RMS системы на страже контента

крис касперски, no-email

появление в Server 2003 системы управления правами (Rights Management Services или, сокращенно, RMS), обещающий защитить содержимое электронных документов от неавторизованного использования, вызывает большой интерес со стороны крупных и мелких компаний, страдающих хроническими утечками информации и хватающихся за каждое решение, словно за соломинку. эффект, однако, превосходит все ожидания и после развертывания RMS проблемы плодятся в геометрической прогрессии…

введение
/ полоса 2, колонки 1, 2 */*

Электронный документооборот, в отличии от бумажного, намного хуже поддается контролю и в больших организациях становится практически неуправляемым. Регулярные утечки данных — лучшее тому подтверждение. Сотрудники сплошь и рядом выкладывают секретные документы в открытый доступ (умышленно или по халатности), копируют их на ноутбуки, которые всюду таскают с собой пока их не украдут (а крадут их достаточно часто), не говоря уже о том, что файлы, хранящиеся на рабочих станциях, становятся легкой добычей для хакеров, особенно, если рабочая станция имеет прямой выход в Интернет.

Списки управления доступом (ACL), поддерживаемые всеми современными операционными системами, малоэффективны в плане безопасности, поскольку они защищают конкретный экземпляр файла, а не сам документ. Поясним это на следующем примере. Допустим, на сервере лежит файл, к которому некоторый сотрудник имеет доступ только на чтение, а подавляющее большинство остальных вообще никакого доступа не имеют. Однако, так продолжается лишь до того момента пока файл не окажется на рабочей станции обозначенного сотрудника, после чего он может делать с ним все что угодно, и любое лицо, имеющее доступ к его машине, автоматически получает доступ к секретному файлу. А если записать файл на носитель типа CD/DVD, то секретности придет полный конец. И не только потому, что файловая система CD/DVD не поддерживает атрибутов разграничения доступа, и даже не потому, что украсть CD/DVD намного легче, чем получить доступ к запароленному компьютеру (ведь не будешь каждому сотруднику ставить сейф) – однажды скопированный документ начинает жить собственной жизнью, зачастую идущую в разрез с интересами организации.

При увольнении сотрудника очень сложно, а точнее практически невозможно, заставить его выдать все электронные документы, которые он успел накопировать за это время. Они могут быть где угодно! Например, в сотовом телефоне, находящимся в рюкзаке, заброшенном на антресоли, так что тут даже обыск не поможет.

Осознав масштабность проблемы, многие компании стали продвигать на рынок системы управления правами (Rights Management Services), забыв о том, что они противоречат самой природе электронного документа: все, что можно просмотреть, можно и скопировать. То есть наличие прав доступа на чтение равносильно праву на полный доступ. В некоторой степени, сказанное справедливо и для бумажных документов — злоумышленнику достаточно увидеть документ, чтобы скопировать его тем или иным образом (переписать от руки, сфотографировать, прогнать через ксерокс), однако, копирование бумажных документов требует либо времени, либо специального оборудования, а потому может быть пресечено чисто организационными мерами (впрочем, с учетом миниатюрности современных камер — едва ли). Но электронные документы защитите от копирования не поддаются в принципе!!!

Тем не менее, системы управления правами все-таки снижают остроту проблемы, предотвращая _непредумышленные_ утечки информации и предъявляя к инсайдерами повышенные требования, поскольку обойти защиту может только хакер или продвинутый пользователь.

Систем управления правами существует много, их сейчас выпускают все кому не лень, но агрессивнее всех себя ведет Microsoft, проталкивая свои далеко не самые лучше разработки, и… как гласит известная пословица, "Bill always wins", и хотя Бил уже давно не Бил, а Стив, у Microsoft есть все шансы занять доминирующее положение на рынке, потеснив или даже

полностью вытеснив остальных, так что к ее продуктам следует присмотреться повнимательнее, что мы сейчас и сделаем.

>>> врезка минимальные системные требования /* полоса 2, колонка 3 */

Развертывание RMS-системы требует, чтобы на сервере в обязательном порядке было установлено следующее программное обеспечение:

- Windows Server 2003;
- файловая система NTFS (FAT поддерживается, но не рекомендуется);
- Microsoft Message Queuing Service (MSMQ);
- Internet Information Services 6.0 (с включенным ASP .NET);
- Windows 2000 Service Pack 3 или выше Active Directory Domain;
- Microsoft SQL Server 2000 (или Desktop Engine) SP3 или выше;

