosty | Sponsr | TG



Новости

Больше материалов: Boosty | Sponsr | TG

BatBadBut

📌 **Идентификация уязвимости:** Критическая уязвимость идентифицируется как "BatBadBut" CVE-2024–24576

📌 **Уязвимое ПО:** Уязвимость существует в стандартной библиотеке Rust и, в частности, затрагивает системы Windows

📌 **Степень критичности:** присвоена наивысшая оценка по шкале CVSS, равная 10,0, что указывает на максимальную степень тяжести

📌 **Подробная информация**: Уязвимость возникает из-за того, что стандартная библиотека Rust неправильно экранирует аргументы при вызове пакетных файлов в Windows с использованием командного API. Это может позволить злоумышленнику выполнять произвольные команды оболочки, обходя экранирующий интерфейс.

📌 **Условия:** выполнение команды в Windows, команда не указывает расширение файла или использует .bat или .cmd, команда содержит управляемый пользователем ввод в качестве части аргументов команды, а среда выполнения не может должным образом обработать аргументы команды для cmd.exe

📌 **Уязвимые версии:** Все версии Rust для Windows до версии 1.77.2 подвержены этой уязвимости

📌 **Воздействие:** Уязвимость также затрагивает другие языки программирования, включая Erlang, Go, Haskell, Java, Node.js, PHP, Python и Ruby, хотя исправления выпущены не для всех из них

📌 **Рекомендации по устранению:** Пользователям рекомендуется перемещать пакетные файлы в каталог, не указанный в переменной среды PATH, чтобы предотвратить непредвиденное выполнение. Разработчикам следует перейти на версию Rust 1.77.2, чтобы устранить уязвимость

📌 **Обнаружение и отчётность**: Уязвимость была обнаружена инженером по безопасности из Flatt Security, известным как RyotaK, и передана в Координационный центр сертификации (CERT/CC).

📌 **Ответ от Rust:** Rust признала проблему и с тех пор улучшила надежность экранирующего кода и модифицировала командный API, чтобы возвращать ошибку InvalidInput, если аргумент не может быть безопасно экранирован

📌 **Реакция разработчиков других языков:** Разработчики Haskell, Node.js, PHP и yt-dlp выпустили исправления для устранения ошибки, связанной с внедрением команд

Уязвимости LG's WebOS / LG SmartTV

Исследователи из Bitdefender выявили множество уязвимостей в WebOS от LG, влияющих на различные модели смарт-телевизоров компании. Использование этих уязвимостей может позволить злоумышленникам получить несанкционированный root-доступ к устройствам.

Уязвимые версии и модели:

📌 Уязвимости затрагивают телевизоры LG, работающие под управлением WebOS версий с 4.9.7 по 7.3.1, в таких моделях, как LG43UM7000PLA, OLED55CXPUA, OLED48C1PUB и OLED55A23LA

Конкретные уязвимости:

📌 **CVE-2023-6317:** Позволяет обойти проверку PIN-кода и добавить профиль привилегированного пользователя без участия пользователя

📌 **CVE-2023-6318:** Позволяет повысить свои привилегии и получить root-доступ

📌 **CVE-2023-6319**: Позволяет внедрять команды операционной системы, манипулируя библиотекой для отображения музыкальных текстов

📌 **CVE-2023-6320**: Позволяет вводить команды, прошедшие проверку подлинности, используя com.webos.конечная точка API service.connectionmanager/tv/setVlanStaticAddress

Масштабы воздействия:

📌 Более 91 000 устройств были идентифицированы как потенциально уязвимые в Южной Корее, Гонконге, США, Швеции и Финляндии

Меры по устранению уязвимостей и действия пользователей:

📌 Компания LG выпустила исправления для этих уязвимостей, которые доступны в меню настроек телевизора в разделе "Обновление программного обеспечения"

📌 Пользователям рекомендуется включить автоматическое обновление ПО, чтобы обеспечить получение на свои устройства последних исправлений безопасности

Потенциальные риски:

📌 Эти уязвимости позволяют получить контроль над телевизором, получить доступ к конфиденциальным пользовательским данным и потенциально использовать скомпрометированное устройство как часть ботнета или для других вредоносных действий

Рекомендации по безопасности:

📌 Помимо применения последних обновлений встроенного ПО, пользователи должны использовать надежные уникальные пароли для своих устройств и защищать свои сети Wi-Fi, чтобы еще больше снизить риск их использования

Больше материалов: Boosty | Sponsr | TG

TA547 ФИШИНГОВАЯ КАМПАНИЯ

Фишинговая кампания TA547 с использованием Rhadamanthys stealer представляет собой эволюцию в тактике киберпреступников, в частности, благодаря интеграции сценариев, созданных с помощью ИИ.

Детали

📌**Имитация и содержимое электронной почты:** Фишинговые электронные письма были созданы для того, чтобы выдавать себя за немецкую компанию Metro AG, и сообщения, связанные со счетами. Эти электронные письма содержали защищённый паролем ZIP-файл, который при открытии запускал удалённый сценарий PowerShell

📌**Способ выполнения:** Скрипт PowerShell выполняется непосредственно в памяти, развёртывая Rhadamanthys stealer без записи на диск. Этот метод помогает избежать обнаружения традиционным антивирусным программным обеспечением

📌**Использование ИИ при создании вредоносных программ:** Есть явные признаки того, что скрипт PowerShell был создан или, по крайней мере, доработан с использованием большой языковой модели (LLM). Скрипт содержал грамматически правильные и очень специфичные комментарии, что нетипично для скриптов вредоносных программ, созданных человеком

TTPs

📌 **Инновационные приманки и методы доставки:** В рамках кампании также были опробованы новые тактики фишинга, такие как уведомления о голосовых сообщениях и встраивание изображений в формате SVG, для повышения эффективности атак по сбору учётных данных

📌**ИИ:** Использование технологий ИИ, таких как ChatGPT или CoPilot, при написании сценариев вредоносного ПО указывает на значительный сдвиг в тактике киберпреступности, предполагая, что киберпреступники все чаще используют ИИ для совершенствования своих методов атаки

📌**Последствия:** кампания не только подчёркивает адаптивность и техническую сложность TA547, но и подчёркивает тенденцию к внедрению инструментов ИИ в свою деятельность. Эта интеграция потенциально может привести к повышению эффективности и сложности обнаружения кибер-угроз

Рекомендации по защите

📌**Обучение сотрудников**: Организациям следует повысить уровень кибербезопасности, обучив сотрудников распознавать попытки фишинга и подозрительный контент электронной почты

📌**Технические меры предосторожности:** Внедрение строгих групповых политик для ограничения трафика из неизвестных источников и рекламных сетей может помочь защитить конечные точки от таких атак.

📌**Обнаружение, основанное на поведении:** Несмотря на использование искусственного интеллекта при разработке атак, механизмы обнаружения, основанные на поведении, остаются эффективными при выявлении и смягчении таких угроз

FBI IC3

Злоумышленники используют различные методы, включая фишинговые электронные письма с вредоносными вложениями, обфусцированные файлы сценариев и Guloader PowerShell, для проникновения в системы жертв и их компрометации. Мошенничество с выставлением счетов, форма взлома деловой электронной почты (BEC), является одним из популярных методов, используемых злоумышленниками для обмана жертв. В этом типе мошенничества третья сторона запрашивает оплату обманным путём, часто выдавая себя за законного поставщика

Мошенничество со счетами-фактурами представляет серьёзную угрозу для бизнеса, поскольку может привести к значительным финансовым потерям и непоправимому ущербу. Согласно отчёту ФБР IC3, в 2022 году атаки BEC нанесли ущерб жертвам в США на сумму 2,7 миллиарда долларов, что сделало их наиболее распространённой формой компрометации деловой электронной почты

Некоторые признаки мошеннических электронных счетов-фактур включают запросы на предоставление личной информации (PII), запросы на изменение банковской или платёжной информации, и счета-фактуры с необычными суммами. Кроме того, злоумышленники часто используют методы обфускации, чтобы обойти защиту и затруднить обнаружение своих вредоносных действий.

TELETRACKER

TeleTracker предлагает набор инструментов для анализа данных об угрозах, ориентированных на каналы Telegram, используемые во вредоносных целях. Его функции облегчают мониторинг и пресечение активных вредоносных кампаний, что делает его ценным ресурсом для специалистов в области кибербезопасности. Эти скрипты особенно полезны для аналитиков по анализу угроз или исследователей, стремящихся отслеживать, собирать и выслеживать злоумышленников, используя Telegram для C2-целей.

Особенности

📌**Просмотр сообщений канала и загрузка содержимого:** позволяет просматривать сообщения в канале и загружать содержимое непосредственно во вновь созданную папку "загрузки" в текущем рабочем каталоге. Программа поддерживает загрузку различных типов файлов, включая документы, фотографии и видео.

📌**Отправка документов через Telegram**: Пользователи могут дополнительно отправлять сообщения и документы через Telegram, поддерживая все типы файлов Telegram с автоматическим определением типа MIME.

📌**Выбор сообщения:** предоставляет возможность выбрать указанное количество сообщений или определённый идентификатор сообщения для загрузки, при этом загрузка всегда происходит от самого нового к самому старому сообщению.

📌**Сохранение логов:** сохраняет логи в удобном текстовом формате с основной информацией в файле с именем <имя_бота>.txt.

Больше материалов: Boosty | Sponsr | TG

Использование

📌 Чтобы отправить сообщение в Telegram-канал: python TeleTexter.py -t YOUR_BOT_TOKEN -c YOUR_CHAT_ID -m "сообщение"

📌 Для непрерывной отправки сообщений (рассылки спама) флаг --spam.

📌 TeleViewer.py это новейший инструмент, позволяющий пользователям просматривать и загружать все сообщения и медиафайлы из контролируемого Telegram-канала, контролируемого threat actor. Доступ к этой функции можно получить, выбрав цифру 6 в начальном меню после запуска TeleGatherer.py.

WSUS: ADCS ESC8 атака через MITM

Статья служит техническим руководством о том, как сочетание сетевого перехвата, MITM-атак и использования ADC-систем может привести к значительным нарушениям безопасности, подчёркивая необходимость принятия надёжных мер безопасности в сетевых конфигурациях и процессах обработки сертификатов.

📌 **Конфигурация и уязвимости WSUS:** В статье подробно описывается, как можно использовать сервер служб обновления Windows Server (WSUS), настроенный для работы по протоколу HTTP. Доступ к конфигурации протокола WSUS-сервера можно получить, запросив определённый раздел реестра. Эта настройка позволяет потенциально перехватывать трафик с помощью таких инструментов, как Wireshark, которые могут перехватывать связь между клиентами и сервером WSUS.

