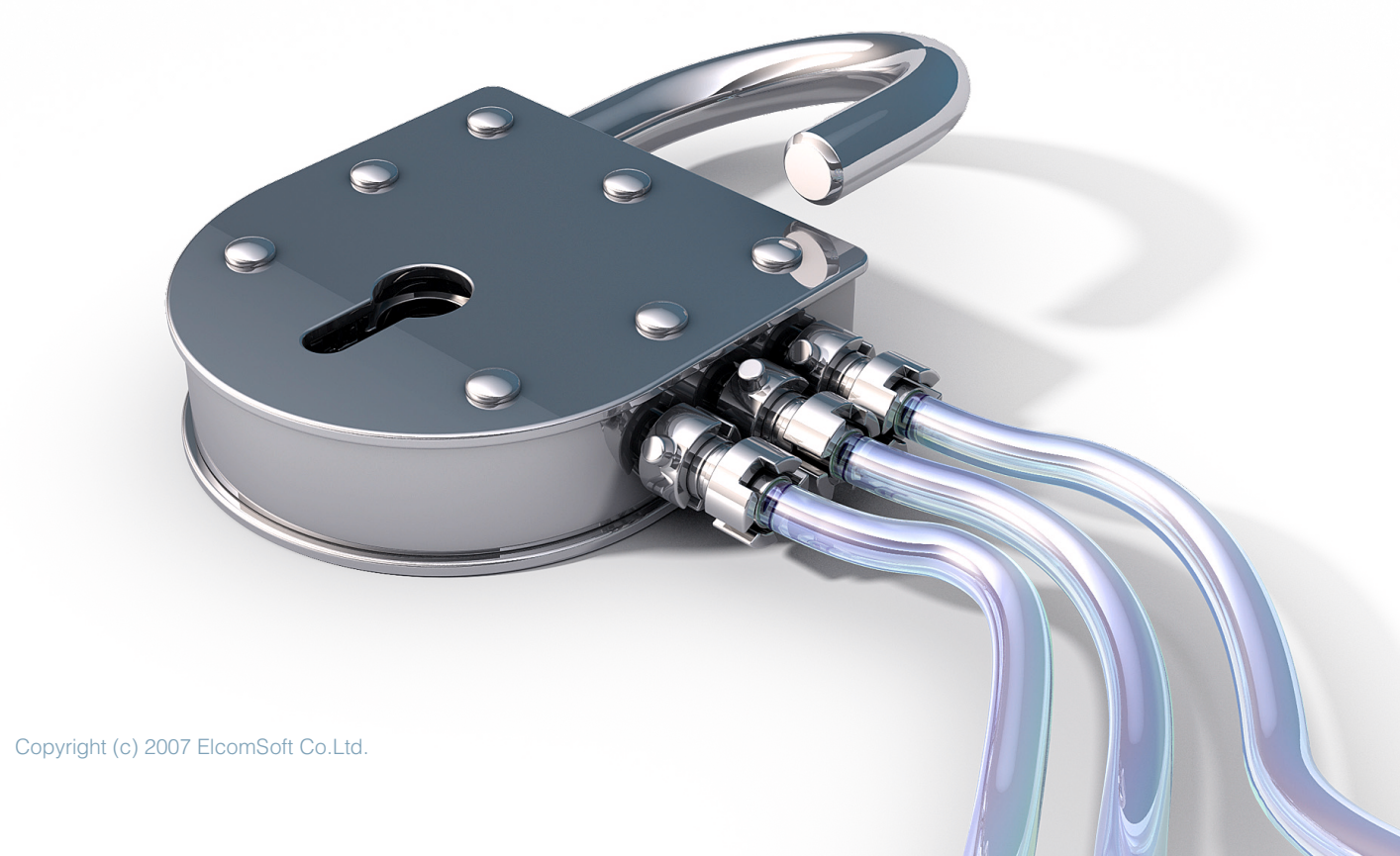
ELCOMSOFT
PROACTIVE SOFTWARE

РАЗМЕР ИМЕЕТ ЗНАЧЕНИЕ

ПРЕИМУЩЕСТВА РАСПРЕДЕЛЕННОЙ АРХИТЕКТУРЫ ВОССТАНОВЛЕНИЯ ДАННЫХ



ELCOMSOFT
PROACTIVE SOFTWARE

СОДЕРЖАНИЕ

Информация – ключ к верным решениям 3

Защита – задача первого приоритета 3

Утрата доступа – ежедневная реальность 4

Немного о паролях 5

Методы восстановления паролей 6

Простой перебор
Перебор по маске
Атака по словарю
Rainbow-атака

Время – деньги 9

Как увеличить скорость нахождения пароля? 10

Распределенные вычисления
Преимущества метода для поиска паролей
Критерии выбора решения

