Неделя кибербезопасности

CYBER FOX

12:00 19.04
онлайн

Crypto Hacker Handbook: Hunting Bugs in Blocks

***Карстен Ноль**, Главный эксперт, SRLabs*

Love it or hate it, crypto has become a playground for techies. As a side effect, the chains fuel criminal ecosystems.Drawing from several hundred bugs, we identified five common blockchain bug types. We discuss the potential impact of each and provide practical tips for finding them. To help you get started, we released a suite of fuzzers.

19:00 21.04
онлайн

Методы фаззинга: от случайных данных к структурированному тестированию

***Роланд Сако**, преподаватель в Университете прикладных наук Западной Швейцарии*

Что нужно, чтобы «ломать» софт умным способом? На этом мастер-классе вы убедитесь, что фаззинг — это не только для экспертов. Когда понимаешь базовые идеи, он оказывается на удивление доступным. Мы пройдем путь от простейших случайных входных данных до более умных мутаций с учётом структуры. Вы научитесь создавать собственные фаззеры, писать или использовать эффективные мутаторы и работать с такими инструментами, как AFL и libFuzzer. Мы также обсудим несколько ключевых тем, включая фаззинг с учётом покрытия, грамматики для мутаций и фаззинг без перезапуска процесса. Цель этого мастер-класса — сделать мир фаззинга понятным и открытым, показать, что начать проще, чем кажется. Будь вы новичком или хотите углубить знания — вы получите ясное представление осовременных техниках и о том, как применять их на практикто нужно, чтобы «ломать» софт умным способом? На этом мастер-классе вы убедитесь, что фаззинг — это не только для экспертов. Когда понимаешь базовые идеи, он оказывается на удивление доступным. Мы пройдем путь от простейших случайных входных данных до более умных мутаций с учётом структуры. Вы научитесь создавать собственные фаззеры, писать или использовать эффективные мутаторы и работать с такими инструментами, как AFL и libFuzzer. Мы также обсудим несколько ключевых тем, включая фаззинг с учётом покрытия, грамматики для мутаций и фаззинг без перезапуска процесса.

19:00 22.04
онлайн

Так ли проста стековая канарейка?

***Мария Недяк**, Разработчик KasperskyOS, АО Лаборатория Касперского*

Стековая канарейка считается одним из самых простых харденингов системы, которую все знают, как атаковать. Но мало кто знает, как сделать канарейку максимально устойчивой к этим атакам. Как реализовать стековую канарейку, сделав выводы из реализаций в других системах и их эволюции? Разберемся, как канарейка защищает от атаки переполнения стека и так ли она проста, как кажется на первый взгляд. Рассмотрим реализации стековых канареек юзерспейса различных операционных систем. Ответим на вопросы «Какой должна быть канарейка в 2025 году?» и «Можно ли полагаться только на стековую канарейку при митигировании атак переполнения стека?».

Неделя кибербезопасности

CYBER FOX

19:00 23.04
онлайн

(Не)Доверенные мобильные платформы: обзор, тренды

***Александр Козлов**, Ведущий эксперт, АО Лаборатория Касперского*

Все чаще мы слышим про утечки пользовательских данных с их мобильных устройств. Уже никого не удивляет, что подготовленный злоумышленник может прослушивать наши телефонные переговоры и читать переписку в мессенджерах и соцсетях. Ответом на это является создание доверенной мобильной платформы - системы, безопасность которой обеспечена by design, а пользовательские данные надежно защищены от компрометации. Но насколько такое изделие возможно создать в реальности?В докладе будет разбираться:из каких технических компонентов состоит современный мобильный телефон и как они влияют на его безопасностькак устроены потоки данных современного телефона, какие возможности есть у злоумышленников по их компрометациикакие технические требования есть к доверенному мобильному, как их можно реализовать на практике, и как снизить связанные риски ИБ

19:00 24.04
онлайн

Введение в аппаратные атаки: от теории к практике

***Сергей Ануфриенко**, Руководитель группы анализа защищенности, АО Лаборатория Касперского*

В современном мире нас окружают устройства, оснащенные процессорами и программным обеспечением различной сложности. Проблема их аппаратной безопасности становится все более актуальной.Исторически производители микросхем и разработчики встроенного ПО уделяли недостаточно внимания аппаратной защите устройств, что облегчало исследователям поиск уязвимостей и извлечение прошивок. Однако технический прогресс привел к усилению защитных механизмов и росту внимания производителей к аппаратной безопасности.Несмотря на это, атаки по побочным каналам остаются эффективным методом исследования защищенных устройств. Доклад рассматривает практические аспекты аппаратных атак, включая анализ энергопотребления, электромагнитные и glitch-атаки. Особое внимание уделяется используемому оборудованию и подготовительным этапам, от идентификации критических точек до точной синхронизации помех.Также рассматриваются эффективные аппаратные и алгоритмические методы защиты. Доклад рассчитан на специалистов по информационной безопасности, разработчиков аппаратных решений и исследователей, интересующихся вопросами защиты и анализа устройств.

17:30 25.04
очно
НИЯУ МИФИ

Ghidra - жизнь после IDA

***Илья Пугачев**, старший преподаватель кафедры «Компьютерной и Информационной безопасности» (КиИБ) РТУ МИРЭА*

Интерактивный дизассемблер IDA долгое время был и остается стандартным программным обеспечением для профессионального реверса ПО. С 2019 года в открытом доступе появилось средство Ghidra, разработанное NSA. Через 6 лет после начала поддержки данного решения сообществом реверсистов остается открытым вопрос стоит ли переходить на этот продукт? Что ждёт специалиста после десятилетий работы в IDA при переходе на дизассемблер Ghidra? Автор доклада много лет работал в IDA, а последние три года плотно работает в Ghidra. Особенностям работы, трудностям перехода и мнением о том, насколько это в целом целесообразно - посвящён этот доклад.

Церемония награждения победителей CryptoFox 2025