📌 **Выполнение MITM-атаки:** В основе атаки лежит подход "Человек посередине" (MITM), при котором злоумышленник перехватывает и ретранслирует запросы с клиентского компьютера на сервер WSUS. Во время этого процесса злоумышленник может манипулировать сообщениями, перенаправляя запросы на сторонний сервер или манипулируя ответами.

📌 **Эксплойт ADCS ESC8:** Перехваченное сообщение затем используется для проведения атаки на службы сертификации Active Directory (ADCS) ESC8. Это включает в себя передачу перехваченных запросов на веб-страницу регистрации Центра сертификации для запроса сертификата с использованием учётных данных скомпрометированного компьютера. Успешное выполнение этой атаки может позволить злоумышленнику получить несанкционированные сертификаты, которые могут быть использованы для дальнейших атак в сети.

📌 **Набор инструментов:** PKINITtools и скрипты для управления запросами Kerberos и их экспорта помогают извлекать и использовать учётные данные из перехваченного трафика для проверки подлинности с помощью ADC и запроса сертификатов.

📌 **Рекомендации по обеспечению безопасности:** Атака демонстрирует значительный риск для безопасности, связанный с использованием незащищённых протоколов (HTTP) для критически важной инфраструктуры, такой как WSUS и ADCS. В статье предполагается, что защита этих коммуникаций с помощью HTTPS и внедрение строгого контроля доступа и мониторинга могут снизить вероятность таких атак.

Разбитые мечты о ключах доступа

В статье представлен критический взгляд на реализацию и удобство использования ключей доступа, особенно в контексте WebAuthn (веб-аутентификации). Автор делится личным анекдотом, чтобы осветить проблемы, с которыми сталкиваются пользователи, что приводит к более широкой критике паролей доступа.

📌 **Личный опыт, связанный с отказом ключа доступа:** Автор начинает с личной истории, в которой его партнёр не смог получить доступ к своей домашней системе управления освещением, потому что с брелка Apple был удалён ключ доступа, который она использовала. Этот инцидент служит примером практических проблем, с которыми сталкиваются пользователи при использовании ключей доступа.

📌 **Критика эволюции WebAuthn:** Автор размышляет об их участии в WebAuthn, начиная с первых дней его существования. Они рассказывают о своем оптимизме и вкладе в работу рабочей группы WebAuthn, направленной на улучшение стандарта. Однако они выражают разочарование тем, как развивалась технология, особенно критикуя концепцию и реализацию паролей доступа.

📌 **Пароли доступа как инструмент блокировки платформы:** В статье утверждается, что пароли доступа, вместо того чтобы быть решением для безопасной и удобной аутентификации, стали для платформ средством привязки пользователей к своим экосистемам. Невозможность извлечения или экспорта учётных данных выделяется как существенный недостаток, приводящий к тому, что автор описывает как "долгосрочное заманивание пользователей в ловушку".

📌 **Проблемы, связанные с работой пользователей:** Автор делится негативным опытом своей партнёрши по работе с паролями доступа, отмечая, что она предпочитает вернуться к традиционным паролям из-за их простоты и надёжности. Это мнение разделяет автор, который неохотно признает, что менеджеры паролей обеспечивают лучший пользовательский опыт, чем пароли доступа.

📌 **Заключение и размышления:** В заключение автор выражает чувство разочарования в паролях доступа, предполагая, что первоначальное обещание безопасного и удобного для пользователя метода аутентификации было нарушено. Они намекают на иронию ситуации с выпуском новой версии своей библиотеки WebAuthn для Rust на фоне этих размышлений.

Lock Bit и конфиденциальные данные, украденные из больницы в Каннах во Франции

📌 LockBit является самой опасной программой-вымогателем в мире и несёт ответственность за значительное количество атак во Франции в период с апреля 2022 по март 2023 года.

📌 За этот период на LockBit пришлось 57% известных атак во Франции, что значительно выше, чем на его ближайшего конкурента, ALPHV.

Больше материалов: Boosty | Sponsr | TG

📌 Количество ежемесячных атак во Франции было крайне нестабильным, и большая часть этой волатильности приходилась на LockBit.

📌 Французская экономика достаточно велика, чтобы стать благодатной почвой для киберпреступников, и вполне возможно, что некоторые из филиалов LockBit решили специализироваться на атаках на французские объекты.

📌 В июле 2022 года оператор мобильной связи La Poste Mobile, принадлежащий французской почтовой компании La Poste, подвергся атаке программы-вымогателя LockBit, в результате которой была опубликована личная информация более полутора миллионов человек во Франции.

📌 В августе 2022 года злоумышленники потребовали 10 миллионов долларов после атаки программы-вымогателя на Center Hospitalier Sud Francilien (CHSF), больницу на 1000 коек недалеко от Парижа, что привело к сбоям в работе компьютерных систем и привело к тому, что пациентов пришлось отправлять в другое место, а операции были отложены.

📌 В середине ноября 2022 года французская оборонная и технологическая группа Thales подтвердила утечку данных, повлиявшую на контракты и партнёрские отношения в Малайзии и Италии, при этом злоумышленники использовали программу-вымогатель LockBit.

📌 В период с апреля 2022 по март 2023 года Франция занимала пятое место в мире по числу нападений, причём государственный сектор подвергался нападениям чаще, чем в аналогичных странах.

📌 Причины доминирования LockBit во Франции неясны, но это может быть связано со способностью группы использовать возможности за пределами Англосферы и возможностью того, что некоторые из её филиалов специализировались на атаках на французские объекты.

📌 LockBit работает по модели "Программа-вымогатель как услуга" (RaaS), при этом атаки осуществляются независимыми преступными группировками, называемыми "аффилированными лицами", которые платят банде LockBit 20% от получаемого ими выкупа.

📌 Истинное количество атак LockBit, вероятно, намного превышает количество известных атак, поскольку многие жертвы предпочитают заплатить выкуп, а не рисковать публикацией своих данных в даркнете.

📌 LockBit был связан с атаками на больницы, правительства и предприятия по всему миру, которые нанесли значительный ущерб тысячам жертв.

📌 Правоохранительные органы работают над пресечением деятельности LockBit, и несколько человек, предположительно связанных с бандой, были арестованы в Украине и Польше.

📌 Несмотря на эти усилия, LockBit продолжает действовать и совершать нападения, а предполагаемый лидер группы клянётся продолжать свою деятельность.

📌 Государственный департамент США объявил о денежном вознаграждении в размере до 15 миллионов долларов за информацию, которая может привести к выявлению ключевых лидеров группы вымогателей LockBit и аресту любого лица, участвующего в операции.

📌 С января 2020 года злоумышленники LockBit совершили более 2000 атак на жертв в США и по всему миру, что привело к дорогостоящим сбоям в работе и уничтожению или утечке конфиденциальной информации.

📌 Было выплачено более 144 миллионов долларов в качестве выкупа за восстановление после событий, связанных с программой-вымогателем LockBit.

📌 В ответ на требование о выкупе CHC-SV заявила: "Государственные учреждения здравоохранения никогда не платят выкуп перед лицом атак такого типа".

📌 Больница также пообещала уведомить пациентов и заинтересованные стороны, если банда вымогателей решит опубликовать какие-либо украденные данные.

📌 На момент подготовки настоящего отчёта от Каннской больницы не поступало никаких заявлений относительно якобы опубликованных данных.

Genzai - IoT инструментарий

Репозиторий Genzai на GitHub, разработанный umair9747, направлен на повышение безопасности Интернета вещей путём выявления связанных с IoT информационных панелей и сканирования их на наличие паролей по умолчанию и уязвимостей.

📌 **Назначение и функциональность:** Genzai предназначен для повышения безопасности устройств Интернета вещей путём идентификации информационных панелей Интернета вещей, доступных через Интернет, и сканирования их на наличие распространённых уязвимостей и паролей по умолчанию (например, admin:admin). Это особенно полезно для защиты административных панелей устройств автоматизации и других IoT-продуктов.

📌 **Fingerprint и сканирование:** инструментарий делает fingerprint с продуктов Интернета вещей, используя набор подписей из файла signatures.json. После идентификации продукта он использует шаблоны, хранящиеся в его базах данных (vendor-logins.json и vendor-vulns.json) для поиска паролей по умолчанию для конкретного поставщика и потенциальных уязвимостей.

📌 **Поддерживаемые устройства и функции:** По состоянию на последнее обновление, Genzai поддерживает снятие отпечатков пальцев с более чем 20 различных информационных панелей на базе Интернета вещей. В него также включены шаблоны для проверки на наличие проблем с паролями по умолчанию в этих информационных панелях. Кроме того, доступно 10 шаблонов уязвимостей, и в будущих обновлениях планируется расширить это число. Некоторые из устройств Интернета вещей, которые можно сканировать, включают беспроводные маршрутизаторы, камеры наблюдения, человеко-машинные интерфейсы (HMI), интеллектуальные системы управления питанием, системы контроля доступа в здания, климат-контроль, системы промышленной автоматизации, домашней автоматизации и системы очистки воды.

📌 **Обновления и контактная информация:** В репозитории указано, что Genzai является активно поддерживаемым проектом, в ближайшие обновления планируется добавить больше шаблонов уязвимостей.

Больше материалов: Boosty | Sponsr | TG

UserManagerEoP / CVE-2024-21447

Эксплойт UserManager EoP нацелен на уязвимость, идентифицированную как CVE-2023–36047, которая позже была отслежена как CVE-2024–21447 после дополнительных исправлений Microsoft.

Эксплойт UserManager EoP

📌 **Обнаружение уязвимости:** Эксплойт был обнаружен владельцем репозитория в прошлом году и влияет на работу службы UserManager в Windows.

📌 **Характер уязвимости:** Уязвимость заключается в том, что служба UserManager неправильно копирует файлы из каталога, которым может управлять пользователь, что приводит к повышению уровня привилегий (EoP).

📌 **Частичное исправление и повторное использование:** Изначально Microsoft обращалась только к аспекту записи в операции копирования файлов. Однако операция чтения продолжала выполняться с правами доступа NT AUTHORITY\SYSTEM, что не было защищено в первом обновлении.

📌 **Механизм эксплойта:** Эксплойт использует незащищённую операцию чтения для доступа к критически важным системным файлам, таким как SAM, SYSTEM и SECURITY hives, из теневой копии.

📌 **Текущее состояние:** Недавно корпорация Майкрософт полностью устранила уязвимость, и теперь она занесена в каталог под новым идентификатором CVE-2024-21447.

Анализ кода

В репозитории GitHub содержится код эксплойта, который демонстрирует, как манипулировать обработкой файлов службой UserManager для повышения привилегий.