Elcomsoft Distributed Password Recovery – пароль здесь и сейчас 13

О компании ElcomSoft 16

ИНФОРМАЦИЯ – КЛЮЧ К ВЕРНЫМ РЕШЕНИЯМ

Такие слова, как «информационная эра», «информационные технологии», «кто владеет информацией, тот владеет миром» прочно поселились в нашем сознании и сегодня каждый верит, что информация – один из самых ценных ресурсов.

Но так ли важна информация сама по себе? Это не совсем верно. Информация нужна для принятия решений. Вот, что действительно важно. Правильное решение – это путь к успеху в любом деле. Поэтому владение информацией является конкурентным преимуществом в современной бизнес-среде.

Неудивительно, что защите информации уделяется повышенное внимание. И поскольку большая ее часть в наше время создается и хранится в электронном виде (документы Microsoft Office, разнообразные базы данных, финансовые данные в формате Intuit Quicken и т.д.), то в первую очередь речь идет о программных и аппаратных средствах защиты.

ЗАЩИТА – ЗАДАЧА ПЕРВОГО ПРИОРИТЕТА

IT-безопасность – это отдельное, динамично развивающееся направление в отрасли информационных технологий. На рынке представлены многочисленные решения, ограничивающие доступ к информации и предотвращающие ее утечку: инструменты контроля доступа и аутентификации, системы предотвращения вторжений, программы резервного копирования, антивирусные приложения и другие.

Но если говорить о самых простых, доступных каждому пользователю, мерах по защите информации, то среди них непременно окажется парольная защита, которая позволяет предотвратить несанкционированный доступ к информации.

Данные о продажах и финансовых потоках, клиентская база данных, бухгалтерская и управленческая отчетность, аналитические отчеты и прогнозы – вся эта информация необходима как для успешного ведения операционной деятельности компании, так и для принятия стратегических решений о развитии бизнеса. Доступ без пароля к большей части подобной информации, как правило, невозможен. Такова элементарная политика безопасности в любой компании.

УТРАТА ДОСТУПА – ЕЖЕДНЕВНАЯ РЕАЛЬНОСТЬ

Известно, что в любой информационной системе самым уязвимым местом остается человек. И ситуация с парольной защитой – не исключение.

Несмотря на то, что существует целый комплекс мер, направленных на укрепление парольной защиты – ограничения минимальной длины и сложности пароля, их аудит, регулярная смена паролей – ничто не может решить самую распространенную проблему в этой области – утрата пароля. Вряд ли найдется человек, который работал за компьютером и ни разу не сталкивался с этим.

Вы можете просто забыть пароль. Признайтесь, ведь было? Как человек разумный, вы его не записали в своем ежедневнике, а предпочли запомнить, используя простую ассоциацию. Например, любимое блюдо + год вашего рождения. С годом рождения все ясно, но вот кулинарные пристрастия изменились и блюдо вспомнить не удается.

Бывает и так, что менеджер по продажам уволился, а пароль для просмотра отчетов о поставках вам не оставил. Связи с ним в данный момент нет, контрагенты грозятся разорвать с вами договора, если вы немедленно не оплатите счета, а на основе каких данных это сделать, не вполне ясно. Знакомо?

В случае же, когда увольнение сотрудника было связано с его участием в финансовых махинациях или работой на конкурирующую компанию, рассчитывать на добровольное раскрытие пароля и вовсе бессмысленно. А доступ к информации нужен. Причем срочно.

