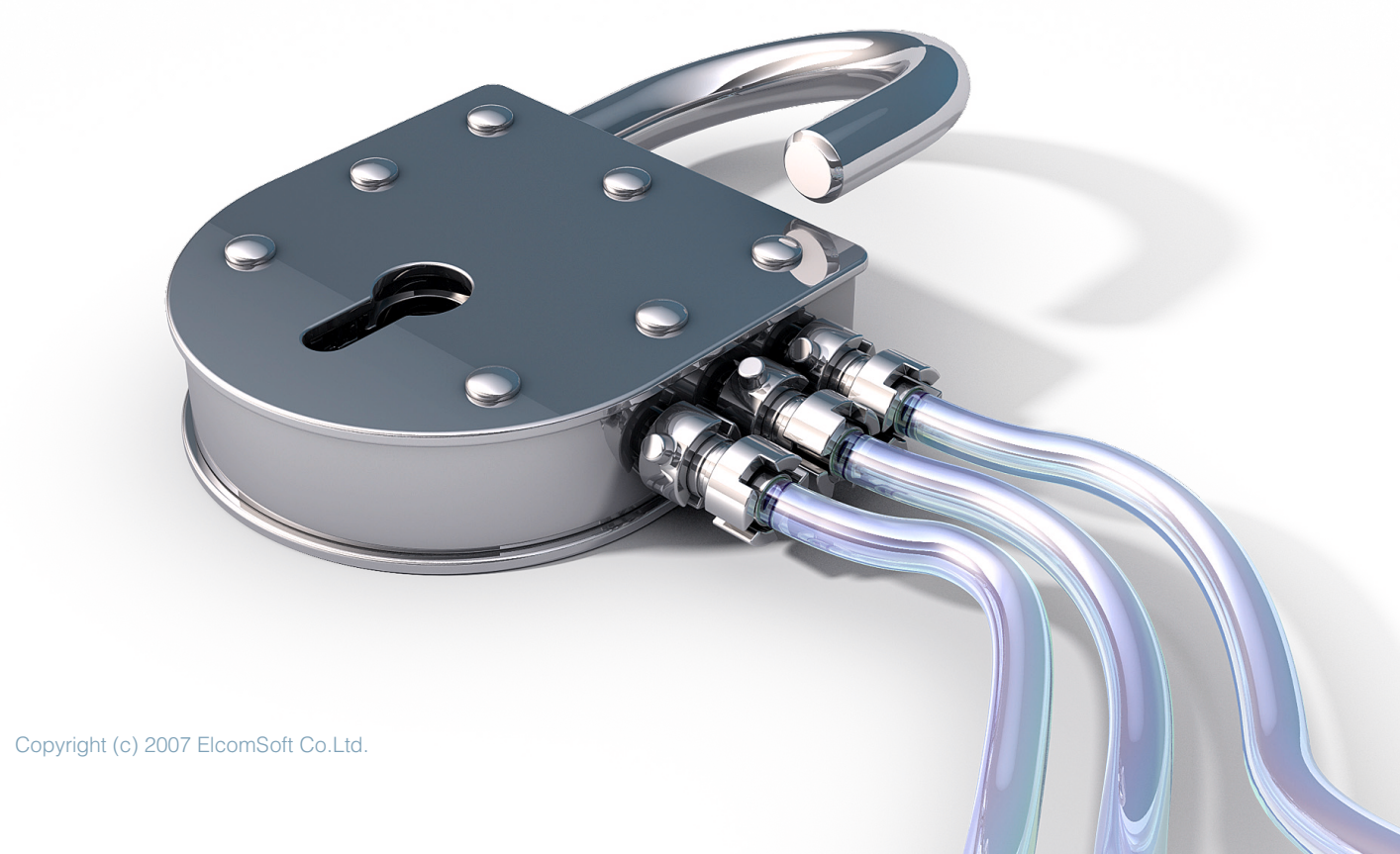
ELCOMSOFT
PROACTIVE SOFTWARE

ДОСТУЧАТЬСЯ ДО PDF

ГАРАНТИРОВАННОЕ ВОССТАНОВЛЕНИЕ КЛЮЧЕЙ ДЛЯ ДОКУМЕНТОВ ADOBE ACROBAT



ELCOMSOFT
PROACTIVE SOFTWARE

СОДЕРЖАНИЕ

ПЕРЕХОД НА «ЦИФРУ»

Стремительное развитие цифровых технологий и электронных коммуникаций, доступность мобильных ПК и смартфонов, обилие инструментов для создания документов и презентаций высокого качества – все это на фоне постоянно растущего объема информации и стремления к эффективному ведению бизнеса ведет к постепенному переходу на обмен информацией в электронном виде.

