

ХАКЕР

WWW.XAKER.RU

3 ВИДЕО ПО ВЗЛОМУ!

○ ТЕМА НОМЕРА

Wi-Fi

Стр. 22 ○ Инструменты
для вардрайвинга

Стр. 38 ○ Атака на
Wi-Fi

Стр. 56 ○ Воздушный
дуршлаг



Стр. 104

Распределенная
атака на Delphi

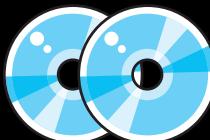
Быстрый взлом
RAR-архива

Стр. 78

Киберсквоттинг:
война за домены

Как сделать состояние на
доменных именах?

ISSN 1609-1019
9771609101009
Barcode



на CD

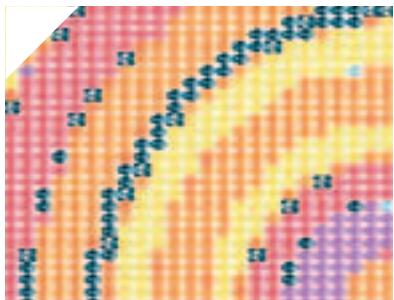
- VirtualDrive 9
- Free Pascal Compiler 1.9.6
- CloneDVD 2.7.1.1
- Blender 2.36
- PSPad 4.3.2.2042
- Linux Kernel 2.6.11-rc2



на DVD БОЛЕЕ 4 ГИГАБАЙТ

- Corel Graphics Suite 12
- NetBSD 2.0 Live
- Alcohol 120%
- Devil-Linux 1.2.2
- VirtualDrive 9
- Gentoo 2004.3
- Музыка
- Соф트 из журнала
- etc.

(game)land



INTRO

Положить десяток противников, играя в Мортал Комбат? Легко! Я и двадцатых вынесу - дай мне только волю. В реальной же жизни можно хорошенько получить по ушам всего от одного паренька, которому не понравилось, что ты громко разговариваешь в кинозале.

За доли секунды успеть прицелиться в хаотично движущегося врага, находящегося в двухстах метрах при fov=130, и точно в него попасть из рейла? Да не проблема! А если останутся хелсы, я его чайником добью, он не успеет даже повернуться. А вот прострелить подкинутую пивную банку из настоящей воздушки - это простите-извините. Не смогу.

При скорости 200 миль в час не наложит в штаны и успевать вовремя поворачивать, не сбив ни единого пешехода и не сосчитав все столбы, запускаю NFS и радуюсь своим умениям. Но когда разгоняюсь на отцовской тойоте до 150 километров в час, нога сама отпускает педаль газа и нервно подергивается, а руки начинают сжимать руль давлением в 19 атмосфер, как челюсти бультьера.

Все, чего мне волею судеб не дано в настоящий, взаимодействия жизнью, все это я могу попробовать осуществить, сидя за компьютером, и получить почти те же эмоции и ощущения. А людям с ограниченными возможностями компьютер вообще помогает сделать то, что им и не снилось. Открывает для них новые возможности хоть как-то реализовать себя в жизни.

И знаешь, я безумно счастлив, что в свое время у человечества появилась такая вещь, как ЭВМ, и не представляю, что бы мы сейчас без нее делали.

b00b1ik,
не главный редактор X

CONTENT

НЬЮСЫ

04/МегаНьюсы

PC ZONE

14/Спаси и сохрани

18/Активные директории

22/Инструменты для вардрайвинга

26/Замути свой гейм-сервак!

30/Клиенты тетушки Ирины

ИМПЛАНТ

32/Шапка-невидимка

ВЗЛОМ

38/Атака на Wi-Fi

44/Hack-FAQ

46/Вторжение в госпиталь

50/Обзор экспloitов

52/VPN по-хакерски

56/Как взломали DalNet(Ru)

60/Секс с IFRAME

64/Воздушный дуршлаг

68/Купи е-контрацептив

70/Шелл - это просто!