RMS: обзор возможностей /* полоса 3, 4, картинки — в полосу 2, колонку 3 */

В линейке NT система управления правами впервые появилась в Windows Server 2003 (кодовое имя — Windows Rights Management Services), получив дальнейшее развитие в Windows Server 2008, где она была интегрирована с Active Directory и переименована в Active Directory Rights Management Services. Обе системы требуют _обязательной_ клиентской поддержки и в настоящее время клиенты выпущены практически для всех операционных систем, когда-либо созданных компаний Microsoft: Windows 9x/Me/2000, XP и Vista. Для UNIX-систем клиентов пока нет и неизвестно появятся ли они в дальнейшем. Протокол закрыт и сторонние разработчики отдыхают. Уже одно это отвращает от такой защиты, но… все-таки пересилим себя и посмотрим, что сотворила Microsoft и насколько "оно" отличается от рекламы.

Нам предлагают систему шифрования документов (включая электронные письма и web-страницы), основанную на сертификатах, контролирующих политику использования документа, создатель которого может по своему желанию управлять правами на редактирование, копирование в буфер обмена, печать и даже время использования документа, по истечении которого его будет уже не открыть. Идея такого подхода не нова и уже давно реализована конкурентами (взять того же Adobe). Степень ее (не)стойкости так же хорошо известна. Нашумевшее дело Склярова помните? Так вот, если мы предоставляем право на открытые документа, то воспользовавшись "нечестной" (читай — "хакнутой") версией клиента, злоумышленник без труда выдерет исходное содержимое, записав его в любом незащищенном формате, например, RTF. Если же мы лишим пользователей прав на чтение документа, то тут же возникает резонный вопрос: что они будут с таким документом делать и чем он отличается от того же RTF, зашифрованного, например, RAR'ом и переданного получателю без пароля. Очень смешно, да. И стоило огород городить?!

Стоило! Система управления правами существенно упрощает процесс документооборота, позволяя сотрудникам расслабится и копировать документы как угодно и куда угодно. Теперь злоумышленнику недостаточно украсть CD/DVD с зашифрованным файлом. Ведь ключа ни на диске, ни в самом файле нет. Ключ хранится на сервере и выдается только при наличии соответствующего сертификата, подтверждающего правда на доступ (в зависимости от настроек клиента копия ключа может храниться и на локальной машине, однако, чтобы до нее "дотянуться" необходимо атаковать рабочую станцию, а если рабочая станция атакована, то _никакие_ защитные меры не смогут предотвратить неавторизованный доступ к охраняемому документу, особенно, если хакер получил права администратора или проник на уровень нулевого кольца через дыру в драйвере).

Таким образом, утечка секретных документов, защищенных RMS, сама по себе не приводит к раскрытию конфиденциальности и хакер (или инсайдер) вынужден предпринять дополнительные активные действия, оставляющие за собой трудноудалимую цепочку следов. Именно на это обстоятельство и делает упор Microsoft. В своем faq (http://technet2.microsoft.com/WindowsServer/en/library/0f14390c-8de5-4829-95af-87f48d13869c1033.mspx) компания прямо так и заявляет, что RMS не есть абсолютная защита, а просто средство автоматизации документооборота, входящее в "обойму" огромного оборонительного комплекса, воздвигнутого на пути атакующего. Без дополнительных защитных мер RMS – ничто и взламывается на раз-два-три. Вот такая официальная позиция разработчиков, идущая вразрез с позицией отдела маркетинга. Ну да бог с ней, с этой рекламой,

лучше посмотрим как происходит при создании, передаче и открытии документа. Весь процесс состоит из пяти шагов (см. рис. 1).

1. автор документа, обращаясь к RMS-серверу, получает сертификат лицензирования клиентов (client licensor certificate или, сокращенно, CLC) в формате XrML, которым и подписывает документ;
2. назначив желаемые права доступа к документу (кто может его открывать и что с ним делать вплоть до указанного времени), автор на основе CLC создает парную ему публичную лицензию (publishing license), включаемую в файл документа и используемую для шифрования его содержимого;
3. автор передает документ пользователю (или группе пользователей) по любым каналам связи, включая ненадежные или спокойно выкладывает документ в открытый доступ, зная, что никто другой все равно не сможет его прочитать;
4. получатель обращается к RMS-серверу. Сервер (убедившись, что получатель имеет достаточные права для открытия файла) передает ему пользовательскую XrML-лицензию, содержащую ключ с помощью которого RMS-клиент расшифровывает содержимое документа, позволяя совершать над ним обозначенные действия (например, смотреть, но не редактировать и не печатать);
5. пользователь работает с документом в MS Office или IE. Для других программ RMS-клиентов не предусмотрено. Кстати говоря, даже если у клиента отсутствует MS Office он все равно может просматривать документы, поскольку в RMS-клиент встроен свой собственный HTML-рендер, что по мнению Microsoft очень хорошо. Ну текстовые документы — это еще куда бы то ни шло (правда, просматривать их в IE не слишком удобно), но вот электронные таблицы в браузер просто не помешаются и без Excel'я здесь никак не обойтись. Вообще говоря, трудно представить себе организацию у которой есть средства на SQL-сервер и RMS-сервер, но которая не может обеспечить своих сотрудников офисными пакетами.