Не только коммерческие предприятия, но и государственные организации внедряют у себя системы электронного документооборота. Размер аудитории онлайн-версий газет и журналов порой превышает печатные тиражи издания, а некоторые СМИ существуют только в сети. Владельцы карманных компьютеров сегодня предпочитают безбумажные версии книг и журналов бумажным: например, в онлайн-магазине Amazon более 80 тысяч книг представлены в электронном формате[1].

При обмене электронными документами всегда возникает вопрос о совместимости платформ, приложений и их версий. Каждый из нас сталкивался с тем, что адресат не может «прочитать» файл. PC или Mac, Windows Vista или Windows XP, Microsoft Word или Corel WordPerfect – что именно будет использовать человек, до которого мы хотим донести информацию? Решением этой проблемы является использование некоторого универсального формата, не зависящего от «железа» и софта.

[1] книги и документы в формате PDF, данные на 12.09.07

ЧЕМ ХОРОШ PDF?

Такой формат существует. Это необычайно популярный на сегодняшний день PDF (Portable Document Format) — кроссплатформенный формат электронных документов фирмы Adobe.

Документы, сохраненные в формате PDF, правильно отображаются на любом компьютере. Их можно открывать, читать и распечатывать с сохранением текста, шрифтов, иллюстраций, макета независимо от платформы, операционной системы, установленных шрифтов и другого программного обеспечения.

PDF широко используется в издательствах и полиграфии, при распространении электронных версий СМИ, публикации отчетов, справочной информации, документации и просто для обмена информацией. Результат поиска документов в формате PDF в Google только на русском языке составляет 2 360 000 страниц!

Немаловажно, что для просмотра документа в формате PDF используется бесплатное ПО – как фирмы Adobe (Acrobat Reader), так и сторонних разработчиков. О том, насколько популярен PDF, говорит, например, такая цифра: за месяц число загрузок Acrobat Reader через сайт CNET Downloads превышает 35 млн.[2].

Помимо своей универсальности, формат PDF обладает массой дополнительных преимуществ. Среди них и удобство навигации по документам большого объема благодаря системе внутренних ссылок; и корректное отображение на мобильных устройствах под управлением Palm OS, Symbian OS, Pocket PC; и доступность текста для поисковых машин; а также компактность (малый размер файла) и – то, что нас сейчас интересует более всего – широкие возможности защиты документа.

[2] за период 08.08.07-13.09.07

ЗАЩИТА ДОКУМЕНТОВ PDF

КОМУ ЭТО НУЖНО?

Сначала определимся, кто и с какой целью будет защищать документ, созданный в формате PDF? Ни для кого не секрет, что владение информацией является конкурентным преимуществом в современном мире. Утечка конфиденциальных данных может привести к прямому финансовому ущербу для компании, косвенным потерям в форме упущенной выгоды и другим неприятным и порой непредсказуемым последствиям.

Неудивительно, что защите информации уделяется повышенное внимание: IT-безопасность – это отдельное, динамично развивающееся направление в отрасли информационных технологий. Но если говорить о самых простых, доступных каждому пользователю, мерах по защите информации, то среди них непременно окажется парольная защита. Инструменты для защиты документов от просмотра или изменения есть во многих офисных приложениях, включая Adobe Acrobat.

Корректная защита документа – это нахождение баланса между безопасностью и легкостью использования. Устанавливая защиту на PDF-документ, необходимо принимать во внимание несколько факторов:

1. целевая аудитория документа (все посетители или ограниченный круг лиц);
2. доступная читателям версия Adobe Acrobat / Acrobat Reader;
3. место хранения или публикации документа (на публичном сайте компании, в интранете, в типографии);
4. тип информации в документе (текст, графика, мультимедиа);
5. особенности использования документа (просмотр, заполнение полей форм, пересылка по почте, правка и редактирование).

МЕТОДЫ ЗАЩИТЫ ДОКУМЕНТОВ PDF

Стандартная система защиты Adobe Acrobat позволяет назначить парольную защиту на открытие файла, а также ограничить его использование. Используя настройки программы, автор может установить права на печать, изменение и редактирование файла.

Adobe Acrobat позволяет использовать для PDF-документов два вида паролей: Document Open (user-пароль) и Permissions (owner-пароль). Первый необходим для открытия документа, а второй ограничивает его использование (редактирование, копирование текста и рисунков, вставка и удаление страниц, печать и изменение настроек защиты документа). Если документу назначены оба пароля, то открыть его можно при помощи любого из них, а для изменения установленных ограничений необходим owner-пароль.