📌 **Идентификация уязвимых операций:** код для идентификации и нацеливания на конкретную уязвимую операцию чтения, выполняемую UserManager.

📌 **Использование уязвимости**: скрипты или команды, которые манипулируют файловыми операциями для перенаправления или доступа к несанкционированным данным.

📌 **Использование системных привилегий:** Использование повышенных привилегий, полученных с помощью эксплойта, для выполнения несанкционированных действий, таких как доступ к системным файлам и настройкам или их изменение.

Архитектура NES консолей

Похоже, вы променяли захватывающий социальный мир на увлекательную область исследований игровых консолей? Что ж, давайте погрузимся в глубины вашей новообретённой одержимости под названием Super Nintendo Entertainment System (SNES).

Фабьен Англар, наш герой, тщательно проанализировал SNES, предложив нам трилогию статей, которые вполне могли бы заменить любое человеческое общение.

Во-первых, статья расскажет о картриджах для SNES, этих волшебных пластиковых блоках, которые, как ни странно, были не просто мечтой детей 90-х. Они были настоящим технологическим чудом со своим собственным оборудованием, включая такой необходимый чип для защиты от копирования CIC, который не мешал копировать и модифицировать игры направо и налево.

Затем автор отправит в историческое путешествие эволюции материнской платы SNES. За двенадцать лет было выпущено двенадцать версий, в каждой из которых количество чипов и компонентов сокращалось. Технологическое разнообразие

И давайте не будем забывать трогательную историю о тактовых генераторах SNES. Эти маленькие хронометристы позаботились о том, чтобы все работало как часы (каламбур вполне уместен). Ведь что такое игровая консоль без обеспечивающего точность ускоренных запусков инструментов?

Итак, вот она, трилогия статей, которая вполне может заменить общение между людьми. Кому нужны друзья, когда у вас есть сложные детали SNES, которые согреют вас ночью? Спасибо тебе, Фабьен Санглар, за то, что дал нам прекрасный повод отказаться от социальных обязательств в пользу исследований игровых консолей.

SNES картриджи:

Картриджи SNES были уникальны тем, что они могли включать в себя дополнительное оборудование, такое как чип защиты от копирования CIC, SRAM и процессоры повышения производительности, такие как «Super Accelerator 1» (SA-1). Эти процессоры значительно расширили возможности консоли, обеспечив улучшенную графику и игровой процесс. В нем рассказывается об эволюционных шагах, предпринятых Nintendo с материнской платой SNES для повышения эффективности и экономичности системы с течением времени.

Ключевые функции

📌 Материнская плата SNES претерпевала значительные изменения на протяжении всего производства, в первую очередь направленные на снижение сложности и стоимости системы.

📌 Изначально материнская плата содержала большое количество микросхем и компонентов, которые постепенно сокращались в более поздних версиях.

Уменьшение количества микросхем

Больше материалов: Boosty | Sponsr | TG

📌 Одним из главных достижений в разработке материнской платы SNES стало появление 1-CHIP версии. Эта версия объединила центральный процессор и два PPU (блока обработки изображений) в единую ASIC (специализированную интегральную схему), сократив общее количество микросхем на материнской плате до девяти.

📌 Это сокращение не только упростило конструкцию, но и потенциально повысило надёжность и производительность системы.

Версии материнских плат

📌 За 12 лет существования Nintendo выпустила двенадцать различных версий материнской платы для SNES.

📌 Эти версии включают в себя различные модели, такие как SHVC-CPU-01, SNS-CPU-GPM-01 и SNS-CPU-1CHIP-01, каждая из которых соответствует различным годам выпуска и особенностям дизайна.

📌 Версии разделены на четыре основных поколения: Classic, APU, 1-CHIP и Junior, причём 1-CHIP и младшие версии представляют собой наиболее значительные изменения в дизайне.

📌 Super Nintendo Jr (также известная как Mini) является окончательной версией SNES, в ней сохранено меньшее количество микросхем и более интегрированный дизайн, в котором на материнской плате больше нет частей, предназначенных для конкретных подсистем.

Эволюция материнской платы SNES:

За 12 лет своего существования Nintendo выпустила двенадцать версий материнской платы SNES, в каждой из которых количество чипов и компонентов было сокращено. Наиболее заметным достижением стала версия 1-CHIP, которая объединила центральный процессор и два блока питания в единый ASIC, упростив конструкцию и потенциально повысив производительность. Это проливает свет на технические чудеса и проблемы системы картриджей SNES, подчёркивая, как Nintendo использовала дополнительное оборудование в картриджах, чтобы расширить границы того, что было возможно в видеоиграх в ту эпоху

Усовершенствованные процессоры

📌 Картриджи SNES отличались способностью включать в себя не только игровые инструкции и ресурсы. Они также могли содержать дополнительные аппаратные компоненты, такие как микросхема защиты от копирования CIC, SRAM и процессоры повышения производительности.

📌 Эти усовершенствованные процессоры, такие как чип «Super Accelerator 1» (SA-1), значительно расширили возможности SNES. Чипом SA-1, который был найден в 34 картриджах, был процессор 65C816, работающий на частоте 10,74 МГц, что в четыре раза быстрее, чем у основного процессора SNES. Он также включал 2 Кбайт оперативной памяти и встроенный CIC.

Механизм защиты от копирования

📌 В SNES использовался механизм защиты от копирования, включающий два чипа CIC, которые взаимодействовали синхронно — один в консоли, а другой в картридже. Если CIC консоли обнаруживал несанкционированную игру, она перезагружала все процессоры в системе.

📌 Некоторые игры, такие как «Super 3D Noah’s Ark», обходили эту защиту, требуя, чтобы к ним подключался официальный картридж, используя для аутентификации официальный CIC игры.

Улучшения в игре

📌 Использование усовершенствованных процессоров позволило значительно улучшить производительность игры и графику. Например, чип SA-1 позволил SNES анимировать и обнаруживать коллизии для всех 128 спрайтов, доступных в PPU, преобразовывать спрайты на лету (поворачивать/масштабировать) и записывать их обратно в видеопамять (PPU VRAM).

📌 Ещё один усовершенствованный чип, Super-GFX, отлично справлялся с рендерингом пикселей и растеризацией полигонов, как правило, рендерингом в кадровый буфер, расположенный на картридже. Затем это содержимое переносилось в видеопамять в процессе VSYNC.

Региональная совместимость и возможность обхода

📌 В статье также рассматриваются меры, которые Nintendo использовала для обеспечения региональной совместимости, такие как различные формы картриджей и система блокировки CIC. Однако в статье упоминается, что эти меры не были надёжными и их можно было обойти.

Информация о сообществе и разработках

📌 В дискуссиях на таких платформах, как Hacker News, обсуждается влияние и потенциал этих картриджей, сравниваются их с другими инновациями Nintendo и обсуждаются технические проблемы и решения, связанные с дизайном SNES

Сердце SNES:

В SNES использовались два основных тактовых генератора для управления синхронизацией различных компонентов. Эти тактовые импульсы имели решающее значение для работы центрального процессора, PPU и APU. Система также включала в себя улучшающие чипы в некоторых картриджах, которые использовали эти тактовые частоты для дополнительной вычислительной мощности, примером чего является чип SuperFX, используемый в таких играх, как StarFox. Этот подробный обзор тактовой системы SNES раскрывает сложный дизайн и инженерные разработки, которые поддерживали сложные графические и звуковые возможности консоли, обеспечивая продвинутые игровые возможности в ту эпоху.

Тактовые генераторы

📌 Материнская плата SNES оснащена двумя основными тактовыми генераторами, расположенными в разъёмах X2 и X1.

📌 В разъёме X2 расположен керамический резонатор синего цвета с частотой 24,576 МГц. Этот резонатор имеет решающее значение для работы блока обработки звука (APU), задающего скорость обработки звука на SNES.

📌 Слот X1 содержит генератор с частотой 21,300 МГц, обозначенный жёлтым цветом D21L3. Этот генератор удобно расположен рядом с центральным процессором и блоком обработки изображений (PPU), тем самым задавая темп их работы.

Больше материалов: Boosty | Sponsr | TG

Микросхемы распределения тактовых импульсов и улучшения качества

📌 SNES использует эти основные тактовые импульсы в сочетании с разделителями для генерации дополнительных тактовых импульсов, необходимых различным компонентам. Например, процессор Ricoh 5A22 работает на частоте, составляющей 1/6 от основной тактовой частоты, в результате чего частота составляет 3,579545 МГц.

📌 Система включает в себя в общей сложности пятнадцать различных тактовых импульсов, что подчёркивает сложность управления синхронизацией в SNES.

📌 Линия SYS-CLK, работающая на частоте 21,47727 МГц, подключена к порту картриджа. Обычно такая настройка не требуется для основной работы картриджей, которые содержат ПЗУ с игровыми данными и инструкциями. Однако этот тактовый сигнал имеет решающее значение для картриджей, которые содержат собственные улучшающие процессоры, такие как чип SuperFX, используемый в таких играх, как StarFox.

📌 Эти усовершенствованные чипы могут использовать SYS-CLK для получения дополнительной вычислительной мощности, а некоторые чипы, такие как версия процессора SuperFX от MARIO, используют внутренний делитель для настройки тактовой частоты в соответствии с конкретными потребностями в обработке.

📌 Точность этих тактовых генераторов жизненно важна для детерминированного выполнения игрового кода, что особенно важно для таких приложений, как ускоренные запуски с помощью инструментов (TAS). Со временем точность керамических резонаторов может ухудшаться, что приводит к несоответствиям в производительности

Архитектура консолей

Серия книг Родриго Копетти «Архитектура консолей: практический анализ» погружает в увлекательный мир игровых консолей, раскрывая секреты их ошеломляющих технологий на тот момент технологий.

В своей серии автор отправляет нас в инженерное путешествие по эволюции консолей, показывая и доказывая, что они — это нечто большее, чем просто набор причудливых цифр. Эти книги, от Nintendo 3DS до серий Xbox и PlayStation, показывают, что каждая из консолей по-своему уникальна и особенна.

Итак, если вы готовы пожертвовать своей социальной жизнью ради глубокого погружения в завораживающий мир консольной архитектуры, книги Копетти — это то, что вам нужно. Это сокровищница технических знаний, идеальная для всех, кто когда-либо задавался вопросом, что заставляет эти волшебные коробки работать.