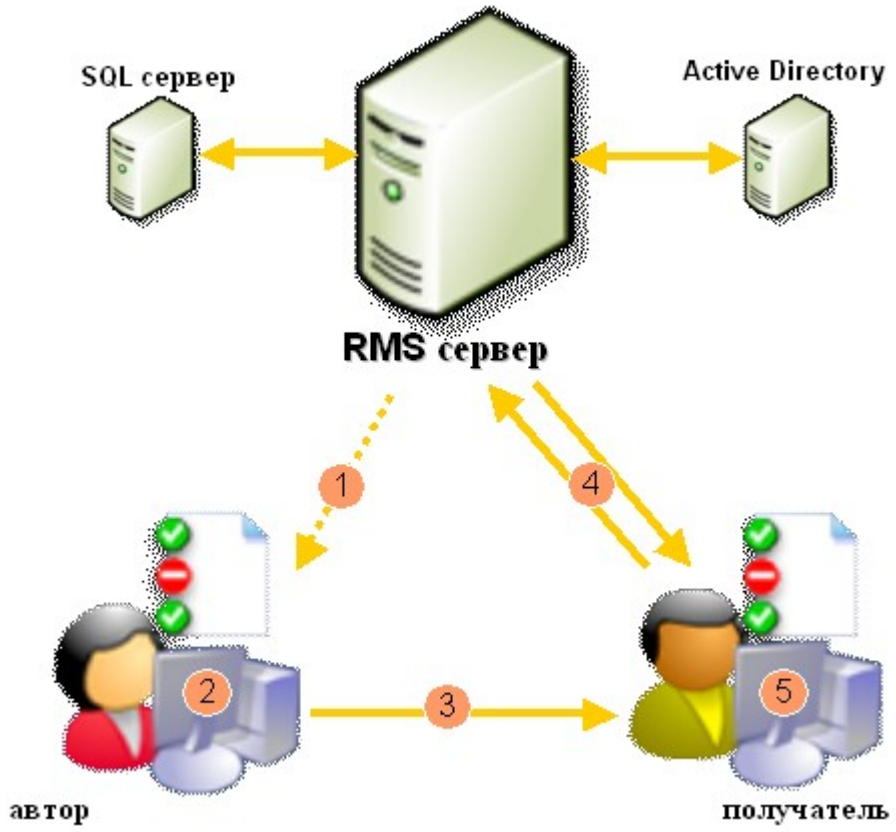

Рисунок 1 схема работы RMS. от подписи документа до открытия

По умолчанию CLC-сертификаты вместе с пользовательскими лицензиями хранятся на локальной машине в папке %USERPROFILE%\Local Settings\Application Data\Microsoft\DRM, что делает их доступными для всех злоумышленников, обладающих правами текущего пользователя, а это очень и очень плохо. Было бы намного лучше разместить лицензии в защищенном хранилище, доступном только псевдопользователю с правами System (что повыше администратора будет) и взаимодействующих с клиентом через специальные API-функции. Тогда прямое копирование лицензий оказалось бы невозможным, что затруднило бы атаку.

Хранение лицензий на пользовательских машинах имеет и другой недостаток — кража машины (например, ноутбука) позволяет злоумышленнику просматривать защищенные документы без обращения к RMS-серверу и никто не в силах ему помешать. Формально, в RMS-систему заложен механизм отзыва лицензий, что очень полезно, например, в случае увольнения сотрудника из компании. Аннулировав лицензию, компания лишает его права доступа ко всем защищенным документам. Очень заманчивая перспектива! Ведь, как известно, большинство должностных нарушений происходит в момент увольнения или после него. Обиженный сотрудник запросто может выложить в открытый доступ конфиденциальные документы. Вместе с лицензией, хранящийся на его компьютере (без лицензии защищенные документы не прочтешь). А чтобы ее не аннулировали, инсайдер просто не будет выходить в сеть или закроет доступ к RMS-серверу на встроенном в XP брандмауэре. И все те, кто скачает лицензии, поступят аналогичным образом. Вот такая, с позволения сказать, защита. Выход один – каждый раз, вместе с попыткой аннулирования ранее выданной лицензии (лицензий) генерировать новый CLC-сертификат и заново подписывать все "защищенные" документы, если, конечно, до них удастся "дотянутся". А это навряд ли. Потому как документы, сохраненные на локальных машинах, полностью автономны и никому не подвластны.