Для парольной защиты Adobe Acrobat применяет алгоритм шифрования RC4 (потоковый шифр, широко применяющийся в различных системах защиты информации), а начиная с версии 7.0 также и AES (расширенный стандарт шифрования). Причем если в ранних версиях Adobe Acrobat ключи были только 40-битными, то, начиная с пятой версии, стало возможным также использование 128-битных ключей, что усложняет задачу нахождения пароля (при 40-битном шифровании количество ключей составляет 240, а для 128-битного их уже 2128).

Кроме этого, есть возможность создавать отдельные наборы прав для разных групп пользователей, используя защиту с помощью сертификатов безопасности. В этом случае, например, некоторые пользователи смогут заполнять поля форм, а участники рабочей группы получат права также и на редактирование документа.

Для защиты документа с помощью сертификатов Adobe Acrobat использует технологию цифровой подписи. Она основана на использовании двух ключей: открытый (public) и закрытый (private). Первый включается в сертификат и используется для зашифровывания информации, а второй - для расшифровывания и цифровой подписи документа.

Как видим, Adobe Acrobat предлагает широкий выбор методов защиты PDF-документов с помощью последних технологий в области информационной безопасности.

УТРАТА ДОСТУПА К ИНФОРМАЦИИ

Однако высокое качество защиты документов может обернуться против вас. Каким образом?

По соображениям конфиденциальности отчеты о продажах, результаты маркетинговых исследований, аналитические записки и другая важная информация часто хранится в PDF-файлах, защищенных паролем на редактирование и печать, а порой и на открытие. Известно, что в любой информационной системе самым уязвимым местом остается человек. И ситуация с парольной защитой – не исключение. Сколько раз вы сами забывали тот или иной пароль? В другой ситуации вам может потребоваться доступ к документу, созданному вашим коллегой или партнером. А человек мог уволиться, уехать в отпуск – да мало ли что еще? Не останавливать же весь рабочий процесс из-за такой досадной оплошности!

Но, пожалуй, чаще всего при работе с документами в формате PDF встречается другая проблема: вам необходима информация из отчета для подготовки тендерной документации, а программа не позволяет выделить и скопировать текст из файла. Вы уважаете авторские права и всегда ссылаетесь на источник информации – только бы побыстрей подготовить все материалы для завтрашнего тендера.

Проблема очевидна: чтобы получить доступ к информации и решить текущие бизнес-задачи, необходимо снять ограничения с PDF-документа или расшифровать его (в случае защиты на открытие). И в большинстве случаев это сделать можно.

КАК РЕШИТЬ ГОЛОВОЛОМКУ?

НЕМНОГО О ПАРОЛЯХ

Поскольку проблема утраченных паролей существует с тех пор, как была изобретена парольная защита, производители ПО уже давно озаботились этим вопросом. В результате сегодня на рынке представлен ряд программных решений для восстановления паролей.

Однако отложим на некоторое время в сторону рассказ о методах, которые используются этими программами для решения проблемы утраченных паролей. Для начала давайте разберемся, какими бывают пароли в принципе и какая дополнительная информация может пригодиться нам при поиске пароля.

Итак, в общем случае при создании пароля на английском языке в нем могут быть использованы следующие символы: 26 строчных латинских букв (a...z), 26 прописных латинских букв (A...Z), 10 цифр (0...9), 33 спецсимвола (!@#$%^ и т.п.), то есть всего 95 символов в любых комбинациях. В некоторых случаях из числа допустимых исключены специальные символы, что сокращает число возможных вариантов пароля. При этом не будем забывать, что пароли могут быть разной длины, что может быть критично в том случае, когда пароль невозможно восстановить или сбросить, а только лишь найти методом прямого перебора.

Кроме того, большим подспорьем в деле поиска пароля может стать знание человеческой психологии. Несмотря на многочисленные ограничения, призванные усилить стойкость парольной защиты (минимальная длина пароля, регулярная смена пароля и пр.), многие пользователи пренебрегают элементарными правилами безопасности, лишний раз доказывая существование уже упомянутого феномена «слабого звена», которым в данной ситуации является человек.

Большая часть используемых паролей состоит из слов и символов на родном или знакомом человеку языке. Эти слова часто имеют отношение к личной жизни пользователя: год рождения, имя любимой собаки, номер телефона или банковской карты и т.д. Новый пароль может быть незначительной модификацией старого пароля. Именно таким образом большая часть пользователей решает для себя проблему регулярной смены пароля, предусмотренной политикой безопасности компании. И последнее, но важное замечание: люди очень часто держат записку с паролями прямо на рабочем столе или хранят их на своем компьютере в отдельном файле, хотя такое лекарство от забывчивости ставит крест на самой идее парольной защиты.

Таким образом, знание требований к паролю (возможные состав и длина) и наличие некоторых сведений о пользователе могут значительно упростить задачу нахождения неизвестного пароля. И технологии, применяемые специализированным ПО для восстановления паролей, предусматривают возможность использования подобной информации.