Эти книги входят в серию, посвящённую консольному архитектуре, и она структурирована аналогично другим работам посвящённым консолям PlayStation, Xbox и другим консолям. Это позволяет читателям, знакомым с архитектурами консолей, сравнить консоли бок о бок. Книги по архитектуре консолей предназначены для людей с базовыми знаниями в области вычислительной техники, которые интересуются эволюцией и внутренней работой игровых консолей. Его труды — это не руководства для разработчиков, а скорее подробное описание того, как каждая система работает внутри. Он пытается адаптировать свой контент для более широкой аудитории, чтобы даже те, кто не разбирается в компьютерных технологиях, могли найти ценность в его работе. Его книги ценятся как техническими, так и нетехническими читателями за глубокие, но доступные объяснения сложных архитектур консолей. Таким образом, его целевую аудиторию можно считать довольно широкой: от обычных читателей, интересующихся технологиями, до профессионалов игровой индустрии, компьютерных инженеров и энтузиастов консольных игр и аппаратного обеспечения.

Ещё несколько книг этого автора

📌 NES Architecture: More than a 6502 machine

📌 Game Boy Architecture

📌 Super Nintendo Architecture

📌 PlayStation Architecture

📌 Nintendo 64 Architecture

📌 GameCube Architecture

📌 Wii Architecture

📌 Nintendo DS Architecture

📌 Master System Architecture

Xbox Original

Если вы не знакомы с оригинальной версией Xbox Original, рекомендуется начать с чтения книги о консоли Xbox Original. Книга представляет собой углублённый взгляд на архитектуру консоли, уделяя особое внимание её уникальным функциям и технологическим инновациям, которые выделяют её от своих конкурентов. Книга начинается с обсуждения исторического контекста развития Xbox, отмечая, что Microsoft стремилась создать систему, которая была бы оценена по достоинству разработчиками и одобрена пользователями благодаря её знакомым возможностям и онлайн-сервисам.

📌 **Одна из основных тем, затронутых в книге, — процессор Xbox.** В консоли используется слегка модифицированная версия Intel Pentium III, популярного в то время серийного процессора для компьютеров, работающего на частоте 733 МГц. В книге исследуются последствия этого выбора и то, как он влияет на общую архитектуру Xbox.

📌 **В книге также рассматривается графика Xbox.** Он использует специальную реализацию Direct3D 8.0, которая была расширена за счёт включения функций, специфичных для Xbox. Это позволило разработчикам ПК портировать свои игры на Xbox с минимальными изменениями.

📌 **Экосистема разработки Xbox — ещё одна ключевая тема:** с оборудованием консоли взаимодействуют различные библиотеки и платформы. В книге представлен подробный анализ этой экосистемы, помогающий читателям разобраться в тонкостях разработки игр на Xbox.

📌 **Также обсуждается сетевая служба Xbox.** Xbox включал в себя подключение Ethernet и централизованную онлайн-инфраструктуру под названием Xbox Live, что в то время было инновационными функциями. В книге исследуется, как эти функции влияют на общую архитектуру Xbox.

📌 **Наконец, в книге также рассматриваются аспекты безопасности Xbox, включая систему борьбы с пиратством.** В нем объясняется, как работает эта система и как она вписывается в общую архитектуру консоли.

Краткая информация об оригинальной архитектуре Xbox

📌 В оригинальной Xbox использовалась привычная система для разработчиков и онлайн -сервисы для пользователей

📌 Процессор Xbox основан на Intel Pentium III с микроархитектурой P6

📌 Консоль имеет 64 Мб оперативной памяти DDR SDRAM, которая используется всеми компонентами совместно

📌 Графический процессор Xbox производится компанией Nvidia и называется NV2A

📌 Оригинальный контроллер Xbox, называемый Duke, был заменён на новую версию под названием ControllerS из-за критики

Xbox 360

Книга «Архитектура Xbox 360: Суперкомпьютер для всех нас» содержит всесторонний и серьёзный анализ архитектуры Xbox 360, в т. ч. её дизайн, возможности и технологические инновации, которые она представила, а также объясняет, как консоль работает внутри в буквальном и переносном смысле. Материал полезен для всех, кто интересуется развитием технологий игровых консолей, однако не ограничивается этой аудиторией. Книга входит в серию «Архитектура консолей: практический анализ», в которой рассматривается эволюция игровых консолей и их уникальные способы работы.

Книга начинается с краткой истории Xbox 360, которая была выпущена на год раньше её главного конкурента, PlayStation 3. В ней обсуждаются бизнес-аспекты процессора Xbox 360 и последовательность событий, которые привели к её разработке.

Затем автор углубляется в технические аспекты архитектуры Xbox 360, где обсуждается процессор консоли, который существенно отличается от одноядерного процессора, использовавшегося в оригинальной Xbox. Процессор Xbox 360, известный как Xenon, представлял собой трёхъядерный процессор, разработанный IBM. Каждое ядро могло обрабатывать два потока одновременно, что позволяло обрабатывать до шести потоков одновременно.

В книге также обсуждается графический процессор Xbox 360, известный как Xenos, который был разработан и изготовлен ATI. Графический процессор был основан на новой архитектуре и мог обеспечить производительность 240 гигафлопс. Графический процессор Xenos представил концепцию единого шейдерного конвейера, который объединил два разных выделенных конвейера для повышения производительности.

В книге далее обсуждается основная память Xbox 360, объем которой значительно увеличился по сравнению с 64 МБ оригинальной Xbox, что позволило запускать на консоли более сложные игры и приложения.

В книге также рассказывается об операционной системе Xbox 360, экосистеме разработки и сетевых службах. В нем обсуждается, как архитектура консоли была спроектирована так, чтобы быть гибкой и простой с точки зрения программирования, со сбалансированной аппаратной архитектурой, которая могла адаптироваться к различным жанрам игр и потребностям разработчиков.

К основным темам, затронутым в книге, относятся:

📌 **ЦП:** подробно рассматривается процессор Xbox, обсуждаются его уникальные особенности и его сравнение с процессорами других консолей. Им также обеспечивается исторический контекст, объясняя, как на конструкцию ЦП повлияли технологические тенденции и проблемы того времени.

📌 **Графика:** представлен подробный анализ графических возможностей Xbox, включая использование полунастраиваемой версии Direct3D 9 и то, как это повлияло на будущие версии Direct3D.

📌 **Безопасность:** обсуждается антипиратская система Xbox, объясняется, как она работает и какой вклад она вносит в общую архитектуру консоли.

📌 **Экосистема разработки:** исследуются сложности разработки игр для Xbox, обсуждает различные используемые библиотеки и платформы, а также то, как они взаимодействуют с оборудованием консоли.

📌 **Сетевая служба**: рассматриваются онлайн-возможности Xbox, обсуждается подключение Ethernet и онлайн-инфраструктура Xbox Live.

Краткие сведения об архитектуре Xbox 360

📌 Xbox 360 была выпущена на год раньше своего главного конкурента, PS3

📌 Центральный процессор Xbox 360, называемый Xenon, является многоядерным процессором, разработанным IBM

📌 В качестве графического процессора консоли используется частично адаптированная версия Direct3D 9, называемая Xenos

📌 Xbox 360 имеет унифицированную архитектуру памяти с 512 МБ оперативной памяти GDDR3

PlayStation 2

«Архитектура PlayStation 2» представляет собой углублённый анализ внутренней работы консоли PlayStation 2. Несмотря на то, что PlayStation 2 не была самой мощной консолью своего поколения, она достигла такого уровня популярности, который был немыслим для других компаний. В книге объясняется, что успех PlayStation 2 был обусловлен её Emotion Engine, мощным пакетом, разработанным Sony и работающим на частоте

~ 294,91 МГц. Этот набор микросхем содержал несколько компонентов, включая основной процессор и другие компоненты, предназначенные для ускорения определённых задач. В книге также обсуждается операционная система PlayStation 2, в которой для воспроизведения DVD и сжатия текстур высокого разрешения использовался блок обработки изображений (IPU). Также рассматривается экосистема разработки PlayStation 2: Sony предоставляет аппаратное и программное обеспечение для помощи в разработке игр.

Краткая информация об архитектуре PS2

📌 PlayStation 2 (PS2) была не самой мощной консолью своего поколения, но завоевала огромную популярность

📌 Сердцем PS2 является процессор Emotion Engine (EE), работающий на частоте ~ 294,91 МГц и содержащий множество компонентов, включая основной процессор

📌 Основным ядром является процессор, совместимый с MIPS R5900, с различными усовершенствованиями

📌 В PS2 используются модули VPU для расширения возможностей обработки данных

📌 Консоль имеет обратную совместимость с оригинальной PlayStation благодаря использованию процессора ввода-вывода (IOP).

📌 В PS2 был представлен контроллер DualShock 2, оснащённый двумя аналоговыми джойстиками и двумя вибромоторами

📌 Операционная система PS2 хранится на чипе ROM объёмом 4 МБ

PlayStation 3

«Архитектура PlayStation 3» предлагает всесторонний анализ внутренней структуры консоли PlayStation 3. В книге объясняется, что базовая аппаратная архитектура PlayStation 3 продолжает идеи Emotion Engine, фокусируясь на векторной обработке для достижения мощности, даже ценой сложности. Процессор PlayStation 3, Cell Broadband Engine, является продуктом кризиса инноваций и должен был идти в ногу с развитием тенденций в сфере мультимедийных услуг. В книге также обсуждается основная память PlayStation 3 и элемент синергетического процессора (SPE), которые представляют собой ускорители, включённые в ячейку PS3. PlayStation 3 также содержит чип графического процессора производства Nvidia под названием Reality Synthesizer или RSX, который работает на частоте 500 МГц и предназначен для разгрузки части графического конвейера.

Краткая информация об архитектуре PS3

📌 В PS3 основное внимание уделяется векторной обработке данных, что позволяет добиться высокой производительности даже ценой сложности

📌 Основным процессором PS3 является Cell Broadband Engine, разработанный совместно Sony, IBM и Toshiba

📌 Центральный процессор PS3 чрезвычайно сложен и оснащен мощным процессорным элементом (PPE) и несколькими синергетическими процессорными элементами (SPE)

📌 В PS3 используется графический процессор Reality Synthesizer (RSX) производства Nvidia

В книгах обсуждаются несколько заметных различий в архитектурах.

Xbox 360 и Xbox Original

📌 **Процессор:** оригинальный Xbox опирался на популярный стандартный процессор (Intel Pentium III) с небольшими изменениями. Это был одноядерный процессор с векторизованными инструкциями и сложной конструкцией кэша. С другой стороны, Xbox 360 представил новый тип процессора, не похожий ни на что, что можно было увидеть на полках магазинов. Это был многоядерный процессор, разработанный IBM, отражающий навязчивую потребность в инновациях, характерную для консолей 7-го поколения.