Опять-таки с формальной точки зрения, можно ограничить срок "валидности" лицензии, по истечении которого пользователь будет вынужден обратиться к RMS-серверу за новой лицензией. Если, конечно, не догадается остановить системные часы. То есть на практике, механизм отзыва лицензий работает только с честными и лояльными сотрудниками, которые удалили бы документ и так, без всякой возни с сертификатами, обработка которых сама по себе представляет нехилую проблему, особенно в распределенных организациях со множеством филиалов. В Server 2003 каждый RMS-сервер, входящий в общую сеть, хранит все сертификаты, даже если ни один из сотрудников данного филиала не имеет к ним доступа. Ну это он до развертывания RMS-системы его не имел, а после — достаточно проникнуть на сервер и все! Конец секретности! Но это еще полбеды. Другая половина заключается в избыточном трафике. Возьмем достаточно крупную организацию, насчитывающую в своем составе 100 тыс. сотрудников. А это как минимум 100 тыс. сертификатов! "Как минимум" потому что в реальности их будет гораздо больше, особенно если используются сертификаты с ограниченным временем "годности". Синхронизация часов всех RMS-серверов — это третья серьезная проблема. А перевод часов вперед — эффективная атака, парализующая работу организации (или одного из ее филиалов).

В Server 2008 протокол обмена сертификатами существенно усовершенствован и теперь по сети передаются только те сертификаты, которые реально нужны данному филиалу, но все равно Microsoft рекомендует использовать _один_ RMS-сервер, что, конечно, решает проблемы синхронизации сертификатов и системных часов, но зато требует надежных каналов связи с центральным сервером, который превращается в весьма соблазнительную мишень для хакеров. Во-первых, он виден не только из локальной сети, но и из Интернет. Во-вторых, на нем есть _все_ сертификаты и в-третьих, если его завалить, то это будет мега-даун, после которого не всякая компания сможет быстро оправиться.

Что поделаешь! Каждая технология имеет свои издержи и RMS-системы — здесь не исключение. Но это в общем то решаемые проблемы. Можно, например, создавать подчиненные RMS-сервера, хранящие сертификаты только данной организации, или сразу загружать все необходимые сертификаты с центрального сервера, кэшируя их на локальных машинах, для обретения автономии. Вариантов много. Администраторы у нас умные, они со всем справятся!

Еще Microsoft предлагает использовать RMS для защиты электронной корреспонденции. А вот это уже совсем не смешно! Проблема защиты почты действительно существует и эта проблема настолько серьезна, что компании хватаются за любую соломинку, которую только им ни кинут. Реклама рисует радужную картину — если у получателя установлен Outlook 2003 и с ним установлены доверительные отношения (то есть он имеет прямой доступ к RMS-серверу через Интернет), ему вообще не придется совершать никаких дополнительных телодвижений. То есть защита достается как бы бесплатно. Но это в теории она бесплатна. А на практике Outlook 2003 — закрытый коммерческий продукт, конкурирующий с

другими почтовыми клиентами. Где гарантия, что получатель не предпочитает The Bat, например, или не сидит под Linux'ом? И в чем состоит суть защиты? Перехватить почту, переданную по защищенным каналам связи или через тот же SSL, хакеру все равно не удастся даже без использования RMS, а если он проникнет на клиентскую машину, с которой RMS-сервер находится в доверительных отношениях, он прочитает не только почту, но и утянет пользовательскую лицензию, позволяющую ему читать остальные RMS-документы. То есть, использование RMS неявно предполагает, что все получатели заботятся о своей безопасности, надежно защищены от атак и не собираются передавать лицензии третьим лицам, но если это так, то какой смысл навязывать им RMS?!

Ответ — RMS страхует лояльных пользователей от элементарной халатности. Ведь конфиденциальное письмо легко переслать по ошибке совсем не тому лицу, которому оно предназначалось! Тоже самое может произойти и в результате сбоя почтового сервера. Если у получателя нет доступа к RMS-серверу, то прочитать письмо он не сможет. Вообще-то, для защиты корреспонденции можно использовать несимметричную криптографию, зашифровав послание с помощью PGP, ставшей стандартом де-факто, но это слишком просто и неинтересно.