Итак, необходимо решить задачу восстановления доступа к зашифрованным данным. Ирония состоит в том, что в этом случае все усилия, направленные на повышение стойкости парольной защиты в организации, оборачиваются против вас. Чем строже политика безопасности, тем сложнее обойти защиту. Однако поспешим вас обрадовать: в большинстве случаев восстановить доступ к информации можно.

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. Не будем забывать также, что пароли могут быть разной длины. Это важно в том случае, когда пароль невозможно восстановить или сбросить, а только лишь найти методом прямого перебора.

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). Кратко 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 если задать 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 оптимального 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.

ВРЕМЯ – ДЕНЬГИ

Итак, разобравшись в том, какими бывают пароли и что представляют из себя основные методы их восстановления, мы можем предположить основные сложности, возникающие при решении проблемы восстановления доступа к данным: это вероятность нахождения пароля и время, за которое задача может быть решена.

В целом сложность задачи поиска пароля или ключа зависит от многих факторов: длины пароля, набора встречающихся в нем символов, типа документа, к которому пароль подбирается, алгоритма шифрования, мощности компьютера. При этом, как правило, вероятность находится в прямой зависимости от времени: современные технологии позволяют найти практически любой утерянный пароль вероятностью 100% в том случае, если время не ограничено.

Заметим также, что в последние годы пользователи стали гораздо более осторожны, они все реже выбирают короткие и простые пароли. Например, около 60% пользователей портала MySpace[1] используют пароли длиной 8 и более символов, и всего лишь в 1% случаев были использованы пароли длиной 5 символов. Что касается состава паролей, то более 80% из них содержат буквы и цифры, а пароли, состоящие из одного слова, которое встречается в словаре, составляют всего лишь 3,8%.

Как уже было сказано выше, может случиться так, что нужный пароль встретится быстро, и все возможные комбинации перебирать не придется. Но всегда стоит рассчитывать на худший вариант развития событий и при определенных обстоятельствах речь может идти о годах вычислений. И кому нужен пароль к документу годовалой давности?

Получается, при решении задачи нахождения пароля время является критически важным фактором, так как информация быстро теряет свою актуальность и становится ненужной. Каким же образом можно сократить время расшифровывания документа?

Алгоритмы шифрования, длина и сложность пароля, а также тип документа являются исходными данными и не могут быть изменены. Поэтому единственное, что находится в нашей власти – это используемые вычислительные мощности.

[1] http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300

КАК УВЕЛИЧИТЬ СКОРОСТЬ НАХОЖДЕНИЯ ПАРОЛЯ?

РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛЕНИЯ

Несмотря на то, что современные процессоры обрабатывают информацию с очень высокой скоростью, для одного компьютера восстановление пароля методом прямого перебора по-прежнему является сложной задачей и может занять непозволительно много времени.

В мире уже давно стоит задача создания крупного вычислительного ресурса для решения трудоемких задач, требующих многих лет машинного времени (например, исследование белков, математических законов, человеческого генома, предсказание погоды и др.). Для таких вычислений необходимы «суперкомпьютеры», то есть компьютеры небывалой производительности. Число суперкомпьютеров постоянно растет, однако их стоимость очень высока: суперкомпьютеры есть не в каждой организации и даже не у каждого государства[2].

А что, если объединить несколько обычных компьютеров вместе? А если их не несколько, а десятки или даже сотни? Мы получим вычислительный ресурс совершенно иного порядка. Так появилась идея распределенных вычислений – способа решения трудоёмких вычислительных задач с использованием двух и более компьютеров объединённых в сеть. Для этого необходимо, чтобы задача была разделена на секции, которые могли бы вычисляться одновременно на разных машинах. Таким образом, каждый отдельный компьютер обрабатывает небольшую порцию данных общего массива глобальной задачи.

Обычный компьютер может справиться с подобной задачей играючи, да еще и в условно свободное время. Не секрет, что при типичной работе, например, в Windows (интернет-браузер, офисные программы и пр.) чуть ли не 99% всего рабочего времени процессор попросту простаивает в ожидании ввода пользователем новых задач и понапрасну потребляет электроэнергию.

