INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

# Сравнение TrueCrypt и InfoWatch CryptoStorage

Anti-Malware.ru, Олег Калядин, эксперт по криптографической защите информации InfoWatch, 15.12.2011

**Одним из эффективных способов защиты конфиденциальных данных от несанкционированного доступа является их шифрование. При этом в идеале работа с зашифрованными объектами не должна приводить к существенному увеличению нагрузки на вычислительные мощности предприятия. В статье рассматривается технология прозрачного шифрования или шифрования «на лету» (On-the-fly encryption) на примере программных продуктов TrueCrypt 7.1 и InfoWatch CryptoStorage 2.1.**



## Введение

Целостность, конфиденциальность и доступность… тут можно было бы добавить, по аналогии с известным высказыванием – вы можете выбрать любые два пункта, но – спрос рождает предложение, – бизнес требует обеспечения конфиденциальности без снижения доступности. Проще говоря, информацию нужно защищать, но при этом нагрузка на инфраструктуру не должна увеличиваться в разы, а доступ легитимного пользователя к необходимым для работы данным не должен сопровождаться временными лагами, замедлением системы и прочими «прелестями» избыточной «секьюрности».

Решение известно давно – технология прозрачного шифрования или шифрования «на лету», когда данные пользователя хранятся на носителе всегда в зашифрованном виде. В оперативной памяти компьютера расшифровывается только та часть, с которой идёт непосредственная работа, а при записи на носитель информация снова зашифровывается. В данной статье мы последовательно рассмотрим два продукта, реализующие, технологии шифрования на лету - TrueCrypt (http://www.truecrypt.org/) и **InfoWatch** CryptoStorage (http://www.cryptostorage.ru/).

Что и как «прозрачно» шифруется в этих программах? В **InfoWatch** CryptoStorage объединены три подсистемы криптографической защиты данных, позволяющие:

создавать виртуальные защищенные диски (защищенные контейнеры) для размещения конфиденциальной информации и работы с ней;

защищать всю информацию в логических разделах жесткого диска (включая системные и загрузочные), на Flash-накопителях и прочих устройствах класса Mass Storage;

создавать отдельные защищенные папки в файловой системе NTFS для размещения конфиденциальной информации и работы с ней.

**InfoWatch** CryptoStorage будет полезен и домашним пользователям, и небольшим компаниям (SOHO), поскольку ко всем объектам защиты возможен многопользовательский доступ. Объекты

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

могут располагаться на локальных компьютерах и в локальной сети (на серверах и рабочих станциях). В TrueCrypt защищенная (зашифрованная) информация пользователя находится в специальных крипто-контейнерах (аналогично защищенным контейнерам в **InfoWatch** CryptoStorage) и на разделах жестких дисков или флеш-накопителей (аналогично защищенным логическим разделам диска в **InfoWatch** CryptoStorage). К каждому защищенному объекту TrueCrypt существует единственный пароль (ключ) доступа.

Полезность многопользовательского доступа в «домашних» продуктах иногда недооценивают, между тем у владельца конфиденциальной информации время от времени возникает необходимость поделиться частью данной информации с кем-либо, но не со всеми. Этот доступ может быть впоследствии прекращен по желанию владельца. В **InfoWatch** CryptoStorage описанные манипуляции можно сделать с уже существующими защищёнными объектами (хранилищами) информации, не создавая новых объектов для общего доступа с новыми паролями (ключами), и не помещая в них информацию для совместного использования.

Объекты и подсистемы защиты

Крипто-контейнеры являются самыми распространенными объектами хранения защищённой (зашифрованной) информации. Именно с крипто-контейнеров практически и начиналось «прозрачное» шифрование. Крипто-контейнеры – это специальные файлы, которые создаются программой защиты. После подключения контейнера программой защиты с ним можно работать как с обычным логическим диском. Только этот диск - виртуальный, а вся информация на нём зашифрована.

Крипто-контейнеры в TrueCrypt и **InfoWatch** CryptoStorage почти не отличаются. Правда, в TrueCrypt контейнеры - это основной вид защищенных объектов, а в **InfoWatch** CryptoStorage они выполняют скорее вспомогательные функции. Контейнер можно записать на CD/DVD, отправить по почте, носить на флешке вместе с незашифрованной информацией. Кроме того, крипто-контейнер можно размещать на внешних сервисах для хранения, передачи и совместной работы с информацией в Интернете. Например, очень удобно хранить информацию в контейнере, используя Dropbox, с установленным агентом на компьютере пользователя. «Прозрачность» работы с данными сохраняется. Конфиденциальность гарантируется.

К сожалению, у крипто-контейнеров есть существенные недостатки:

Контейнер, в неподключённом состоянии – это просто файл. Его можно стереть со всей информацией в нём, даже не зная пароля (ключа) доступа.