МЕТОДЫ ВОССТАНОВЛЕНИЯ ПАРОЛЕЙ

На сегодня основными методами поиска паролей программными средствами являются простой перебор, перебор по маске, атака по словарю, перебор ключей шифрования (вариантов здесь может быть меньше, чем при переборе паролей) и так называемая rainbow-атака. В некоторых случаях применяются и другие виды восстановления доступа к файлу – например, так называемая plaintext-атака (на основе известного содержимого). Давайте рассмотрим некоторые из этих методов.

Простой перебор

Суть метода прямого перебора (brute force) проста: программа перебирает все возможные комбинации символов, пытаясь подобрать подходящий пароль. Поиск можно несколько ограничить, указав количество символов в пароле, их тип (буквы, цифры, другие знаки), а также символы, с которых должен начаться поиск.

Сколько же времени может потребоваться, чтобы восстановить утерянный пароль методом «грубой силы»? Это зависит от длины пароля, набора использованных в нем символов, мощности компьютера, а также типа документа, к которому пароль подбирается.

Конечно, может случиться так, что правильный пароль встретится быстро, и все возможные комбинации перебирать не придется. Но вряд ли стоит на это рассчитывать. При решении задачи на обычном компьютере счет может идти на годы! Метод прямого перебора самый трудоемкий, поэтому прибегать к нему рекомендуется лишь при отсутствии других альтернатив.

Перебор по маске

В случае, если пароль создавали вы сами, всегда есть шанс попробовать восстановить его по маске, сильно сузив область поиска. Возможно, вы помните длину пароля и некоторые символы из него. Пригодится любая информация.

Например, вы уверены, что использовали лишь цифры и строчные латинские буквы. Тогда при поиске можно исключить спецсимволы и прописные латинские буквы. Неплохо, если вы знаете, что тот или иной символ стоял на определенной позиции в пароле. Например, зная, что пароль имеет длину 10 символов, начинается с буквы «a» и заканчивается «2007», для поиска можно задать шаблон «a?????2007». Неизвестные символы обозначены в шаблоне вопросительными знаками.

Смысл использования маски очевиден: программе приходится перебирать меньшее количество возможных комбинаций, а значит, срок, за который может быть найден пароль, значительно сокращается.

К сожалению, не так часто о пароле известны какие-либо подробности, поэтому использовать маску удается редко. К счастью, существует еще один метод восстановления пароля, который дает очень и очень хорошие результаты.

Атака по словарю

Предположим, у вас есть информация о возможных словах или именах, используемых в пароле. В этом случае можно воспользоваться методом поиска по словарю.

Дело в том, что часто пользователи используют в качестве пароля обычные слова. Как правило, это слова из английского языка: open, access, password и т.д. Ведь такой пароль запомнить значительно проще, чем бессмысленные комбинации букв и цифр. На самом деле забывается такой пароль точно так же, как и любые другие, зато восстанавливается довольно легко.

Где взять такой словарь (а если быть более точным, то список слов)? Во-первых, он может входить в поставку программы. Во-вторых, его можно поискать в сети – на FTP-серверах можно найти самые разнообразные списки общеупотребимых слов и их модификаций, тематические списки (животные, футбольные команды и пр.), аббревиатуры и т.д. В-третьих, словарик можно составить и самостоятельно.

Преимущества этого метода очевидны. Список слов, которые пользователи вводят в качестве пароля, весьма и весьма ограничен и его размер редко превышает сто тысяч. А перебрать сотню тысяч вариантов для современного компьютера – вполне посильная задача. Вот и получается, что метод перебора по словарю стоит попробовать раньше всех остальных. Вполне возможно, что он быстро принесет удачу.

Rainbow-атака

Как видим, самым важным параметром при восстановлении пароля является срок, за который его можно найти. Мы уже знаем, что при простом переборе выполняется проход по всем возможным вариантам пароля, а для сложных комбинаций это требует слишком много времени. Если речь идет о месяцах или годах вычислений, то целесообразность такого мероприятия стремится к нулю.

Для решения этой проблемы применяется так называемая rainbow-атака (rainbow attack), основная идея которой состоит в использовании предвычислений при поиске пароля: для поиска пароля используют результаты предварительных вычислений возможных его вариантов для некоторого набора символов.

Мысль о замене ресурсоемких вычислений обычным поиском по предварительно подготовленной таблице поиска (lookup table), не нова. Таблицы поиска применяются в тех случаях, когда данные гораздо проще извлекать из памяти, чем создавать. Основной сложностью при использовании таблиц поиска является их размер – не каждая компания располагает ресурсами для хранения терабайтов информации. Именно поэтому и появились радужные таблицы, представляющие собой оптимизированные таблицы поиска. Их размер на порядки меньше, чем обычных таблиц поиска.