Специальное ПО, используемое в проектах распределенных вычислений загружает полезной работой процессор именно в это «свободное» время. Программа работает в фоновом режиме или начинает работу только тогда, когда процессор свободен и при необходимости немедленно сворачивает свою деятельность, чтобы возобновить её, когда он опять освободится, поэтому для пользователя работа такой программы почти незаметна.

[2] По данным http://www.top500.org/ на июнь 2007 г. из 8 из 10 суперкомпьютеров, возглавляющих список 500 самых мощных компьютеров, находились в США

ПРЕИМУЩЕСТВА МЕТОДА ДЛЯ ПОИСКА ПАРОЛЕЙ

Итак, наша задача – перебор всех возможных комбинаций символов для нахождения искомого пароля и получения доступа к документу – относится именно к тому типу задач, которые могут быть успешно решены путем распределенных вычислений. Каждая машина может работать лишь с порцией паролей или документов, значительно сокращая общее время нахождения пароля.

Необходимо учитывать, что если доступ к некоторым документам и приложениям можно восстановить за короткий срок на обычном компьютере (например, пароли к документам, созданным в приложениях IBM® Lotus® SmartSuite® и Corel® WordPerfect® Office, независимо от их длины и сложности или пароли к ICQ или Google Talk, сохраненные локально), то для взлома других паролей ресурсов одного компьютера будет недостаточно – о каком бы сроке ни шла речь. Для некоторых форматов документов и алгоритмов шифрования в силу их особенностей не может быть обеспечена высокая скорость перебора. Например, при использовании процессора Intel® Core™2 Duo для документов формата Microsoft Office 2007 скорость перебора составляет не больше 100 паролей в секунду, а для RAR-архивов и вовсе не более десяти. Поиск ключей PGP также довольно трудоемок: в зависимости от форматов и алгоритмов скорость может меняться от десятков до тысяч паролей в секунду. Но и для тех случаев, когда скорость перебора приличная (например, для используемых по умолчанию 40-битных ключей к документам Word/Excel 97/2000/XP/2003, Adobe Acrobat PDF), распределенные вычисления имеют вполне реальные преимущества. На одной машине, даже очень мощной, процесс займет несколько дней, а при использовании сети компьютеров – несколько часов, а то и минут. Кроме этого, если документов много, то без распределенных вычислений задачу быстро не решить, как ни крути.

Помимо самого главного преимущества – экономии времени – также отметим следующие плюсы такого метода:

- нет необходимости выделять отдельный компьютер(ы) для решения задачи восстановления пароля;
- можно обрабатывать большое количество документов;
- компьютеры могут использоваться как в нерабочее, так и рабочее время (не мешая работе сотрудников);
- можно использовать даже самые слабые компьютеры сети, они тоже внесут свою скромную лепту в общее дело;
- можно варьировать число задействованных компьютеров в зависимости от количества документов, предполагаемой сложности пароля и срочности задачи.

КРИТЕРИИ ВЫБОРА РЕШЕНИЯ

Итак, вопрос о целесообразности применения программы распределенных вычислений для быстрого восстановления паролей не стоит. Такой инструмент должен иметь под рукой каждый системный администратор. Затраты на его приобретение очень быстро окупятся. На что важно обратить внимание при выборе 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 Microsoft Office или Adobe Acrobat вам придется столкнуться при восстановлении пароля. Узнайте также, как быстро добавляется поддержка новых версий приложений.

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.

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

ELCOMSOFT DISTRIBUTED PASSWORD RECOVERY – ПАРОЛЬ ЗДЕСЬ И СЕЙЧАС

Решение Elcomsoft Distributed Password Recovery позволяет задействовать вычислительные мощности всех компьютеров, объединенных в сеть – как локальную, так и глобальную.

С ее помощью вы сможете восстановить пароль практически к любому документу формата Microsoft Office – Word, Excel, PowerPoint (любых версий), а также пароли Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes, пароли пользователей Windows 2000/XP/2003/Vista, секретные ключи PGP (*.skr), PGP Disk (*.pgd), PGP Whole Disk Encryption, ZIP-архивы PGP (*.pgp), сертификаты PKCS #12 (*.pfx), хеши MD5.