>>> врезка защита от грабежа
/ полоса 4, колонка 3 */*

RMS-клиент от Microsoft поддерживает защиту документа от грабежа по <Alt-Print Screen>, чего не делает Abode. Естественно, грабить текст через <Alt-Print Screen>, а потом прогонять его через OCR, никто не собирается — проще хакнуть клиента, заставив его проигнорировать атрибуты защиты. Грабеж графических изображений — другое дело. Главный недостаток Abode Acrobat Reader'a как раз и состоит в том, что выдрать изображение из защищенного документа может любой мало-мальски грамотный пользователь. Так что RMS в этом смысле выглядит намного более предпочтительным решением для защиты. В теории.

На практике же, об <Alt-Print Screen> (копирующим в буфер обмена содержимое активного окна) знает гораздо меньше пользователей, чем о кнопке <Print Screen> (копирующей весь экран целиком). Достаточно забрать у RMS-клиента фокус (щелкнув мышью по Рабочему Столу, например) и… <Print Screen> скопирует защищенный документ как ни в чем ни бывало!

Хорошо, простим Microsoft'у этот ляп, который, возможно будет исправлен в следующих версиях (хотя исправить его будет довольно трудно, поскольку блокировать <Print Screen> RMS-клиент не имеет морального права, поэтому ему придется отслеживать каждое нажатие оного, установив глобальный хук на клавиатурный ввод и анализировать Z-порядок окон, "вырезая" из изображения содержимое защищенного документа, но оставляя нетронутым все остальное). Но ведь помимо Print Screen'a существуют и другие грабберы, самые простые из которых просто подменяют контекст графического устройства на контекст метафайла или принтера, после чего RMS-клиент будет послушно выводить защищенный файл на принтер или метафайл, ошибочно полагая, что имеет дело с монитором.

А вот если бы RMS-клиент использовал так называемый overlay mode (поддерживаемый практически всеми современными графическими картами), то <Print Screen> показал бы просто фиолетовый (реже — зеленый, но это уж как драйвер видео-карты захочет) прямоугольник. Грабеж в overlay mode поддерживают очень немногие программы, о существовании которых осведомлены только хакеры и продвинутые пользователи. Однако, overlay mode в каждый момент времени может использовать только одно окно одного приложения. И при открытии еще одного RMS-документа в соседнем окне, клиент вынужден либо закрыть (свернуть) первое, либо отказаться выполнять данную операцию, сославшись на недостаток ресурсов.

внутри RMS
/ полоса 5, колонка 1 */*

Рекламные обзоры, посвященные RMS, утверждают, что для защиты документов используется 2048-битные RSA-ключи, взломать которые невозможно даже если напрячь распределенную сеть, состоящую из суперкомпьютеров. Короче, даже правительство при всем своем желании не сможет узнать, чем мы тут занимаемся (ну разве что задействует специалистов по терморектальному криптоанализу).

На самом деле, содержимое защищенного документа зашифровано 128-битным AES ключом, подобрать который вполне реально, пускай для этого потребуется серьезные финансовые вложения (ну или ботнет средних размеров). Однако, AES ключи (они же — content

keys) генерируются произвольным образом для каждого документа и потому взлом одного из них позволяет прочесть лишь данный документ или даже часть его. Для остальных документов, найденный AES ключ бесполезен и перебор необходимо начинать по новой.

Content keys хранятся непосредственно в самом защищенном файле в зашифрованном виде. Для шифрования используется 1024-битный RSA ключ. А вот 2048-битное шифрование встречается только непосредственно на RMS-сервере.