📌 **Графический процессор:** оригинальный графический процессор Xbox был основан на архитектуре NV20 с некоторыми модификациями для работы в среде унифицированной архитектуры памяти (UMA). Однако Xbox 360 использовал полунастраиваемую версию Direct3D 9 для своего графического процессора под названием Xenos.

📌 **Память:** оригинальный Xbox имел в общей сложности 64 МБ памяти DDR SDRAM, которая использовалась всеми компонентами системы. С другой стороны, Xbox 360 имел унифицированную архитектуру памяти с 512 МБ оперативной памяти GDDR3.

📌 **Экосистема разработки:** оригинальный Xbox был разработан с учётом особенностей, которые ценятся разработчиками, и онлайн-сервисов, приветствуемых пользователями. Однако Xbox 360 был разработан с упором на новый «многоядерный» процессор и нестандартный симбиоз между компонентами, что позволило инженерам решать неразрешимые проблемы с помощью экономически эффективных решений.

📌 **Сроки выпуска:** Xbox 360 была выпущена на год раньше своего главного конкурента, PlayStation 3, и уже заявляла о технологическом превосходстве над ещё не выпущенной PlayStation 3.

PS2 и PS3:

📌 **Процессор:** Emotion Engine для PS2 был разработан Toshiba с использованием технологии MIPS и ориентирован на достижение приемлемой производительности в 3D при меньших затратах. Напротив, процессор PS3, Cell Broadband Engine, был разработан в результате

сотрудничества Sony, IBM и Toshiba и представляет собой очень сложный и инновационный процессор, который сочетает в себе сложные потребности и необычные решения.

📌 **Графический процессор:** Графический синтезатор PS2 представлял собой графический процессор с фиксированной функциональностью, предназначенный для работы в 3D. Графический процессор PS3, Reality Synthesizer (RSX), был произведён Nvidia и был разработан для разгрузки части графического конвейера, предлагая лучшие возможности параллельной обработки.

📌 **Память:** PS2 имела 32 МБ RDRAM, а PS3 имела более продвинутую систему памяти: 256 МБ XDR DRAM для ЦП и 256 МБ GDDR3 RAM для графического процессора.

📌 **Экосистема разработки:** Экосистема разработки PS2 была основана на технологии MIPS и ориентирована на достижение приемлемой производительности 3D при меньших затратах. Экосистема разработки PS3 была более сложной и включала сотрудничество между Sony, IBM и Toshiba и была сосредоточена на создании мощной и инновационной системы.

📌 **Обратная совместимость:** PS2 была обратно совместима с играми для PS1 благодаря включению оригинального процессора PS1 и дополнительных аппаратных компонентов. PS3 также предлагала обратную совместимость с играми для PS2, но в более поздних версиях консоли это было достигнуто за счёт программной эмуляции.

PS2 и Xbox Original:

📌 **Процессор:** Emotion Engine для PS2 был разработан Toshiba с использованием технологии MIPS и ориентирован на достижение приемлемой производительности в 3D при меньших затратах. Напротив, процессор Xbox Original был основан на процессоре Intel Pentium III, который был популярным серийным процессором с небольшими изменениями.

📌 **Графический процессор:** Графический синтезатор PS2 представлял собой графический процессор с фиксированной функциональностью, предназначенный для работы в 3D. Графический процессор Xbox Original был основан на архитектуре NV20 с некоторыми модификациями для работы в среде унифицированной архитектуры памяти (UMA).

📌 **Память:** PS2 имела 32 МБ RDRAM, а Xbox Original включала в общей сложности 64 МБ DDR SDRAM, которая использовалась всеми компонентами системы.

📌 **Экосистема разработки:** Экосистема разработки PS2 была основана на технологии MIPS и ориентирована на достижение приемлемой производительности 3D при меньших затратах. Xbox Original был разработан с учётом особенностей, которые ценят разработчики, и онлайн-сервисов, приветствуемых пользователями.

PS3 и Xbox 360:

📌 **ЦП:** ЦП PS3, Cell Broadband Engine, представляет собой очень сложный и инновационный процессор, который сочетает в себе сложные потребности и необычные решения. Он был разработан в результате сотрудничества Sony, IBM и Toshiba. С другой стороны, процессор Xenon для Xbox 360 представлял собой процессор нового типа, не похожий ни на что, что можно было увидеть на полках магазинов. Он отражает навязчивую потребность в инновациях, характерную черту той эпохи.

📌 **Графический процессор:** графический процессор PS3, синтезатор реальности или RSX, был произведён Nvidia и был разработан для разгрузки части графического конвейера. Графический процессор Xenos Xbox 360 представлял собой полунастраиваемую версию Direct3D 9, в которой есть место для дополнительных функций Xenos.

📌 **Память:** Память PS3 была распределена по разным микросхемам памяти, и, хотя она не реализовала архитектуру UMA, она все равно могла распределять графические данные по разным микросхемам памяти, если программисты решат это сделать.

📌 **Экосистема разработки**: Экосистема разработки PS3 была основана на Cell Broadband Engine, совместном проекте Sony, IBM, Toshiba и Nvidia. Экосистема разработки Xbox 360 была основана на процессоре Xenon и полунастраиваемой версии Direct3D 9.

Содержание

Больше материалов: Boosty | Sponsr | TG

Left Over Locals

По иронии судьбы, та самая технология, которая поддерживает наши модели искусственного интеллекта и машинного обучения, теперь стала объектом новой уязвимости, получившей название "LeftoverLocals". Как сообщает Trail of Bits, этот недостаток безопасности позволяет восстанавливать данные из локальной памяти графического процессора, созданные другим процессом, и влияет на графические процессоры Apple, Qualcomm, AMD и Imagination

В документ приводится подробный анализ уязвимости "LeftoverLocals" CVE-2023–4969, которая имеет значительные последствия для целостности приложений с графическим процессором, особенно для больших языковых моделях (LLM) и машинного обучения (ML), выполняемых на затронутых платформах с графическим процессором, включая платформы Apple, Qualcomm, AMD и Imagination.

BitLockerBypass

Ещё один поучительный документ, который погружает в захватывающий мир взлома BitLocker. Этот анализ познакомит со множеством креативных способов взлома, от классических атак с "холодной загрузкой" — ведь кто не любит замораживать свой компьютер, чтобы украсть какие—то данные, - до использования очень надёжных микросхем TPM, на которых с таким же успехом может быть надпись "взломай меня".

Также рассмотрим некоторые уязвимости в ПО обеспечении, потому что Microsoft просто не была бы собой без них, например, возможность перехватить ключи дешифрования.

Итак, вне зависимости являетесь ли вы экспертом по ИБ, криминалистом или просто любознательным человеком в мире кибербезопасности, наслаждайтесь чтением и, возможно, сохраните резервную копию в надёжном месте.

Рубрика: Новичок

LEFT OVER LOCALS

Аннотация – в документ приводится подробный анализ уязвимости "LeftoverLocals" CVE-2023–4969, которая имеет значительные последствия для целостности приложений с графическим процессором, особенно для больших языковых моделях (LLM) и машинного обучения (ML), выполняемых на затронутых платформах с графическим процессором, включая платформы Apple, Qualcomm, AMD и Imagination.

Этот документ предоставляет ценную информацию для специалистов по кибербезопасности, команд DevOps, ИТ-специалистов и заинтересованных сторон в различных отраслях. Анализ призван углубить понимание проблем безопасности графических процессоров и помочь в разработке эффективных стратегий защиты конфиденциальных данных от аналогичных угроз в будущем.

A. Введение

Компания Trail of Bits раскрыла уязвимость под LeftoverLocals, которая позволяет восстанавливать данные из локальной памяти графического процессора, созданные другим процессом. Эта уязвимость затрагивает графические процессоры Apple, Qualcomm, AMD и Imagination и имеет значительные последствия для безопасности приложений на графических процессорах, особенно больших языковых моделях (LLM) и машинного обучения (ML), работающих на затронутых платформах.

Уязвимость позволяет злоумышленнику прослушивать интерактивный сеанс LLM другого пользователя несмотря на разграничения процессов и контейнеров., особенно в контексте LLMS и моделей ML, поскольку может привести к утечке конфиденциальных данных, участвующих в обучении этих моделей.

B. Уязвимая среда

Уязвимость LeftoverLocals может использоваться в различных средах, включая облачных провайдеров, мобильные приложения и даже при удалённых атаках.

- **Облачные провайдеры**: облачные провайдеры часто предлагают своим клиентам ресурсы графического процессора, которые используются совместно несколькими пользователями. В таких средах LeftoverLocals может быть использована при наличии доступа к тому же физическому графическому процессору, что и жертва. Это может позволить злоумышленнику восстановить данные из локальной памяти графического процессора, которые были созданы другим процессом, что приведёт к значительной утечке данных. Это особенно актуально для приложений, использующих LLM и ML для обработки данных.
- **Мобильные приложения**: Мобильные устройства, использующие уязвимые графические процессоры, также подвержены риску. Например, Apple признала, что такие устройства, как iPhone 12 и M2 MacBook Air, подвержены уязвимости LeftoverLocals..
- **Удалённые атаки**: LeftoverLocals потенциально можно использовать удалённо, когда злоумышленник скомпрометировал систему и получил возможность запуска пользовательского кода, либо в средах, где пользователи могут запускать пользовательские GPU вычислительных приложений.

C. Leftoverlocals в сравнении с другими уязвимостями

1) Leftoverlocals и другие GPU-уязвимости

Уязвимость LeftoverLocals отличается от других уязвимостей GPU прежде всего методом утечки данных через локальную память GPU. В отличие от многих уязвимостей, которые используют определённые программные или аппаратные ошибки, LeftoverLocals основана на неспособности графических процессоров полностью изолировать память между процессами. Это позволяет злоумышленнику запускать вычислительное приложение на графическом процессоре для чтения данных, оставленных в локальной памяти графического процессора другим пользователем.

Другие же уязвимости графического процессора могут быть нацелены на различные аспекты архитектуры или программного обеспечения графического процессора, такие как переполнение буфера, или эксплойты на уровне драйверов. Эти уязвимости часто требуют выполнения определённых условий или зависят от сложного взаимодействия программного и аппаратного обеспечения.

Утечка данных может быть достаточно существенной для восстановления моделей или ответов, что представляет значительный риск для конфиденциальности обрабатываемой информации.

Факторы критичности уязвимости LeftoverLocals:

- **Широкое воздействие**: Уязвимость затрагивает широкий спектр графических процессоров крупных производителей, таких как AMD, Apple, Qualcomm и Imagination Technologies.
- **Утечка данных**: например, на графическом процессоре AMD Radeon RX 7900 XT может

произойти утечка около 5,5 МБ данных за один вызов графического процессора, что может составлять около 181 МБ для каждого LLM-запроса. Этого достаточно для восстановления отклика LLM с высокой точностью.