Для документов, созданных в Word 97-2003, Excel 97-2003, разработчики гарантируют 100% восстановление пароля на открытие при условии применения 40-битного ключа шифрования (используется в Microsoft Office этих версий по умолчанию). Гарантируется также расшифровка документов Adobe Acrobat PDF с длиной ключа 40 бит (он используется по умолчанию в ранних (до 6.0) версиях Adobe Acrobat, а также может быть выбран пользователем в Acrobat 6, 7 и 8). С помощью Elcomsoft Distributed Password Recovery для документов PDF могут быть найдены оба вида стандартных паролей: на открытие (Document Open или user-пароль) и на изменение (Permissions или owner-пароль) – при использовании как 40-битных, так и 128-битных ключей шифрования.

Благодаря хорошо продуманной архитектуре программы, список поддерживаемых в Elcomsoft Distributed Password Recovery форматов файлов постоянно расширяется.

Программа использует архитектуру «клиент-сервер» и состоит из трех компонентов: сервер, агент и консоль (см.рис. 1).

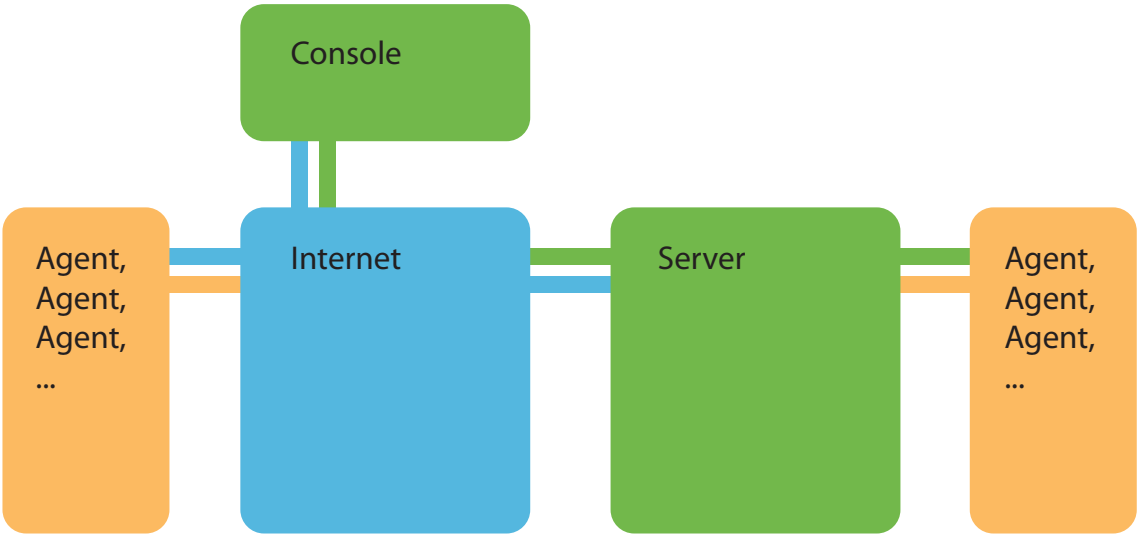


Рис.1. Архитектура Elcomsoft Distributed Password Recovery

Сервер 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. Для отправки обработанных данных и получения новых агенты периодически обращаются к серверу. Данные передаются в упакованном виде, а связь между агентом и сервером активна только в момент обмена информацией, поэтому нагрузка на сеть и объем трафика минимальны даже при большом количестве агентов, что не может не радовать системного администратора.

С любого компьютера может быть запущена консоль, которая позволяет управлять сервером перебора, добавлять новые задачи и просматривать статистику. Сервер перебора паролей может управляться как локально, так и удаленно. Для агентов могут быть заданы время работы (по дням недели и часам в любой из дней) и приоритет выполняемой задачи.

При создании задачи может быть выбран метод восстановления доступа к документу: поиск по длине пароля (задаются минимальная и максимальная длина), поиск по маске (если известна часть пароля) или поиск ключа с гарантированным восстановлением. Есть возможность ограничить набор возможных символов пароля (прописные и/или строчные символы, цифры, специальные символы, пробелы). В любой момент по запросу администратора обработка задачи может быть приостановлена / возобновлена.