Размер контейнера необходимо определять при его создании. Это верхняя граница количества информации, которую можно записать в контейнер. В общем случае файл-контейнер занимает на диске место, равное размеру своего виртуального диска, даже если в контейнере пока нет никакой информации. И в TrueCrypt, и в **InfoWatch** CryptoStorage существует возможность создания динамических контейнеров, файлы которых увеличиваются в размере по мере заполнения контейнера. Но при стирании информации в таких контейнерах размер их файлов, а, значит, и место на диске, занимаемое ими, не уменьшается. В TrueCrypt для создания динамических контейнеров используются разреженные (sparse) файлы. Поэтому такой контейнер можно создать только на диске с NTFS – недостаток для пользователей флешек, где, как правило, используется FAT.

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

Потребуется либо переформатирование, либо конвертирование флешки, со всеми вытекающими последствиями. Другой недостаток заключается в том, что копия такого динамического контейнера (разреженного файла) всегда им

еет максимально заданный размер и утрачивает свои «динамические» свойства. Данный способ создания динамических контейнеров существует и в **InfoWatch** CryptoStorage. Кроме этого, в **InfoWatch** CryptoStorage для создания динамического контейнера можно использовать быстрое (quick) форматирование под любой из FAT при создании контейнера. Такой контейнер может быть создан на диске с любой файловой системой. Копия такого контейнера всегда имеет размер оригинала.

После подключения контейнера вся информация на виртуальном диске подключённого контейнера доступна всем пользователям, имеющим соответствующие административные права. Кроме этого, возможен доступ из любых сеансов пользователей на данном компьютере, а также по сети. В отличие от TrueCrypt и многих других программ, использующих крипто-контейнеры, в **InfoWatch** CryptoStorage имеется возможность подключения контейнера только для текущего пользователя. Это делает контейнер доступным только из сеанса пользователя, его подключившего. Другие пользователи работать с контейнером не могут.

Затруднена одновременная многопользовательская работа по сети. Если контейнер подключить, а виртуальный диск подключённого контейнера «расшарить» для других пользователей, то данные между компьютерами будут передаваться в открытом виде, информация в контейнере будет доступна всем пользователям, имеющим права сетевого доступа, как на обычном незащищённом диске. Если же каждый пользователь подключит контейнер как диск на своём компьютере, то информация по сети будет передаваться в зашифрованном виде, но в этом случае контейнер будет доступен только для чтения.

Защита жестких дисков

В TrueCrypt подсистема шифрованных разделов жесткого диска дифференцирована. Правила работы с каждым типом разделов – системных и не системных - значительно отличаются друг от друга.

Защита несистемных разделов – это типовая потребность большинства пользователей. Несистемные разделы - это и флеш-накопители, и просто логические разделы дисков, на которых хранится информация пользователей.

Зачастую у пользователя в данных разделах информация уже существует. Причем, объем этой информации может быть очень большим, соизмеримый с размером HDD, десятки и даже сотни ГБ. Возникает потребность установить защиту на раздел с данными (зашифровать раздел с уже существующими данными). Данные при установке защиты должны сохраниться. Такая возможность, якобы, предусмотрена в TrueCrypt и называется она Encrypt partition in place.

Почему «якобы»?

Это возможно только начиная с ОС MS Windows Vista. В распространенной, на сегодняшний день ОС MS Windows XP этого делать нельзя.

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

Раздел должен быть отформатирован под NTFS.

Если флешка была переформатирована или конвертирована под NTFS и на ней хранится информация, которую пользователь решил зашифровать, то процесс установки защиты нельзя прерывать даже штатной для этого случая кнопкой, не говоря уже о различных сбоях, которые могут возникнуть в процессе (по питанию, зависание системы и т.д.). Процесс установки защиты на флешку не очень быстрый, поэтому может произойти прерывание. Данные в этом случае теряются, и продолжить процесс установки защиты невозможно.

Время установки защиты (шифрования) на раздел с данными может измеряться часами, причем во время установки защиты работать с этим разделом нельзя. Более того, если раздел «недошифрован», подключить его и работать с ним нельзя до тех пор, пока процесс не завершится. Откатить назад установку защиты на «недошифрованном» разделе невозможно. Весь путь придется пройти до конца, прежде чем удастся добраться до данных.

Предположим, что пользователь всё-таки создал зашифрованный несистемный раздел. Существует ряд проблем при работе с такими разделами, а именно:

Раздел невозможно подключить в ту же букву, в которую он был подключён. Защищенный раздел в подключенном состоянии занимает теперь две буквы. Одна – это точка монтирования, другая - бывшая точка монтирования. Причём работать можно только с первой.

Данные в неподключенном зашифрованном (защищенном разделе) не защищены от уничтожения, стирания. Любой пользователь или программа могут это сделать случайно или нарочно, даже если не известен пароль (ключ) пользователя, допущенного к этим данным. Более того, при попытке обратиться к такому разделу в неподключённом состоянии ОС сообщает, что раздел не форматирован и предлагает выполнить форматирование. Пользователь может забыть или не знать, что раздел содержит зашифрованные данные, и выполнить форматирование. Пользователь может быть и злоумышленником, или от его лица может быть запущен вредоносный код. Для недошифрованных разделов диска картина аналогичная, даже несмотря на то, что подключить такой раздел невозможно.