73/X-Конкурс

СЦЕНА

74/CeBit: весь мир хай-тека в одном месте

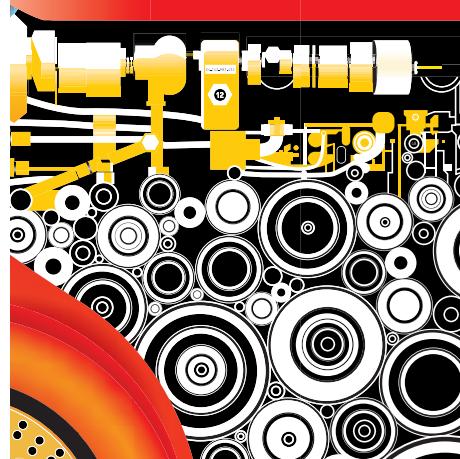
78/Киберсквоттинг: война за домены

82/Симфония Soundblaster'a

88/Мировая кузница хай-тека

АТАКА НА WI-FI

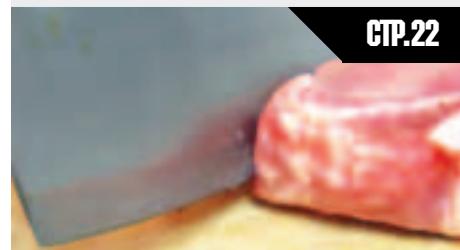
СТР.38



Прочтай рассказ человека, регулярно занимающегося вардрайвингом

ИНСТРУМЕНТЫ ДЛЯ ВАРДРАЙВИНГА

СТР.22



Собери чемоданчик для беспроводного взлома

КАК ВЗЛОМАЛИ DALNET (RU)

56



IRC тоже подвержен взлому, как и все в электронном мире

CENSORED

ШАПКА-НЕВИДИМКА



Сказочная шапка-невидимка, «Человек-невидимка» Чэллса, кольцо Толкиена, голливудский «Жищник», глаз инвизибилисти в аське... В этом логическом ряду заключена неуемная тяга человечества к невидимости. Невидимость была и остается слишком соблазнительной для военных и шпионских ведомств, чтобы они так просто оставили ее сказочникам и фантастам, не воплотив технологию в жизнь. Пока биологи делают прозрачными и без того мелких грызунов, инженеры успешно решают задачки с неживыми объектами - от невидимых чернил до плащей, самолетов и зданий-невидимок. А там, где наука пока еще бессильна, в ход идет хитрость или прямое надувательство.

ТЕХНОЛОГИИ НЕВИДИМОСТИ

Сначала определимся, о чем вообще речь и зачем все это нужно. Самые очевидные цели - военные. Шпионы, разведчики, диверсанты, войска и техника, будучи невидимыми, смогут проникать в глубокие тылы противника и, соответственно, шпионить, разведывать, вредить и наносить внезапные удары по изумленному врагу. Однако, если и враг окажется не менее продвинут в технологиях невидимости, обнаружить секретные штабы и склады с оружием не представляется возможным, потому что вражеские здания, в свою очередь, будут невидимыми. Попасть в невидимого



солдата тоже станет весьма затруднительно. Вот это война! Невидимые войска носятся по тылам и линии фронта, не замечая друг друга. Над ними кружат самолеты-невидимки, шмаляя напропалую по невидимым целям...

Сомневаться в полезности технологий невидимости в мирной жизни не приходится. С невидимыми зданиями и архитектурными сооружениями можно не париться в отношении дизайна - урбанистический пейзаж не будет портить вид из твоего окна. В медицине, если сделать нужные участки тела человека прозрачными, врачи смогут непосредственно наблюдать, что творится внутри пациента, не прибегая к помощи рентгенов, томографов и прочих ультразвуков.

Во всех вариантах военного и гражданского применения невидимости речь идет о восприятии объектов человеческим глазом - в оптическом диапазоне. По сути, можно выделить два вида невидимости: прозрачность и незаметность, или маскировку. В последнем случае ты не видишь, что находится позади объекта, но при этом не можешь выделить его на общем фоне.