- **Простота использования**: уязвимостью можно воспользоваться, просто запустив приложение для вычислений на графическом процессоре для чтения данных, оставленных в локальной памяти графического процессора другим пользователем.
- **Проблемы с устранением уязвимости**: Устранение уязвимости может оказаться трудным для многих пользователей. Одним из предлагаемых решений является изменение исходного кода всех ядер GPU, использующих локальную память, для сохранения 0 в любых ячейках локальной памяти, которые использовались в ядре до его завершения. Однако это может повлиять на производительность.
- **Раскрытие конфиденциальных данных**: Уязвимость актуальна в контексте ИИ и машинного обучения, где конфиденциальные данные часто используются при обучении моделей.

2) Leftoverlocals и другие CPU-уязвимости

Spectre и Meltdown являются уязвимостями ЦП, использующими атаки по "побочным каналам", которые включают извлечение информации из физической реализации компьютерных систем, а не программных ошибок. Spectre позволяет другим приложениям получать доступ к произвольным местоположениям в их памяти. Meltdown, с другой стороны, нарушает фундаментальную изоляцию между пользовательскими приложениями и операционной системой, позволяя приложению получать доступ ко всей системной памяти, включая память, выделенную для ядра.

Все три уязвимости серьёзны, поскольку могут привести к несанкционированному доступу к конфиденциальным данным. Однако они различаются по своему охвату и характеру данных, которые они могут раскрывать. LeftoverLocals в первую очередь влияет на приложения с графическим процессором и может привести к утечке данных из LLM и ML-моделей. Spectre и Meltdown, с другой стороны, потенциально могут раскрыть любые данные, обрабатываемые CPU, включая пароли, ключи шифрования и другую конфиденциальную информацию.

Потенциальные последствия уязвимостей:

- Они затрагивают почти все процессоры, выпущенные с 1995 года, что делает их влияние чрезвычайно распространённым.
- Они потенциально могут раскрыть любые данные, обрабатываемые центральным процессором, включая пароли, ключи шифрования и другую конфиденциальную информацию.
- Их трудно обнаружить, поскольку эксплуатация не оставляет никаких следов в традиционных файлах журналов.

3) Сходство признаков уязвимостей

LeftoverLocals имеет некоторое сходство с Spectre и Meltdown с точки зрения их последствий для безопасности:

- **Утечка данных**: как LeftoverLocals, так и Spectre / Meltdown допускают несанкционированный доступ к конфиденциальным данным. LeftoverLocals позволяет восстанавливать данные из локальной памяти графического процессора, в то время как Spectre и Meltdown используют спекулятивное выполнение ЦП для доступа к защищённой памяти.
- **Использование аппаратных возможностей**: Оба набора уязвимостей используют аппаратные возможности, предназначенные для оптимизации производительности.
- **Нарушение разграничения процессов**: оба механизмы обходят механизмы изоляции процесса для считывания данных на графических и центральных процессорах соответственно.
- **Влияние на нескольких поставщиков**: Обе уязвимости влияют на продукты нескольких поставщиков. LeftoverLocals влияет на графические процессоры Apple, Qualcomm, AMD и Imagination Technologies, в то время как Spectre и Meltdown влияют на процессоры Intel, AMD и ARM.
- **Смягчение последствий**: Устранение обеих уязвимостей является нетривиальным. LeftoverLocals может потребовать внесения изменений в код ядра GPU, в то время как Spectre и Meltdown потребовали сочетания обновлений микрокода, исправлений операционной системы и, в некоторых случаях, редизайна оборудования.
- **Скрытый характер атак**: Атаки, использующие эти уязвимости, трудно обнаружить, поскольку они не оставляют традиционных следов в файлах журналов, что затрудняет определение того, использовались ли они в реальных атаках.

D. Требования к эксплуатации LeftoverLocals

1) Общий доступ к графическому процессору

Для использования LeftoverLocals требуется общий доступ к графическому процессору, что является обычным сценарием в многопользовательских средах, где несколько пользователей или приложений могут использовать одни и те же физические ресурсы графического процессора. Например, на платформах облачных вычислений, в общих центрах обработки данных или в любой системе, где GPU-ресурсы динамически распределяются между различными пользователями или задачами. В таких средах локальная память графического процессора не всегда очищается между различными исполнениями ядра или между использованием разными процессами.

2) Модель "Listener-Writer"

Модель Listener-Writer — это метод, используемый для эксплуатации уязвимости LeftoverLocals. Эти программы взаимодействуют с локальной памятью графического процессора, чтобы продемонстрировать уязвимость.

Writer служит для преднамеренного сохранения определённых canary-значений в локальной памяти

графического процессора. Эти значения уникальны и идентифицируемы, они служат маркерами, которые могут быть обнаружены позже. Программа Writer не удаляет эти значения из локальной памяти после завершения своего выполнения.

Listener служит для чтения неинициализированной локальной памяти на графическом процессоре. Она сканирует локальную память в поисках значений canary, которые оставила программа записи. Если обнаруживает эти значения, это указывает на то, что локальная память не была должным образом очищена между выполнением разных программ.

3) Доступ к устройствам

Доступ к устройствам подразумевает определённый уровень доступа к ОС на целевом устройстве, чтобы воспользоваться уязвимостью. Этот доступ не обязательно должны быть root или администратор; это может быть любой уровень доступа, что позволяет злоумышленнику выполнить GPU-приложения.

В случае устройств Apple компания признала, что такие устройства, как iPhone 12 и M2 MacBook Air, подвержены уязвимости LeftoverLocals. Несмотря на то, что Apple выпустила исправления для своего новейшего оборудования, миллионы существующих устройств, использующих кремний Apple предыдущих поколений, остаются потенциально уязвимыми.

Qualcomm и AMD также подтвердили влияние уязвимости на свои графические процессоры и предприняли шаги по её устранению. Qualcomm выпустила исправления для прошивки, а AMD имеет подробные планы по предоставлению дополнительных улучшений

E. Технологический процесс и PoC

1) Модификация

Первым шагом является изменение кода ядра графического процессора для чтения и записи в локальную память графического процессора, что позволяет создать PoC для прослушивания интерактивного сеанса LLM другого пользователя.

2) Получение признаков LLM

Получение признаков модели включает идентификацию конкретной используемой LLM путём наблюдения за шаблонами использования памяти графического процессора LLM. Разные LLM будут иметь разные схемы использования памяти, и, наблюдая за этими шаблонами, злоумышленник может определить, какая LLM используется. Информация может быть использована для адаптации атаки к конкретному LLM, повышая шансы на успешное использование уязвимости.

3) Прослушивание выходных данных LLM

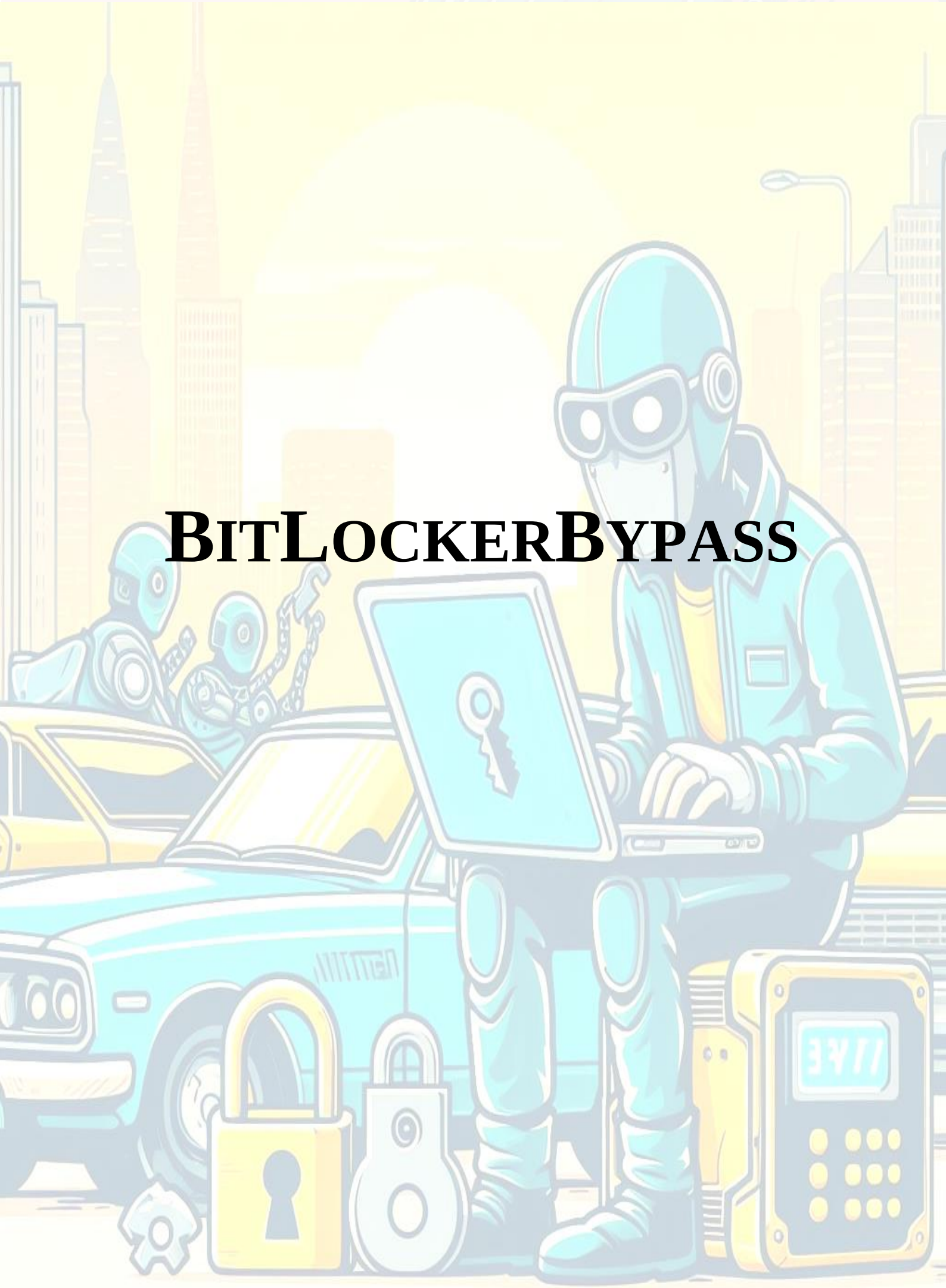
После получения признаков модели злоумышленник может начать прослушивание выходных данных LLM. Это включает в себя повторный запуск GPU-ядра, которое считывает данные из неинициализированной локальной памяти на графическом процессоре. Далее сканируется локальная память в поисках определённых значений, оставленных LLM. Их обнаружение указывает на то, что локальная память не была должным образом очищена между выполнением различных программ. Это позволяет восстановить данные из вычислений LLM.