А теперь, – самое главное – снять защиту с такого раздела (расшифровать данные) невозможно! Чтобы снять защиту TrueCrypt, пользователь должен подключить раздел, скопировать из него куда-либо всю информацию (например, несколько сотен ГБ) после чего переформатировать раздел и записать всю информацию (те же несколько сотен ГБ) обратно.

При работе с системными разделами прерывание процесса шифрования («crash-test» на отключение питания) как при установке, так и при снятии защиты приводит к «синему экрану смерти» (BSOD) при последующих загрузках и невозможности восстановить информацию на системном разделе.

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

**InfoWatch** CryptoStorage перечисленных недостатков лишен. Защита может устанавливаться на раздел с данными и сниматься с такого раздела независимо от типа раздела, файловой системы и ОС. В процессе установки/снятия/переустановки защиты возможна работа с данными на этом разделе. Процесс может быть прерван с последующим прерыванием или отменой. Прерывание процессов установки/снятия/переустановки защиты не приводит к потере данных ни при каких обстоятельствах: ни при корректном прерывании пользователем, ни при сбое питания.

Общим недостатком защиты (шифрования) дисков является то, что диск должен быть подключён на том компьютере, на котором он установлен физически. Дальнейшая работа с этим диском после подключения идёт как с незащищённым. При этом вся информация на диске становится доступна всем пользователям, имеющим соответствующие административные права доступа, и из всех сеансов на данном компьютере и по сети. При «расшаривании» такого диска данные передаются по сети в незашифрованном виде.

Ещё одним типом естественных объектов хранения информации ОС, которые можно защитить при помощи **InfoWatch** CryptoStorage, являются папки файловой системы. В TrueCrypt и во многих других продуктах с «прозрачным» шифрованием аналогичных объектов защиты просто не существует. А между тем использование защищённых папок как отдельных объектов защиты или совместно с другими типами защищённых объектов позволяет качественно повысить защищённость и решить многие проблемы.

Защищенные (зашифрованные) папки могут быть созданы средствами **InfoWatch** CryptoStorage на дисковом разделе (томе) с NTFS.

Папка, как объект файловой системы предоставляет большие возможности по удобству хранения информации. Она занимает на томе столько места, сколько занимают файлы внутри неё и её подпапок. Размер папки всегда поддерживается файловой системой ОС в актуальном состоянии. Все файлы внутри защищенной папки и её подпапок всегда зашифрованы.

Важным свойством защищенной папки является то, что в неподключенном состоянии (пользователь не ввёл ключ или пароль доступа) папка никому не доступна на компьютере с установленной системой защиты, а содержимое файлов внутри папки нельзя посмотреть, нельзя стереть или исправить информацию. Если же система защиты отключена или папка находится на удаленном компьютере (файловом сервере), то в обход системы защиты пользователь вместо содержимого файлов из защищённой папки видит цифровой мусор (информацию в зашифрованном виде).

Защищенная папка, расположенная на компьютере с установленным решением для защиты, даже в подключенном состоянии доступна только пользователю (программам пользователя), в сеансе которого произошло подключение, причем только на компьютере, на котором находится данная папка. Сетевой доступ к защищенной папке невозможен даже для администратора сети (домена).

Важным свойством защищенной папки является возможность организации многопользовательского иерархического доступа к подпапкам защищённой папки, одновременная работа с защищенной информацией группы пользователей. При этом вся информация расшифровывается непосредственно в оперативной памяти компьютеров пользователей, имеющих ключи доступа к подпапкам. По сети до компьютеров пользователей информация передаётся в

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

шифрованном виде. Не требуется установка решения защиты непосредственно на файловый сервер. Сервер используется только для хранения зашифрованных папок.

В **InfoWatch** CryptoStorage реализована возможность гарантированного удаления файлов и папок - в TrueCrypt этой возможности нет.

Как уже говорилось ранее, **InfoWatch** CryptoStorage состоит из трёх подсистем. Все подсистемы защиты являются независимыми друг от друга. Внутри любого защищенного объекта может находиться другой защищённый объект. При этом типы объектов могут быть различны, а глубина вложенности практически не ограничена. При необходимости пользователь может отключить любые подсистемы защиты. В этом случае соответствующие подсистемы никак не будут проявлять себя.

Осталось добавить, что TrueCrypt имеет одно неоспоримое преимущество – программа распространяется бесплатно. Насколько это весомый аргумент – каждый пусть решит для себя сам.

Оригинал публикации: http://www.anti-malware.ru/compare/TrueCrypt_vs_InfoWatch_CryptoStorage