Итак, какие конкретно достижения есть на сегодняшний день? Секретные военные разработки ведутся, в частности, в лаборатории NASA Jet Propulsion Laboratory и финансируются пентагоновским ведомством DARPA. Об этом все знают, но толком никто ничего не видел (что может говорить о некоторых успехах в создании невидимости ;)). Пока человечество ждет новостей из таких секретных лабораторий, пресса времени от времени балует «сенсациями» от гениев-одиночек.

У-У-У, БИОЛОГИЯ

Прямыми последователями уэлловского человека-невидимки Гриффина являются биологи, работающие над прозрачностью живых тканей. Основные идеи они заимствуют у природы. В животном мире примеров невидимости полно. Это не только ка-



▲ Узнай больше о стелс-технологиях:
www.lowobservable.com



▲ Роман Герберта Уэллса «Человек-невидимка», ставший настольной книгой по невидимости <http://lib.ru/INOFANT/UELS/invisibl.txt>



▲ Читай о попытках запатентовать, в общем-то, лежащие на поверхности идеи невидимости: www.chameleo.net/news.html



Профессор Сусуми Тashi демонстрирует плащ-невидимку в действии

муфляжники и имитаторы - хамелеоны, осьминоги, палочки... Настоящей прозрачностью обладают, в основном, морские организмы. Некоторые из них обитают на километровой глубине - там, где кромешная тьма. Тела этих морских существ настолько тонкие, что просвечивают насквозь. С ребра они тоже неразличимы, как магнитофонная лента. Так неслабо плющит обитателей глубин чудовищное давление.

Интерес для ученых представляет желатинообразное вещество в организме всех прозрачных морских существ. Именно оно отвечает за прозрачность, имея коэффициент преломления, близкий к воде. Этот же желатин обеспечивает животным плавучесть и защиту от давления.

Достичь прозрачности под водой, конечно, проще, чем на воздухе. Однако у исследова-

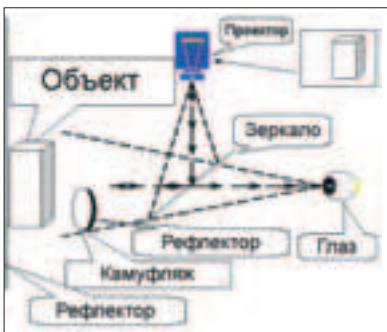
телей из Техасского университета в Остине под руководством доктора Эшли Уэлша в августе 2000 года кое-что получилось. При помощи хитрого вещества на основе глицерина они сумели на короткое время сделать прозрачным участок кожи лабораторной крысы. В течение 20 минут сквозь «окно» можно было созерцать под кожные ткани на глубине в несколько миллиметров. После этого несчастной крысе залезли под кожу и нарисовали там настроичную таблицу на манер телевизионной. Шприцом ввели раствор, и через некоторое время можно было оценить четкость под-



Такой шлем с проектором обеспечивает волшебный эффект плаща-невидимки

кожного изображения. Ученые утверждают, что к моменту испытаний на людях они придумают вариант с менее болезненным втиранием «раствора невидимости». Химический состав препарата запатентован в Штатах.

Итак, Уэллс предположил, а Уэлш доказал, что теоретически можно сделать живые ткани прозрачными. Но вот технически реали-



Принципы работы устройства оптического камуфляжа

«ЧЕЛОВЕК-НЕВИДИМКА» ГЕРБЕРТА УЭЛЛСА

Научный подход к проблеме невидимости был впервые продемонстрирован более ста лет назад в романе «Человек-невидимка» Уэллса. Сие бессмертное творение до сих пор является настольной книгой любителей и гуру невидимости. Способы достижения невидимости живого тела по Уэллсу даже спустя время не выглядят столь уж наивными, а описание сопутствующих физиологических деталей представляет собой настоящий научный отчет! Психиатрические нюансы с идеями сверхчеловека тоже выглядят убедительно и могут помочь будущим невидимкам не свихнуться.



Демонстрация на Wired Nextfest 2004. Лаборатория Таши - почетный гость любой выставки хай-тека

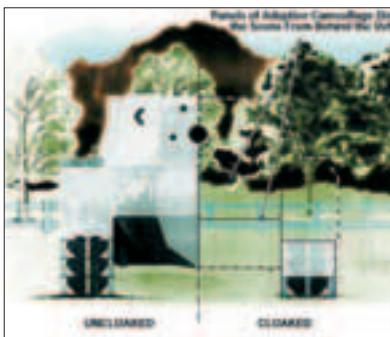
зователь обработку, скажем, внутренних органов пока весьма проблематично. Попробуй представить себе, например, втирание глицерина в мозги... ;).

Кстати, в голливудских фильмах про невидимок обнаруживаются существенные технические ляпы. Совершенно прозрачный человек сам не может ничего видеть! Ведь его хрусталик и сетчатка тоже прозрачные, а значит, не преломляют свет, не фокусируют картинку и не преобразуют ее в нервные импульсы. Природные невидимки сталкиваются с аналогичной трудностью. Подводные животные, имеющие зрение, при всей своей невидимости не могут иметь прозрачные зрачки и сетчатку, иначе они сами ничего не увидят. Обитатели морских глубин практикуют несколько подходов к решению этой проблемы. Первый способ - «перископ» - для дезориентации хищников (или жертв) глаза выносятся из тела на длинных ножках. Второй вариант - «оптоволокно» - очень маленькая сетчатка, собирающая свет по специальному органическим световодам. Другой, противоположный, - «бледные глаза». Глаза у таких существ очень большие с большой сетчаткой, собирающей достаточно света, чтобы видеть, но при этом очень тонкой и почти прозрачной. Человек давно дотумкал использовать все эти перископы и эндоскопы для того, чтобы подглядывать и заглядывать поглубже.

ОТОЙДИ, ТЫ НЕ СТЕКЛЯННЫЙ

Да-а, видно, биологи еще не совсем готовы втереть нам что-нибудь для невидимости. Реалистичные надежды сулит инженерная мысль. Без издевательств над родимым телом можно просто надеть специальный костюм или спрятаться в танк-невидимку.

Пара лет назад мир облетела «сенсация» об изобретении в Японии (ох уж эти японцы!) плаща-невидимки. На страницах уважаемых изданий красовались снимки профессора Сусуми Тashi в своем чудесном плаще на фоне оживленных улиц. Выглядело это весьма эффектно, но по сути оказалось, скорее, фокусом в духе Копперфильда. Однако и сам профессор не скрывал детали технологии. Достаточно было покопаться в описаниях на сайте Токийского университета (<http://projects.star.t.u-tokyo.ac.jp/projects/MEDIA/xv/oc.html>). В общем приближении это похоже на ситуацию, когда человек оказывается на фоне экрана в луче кинопроектора. Хитрость состояла в том, чтобы отображать на плаще кусок реального мира, который в данный момент загораживается от наблюдателя. При этом псевдопрозрачность наблюдалась с различных ракурсов, а проектор располагается на голове (шлеме) наблю-



Танк, закрытый «невидимыми» панелями. Одна из первых разработок аддаптивного камуфляжа в лаборатории Jet Propulsion Laboratory (NASA)



▲ Рецепты простых в изготовлении симпатических (невидимых) чернил:
<http://chemworld.net/aod.ru/practic/simpat.html>



Ultima Online. Лицом к лицу с невидимым врагом

дателя. Плащ имеет особое световозвращающее покрытие.

Вот такие навороты :-). Профессор Тashi предложил несколько вариантов практического использования своего изобретения. Все они, похоже, были придуманы на ходу, так как выглядят несколько притянутыми за уши. Например предлагается сделать прозрачной для летчика нижнюю часть кабины самолета, чтобы он мог непосредственно видеть, куда садится или кидает бомбу. Другой вариант - прозрачные руки и инструменты хирурга во время операции. Имитацию сего процесса демонстрирует видеоролик на сайте лаборатории (<http://projects.star.t.u-tokyo.ac.jp/projects/MEDIA/xv/images/oc-phantom.mpg>). Тут можно заметить лишь одно - плохому хирургу и руки мешают ;-). Пилоту, видимо, придется поначалу привыкать к зависанию своего тела над пропастью и воздерживаться от рефлекторного катапультирования - говорят, такое иногда случалось с летчиками, управлявшими ракетами с телевизионным наведением.

▲ МАСКИРУЕМСЯ СВЕТОДИОДАМИ
Идея отображать на скрываемом предмете динамичное изображение подстилающего фона стара как мир. Она является развити-

ем концепции классического камуфляжа. В терминологии военных ученых это так и называется - аддаптивный камуфляж. В век миниатюрной электроники и оптоволокна реализация в общих чертах выглядит так. Маскируемый объект со всех сторон напичкан микрокамерами, которые передают картинку на противоположную сторону и там ее отображают. В итоге получается что-то вроде Хищника из одноименного фильма. В военных лабораториях Пентагона на полном серьезе разрабатывают подобные системы камуфляжа техники и неподвижных строений.

В ход идут самые современные техноштучки: микрокамеры с волноводами, дисп-

леи на полимерных OLED-светодиодах, мощные процессоры для обработки и корректировки аддативной картинки. Трудно, но вполне достижимо. Так, NASA приводит примерные расклады, что для маскировки со всех сторон объекта величиной с танк потребуется оборудование весом всего ничего 45 килограмм.

В среде теоретиков-ботаников часто принято критиковать в пух и прах идеи невидимости. Дескать, всего не спрятать и все равно что-то будет видно. А раз уж полную невидимость при современных технологиях получить так сложно, то стоит ли корячиться изо всех сил? Однако практико-военспецы такую задачу и не ставят. Для



В африканских прериях ставят дорожные знаки, предупреждающие об опасности эффекта невидимости в природе

СТЕЛС: ВИДИМОСТЬ НЕВИДИМОСТИ?



Легендарный истребитель-невидимка F-117A с суммарной способностью летать и быть незаметным

Сама мысль о том, что враг может оказаться невидимым, способна сильно поколебать неустрешимость противника. Поэтому можно, например, сорудить жуткий самолет-ракозябру, обозвать его невидимкой и растроить об этом в прессе. Именно такова была судьба нашумевшей технологии стелс. Взяли два самолета - большой и маленький, сплющили их, как камбалу, и получили легендарные B-2 и F-117, «невидимые» для радаров. Летные характеристики стали те еще - попробуй долететь, не вильнув в сторону. Эффективная площадь отражения действительно побаивалась, но не исчезла вовсе. Фактически эти аппараты представляют собой летающую мишень, потому что увернуться от атаки у них нет никаких шансов. Однако стелс стал весьма удачным фейком от пропагандистов Пентагона. В свое время этой штукой, также как и дутой программой СОИ, удалось задурить голову и напугать советское партийное руководство, заставляя тратить баснословные деньги на адекватный ответ. Достаточно эффективные алгоритмы распознавания самолетов-невидимок были разработаны без особых усилий. И вот сейчас, через 20 лет после появления стелсов, выяснилось, что для их обнаружения вообще никаких локаторов не нужно ;). Самолеты, проносясь на высокой скорости, нарушают интерференционную картину, которую создают базовые станции сотовых операторов. По этим изменениям можно, например, вычислить, что летит истребитель. Если при этом он дает на радаре уменьшенную засветку, как от стайки уток, это и есть наша «невидимка».

успешного боевого применения вполне достаточно частичной невидимости, которую можно изготовить если не прямо сейчас, то в ближайшем будущем. Вспомни, как ловко бегал от железного Шварца Хищник, пока у него не закоротило прозрачность. Геймеры в Unreal Tournament хорошо знают, как трудно в динамике боя отследить, в принципе, заметного врага, схватившего «стакан с невидимостью». Пожалуй, учёные стараются не зря. Частичная прозрачность и какая ни есть аддитивная маскировка все равно гораздо эффективнее камуфляжа и размалеванного лица.

▲ ПРОТИВОБОРСТВО ТЕХНОЛОГИИ. СУПЕРЗРЕНИЕ

Что же можно противопоставить активно маскирующимся буржуям? Первое, что приходит в голову, - это инфракрасные приборы и радары. Таскать все эти штуки на себе довольно утомительно. Однако со временем, когда технологии невидимости будут достаточно развиты, такие приборы будут доступны на уровне имплантатов.

Искусственные фотоэлементы, вживляемые на место поврежденной сетчатки, доступны уже сейчас. Активно внедряются нанотехнологии. Наноэлементы с расширенным диапазоном частот позволят человеку видеть в инфракрасном и ультрафиолетовом примыкающих участках спектра. Существенно увеличится число различимых глазом оттенков и градаций серого. Можно будет видеть в темноте и различать поляризованный свет. Кстати, все вражеские невидимки прекрасно наблюдаются в поляризованном свете. Это хорошо известно многим морским хищникам, особенно ракообразным и головоногим, которые запросто охотятся на прозрачных жертв. Интерфейсные имплантаты сделают возможным предъявить глазу разного рода служебную информацию. Человек в буквальном смысле сможет взглянуть на мир другими глазами. Что он увидит, невозможно сегодня представить никакой киношной анимацией, ведь ее мы наблюдаем, опять же, обычным зрением.

Кое-кто спешит стать всевидящим уже сейчас. Технология суперзрения - лазерной микрохирургии глаза - уже поставлена на поток, в том числе и в нашей стране. Буквально недавно учёные преодолели давний технологический барьер - aberrации высшего порядка при изготовлении оптики. Применив метод коррекции волнового фронта, теперь можно создавать практически идеальные линзы, что раньше считалось теоретически невозможным. Пересяв эту технологию на глазную лазерную хирургию, специалисты получили невероятные результаты. Компоненты глаза можно затачивать столь идеально, что получается сверхчеловеческое зрение, например 200 или 300%! При этом зоркость становится соизмеримой со зрением кошки. Специалисты начали высказывать опасения, что психика человека не сможет выдержать не свойственный людям поток зрительной информации. Проще говоря, от наплыва деталей у новоявленного сверхчеловека просто снесет башню. Поэтому, если ты решил снять очки в клинике лазерной хирургии, будь предельно осторожен в своих запросах. ☺

НЕВИДИМОСТЬ В ГОЛОВЕ

Давай немножко пофилософствуем. Цвет и образ не являются неотъемлемыми свойствами объекта. Скорее, это свойства восприятия наблюдателем. Ведь предмет не является красным сам по себе - с точки зрения человека и собаки он будет разным. Так и невидимости можно достичь, заставив человека не воспринимать предмет. Научный факт: под гипнозом тебе могут внушить, что у тебя, например, нет системного блока - и ты реально перестанешь его замечать. Долго будешь ходить по комнате, плятаться по сторонам и недоумевать, как это комп работает без системника. Один мой приятель серьезно помешан на психотехнике, экстрасенсорике и прочей лабуде: постоянно делает пассы руками и настраивает ауру... Так вот, он утверждает, что способен так воздействовать на встречных гишников, что они его автомобиль просто не видят на дороге, хотя радар у них пищит. Над этим можно долго смеяться и даже сочувствовать, пока сам не убедишься, что это работает. Наверное, дистанционно срабатывают некие флюиды сверхнаглости, которые излучают люди, твердо уверенные в своих суперспособностях ;-).

www.oklick.ru

ПРОТИЯНИ РУКУ
УДОБСТВУ

oklick 323 M
Optical Mouse

oklick 780 L

Multimedia Keyboard

Когда-то в древности Великий Учитель решил испытать своих учеников, предложив им выбрать для себя мечи.

Один из них выбрал легкий меч, надеясь сохранить силы в долгом походе. Другой выбрал длинный меч, надеясь поразить им больше противников с безопасного расстояния.

Но самым мудрым оказался третий ученик, который выбрал для себя самый удобный меч, ставший продолжением его руки.

Удобство — вот разумный выбор!