Аннотация - В этом 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.

I. 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.

II. 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.

III. 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.

IV. 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).

A. 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.

B. 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

C. 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.

D. 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.

V. Перехват / Снифинг TPM

A. *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.

B. *Цель сниффинга TPM*

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

C. *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.

D. *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.

1) *Особенности LPC Sniffer TPM*

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

2) *Как использовать 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.
- *Подключить 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}".

VI. 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

A. *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.

B. *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.

C. *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.

D. *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.

VII. Апробация

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

A. *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.

B. *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.

C. *Анализ результатов*

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

D. *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.

VIII. Программные и аппаратные компоненты атаки

A. *Аппаратные компоненты:*

1) *Атака обхода TPM:*
   - Raspberry Pi 3 Модель B+
   - Bus Pirate v3.6
   - Провода Dupont
   - Паяльник
   - Припой
2) *Атака на процесс загрузки:*
   - Флэш-накопитель USB
   - Rufus
   - Загрузочный дистрибутив Linux

B. *Программные компоненты:*

1) *Атака в обход TPM:*
   - TPM2-Инструменты
   - Python
   - Scapy

C. *Атака процесса загрузки:*

- ПО для кастомизации GRUB
- Syslinux

D. *Применение в атаках:*

1) *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.
2) *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.

E. 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.

IX. 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.

X. 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.

A. Предотвращение сниффинга 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.