При генерации радужных таблиц с помощью различных параметров можно задать вероятность восстановления пароля/ключа, примерное время атаки и время генерации самих таблиц. Подбор параметров и нахождение оптимильного баланса между временем атаки и вероятностью нахождения пароля/ключа – отдельная задача. В результате за сравнительно небольшое время получают таблицы, по которым с очень высокой вероятностью можно в тысячи раз быстрее найти любой ключ/пароль из проверенного диапазона.

Справедливости ради стоит признать, что по сравнению с обычными таблицами поиска вероятность здесь, как правило, составляет менее 100%, но результат того стоит. Например, при использовании таблицы для семи алфавитно-цифровых символов (на ее создание потребуется около недели), метод rainbow-атаки позволит восстановить практически любой пароль из семи алфавитно-цифровых символов за 20-30 секунд. А вот прямой перебор в этом случае займет уже более суток. Выгода – налицо.

ВЫБОР РЕШЕНИЯ

Итак, вопрос о целесообразности покупки программы для быстрого восстановления доступа (в нашем случае к PDF-документам) не стоит. Такой инструмент должен иметь под рукой каждый системный администратор. Затраты на его приобретение с лихвой окупятся при первом же инциденте утраты пароля.

На что стоит обратить внимание при выборе такого решения?

Во-первых, какова вероятность восстановления пароля, заявляемая производителем? Собственно, это главный критерий оценки эффективности решения. Ведь именно для этого вы его и покупаете. Конечно, при отсутствии временных ограничений можно гарантировать 100% вероятность нахождения пароля, но вряд ли такая ситуация вас устроит. Как правило, получить доступ к документу необходимо как можно скорее.

Во-вторых, стоит обратить внимание на спектр поддерживаемых ОС и версий приложений, форматов файлов, языков и кодировок. Трудно предсказать, с документом какой версии Adobe Acrobat вам придется столкнуться при восстановлении пароля. Узнайте также, как быстро добавляется поддержка новых версий приложений.

В-третьих, поинтересуйтесь временем восстановления пароля. Конечно, в зависимости от мощности вашего компьютера время нахождения пароля может варьироваться, но обычно производители сообщают некоторые усредненные данные. Важно понимать, о каком сроке идет речь – минуты, дни, недели или месяцы?

И последнее – предоставляет ли программа возможность организации распределенных вычислений? Этот способ решения трудоёмких вычислительных задач предполагает использование мощностей целой группы компьютеров – как в локальной сети, так и удаленных. Применяют его и при решении задачи взлома паролей. Ведь если доступ к некоторым документам и приложениям можно восстановить за короткий срок на обычном компьютере (например, пароль к ICQ или Google Talk, сохраненный локально), то для взлома других паролей ресурсов одного компьютера будет недостаточно – о каком бы сроке ни шла речь. Например, пароли PGP настолько стойкие, что их подбор возможен только при использовании распределенных вычислений.

Таковы, пожалуй, основные критерии выбора решения для восстановления утраченных паролей.

РЕШЕНИЯ «ЭЛКОМСОФТ» - ЭТО ГАРАНТИРОВАННЫЙ ДОСТУП К PDF-ФАЙЛАМ

Российская компания «ЭлкомСофт» предлагает клиентам целый спектр решений для восстановления паролей практически к любым системам: от офисных приложений и инстант-мессенджеров до системных паролей Windows и архивов.

Уникальные технологии и штат специалистов с многолетним опытом работы в области криптографии позволяют компании «ЭлкомСофт» создавать высококлассные программы класса password recovery. Вероятность нахождения пароля в зависимости от его длины, сложности и технологии шифрования, используемой в приложении, составляет не менее 80%. В большинстве же случаев гарантируется 100% восстановление пароля.

Для восстановления доступа к документам Adobe Acrobat «ЭлкомСофт» разработал специальную программу – Advanced PDF Password Recovery. Кроме этого, можно также приобрести решение ElcomSoft Distributed Password Recovery, возможности которого позволяют работать с защищенными PDF-файлами, но здесь применяются распределенные вычисления с привлечением как локальных, так и удаленных ресурсов.

ADVANCED PDF PASSWORD RECOVERY

Advanced PDF Password Recovery поддерживает все версии и все алгоритмы шифрования Adobe Acrobat от 3.x до 8.x (при использовании стандартных методов защиты PDF) и позволяет вскрывать PDF-файлы, а также снимать ограничения, предусмотренные форматом PDF (рис.1).