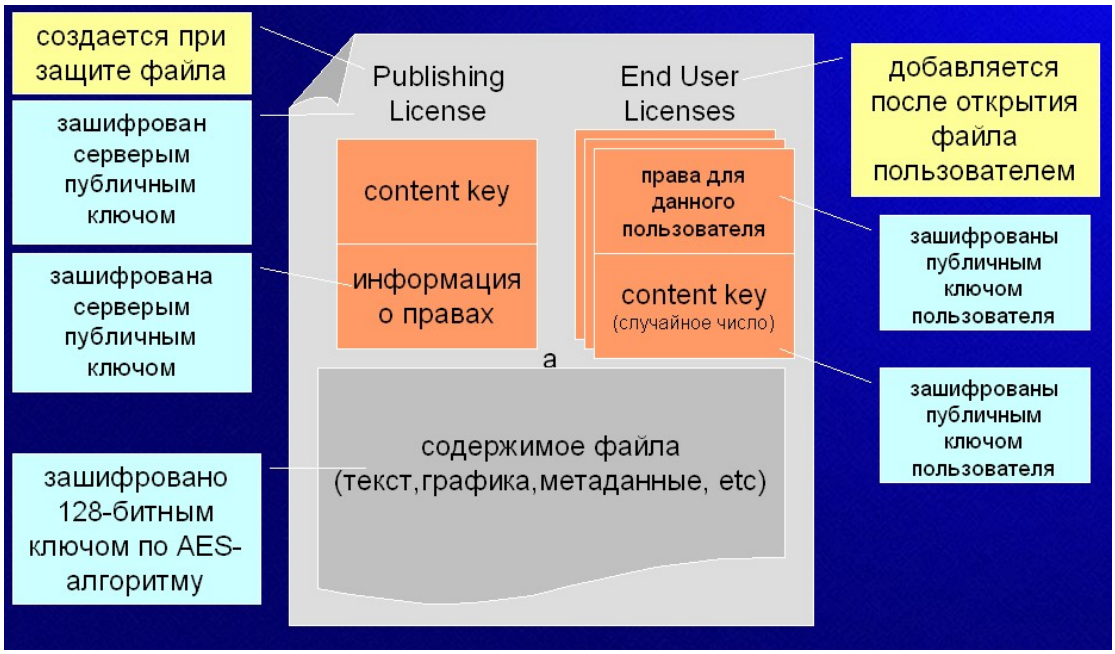

Рисунок 2 структура документа, защищенного системой RMS

Трудно сказать насколько корректно выполнено шифрование. Возможно, в нем есть ошибки, снижающие стойкость защиты, однако, в первом приближении можно считать, что открыть документ, не имея пользовательской лицензии, выданной RMS-сервером, действительно невозможно, да и не нужно, поскольку если мы заполучи защищенный документ, то есть все основания полагать, что мы можем заполучить и пользовательскую лицензию с ключом. После чего остается расшифровать content key, открывающий доступ к содержимому документа.

Самое интересное, что content key в защищенном файле встречается дважды. Первый раз — в публичной лицензии, зашифрованной публичным серверным RSA-ключом (2024 бит), и второй раз в — в пользовательской лицензии, зашифрованной битным пользовательским RSA-ключом (1024 бит), добавляемым в файл после его первого открытия данным пользователем. То есть, даже если хакер не имеет доступа к RMS-серверу, ему достаточно добыть ключ любого из пользователей, когда-либо открывавших данный документ. А добыть его несложно, ведь рабочие станции защищены от атаки намного хуже серверов!

Рисунок 3 не вскрываемых шифров не бывает! бывают — плохо разогретые паяльники!

недостатки RMS от Microsoft
/ полоса 5, колонка 2, 3 */*

Крупным фирмам очень важно иметь возможность прочитать файл через десять или даже пятьдесят лет после его создания, поэтому, предпочтения отдаются открытым форматам (например, PDF). Закрытые используются с большой осторожностью, особенно если они завязаны на конкретную операционную систему типа Windows. Кто знает, что случится с Microsoft через четверть века — быть может к тому времени рынок окажется во власти UNIX-клонов… Зачем же становится добровольным заложником RMS?

Мелкие фирмы такими проблемами не озадачиваются, но RMS, очевидно, сделан отнюдь не для мелких фирм. Это довольно масштабная система, требующая серьезных аппаратных ресурсов, а они, между прочим, денег стоят, в результате чего, затраты на внедрение и эксплуатацию RMS вплотную приближаются к стоимости самой охраняемой информации, которая в мелких фирмах быстро теряет свою актуальность даже без всякой системы отзыва сертификатов. Если хакер утянет смету строительной организации и передаст ее конкурентам до подписания договора, жертва потеряет сумму с пять шестью нулями. И двумя цифрами спереди. Но после того, как договор заключен, красть документ бесполезно. Тем более, что RMS от целенаправленной атаки все равно не защищает…

Самое прискорбное, что защищать документы _внутри_ организации дело, конечно, нужное, но бесполезное, тем более с помощью RMS, которая в данном случае работает ничуть не лучше ACL — если инсайдер имеет права на чтение документа, то "отодрать" RMS от содержимого — дело техники. Microsoft отлично это осознает и предлагает… использовать RMS для защиты документов извне организации. Действительно, многие фирмы испытывают острую необходимость защиты документов, выкладываемых в публичный доступ. Никому же ведь не хочется, чтобы злоумышленники выдирали из них куски текста или элементы графического оформления, используя их без выплаты всяких отчислений. Adobe Acrobat Reader (популярный клиент для просмотра PDF-документов) поддерживает атрибуты защиты, но! уровень защищенности на 100% определяется "честностью" клиента и существует множество "нечестных" клиентов, игнорирующих атрибуты защиты и практически все продвинутые пользователи знают как сломать защищенный PDF.