Одно из важных преимуществ программы – удобство работы с большим количеством файлов. Elcomsoft Distributed Password Recovery позволяет создать очередь из любого количества документов, приоритет обработки которых может быть в любой момент изменен. Таким образом, мы благодаря решению «ЭлкомСофт» мы экономим не только вычислительные ресурсы, но и рабочее время сотрудников службы безопасности.

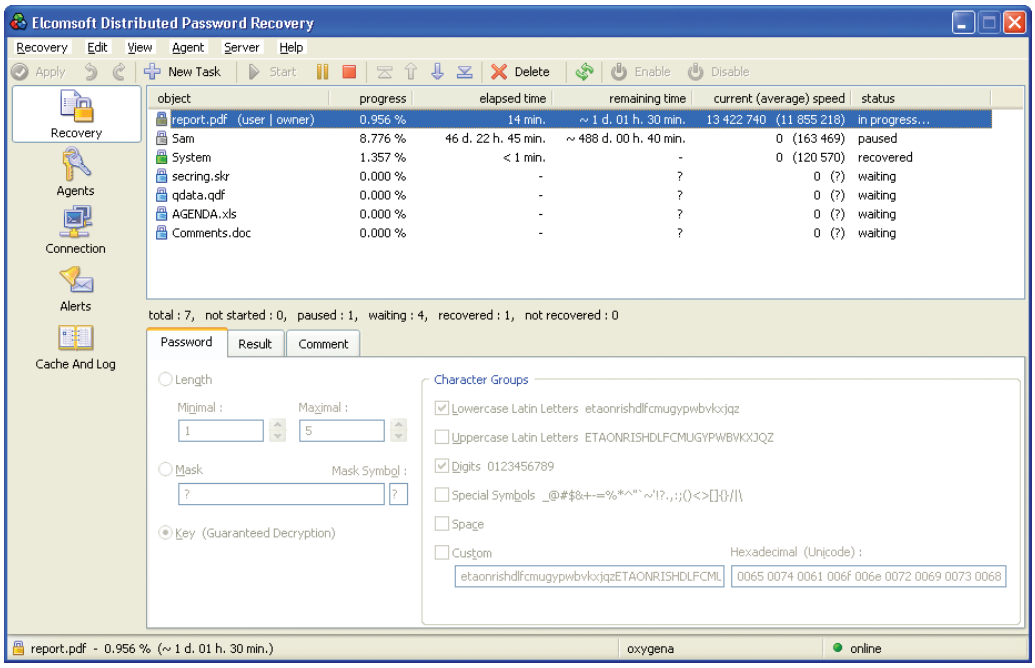


Рис 2. Главное окно Elcomsoft Distributed Password Recovery (компонент «сервер»)

Итак, в дополнение к обозначенным выше преимуществам использования распределенных вычислений для поиска паролей и ключей, подытожим сильные стороны Elcomsoft Distributed Password Recovery:

- **Поддержка широкого спектра приложений**. С помощью Elcomsoft Distributed Password Recovery вы сможете быстро и эффективно восстановить доступ практически к любым документам.
- **Масштабируемость**. Программа может быть эффективно использована в сети любого размера.
- **Минимальная нагрузка на сеть**. Обмен данными в упакованном виде и минимизация сетевого трафика обеспечивают минимальную нагрузку на вашу сеть.
- **Тонкая настройка работы агентов**. Для каждого агента может быть обозначен приоритет задачи поиска пароля, а также точное время работы (по дням и часам в каждый из дней).
- **Использование всех доступных компьютеров**. Назначение приоритета задаче поиска паролей и ключей, настройка времени работы агентов, минимальные требования к программному и аппаратному обеспечению агентов позволяют использовать даже самые слабые машины в сети.
- **Работа с большим потоком документов**. В очереди на обработку может находиться любое количество документов.
- **Выбор порядка обработки документов**. Для каждого файла обозначается приоритет обработки – он может быть изменен в любое время.

Для сервера и агента доступны пробные версии.

ELCOMSOFT
PROACTIVE SOFTWARE

О КОМПАНИИ ELCOMSOFT

Основанная в 1990 году, российская компания Elcomsoft 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 Elcomsoft 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