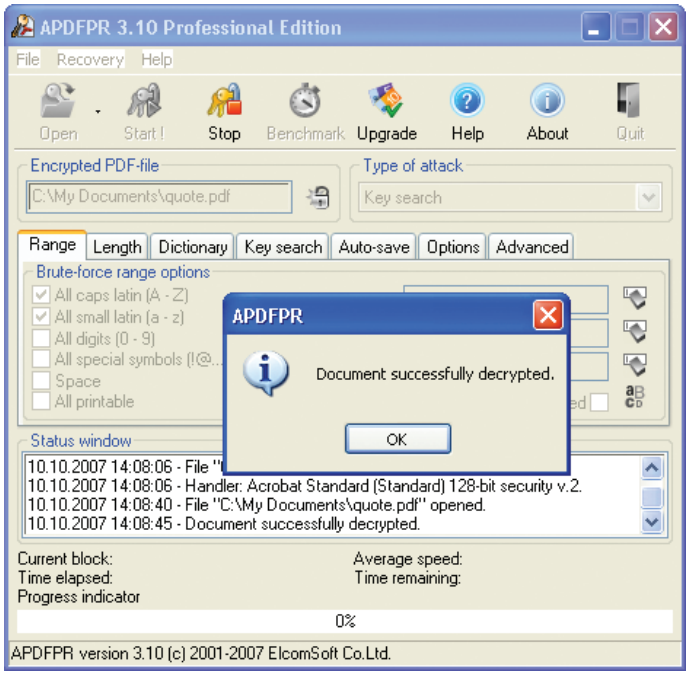


Рис.1. Снятие ограничений с PDF-файла.

Возможности программы зависят от выбранной версии: Standard, Professional, Enterprise. Базовая редакция программы, позволяет снимать с документа ограничения на редактирование и печать. Версия Professional позволяет также находить пароль на открытие файла. Enterprise-версия может подобрать ключ шифрования методом rainbow-атаки за несколько минут с помощью поставляемых на отдельном DVD-диске радужных таблиц.

Рассмотрим основные возможности программы.

Зачастую пароль на открытие документа (user-пароль) известен или не установлен вообще, то есть требуется найти только owner-пароль, ограничивающий редактирование и печать документа. Для решения этой задачи Advanced PDF Password Recovery использует уникальную технологию, не требующую перебора паролей, что позволяет мгновенно расшифровать документ независимо от использованного алгоритма шифрования и длины ключа. Длина пароля при этом значения не имеет (рис.1).

Для поиска пароля на открытие файла (user-пароль) Advanced PDF Password Recovery используется целый ряд методов: прямой перебор, перебор по маске, атака по словарю, а также специальная технология перебора ключей (рис.2). Если при использовании традиционных методов (прямой перебор и атака по словарю) вероятность нахождения пароля по некоторым оценкам может достигать 80%, то технология перебора ключей дает гарантированный результат (применима для файлов с 40-битным шифрованием и может занимать до нескольких дней на обычном компьютере).

Помимо высокой вероятности восстановления доступа важна еще и скорость. Тут Advanced PDF Password Recovery, несомненно, на высоте. Гарантированное восстановление доступа (при защите user-паролем) к документам с 40-битным шифрованием RC4 может занять несколько дней на компьютере со средними возможностями.

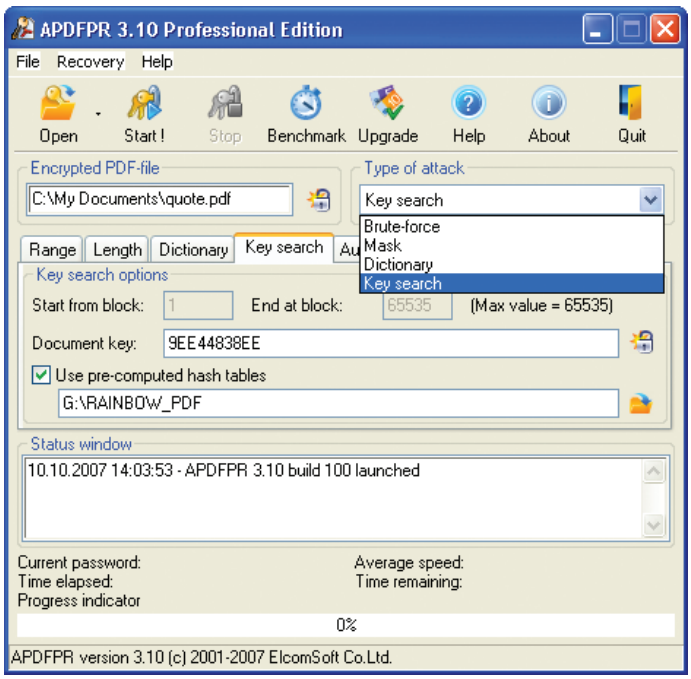


Рис.2. Выбор метода расшифровки файла.