Документы, защищенные RMS, подвержены той же самой болезни. Нечестный клиент позволит скопировать/распечатать документ даже если его создатель строго запретил это делать. Разница между PDF и RMS в том, что PDF – открытый формат, подробно описанный в спецификациях от Abode и написать клиента может кто угодно, а RMS еще необходимо "распотрошить" или "хануть" двоичный файл фирменного клиента от Microsoft, что требует на порядок больше времени. Однако, если для чтения PDF'a достаточно установить Adobe Acrobat Reader, реализованный практически на всех операционных системах, то прочитать RMS-документ можно только под Windows после установки соответствующего клиента и только при наличии соединения с Интнернетом, позволяющим "достучаться" до RMS-сервера по HTTP/HTTPS-протоколам, которые администратор локальной сети вполне мог закрыть на брандмауэре, чтобы сотрудники на качали порнушку, а занимались делом. То есть, если получатель документа по каким-либо причинам решил воздержаться от развертывания RMS, прочитать защищенный документ он не сможет.

Очевидно, что RMS – это система с избыточной сложностью. Существует множество плагинов для Adobe Acrobat Reader'a обладающих совершенно идентичным функционалом, но довольствующихся намного более скоромными аппаратными ресурсами и не привязанных к Windows. Обычно они используются для защиты электронных книг, при первом открытии которых обращаются к удаленному серверу, получают сертификат, указывающий какие действия может совершать читатель и через какое время книга должна быть удалена/заблокирована. Ряд плагинов кэширует сертификаты на локальной машине подобно RMS, что позволяет работать с документом автономно, т. е. в офф-лайне. Другие же плагины "стучаться" на сервер при каждом открытии документа, что не слишком удобно для пользователей, зато намного более надежно в плане защиты. Естественно, нечестный клиент сможет отодрать защиту при первом же открытии документа, и в этом плане PDF ничуть не лучше RMS, но ведь и не хуже! Зато использование PDF обойдется намного дешевле, его смогут прочесть _намного_ больше людей и самое главное, расширения сторонних производителей уже не взламываются стандартными "хакерскими" PDF-клиентами и под каждый планин требуется писать отдельного нечестного клиента. Поиск по хакерским сайтам показывает, что с такими клиентами дела обстоят не самым лучшим (для взломщиков) образом и из десятков популярных плагинов реально хакнуты всего два или три. Почему? А потому, что каждый плагин по отдельности захватывает лишь небольшую часть рынка и хакерам просто лень возиться. Любое же широко распространенное решение (типа RMS) обречено на поражение.

заключение

Выходит, что RMS – просто очередной монстр, рожденный в недрах Microsoft? В каком-то смысле, да (для Microsoft вообще характерны тяжеловесные решения, взять хотя бы десятки тысяч API-функций и сравнить их с сотней системных вызовов UNIX или сопоставить основную файловую систему FreeBSD – UFS основной файловой системе NT – NTFS, сложность различается на порядок, а ведь и UNIX и NT решают сходные задачи). Однако, если у нас уже есть SQL-сервер, Active Directory-сервер и мы используем Microsoft Office, то как дополнительный уровень защиты документов RMS-система будет вовсе не лишней.

Естественно, мы должны отдавать себе отчет в том, что защищенные документы не удастся прочитать под другими операционными системами, поэтому, имеет смысл защищать только "скоропортящиеся" документы, которые все равно должны быть уничтожены по прошествии некоторого времени. Тогда система временных сертификатов автоматически превращается в шредер, страхующий нас от _непреднамеренного_ оседания копий документа на разных резервных носителях.

Кстати, свежий случай из жизни. Шеф говорит: "этот документ нужно удалить, т. к. он содержит компрометирующую нас информацию!". "Ага", отвечает администратор, — "и он восстановится при первом же восстановлении с бэкапа, или же придется отследить и уничтожить все DVD-R, на которых он был зарезервирован". А вот использование RMS позволило бы решить эту проблему одним махом.

мнение экспертов
Пьер Зимерман (Pierre Zimmermann)
аналитик одного из подразделений корпорации IBM
/ полоса 6, колонки 1, 2, 3 */*

Рисунок 4 Пьер Зимерман, исследовавший RMS

A: Пьер, какое отношение Вы имеете к RMS?
Q: Я входил в состав исследовательской группы, которой было поручено проанализировать RMS-систему от Microsoft и протестировать ее на предмет стойкости, надежности, масштабируемости, целесообразности внедрения и т. д. Мы изучили RMS и отправили "наверх"

270-страничный отчет, в котором лично я написал пару десятков страниц. Несмотря на то, что отчет не содержит конфиденциальной информации, без разрешения моих боссов я не в праве предоставить его электронную копию для ознакомления, но, по крайней мере я могу ответить на ваши вопросы.