4) PoC

PoC разработан с использованием фреймворка-OpenCL, фреймворка для выполнения на разнородных платформах для демонстрации ключевых особенностей:

- **Получение признаков модели**: PoC включает в себя идентификацию конкретной используемой LLM путём наблюдения за шаблонами использования GPU-памяти. Разные LLM имеют разные схемы использования памяти, по которым можно определить, какой LLM используется.
- **Прослушивание выходных данных LLM**: PoC включает повторный запуск GPU-ядра, которое считывает данные из неинициализированной локальной памяти на графическом процессоре. Злоумышленник сканирует локальную память в поисках определённых значений, оставленных LLM. Если эти значения обнаружены, это указывает на то, что локальная память не была должным образом очищена между выполнением различных программ, что позволяет злоумышленнику восстановить данные из вычислений LLM.
- **Утечка данных**: обнаружено что LeftoverLocals приводит к утечке ~5,5 МБ за каждый GPU-вызов на AMD Radeon RX 7900 XT, что при запуске модели 7B составляет около 181 МБ за каждый запрос LLM. Этой информации достаточно для восстановления ответа LLM с высокой точностью.
- **Обход механизмов изоляции процессов и контейнеров**: PoC демонстрирует, что злоумышленник может прослушивать интерактивный сеанс LLM другого пользователя в обход изоляции процесса или контейнера. Это показывает, что уязвимость может быть использована в многопользовательских средах, таких как платформы облачных вычислений, где несколько пользователей используют один и тот же физический графический процессор.
- **Доступ к устройствам**: PoC требует, чтобы злоумышленник имел доступ к целевому устройству. Это может быть любой уровень доступа, позволяющий злоумышленнику выполнять свои собственные вычислительные приложения на графическом процессоре.

BitLockerBypass



Аннотация – в документе представлен анализ метода, продемонстрированного в видео "Breaking Bitlocker - Bypassing the Windows Disk Encryption" с использованием недорогой аппаратной атаки, способной обойти шифрование BitLocker. Анализ будет охватывать различные аспекты атаки, включая технический подход, использование TPM-чипа и последствия для практики обеспечения безопасности.

Материал предоставляет информацию, которая может быть использована специалистами в области безопасности и других областей с целью понять потенциальные риски и принять необходимые контрмеры. Документ также особенно полезен экспертам по кибербезопасности, ИТ-специалистам и организациям, которые полагаются на BitLocker для защиты данных и подчёркивают необходимость постоянных оценок безопасности и потенциал аналогичных уязвимостей в других системах шифрования.

A. Введение

В видео "Breaking Bitlocker - Bypassing the Windows Disk Encryption" автор рассказывает о методе обхода шифрования диска Windows (BitLocker) с использованием различных атак, в том числе с использованием недорогого аппаратного решения. Показывается, как злоумышленник может использовать простое устройство для извлечения ключа шифрования из чипа TPM (Trusted Platform Module) компьютера, реализующего хранение ключа шифрования для BitLocker. В результате атаки злоумышленник сможет расшифровать жёсткий диск компьютера и получить доступ к данным, не зная пароля BitLocker.

В видео представлено:

- демонстрируется метод обхода BitLocker с использованием недорогой аппаратной атаки.
- нацеленность на чип TPM, который используется для хранения ключа шифрования BitLocker.
- даётся подробное объяснение атаки, включая задействованные аппаратные и программные компоненты.
- обсуждаются последствия этой атаки и предлагаются рекомендации по защите данных от данного типа атак.

B. Методология

Методология анализа BitLocker включает в себя несколько этапов:

- **Понимание технических деталей**: стартовой точкой выступает тщательное изучение технических аспектов BitLocker, включая его алгоритмы шифрования, механизмы управления ключами и функции безопасности, чтобы сформировать знание для выявления потенциальных уязвимостей.
- **Обзор исследований и литературы**: рассматриваются актуальные исследовательские работы, статьи и рекомендации по безопасности, связанные с BitLocker.
- **Демонстрация атаки в обход TPM**: даётся подробное объяснение атаки в обход TPM, включая необходимые аппаратные и программные компоненты с практической демонстрацией работы атаки с целью извлечения ключа шифрования из чипа TPM.
- **Анализ алгоритмов шифрования BitLocker**: анализируются алгоритмы шифрования BitLocker, включая AES и XTS-AES, и обсуждаются их сильные и слабые стороны. Также рассматриваются механизмы управления ключами BitLocker, и то, как они могут быть использованы злоумышленниками, что обеспечивает более глубокое понимание уязвимостей в BitLocker и помогает оценить значимость атаки.
- **Анализ уязвимостей**: на основе технического понимания, обзора литературы и практического тестирования выполняется комплексный анализ уязвимостей BitLocker с целью определения потенциальных векторов атак, использования уязвимостей и оценку влияния этих уязвимостей на безопасность BitLocker.
- **Практическое тестирование и эксперименты**: проводятся практические тесты и эксперименты для оценки эффективности функций безопасности BitLocker с использованием тестовых сред, имитации атак и анализа результатов для выявления потенциальных слабых мест.
- **Разработка контрмер и рекомендаций**: в заключении предлагаются контрмеры и рекомендации по устранению выявленных уязвимостей и повышению общей безопасности BitLocker, включающие рекомендации по настройке, обновления системы безопасности и

дополнительные меры для усиления защиты данных, зашифрованных с помощью BitLocker.

C. Причины возникновения атаки

Атака возможна из-за нескольких факторов:

- **Слабые алгоритмы шифрования**: BitLocker использует слабые алгоритмы шифрования, такие как AES-128 и XTS-AES, которые можно легко взломать с помощью атак методом перебора.
- **Плохая реализация BitLocker**: BitLocker плохо реализован, что делает его уязвимым для различных атак, включая атаку обхода TPM и атаку процесса загрузки.
- **Недостаточная осведомлённость о безопасности**: многие пользователи не осведомлены о рисках безопасности, связанных с BitLocker, и не предпринимают адекватных шагов для защиты своих данных.

Атака также возможна из-за доступности недорогих аппаратных устройств, которые можно использовать для обхода функций безопасности BitLocker.

С точки зрения аппаратного обеспечения эта атака возможна, поскольку шина LPC, связанная с обменом данными TPM, не зашифрована. Это означает, что злоумышленник, имеющий физический доступ к компьютеру, может легко отслеживать данные, которые передаются по шине.

D. Шина lpc

Шина LPC (Low Pin Count) – компьютерная шина, используемая на IBM-совместимых персональных компьютерах для подключения к материнской плате устройств с низкой пропускной способностью, таких как загрузочное ПЗУ, "устаревшие" устройства ввода-вывода (интегрированные в микросхему super I / O) и доверенный платформенный модуль (TPM).

1) Назначение шины LPC в TPM

Шина LPC — это низкоскоростная мультиплексируемая шина типа «точка-точка», которая используется для подключения устройств с низкой пропускной способностью к материнской плате. Шина LPC является устаревшей шиной и больше не используется в новых компьютерных системах.

Чип TPM — это аппаратный модуль безопасности, который используется для хранения криптографических ключей и выполнения криптографических операций. Шина LPC используется для отправки команд на микросхему TPM и получения ответов от неё. Ключевые детали:

- Шина LPC — это низкоскоростная шина, работающая на частоте 33 МГц.
- Шина LPC является мультиплексированной шиной, что означает, что она использует одни и те же провода для передачи данных в обоих направлениях.
- Шина LPC — это шина «точка-точка», что означает, что она соединяет только два устройства.
- Шина LPC является устаревшей шиной и больше не используется в новых компьютерных системах.

2) Возможности использования шины LPC в компьютерных системах

- Подключение устройств с низкой пропускной способностью к материнской плате, таких как загрузочное ПЗУ и ПЗУ BIOS
- Подключение устаревших устройств ISA к материнской плате
- Подключение TPM к материнской плате
- Подключение других устройств с низкой пропускной способностью к материнской плате, таких как последовательные и параллельные порты

3) Извлечение BitLocker

Чтобы извлечь ключ BitLocker из TPM с использованием шины LPC, злоумышленнику потребуется:

- **Получение физического доступа к компьютер**у. Выполняется путём кражи компьютера или получения доступа к нему с помощью социальной инженерии или другими способами.
- **Открытие корпуса компьютера и обнаружение чипа TPM**. Чип TPM обычно находится на материнской плате.
- **Подключение логического анализатора или другого аппаратного устройства к шине LPC**. Это позволяет злоумышленнику отслеживать данные, которые передаются по шине.
- **Загрузка компьютера и ожидание отправки ключа BitLocker по шине LPC**. Ключ BitLocker отправляется из чипа TPM в операционную систему при загрузке компьютера.
- **Извлечение ключа BitLocker с помощью логического анализатора или другого аппаратного устройства**. Как только ключ BitLocker будет извлечён, злоумышленник сможет использовать его для расшифровки диска, зашифрованного BitLocker.

4) Безопасность LPC

Фактически, шина LPC является потенциальным вектором атаки, который может быть использован для извлечения ключа BitLocker из чипа TPM.

Злоумышленник может использовать аппаратное устройство для подключения к шине LPC и отслеживания данных, которые передаются между чипом TPM и материнской платой компьютера. Эти данные включают ключ BitLocker.

Для защиты от этой атаки пользователям следует включить в BitLocker режим "только для доверенного модуля". Для этого режима требуется наличие и

функциональность чипа TPM для расшифровки диска, зашифрованного BitLocker. Это значительно затрудняет злоумышленнику извлечение ключа BitLocker из чипа TPM.

E. Перехват / Сниффинг TPM

1) Сниффинг TPM: взаимодействие Bootmgr с TPM в открытом режиме

Сниффинг TPM — это метод, который позволяет злоумышленнику извлечь ключ BitLocker из чипа TPM, отслеживая обмен данными между менеджером загрузки и чипом TPM. Это возможно, ввиду обмена данными в открытом виде (без шифрования) между диспетчером загрузки с чипом TPM.

2) Цель сниффинга TPM

Целью сниффинга TPM является извлечение ключа BitLocker из чипа TPM для расшифровки диска, зашифрованного BitLocker.

3) Как работает перехват TPM

Сниффинг TPM работает путём мониторинга связи между менеджером загрузки и чипом TPM. Эта связь осуществляется по шине LPC. Злоумышленник может использовать аппаратное устройство для подключения к шине LPC и мониторинга данных, которые передаются между диспетчером загрузки и чипом TPM.

Менеджер загрузки — это небольшая программа, которая отвечает за загрузку операционной системы. Когда компьютер включён, диспетчер загрузки попадает в память и начинает выполняться. Затем он загружает операционную систему в память и передаёт ей управление.

Диспетчер загрузки взаимодействует с чипом TPM. Это сообщение используется для проверки целостности процесса загрузки и загрузки ключа шифрования для диска, зашифрованного BitLocker.

Злоумышленник может использовать аппаратное устройство для подключения к шине LPC и отслеживания связи между диспетчером загрузки и чипом TPM. Это позволяет ему извлечь ключ шифрования для диска, зашифрованного BitLocker.

4) denandz/lpc_sniffer_tpm

LPC Sniffer TPM – проект с открытым исходным кодом и использовался для извлечения ключей BitLocker VMK путём прослушивания шины LPC, когда BitLocker был включён в конфигурации по умолчанию.

LPC Sniffer TPM – это аппаратное устройство, которое может использоваться для извлечения ключа BitLocker из чипа TPM путём прослушивания связи между менеджером загрузки и чипом TPM. Устройство подключается к шине LPC и отслеживает данные, которые передаются между диспетчером загрузки и чипом TPM.

a) Особенности LPC Sniffer TPM

- Считывание ввода-вывода и запись
- Чтение из памяти и запись
- Ошибки синхронизации

b) Использование LPC Sniffer TPM

- Изменить EEPROM FTDI и включить оптический режим на канале B.
- Запрограммировать lpc_sniffer.bin в ice40 с помощью iceprog lpc_sniffer.bin.

c) Подключение шину LPC.

- Извлечь данные LPC: python3 ./parse/read_serial.py /dev/ttyUSB1| tee outlog.
- Извлечь ключ из данных: cut -f 2 -d' outlog | grep '2...00$' | perl -pe 's/.{8}(..)..\n/$1/' | grep -Po "2c000000010000000320000(..){32}".

F. Демонстрация атаки обхода механизмов TPM

Атак с целью обхода механизмов TPM позволяет извлечь ключ шифрования, используемый BitLocker для шифрования данных на компьютере и в дальнейшем расшифровать жёсткий диск компьютера и получить доступ к данным, не зная пароля BitLocker.

Используемое в видео устройство подключается к материнской плате компьютера и позволяет злоумышленнику напрямую получить доступ к чипу TPM. Получив доступ к чипу TPM, можно извлечь ключ шифрования и использовать его для расшифровки жёсткого диска компьютера.

Далее приводится несколько примеров атак, которые могут быть скомбинированы для обхода BitLocker

1) Обход TPM

Атака нацелена на чип TPM, который является аппаратным компонентом, используемым для хранения ключа шифрования BitLockerСуществует несколько способов обойти TPM:

- **Физические атаки**: злоумышленник может физически удалить чип TPM с компьютера или использовать аппаратное устройство для прямого доступа к чипу TPM.
- **Атаки с использованием встроенного ПО**: злоумышленник может воспользоваться уязвимостями во встроенном ПО чипа TPM для извлечения ключа шифрования.
- **Программные атаки**: злоумышленник может использовать программный эксплойт для обхода чипа TPM и доступа к ключу шифрования.

2) Атака на процесс загрузки

Оказывая воздействие на процесс загрузки, злоумышленник в конечном счёте сможет расшифровать жёсткий диск компьютера.

Существует несколько способов изменить процесс загрузки:

- **Изменение загрузчика**: злоумышленник может изменить загрузчик, чтобы предотвратить загрузку BitLocker или загрузить вредоносную версию BitLocker.

- **Использование буткита**: злоумышленник может использовать буткит для изменения процесса загрузки и загрузки вредоносной версии BitLocker.
- **Использование уязвимостей в процессе загрузки**: злоумышленник может использовать уязвимости в процессе загрузки для обхода BitLocker.

3) Атаки по побочным каналам

Атаки по побочным каналам используют изначально недоступную информацию, но которая становится доступна в процессе шифрования или дешифрования. Анализируя эту информацию, злоумышленник потенциально может восстановить ключ шифрования.

Существует несколько типов атак по побочным каналам:

- **Временные атаки**: выполнение измерения время, необходимое для шифрования или дешифрования данных, и использовать эту информацию для восстановления ключа шифрования.
- **Атаки с анализом энергопотребления**: выполнение измерения энергопотребления компьютера в процессе шифрования или дешифрования и использовать эту информацию для восстановления ключа шифрования.
- **Электромагнитные атаки**: выполнение измерения электромагнитного излучения компьютера в процессе шифрования или дешифрования и использовать эту информацию для восстановления ключа шифрования.

4) Атаки методом "грубой силы"

Атака направлена на перебор возможных комбинаций пароля или ключа шифрования, пока не будет найдена правильная. Атаки методом перебора занимают много времени, но быть успешными, если пароль или ключ шифрования недостаточно надёжны.

G. Апробация

В видео проводится апробация для оценки эффективности функций безопасности BitLocker и анализ результатов для выявления потенциальных слабых мест.

1) Тестовые среды

Используются несколько тестовых сред для моделирования различных сценариев и конфигураций, что позволяет протестировать эффективность функций безопасности BitLocker в различных ситуациях, например, при загрузке компьютера с USB-накопителя или при отключении чипа TPM.

2) Имитация атак

Моделируются различные атаки на BitLocker, включая атаки методом перебора, атаки по побочным каналам и аппаратные атаки. Эти атаки предназначены для проверки надёжности алгоритмов шифрования BitLocker и механизмов управления ключами.

3) Анализ результатов

Этот анализ включает изучение времени, необходимого для взлома шифрования BitLocker, ресурсов, необходимых для проведения атаки, и влияния атаки на целостность данных.

4) Демонстрация атаки в обход TPM

Практическое тестирование и эксперименты, проведённые автором, предоставляют убедительные доказательства в поддержку аргумента о том, что BitLocker можно обойти с помощью относительно простой и недорогой атаки.

H. Программные и аппаратные компоненты атаки

1) Аппаратные компоненты:

a) Атака обхода TPM:

- Raspberry Pi 3 Модель B+
- Bus Pirate v3.6
- Провода Dupont
- Паяльник
- Припой

b) Атака на процесс загрузки:

- Флэш-накопитель USB
- Rufus
- Загрузочный дистрибутив Linux

2) Программные компоненты:

a) Атака в обход TPM:

- TPM2-Инструменты
- Python
- Scapy

3) Атака процесса загрузки:

- ПО для кастомизации GRUB
- Syslinux

4) Применение в атаках:

a) Атака обхода TPM:

- **Настройка оборудования**: подключение Raspberry Pi к разъёму TPM компьютера с помощью проводов Dupont.
- **Настройка программного обеспечения**: установка TPM2-Tools, Python и Scapy на Raspberry Pi.
- **Извлечение ключа шифрования**: использование TPM2-Tools для извлечения ключа шифрования из чипа TPM.

b) Атака на процесс загрузки:

- **Создание загрузочного USB-накопитель**: использование Rufus для создания загрузочного USB-накопителя с дистрибутивом Linux.
- **Изменение загрузчика**: использование GRUB Customizer, чтобы изменить загрузчик на USB-накопителе для загрузки вредоносной версии BitLocker.
- **Загрузка с USB-накопителя**: загрузка компьютера с USB-накопителя.

- **Расшифровка жесткого диска**: вредоносная версия BitLocker расшифровывает жесткий диск компьютера.

5) *Шаги по извлечению ключа BitLocker*

- Подключение Raspberry Pi к TPM-header. Использование провода Dupont для подключения выводов GPIO Raspberry Pi к разъёму TPM компьютера.
- Установка TPM2-Tools, Python и Scapy на Raspberry Pi с использованием авторских инструкций.
- Загрузка Raspberry Pi.
- Выполнение команды для извлечения ключа шифрования из чипа TPM: **python tpm2_extractkey.py -d /dev/tpm0 -o key.bin**
- Ключ шифрования будет сохранен в файле key.bin.

I. Последствия атаки

- **Потеря данных**: атака позволяет злоумышленникам расшифровать данные на компьютере жертвы и получить к ним доступ, включая личные файлы, финансовую информацию и коммерческие секреты. Это может привести к значительным финансовым потерям, репутационному ущербу и юридической ответственности жертвы.
- **Заражение вредоносным ПО**: злоумышленники могут использовать атаку для установки вредоносного ПО на компьютер жертвы, такого как программы-вымогатели, шпионское ПО или ботнеты. Это может дать удалённый контроль над компьютером жертвы, позволяя им красть данные, запускать атаки на другие системы или шпионить за действиями жертвы.
- **Отказ в обслуживании**: атака может быть превращена в атаку типа отказа в обслуживании компьютера жертвы, не позволяя ей получить доступ к своим данным или использовать свой компьютер в рабочих или личных целях. Это приведёт к потере производительности, финансовым потерям и репутационному ущербу.
- **Компрометация конфиденциальной информации**: атака может быть использована для компрометации конфиденциальной информации, такой как государственные секреты, военные планы или корпоративные коммерческие секреты. Это имеет серьёзные последствия для национальной безопасности, общественного спокойствия и экономической стабильности.

J. Контрмеры

Несколько контрмер и рекомендаций по устранению выявленных уязвимостей и повышению общей безопасности BitLocker:

- **Использование надёжного пароля BitLocker**: надёжный пароль затрудняет злоумышленнику принудительное использование ключа шифрования.
- **Включение дополнительных функций безопасности**: BitLocker предлагает несколько дополнительных функций безопасности, таких как двухфакторная аутентификация и безопасная загрузка, которые могут помочь защитить от атак.
- **Поддержание актуальности операционной системы и программного обеспечения компьютера**: обновления программного обеспечения часто включают исправления безопасности для защиты от уязвимостей.
- **Использование аппаратного TPM-чипа**: аппаратные TPM-чипы более безопасны, чем программные TPM-чипы.

1) *Предотвращение снифинга TPM*

Есть несколько вещей, которые можно сделать, чтобы предотвратить перехват TPM, в том числе:

- **Включение режима BitLocker "только для доверенного модуля"** значительно затрудняет извлечение ключа BitLocker из чипа TPM.
- **Поддержание операционной системы и встроенного ПО компьютера в актуальном состоянии** помогает защититься от уязвимостей, которые могут быть использованы для получения доступа к шине LPC.
- **Использование надёжного пароля или кодовой фразы для ключа шифрования BitLocker** затруднит злоумышленнику принудительное использование ключа шифрования.