А в Enterprise-версии для решения этой задачи применяется rainbow-атака, позволяющая гарантированно расшифровать файл за несколько минут! Программа использует специально подготовленные таблицы объемом около 4 Гб (поставляются на отдельном DVD). Уникальная технология Thunder Tables™ [3], разработанная специалистами «ЭлкомСофт», позволяет достичь 100% вероятности нахождения ключа (т.е. расшифровки файла), что не имеет аналогов в мировой практике. Метод сочетает применение таблиц поиска и радужных таблиц, что, с одной стороны, гарантирует успех (как по обычным таблицам поиска), а с другой – по-прежнему позволяет создать таблицы за разумное время и уместить их на один DVD-диск. Другие производители могут гарантировать такой результат только методом прямого перебора (занимает несколько дней) или с использованием таблиц поиска огромного размера (несколько терабайт).

Количество расшифрованных файлов зависит от времени атаки (рис.3). Половина файлов раскрывается менее чем за 10 секунд. Максимальное время атаки составляет 15 минут, минимальное – меньше секунды, среднее – 25 секунд. Рекомендуется использование машин с современными многоядерными процессорами (например, Intel® Core™ 2 Duo) и чтение таблиц с флэш-карты (а не с DVD). Повторимся, что гарантия расшифровки составляет 100%.

Программа также позволяет восстанавливать доступ к документам, защищенным 128-битным шифрованием (включая расширенный стандарт шифрования AES) методами прямого перебора, перебора по маске и атаки по словарю. Технология перебора ключей для таких файлов не применяется.

[3] подана заявка на патентование технологии

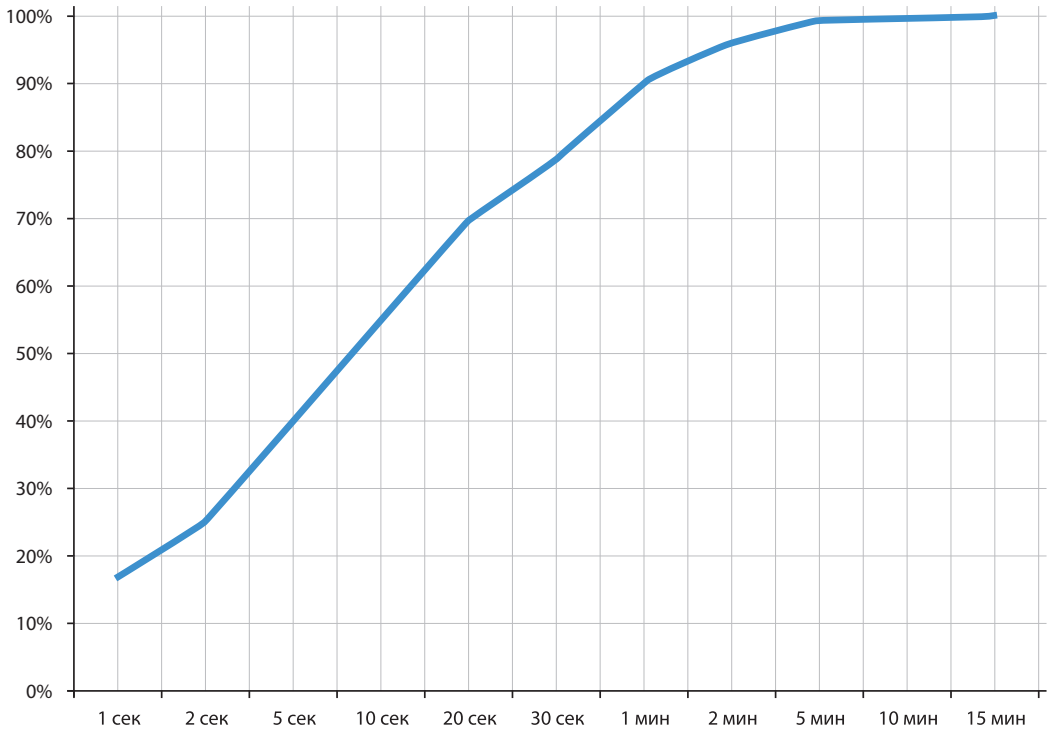


Рис.3. Количество расшифрованных PDF-файлов в зависимости от времени атаки.

При настройке программы есть возможность выбрать тип используемого процессора, что позволяет оптимизировать перебор вариантов. В любом случае программа предлагает оптимальный режим работы в зависимости от вашего процессора, в список которых входят Non-MMX processors, Intel PII/PIII/Celeron, AMD Athlon, Intel P4 SSE2. Для процессоров Intel Core, Core Duo or Core 2 Duo, наибольшая скорость работы достигается при выборе из списка значения Intel PII/PIII/Celeron.