A: каковы планы IBM в отношении RMS?
Q: Вот этого я сказать не могу, поскольку такие решения принимаются на высоком корпоративном уровне, причем, зачастую принимаются неожиданно, и всем нам приходится лишь подчиняться. Впрочем, IBM – очень большая корпорация со множеством подразделений, многие из которых достаточно автономны и могут выбирать программные продукты самостоятельно, естественно, в рамках своих локальных сетей. Однако, исходя из самых общих рассуждений, я склонен считать, что IBM скорее всего откажется от RMS. Во-первых, в IBM не очень-то любят Microsoft (и это ни для кого не секрет), у нас используется множество альтернативных операционных систем — коммерческие клоны UNIX'a, xBSD, различные Linux'и, наконец, экспериментальны оси собственной разработки, предназначенные для внутреннего использования, поэтому, документооборот организован с учетом этой разнородной среды и основан на открытых стандартах и пакетах. Возможно, какое-то отдельное подразделение и будет использовать RMS, но в масштабе всей корпорации переход на него попросту невозможен. Лично у меня и у моих коллег на компьютере установлен Linux, а сервера нашего подразделения работают под управлением FreeBSD. И хотя запланировано введение в эксплуатацию нескольких экспериментальных серверов, работающих под управлением Windows Server 2008, сносить уже работающие операционные системы никто не собирается. Во-вторых (и это главное!), RMS не обеспечивает реальной защиты документов и организационные меры вкупе с ACL оказываются намного более эффективным решением.

A: назовите основные недостатки RMS в реализации от Microsoft
Q: прежде всего это интеграция RMS с остальными продуктами от Microsoft и невозможность ее использования на альтернативных операционных системах. Документооборот крупных компаний не должен быть привязан к конкретным операционным системам. В каком-то смысле RMS можно сравнить с наркотиком. Однажды начав использовать ее, вы попадаете в жестокую зависимость от воли Microsoft. Вы не можете "соскочить с иглы", обратившись к конкурентам, поскольку RMS это не часть системы документооборота, это _сам_ документ. В таких условиях, стандартные рыночные механизмы уже не работают и вы вынуждены следовать за Microsoft не потому, что она предлагает более удачные решения, а потому что программное обеспечение конкурентов не поддерживает закрытый формат, а как только оно его поддержит (хотя бы частично), Microsoft тут же внесет небольшие, но очень противные изменения и совместимость окажется утеряна. Возможно, в будущем ситуация радикально измениться, но сейчас дела обстоят именно так. Другой недостаток связан с механизмом шифрования, стойкость которого находится под большим сомнением, и развеять эти сомнения может только всесторонний анализ, выполненный известными крипитоаналетиками, но для этого формат документов должен быть открыт всем желающим, поскольку, дизассемблировать двоичные файлы RMS-клиентов от Microsoft только затем, чтобы убедиться, что продукт — дерьмо, желающих нет. Тут действует такой принцип, если продукт _возможно_ содержит скрытый дефект, то мы просто отказывается от него. В конечном счете, никто же не требует от нас мотивированного отказа.

A: тем не менее RMS, несмотря на очевидные недостатки, все-таки продвигается на рынок. Почему?
Q: Это для нас с вами они очевидны. Крупные компании и корпорации могут позволить себе напрячь целый отдел изучением очередного "подарка" от Microsoft, чтобы выявить его реальные, а не заявленные достоинства и недостатки. Компании рангом поменьше ограничиваются чтением популярных журналов, в которых RMS преподносится если не как восьмое чудо света, то как значительный шаг вперед. Microsoft хорошо известна своим агрессивным маркетингом, но в ситуации с RMS она превзошла сама себя. Вот, например, предлагается использовать RMS для защиты… патентов. Но ведь любому человеку известно, что всякий патент можно получить в патентом бюро за чисто символическую сумму или даже вообще бесплатно. Еще предлагается использовать RMS в медицине. А вот это уже откровенное надувательство. Практически все развитые государства предъявляют к системам охраны медицинских документов вполне определенные требования, которым RMS не отвечает. Во всяком случае, еще ни одна страна не сертифицировала RMS для использования в медицинской

отрасли, следовательно, крупные учреждения не могут использовать RMS даже если сильно захотят. Так о каком продвижении RMS-систем на рынок мы говорим? Нету этого продвижения. И не будет. Мелкие компании, впечатленные рекламными буклетами, могут использовать все, что угодно и RMS в том числе, но критические инфрастуктуры Microsoft пока что не по зубам.