CHIP DVD ПРОГРАММЫ, КЛЮЧИ ДЛЯ АНТИВИРУСОВ

LIBREOFFICE

CHIP DVD 11 2015

БЕСПЛАТНЫЙ ОФИСНЫЙ ПАКЕТ

+135 ПОЛЕЗНЫХ ПРОГРАММ

ЛИЦЕНЗИОННЫЕ КЛЮЧИ ДЛЯ АНТИВИРУСОВ KASPERSKY eset

МУЖСКОЙ ЖУРНАЛ О ТЕХНОЛОГИЯХ

CHIP

11/2015

КАК БЫСТРО И ПРОСТО

УСКОРИТЬ WI-FI

ГЛАВНЫЕ ВЗЛОМЫ 2015

Старое «железо» ЛУЧШЕ НОВОГО

ТЮНИНГ КОМПЬЮТЕРА, НОУТБУКА, СМАРТФОНА

НЕМЕЦКИЙ

КОНКУРЕНТ TESLA

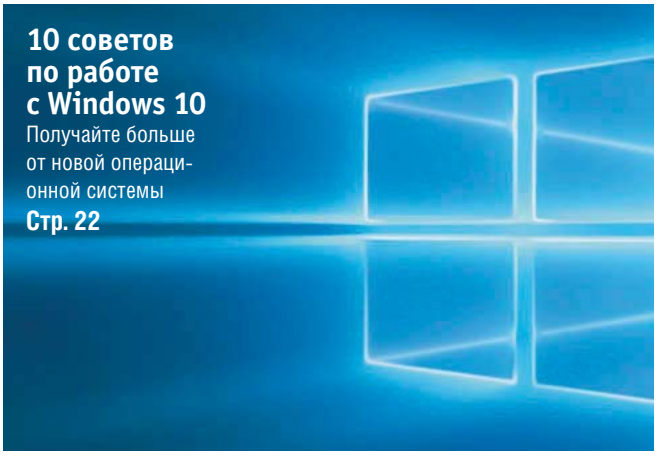
БОЛЬШЕ ИНФОРМАЦИИ НА ichip.ru CHIPRussia CHIPRussia

ISSN 1609-4212

Содержание

Главные взломы года
Смартфоны, банковские карты, автомобили — что еще взломали на хакерской конференции Black Hat?
Стр. 8

10 советов по работе с Windows 10
Получайте больше от новой операционной системы
Стр. 22



ТРЕНДЫ

Немецкий конкурент Tesla
Мы протестировали новый электрический Mercedes
Стр. 14

ТЕСТЫ

135 ПРОГРАММ НА CHIP DVD

Содержание DVD

Старое «железо» лучше нового
Пять самых распространенных системных «тормозов» — быстрое решение!
Стр. 62

ПРАКТИКА

Больше скорости для домашнего Wi-Fi
Всего несколько несложных шагов — и сеть Wi-Fi будет работать быстро и устойчиво по всей квартире
Стр. 58

ОБЛОЖКА: компании-производители; HBO/ZUMAPRESS.com/Russian Look
СЛОВО РЕДАКТОРА: компании-производители
ФОТО: компании-производители; HBO/ZUMAPRESS.com/Russian Look; Steve Marcus/Reuters; rightcameraman/Fotolia.com

CHIP
Журнал информационных технологий
ISSN 1609-4212
Выходит ежемесячно. 11'2015 (200)
(Подписной месяц — октябрь)

И. О. ГЛАВНОГО РЕДАКТОРА	**Максим Амелин**, m.amelin@burda.ru
ВЫПУСКАЮЩИЙ РЕДАКТОР	**Юлия Соболева**, yu.soboleva@burda.ru
РУКОВОДИТЕЛЬ ТЕСТОВОЙ ЛАБОРАТОРИИ	**Роман Ларионов**, r.larionov@burda.ru
РЕДАКТОРЫ	**Андрей Киреев**, a.kireev@burda.ru
	Наталья Романенко, n.romanenko@burda.ru
	Алексей Мирошниченко, a.miroshnichenko@burda.ru
	Сергей Суслов, s.suslov@burda.ru
ЛИТЕРАТУРНЫЙ РЕДАКТОР	**Полина Корягина**, p.koryagina@burda.ru
АРТ-ДИРЕКТОР	**Анна Бондарь**, a.bondar@burda.ru
ДИЗАЙНЕР	**Андрей Баранов**, a.baranov@burda.ru
АССИСТЕНТ РЕДАКЦИИ	**Дарья Литвинова**, d.litvinova@burda.ru
ОТДЕЛ РЕКЛАМЫ (495) 787-33-91	
ДИРЕКТОР ПО РЕКЛАМЕ (495) 787-94-01	**Александр Руднев**, rudnev@burda.ru
ДИРЕКТОР ПО КОРПОРАТИВНЫМ ПРОДАЖАМ	**Христос Христоу**, c.christou@burda.ru
ЗАМ. ДИРЕКТОРА ПО КОРПОРАТИВНЫМ ПРОДАЖАМ	**Сурен Хачиян**, s.khachiyan@burda.ru
ДИРЕКТОР ПО ИНТЕГРИРОВАННЫМ ПРОДАЖАМ	**Светлана Гайдукова**, s.gaydukova@burda.ru
МЕНЕДЖЕР ПО РЕКЛАМЕ	**Сергей Вербицкий**, verbitskiy@burda.ru
МЕНЕДЖЕР ПО РЕКЛАМЕ	**Вера Семенова**, v.semenova@burda.ru
КООРДИНАТОР ПЕЧАТИ РЕКЛАМЫ (495) 797-42-80	**Алексей Матвеев**, a.matveev@burda.ru
РЕКЛАМА В ДРУГИХ СТРАНАХ:	
BURDA INTERNATIONAL	
ITALY	**Mariolina Siclari**, International Advertising Sales Director, T. +39 02 91 32 34 66, mariolina.siclari@burda.com
BURDA COMMUNITY NETWORK	
GERMANY	**Vanessa Noetzel**, T. +49 89 9250 3532, vanessa.noetzel@burda.com **Michael Neuwirth**, T. +49 89 9250 3629, michael.neuwirth@burda.com
AUSTRIA/SWITZERLAND	**Goran Vukota**, T. +41 44 810 21 46, goran.vukota@burda.com
FRANCE/LUXEMBOURG	**Marion Badolle-Feick**, T. +33 1 72 71 25 24, marion.badolle-feick@burda.com
UK/IRELAND	**Jeannine Soeldner**, T. +44 20 3440 5832, jeannine.soeldner@burda.com
USA/CANADA/MEXICO	**Salvatore Zammuto**, T. +1 212 884 48 24, salvatore.zammuto@burda.com
СТАРШИЙ БРЕНД-МЕНЕДЖЕР	**Светлана Федорова**, s.fedorova@burda.ru
БРЕНД-МЕНЕДЖЕР	**Василиса Тарунова**, v.tarunova@burda.ru
ОТДЕЛ РАСПРОСТРАНЕНИЯ (495) 797-45-60 (доб. 33-32)	vertrieb@burda.ru
ИЗДАТЕЛЬСКИЙ ДИРЕКТОР	**Денис Седякин**, d.sedyakin@burda.ru

Учреждено и издается ЗАО «Издательский дом «Бурда»
Адрес издателя: Россия, 127018, г. Москва, ул. Полковая, д. 3, стр. 4
Адрес в Интернете: burda.ru
Адрес редакции: Россия, 127018, г. Москва, ул. Полковая, д. 3, стр. 4
Телефон: (495) 797-45-60 (доб. 30-10), факс: (495) 787-05-88
E-mail: chip@burda.ru
Для писем: 127521, г. Москва, а/я 68 «CHIP»

Журнал зарегистрирован в Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия. Свидетельство о регистрации ПИ №ФС77-28958 от 20 июля 2007 г.

Информационная продукция для читателей старше 16 лет.

ПОДПИСКА
Подписной индекс 60500 в каталоге «Почта России»
Подписной индекс 18164 в каталогах «Пресса России» и «Роспечать»
Телефон отдела подписки: (495) 660-73-69
E-mail: abo@burda.ru
Адрес в Интернете: burda.ru/subs

РАСПРОСТРАНЕНИЕ И ПОДПИСКА В ДРУГИХ СТРАНАХ
Беларусь
ООО «РЭМ-Инфо», г. Минск, тел.:+375 (17) 297-92-75, 297-92-74, 297-92-69
ООО «Росчерк», г. Минск, тел.:+375 (17) 331-94-27, 331-94-72, 331-94-41
Подписной индекс 60500 в каталоге «Белпочта»

Германия
DMR Rusexpress GmbH, Atriumstr. 4, 04315 Leipzig
Адрес в Интернете: www.pressa.de; www.mini-abo.eu
Тел.:+49 (341) 68706-0, факс:+49 (341) 68706-10

Казахстан
Подписной индекс 44087 в каталоге «Казпочта»

ТИПОГРАФИЯ: 143405, Московская область, Красногорский р-он, п/о «Красногорск-5», Ильинское шоссе, 4 км

ДАТА ВЫХОДА В СВЕТ: 22.10.2015

ТИРАЖ: 40 000 экз.*

ЦЕНА: свободная
*Отпечатанный тираж

BurdaInternational

Самые интересные события ноября

Самые ожидаемые новинки игрового мира и киноиндустрии, актуальные события, а также интересные мероприятия, которые непременно стоит посетить.

КИНО
12 ноября

«Стив Джобс»

Биографическая драма о легенде IT-индустрии Стиве Джобсе. На этот раз гениального предпринимателя сыграет не Эштон Кутчер, а Майкл Фассбендер, причем последний, на наш взгляд, лучше подходит на роль протагониста. Кинокартина базируется на трех самых значимых презентациях компании Apple и охватывает 16 лет жизни Джобса.

ИГРЫ
3 ноября

Need for Speed

Новая Need For Speed — это полная перезагрузка гоночной франшизы от Electronic Arts. Помимо фотореалистичной графики игра получит гибкую систему прокачки автомобилей и позволит геймерам создавать уникальные стритрейсинговые болиды. Территория игрового мира будет в два раза превосходить предыдущую NFS Rivals.
Платформы: PC, PS, XONE

КИНО
6 ноября

«007: Спектр»

Двадцать четвертый фильм о суперагенте Джеймсе Бонде. Зашифрованное послание из неизвестного источника приводит Бонда к глобальной организации «СПЕКТР», вынашивающей зловещие планы. Чтобы разоблачить врага, спецагенту в очередной раз придется использовать смекалку вкупе с высокотехнологичными гаджетами.

ИГРЫ
17 ноября

Star Wars: Battlefront

Одна из самых ожидаемых новинок осени, Star Wars: Battlefront, построена на движке Frostbite 3, благодаря которому графика в игре будет максимально реалистичной, а окружение — полностью разрушаемым. Поклонники самой известной космической саги смогут с головой окунуться в целый ряд героических моментов и захватывающих боевых эпизодов любимого фильма. Кроме того, данная игра получит полный русский перевод.

Знакомьтесь, злоумышленник

Каждый год на конференции Black Hat ведущие хакеры делятся новейшими методами атак.

Главные взломы года

Неважно где — в автомобилях, смартфонах, оружии или дронах — большинство систем безопасности нынешние хакеры обходят с легкостью.

На конференцию Black Hat, которую основал хакер с 25-летним стажем Джефф Мосс, съезжаются IT-эксперты со всего мира, и в этом году число гостей составило 9000 человек. Они обсуждают новейшие методы хакерских атак и слабые места безопасности. Порой здесь делятся инсайдерской информацией о специальных методах защиты, используемых секретными службами. А бывает и так, что авторы многообещающих докладов отказываются выступать буквально за несколько часов до начала.

ФОТО: компании-производители; Steve Marcus/Reuters; rightcameraman, ldprod/Fotolia.com

Мобильная угроза

Смартфоны становятся центрами сбора данных, где хранится масса личной информации. Стоящая цель для хакеров.

Смартфоны заменяют Windows в роли главной цели хакерских атак. Сегодня существует около 865 000 мобильных угроз, и они становятся все более опасными (см. колонку справа). Хакеры могут даже навсегда парализовать смартфон на базе Android. По словам Виш Ву, исследователя из компании Trend Micro, этот баг в операционной системе содержится в компоненте MediaServer. Когда пользователь открывает вирусное видео, медиаплеер выходит из строя, а вместе с ним и вся система. Такое видео попадает в смартфон через вредоносное приложение. Самое неприятное заключается в том, что программа записывается в автозапуск системы, и баг компонента MediaServer срабатывает после каждой перезагрузки. Это касается версий от 4.3 до 5.11, то есть примерно половины всех Android-устройств. И универсального патча пока не существует.

За несколько дней до опубликования информации об уязвимых местах в MediaServer был обнаружен новый баг — Stagefright. Он затрагивает около 950 млн устройств с Android, то есть порядка 95% гаджетов, на которых установлена данная ОС. За счет этой уязвимости хакеры могут захватывать смартфоны с помощью простого MMS. Ошибка скрыта в модуле Stagefright, отвечающем за обработку мультимедиа (отсюда и его название — англ. «Страх сцены»). Если хакер отправляет на телефон зараженное MMS, пользователю открывается содержание сообщения, но при этом автоматически срабатывает вредоносный код. И в таком случае «заплата» имеется только для нескольких видов устройств.

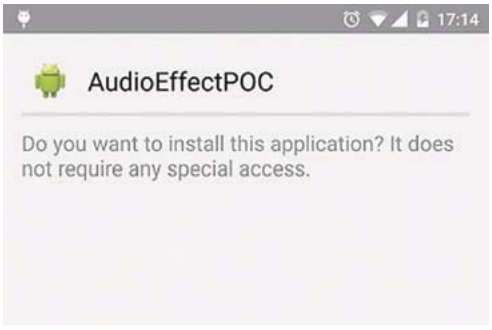
Логин — больше не гарантия безопасности

Некоторые атаки могут повлечь за собой даже еще более серьезные последствия, чем парализованный смартфон. Уязвимость в смартфонах HTC позволяет хакерам считывать сохраненные в них отпечатки пальцев пользователей. Это удалось сделать специалистам фирмы FireEye, занимающейся вопросами безопасности. Гаджет HTC One Max записывает скан отпечатка пальца в виде доступного всем изображения в формате BMP. Самое неприятное, что с помощью этого изображения хакеры могут проникать во все системы, которые пользователь защищает и будет защищать своим отпечатком пальца. А таких систем может быть и несколько: согласно прогнозам IHS, к 2019 году примерно половина производителей смартфонов будут обеспечивать защиту данных посредством сканера отпечатков пальцев. Впрочем, HTC уже разработала патч, который надежнее защищает отпечаток.

Взломан и защитный модуль SIM-карт. Эти USIM (Universal Subscriber Identity Module) до сих пор считались неуязвимыми для взлома. У исследователя Ю Ю получилось клонировать такие зашифрованные карты, причем необычным способом. С помощью осциллоскопа он исследовал потоки данных и разгадал шифровальный код. Примерно за час ему удалось клонировать карту и затем посредством копий сделать звонки от имени пользователя, прослушать его разговоры и считать пароли двухфакторной аутентификации — например, код mTAN. ➜

Уязвимости Android в 500 млн устройств

Ошибка в MediaServer аппаратов с Android позволяет хакерам надолго парализовать работу всей системы. Патч же пока доступен не для всех гаджетов.



Топ-3 вредоносных программ для мобильных устройств в Германии

ИСТОЧНИК: «Лаборатория Касперского»

- **DangerousObject.Multi.Generic.** Пока не исследованные вредоносные программы. Ответственны за 17,5% всех заражений.
- **Trojan-SMS.AndroidOS.Podec.a.** Во втором квартале 2015 года в 9,7% атак участвовал этот троян. Он входит в Топ-3 мобильных угроз уже три квартала подряд, что обуславливается его весьма активным распространением.
- **Backdoor.AndroidOS.Obad.f.** Многофункциональный троян. Он способен отправлять SMS на премиум-номера, загружать и устанавливать на устройство другие вредоносные программы. Данный троян стал причиной 7,3% атак.

Считать отпечаток пальца

Ошибки в ПО смартфонов HTC позволяют хакерам считать отпечаток пальца. Так им становится доступной практически любая система, которую пользователь открывает посредством отпечатка пальца.

Клонированная SIM-карта

Исследователь из Шанхая с помощью осциллоскопа считал шифровальный код SIM-карт, который ранее считался неуязвимым. Далее с их помощью он взломал пароли двухфакторной аутентификации.

Взлом через радиосигнал

Беспроводная коммуникация — то, без чего в наше время уже не обойтись. К сожалению, многие сети не защищены от взлома, и это может привести к смертельным последствиям.

Проникновение в другие устройства с помощью радиосигнала для хакеров не только удобно, но и во многих случаях наиболее просто, как в случае с дроном Bebop фирмы Parrot. На конференции хакеров Defcon Майкл Робинсон продемонстрировал, как он может захватывать подобные дроны коммерческого назначения. Для этого хакер использует сеть Wi-Fi, через которую пилот управляет дроном со смартфона или планшета. Поскольку сеть дрона не закодирована, Робинсону достаточно парализовать соединение между дроном и смартфоном на одну минуту с помощью генератора помех. В это время дрон зависает в воздухе. Теперь хакер может подключиться к дрону быстрее, чем пользователь, и перехватить контроль над ним.

Системы бесконтактной оплаты защищены лучше, чем WLAN-сети дронов, но и они уязвимы для хакеров. Питер Филлмор, специалист по финансовым взломам, исследовал NFC-карты Visa и MasterCard и обнаружил некоторые лазейки. Хотя копирование современных карт должно быть невозможным, оно запросто удается при использовании устаревших платежных терминалов. Как правило, Visa и MasterCard могут обслуживаться и старыми терминалами оплаты, которые считывают информацию с магнитной полосы. С помощью специальной программы хакер проводил манипуляции картами, и их использование становилось возможным только на кассовых терминалах со старой уязвимой технологией.

Манипуляции: передозировка снотворного

Чаще всего хакерские атаки отнимают у своих жертв деньги и портят нервы. В случае взлома в исполнении Руны Сэндвик и Майкла Оджера речь идет уже о жизни и смерти: хакеры научились манипулировать оружием фирмы TrackingPoint с беспроводной системой наведения. Взломщики использовали баг в беспроводном модуле. С его помощью можно манипулировать вводом цели, задавать новые цели или удалить внутреннюю операционную систему, сделав оружие негодным к применению. Компания пытается противостоять хакерским атакам посредством наивной рекомендации: «Следите за тем, чтобы вблизи WLAN вашего оружия не было ни одного хакера» — так можно вкратце передать то, что написано на сайте TrackingPoint.

Смертельная опасность исходит не только от оружия. Исследователь по вопросам безопасности Билли Райос нашел способ манипуляции инфузионными насосами фирмы Hospira, которые используются в больницах для вливания обезболивающих средств. Через баги можно, например, изменить дозу медикамента и вызвать тем самым передозировку, которая приведет к смерти. Присоединенные устройства, подающие сигнал тревоги при остановке сердца, здесь тоже уже не помогут. Специалист по IT Флориан Груноу посредством взлома запросто отключает эти аппараты.

Угон дронов

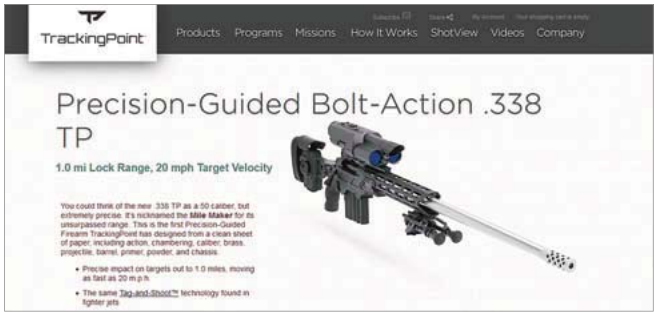
Дрон Bebop хакеры захватили через незащищенную беспроводную сеть. Связь с пилотом была нейтрализована с помощью генератора помех.

Взлом кредитных карт NFC

Модифицируя микропрограмму бесконтактной карты, хакер вынуждает владельцев использовать старые ненадежные способы оплаты.

Захват оружия

Беспроводной модуль оружия с системой самонаведения TrackingPoint имеет баг, через который хакер может задать винтовке новую цель.



«Подключаемые к Интернету гаджеты предлагают хакерам огромное поле деятельности».

КРИСТОФ ПААР,
профессор кафедры систем безопасности Рурского университета в Бохуме

Манипуляции с инфузионными насосами

С пугающей легкостью хакеры могут изменять дозировку обезболивающих препаратов. Для этого они проникают в систему насосов Hospira, а в дополнение отключают и спасительную систему оповещения.

Поездка с хакером

Неважно, какую киберзащиту устанавливают производители автомобилей — хакеры действуют на опережение. А причина кроется в провальной политике обновления.

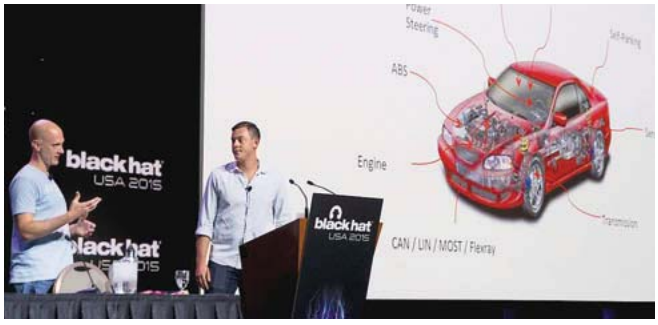
В этом году на конференции Black Hat Чарли Миллер и Крис Валазек показали, как можно захватить автомобильный компьютер. Подобное уже демонстрировали в прошлом году. Однако теперь хакерам уже не нужно сидеть непосредственно в автомобиле и через кабель подключать свой ноутбук к бортовой системе: все работает удаленно, через Интернет. В качестве жертвы был выбран актуальный внедорожник Jeep. Он оснащен системой сбора данных UConnect. С ее помощью владелец может через приложение считывать различную информацию, например, узнать местонахождение транспортного средства. Миллер и его партнер использовали эту систему как лазейку, ведь у каждого автомобиля, оснащенного UConnect, есть IP-адрес для доступа к нему через Сеть. Хакеры нашли его посредством специальных поисковых запросов в мобильной сети Sprint, которую используют машины. Затем через уязвимость нулевого дня в микропрограммном обеспечении бортового компьютера они переписали часть операционной системы. Хакеры получили контроль над рулевым управлением, тормозом, газом и почти всеми электронными системами автомобиля, например, вентиляцией, радио или центральной блокировкой дверей. Группа Fiat-Chrysler, производитель уязвимой модели Jeep, отреагировала быстро и опубликовала патч. Но обновление требует хлопотной загрузки с USB-флешки, что для многих владельцев автомобиля слишком утомительно. Поэтому 1,4 млн машин были отозваны производителем для апдейта ПО. Как это можно сделать по-другому, показывает Tesla. Здесь у всех транспортных средств обновление производится через беспроводное соединение. От хакерских атак это не защитит, и эти автомобили уже подвергались взлому. Однако программные ошибки были исправлены в течение нескольких дней без необходимости обращения в автосервис.

Надежно запертых авто не существует

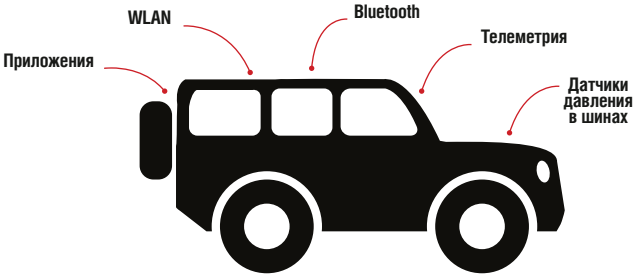
Уязвимы не только автомобили, подключенные к Сети. Специалист по безопасности Сэми Камкар разработал устройство под названием RollJam, с помощью которого он может открывать все машины. Камкар прослушивает код дистанционного радиоуправления и через некоторое время посылает его транспортному средству. Система безопасности должна этому воспрепятствовать: при каждом нажатии кнопки ключа создается новый код безопасности, который можно использовать только один раз. После получения кода автомобилем он деактивируется. Устройство Камкара легко обходит эту технологию. Две антенны на хакерском аппарате излучают помехи, и автомобиль не получает ключ. Когда жертва снова нажимает на кнопку несработавшего ключа, устройство Камкара отправляет машине первый ключ и сохраняет второй для использования хакером. Помочь здесь может ограниченный срок действия открывающего кода, и это будет установлено в последующих сериях многих производителей. ➜

Хакерский бум вокруг автомобилей

С помощью уязвимости нулевого дня хакеры проникают в бортовую систему извне и получают доступ ко всем важным системам, например, тормозам и рулевому управлению.



Чарли Миллер и Крис Валазек слывут королями взлома автомобилей. Они много лет исследуют баги в их системах



Хакеры используют многочисленные лазейки для доступа в системы автомобиля. Во всех показанных выше системах уже есть уязвимости

Все двери открыты

Специалист по IT Сэми Камкар может открыть любую автомобильную дверь при помощи своего устройства RollJam, перехватив открывающий код посредством специального аппаратного обеспечения.