Возможности программы можно оценить на примере пробной версии, которая хотя и имеет ограниченный функционал (восстановление паролей длиной до 4 символов и расшифровка только первых 10% страниц документа), однако дает полноценное представление о продукте.

ELCOMSOFT DISTRIBUTED PASSWORD RECOVERY

О пользе распределенных вычислений для решения трудоемких задач мы говорили выше. В случае с восстановлением доступа к PDF-документам это может понадобится при работе с большим объемом документов, стойкими паролями и расширенными алгоритмами шифрования.

Программа состоит из трех компонентов: сервер, агент и консоль. Сервер (рис.4) устанавливается на один из компьютеров в сети и управляет процессом перебора паролей. На любые компьютеры в сети может быть установлен агент, который перебирает порции паролей, выдаваемые сервером. С любого компьютера может быть запущена консоль, которая позволяет управлять сервером перебора, добавлять новые задачи и просматривать статистику. Для сервера и агента доступны пробные версии.

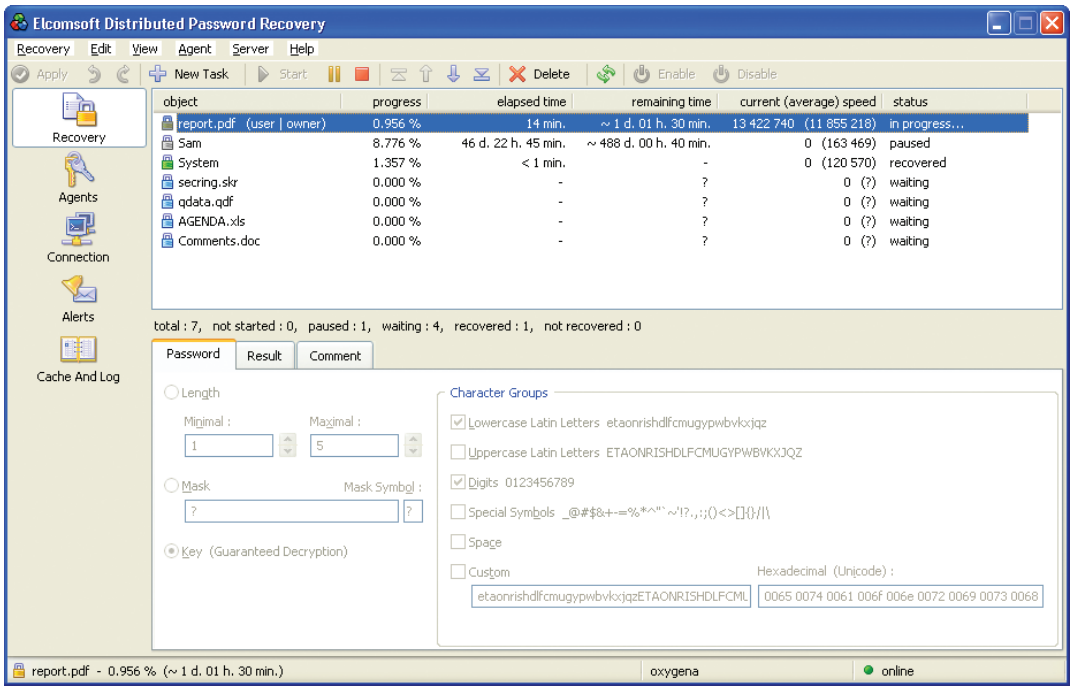


Рис.4. Главное окно ElcomSoft Distributed Password Recovery (компонент «сервер»).

ELCOMSOFT
PROACTIVE SOFTWARE

О КОМПАНИИ «ЭЛКОМСОФТ»

Основанная в 1990 году, российская компания «ЭлкомСофт» является одним из лидеров рынка программного обеспечения для восстановления доступа к системам, приложениям и документам. Благодаря уникальным технологиям, продукты компании получили широкое признание как в России, так и за рубежом.

В число клиентов «ЭлкомСофт» входят многие известные в мире из следующих отраслей:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Компания имеет статусы Microsoft Gold Certified Partner, Intel Software Partner, а также является членом Российской криптографической ассоциации, Computer Security Institute (CSI), Association of Shareware Professionals (ASP).

Компания «ЭлкомСофт» является признанным экспертом на рынке, на ее технологические разработки ссылаются во многих известных книгах, например, «Microsoft Encyclopedia of Security», «The art of deception» (Kevin Mitnick), «IT Auditing: Using Controls to Protect Information Assets» (Chris Davis), «Hacking exposed» (Stuart McClure).

Чтобы узнать больше, посетите сайт компании.

АДРЕС:
ООО «ЭлкомСофт»
Звездный б-р, 21, офис 541
129085 Москва

ФАКСЫ:
US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

ВЕБ-САЙТЫ:
http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr