УДК 004.62

ИСПОЛЬЗОВАНИЕ УПРАВЛЯЮЩИХ ГРАФОВ ДЛЯ АНАЛИЗА ЭКСПЛОЙТОВ, НАЦЕЛЕННЫХ НА UEFI

Рябинин И.А. (ВКА)
Научный руководитель – кандидат технических наук, доцент Компаниец Р.И. (ВКА)

Введение. Эксплойты, нацеленные на модули UEFI (Unified Extensible Firmware Interface), представляют собой особую угрозу, поскольку они могут воздействовать на систему еще до загрузки операционной системы. Эти уязвимости часто связаны с неправильным использованием памяти, переполнением буфера и неконтролируемым доступом к привилегированным функциям. Знание таких уязвимостей и методов их эксплуатации является важным для обеспечения безопасности системы. Управляющие графы, являясь мощным инструментом анализа, позволяют изучить структуру и поток выполнения кода в модулях UEFI, что способствует глубокому пониманию работы эксплойтов и обнаружению уязвимостей. Рассмотрение возможностей использования управляющих графов для анализа и предотвращения атак на основе UEFI имеет важное практическое значение в контексте современных угроз информационной безопасности.

Основная часть. С помощью управляющих графов можно решить следующие задачи:

1. **Анализ эксплойтов, нацеленных на UEFI: уязвимости на уровне загрузчика.** Уязвимости, которые могут затронуть загрузчик системы, играют ключевую роль в эксплойтах, нацеленных на модули UEFI. Управляющие графы помогают выявить уязвимости, такие как неправильное использование памяти или переполнение буфера, которые могут быть использованы злоумышленниками для внедрения вредоносного кода до загрузки операционной системы. Такие уязвимости могут быть критическими, так как они позволяют обойти механизмы защиты, включая Secure Boot.
2. **Роль управляющих графов в анализе эксплойтов UEFI.** Управляющие графы играют важную роль в визуализации и анализе структуры кода в модулях UEFI. С их помощью можно отслеживать вызовы функций, переходы и уязвимости, которые становятся потенциальными точками входа для эксплойтов. Анализ управляющих графов позволяет детально исследовать, как эксплойты могут изменять состояние системы и обеспечивать её компрометацию.
3. **Примеры реальных эксплойтов, нацеленных на UEFI, и их анализ с помощью управляющих графов.** Примером могут служить атаки, использующие уязвимости в процессе загрузки или в драйверах оборудования, которые связаны с нарушением безопасности загрузчика или проверки подписей. Управляющие графы позволяют выявить цепочку операций, ведущих к эксплуатации уязвимости, и подробно рассмотреть, как злоумышленник может манипулировать кодом, чтобы осуществить эксплойт.
4. **Как управляющие графы помогают в понимании работы эксплойтов на уровне UEFI.** Управляющие графы позволяют исследовать весь путь эксплойта, начиная с его внедрения и заканчивая выполнением, выявляя взаимодействие между различными участками кода и данные, которые могут быть изменены. Это помогает исследователям лучше понять, как именно происходит эксплуатация уязвимости и какие взаимодействия могут быть использованы для дальнейших атак.

5. **Методы предотвращения атак на базе управляющих графов.** Применение управляющих графов помогает не только анализировать уязвимости, но и разрабатывать меры защиты от атак. Например, с их помощью можно выявить уязвимые участки кода и спроектировать контрмеры, такие как улучшенные механизмы проверки целостности и подписей, а также внедрение защитных технологий, таких как Secure Boot и аппаратная защита с использованием TPM. Управляющие графы могут быть использованы для мониторинга системы и своевременного выявления аномальной активности на стадии загрузки.
6. **Перспективы использования управляющих графов для обнаружения новых типов атак.** С развитием технологий и новыми типами атак, использование управляющих графов открывает возможности для более глубокой аналитики и предотвращения угроз. Это позволит выявлять ранее неизвестные эксплойты, которые используют уязвимости в новых версиях UEFI или в аппаратных компонентах, и разрабатывать новые методы защиты, адаптированные к современным угрозам.
7. **Обзор инструментов для анализа эксплойтов с помощью управляющих графов.** В исследовании используются такие инструменты, как IDA Pro, Ghidra, UEFI Tool и другие, которые помогают создавать управляющие графы и анализировать код на уровне UEFI. Эти инструменты помогают исследователям выявлять эксплойты и уязвимости, а также оптимизировать процесс анализа и разработки защитных мер.

Выводы. В работе рассмотрено использование управляющих графов для анализа эксплойтов, нацеленных на UEFI. Описаны методы и подходы, которые позволяют выявить уязвимости и разработать методы защиты на основе анализа управляющих графов.

Список использованных источников:

1. Саркисян А.А. Машинонезависимая оптимизация исходных программ. – М.: Наука, 2018.
2. Матросов А. Руткиты и Буткиты: Обратная разработка программ. – М.: Издательство "Кибербезопасность", 2020.