РЕШЕНИЕ КЕЙСА ИНФОБЕЗ

команда ибэшники

Наша команда решила основную проблематику кейса Централизации управления защищенными ресурсами посредством разработки новой системы менеджмента паролей, способной поддерживать безопасность всей системы области в случае, если произошел несанкционированный доступ к центральному серверу, а так же предложением внедрения системы администрирования средств криптографической защиты информации Secret Disk Enterprise и системы выявления и реагирования на инциденты информационной безопасности DeviceLock DLP.

Суть метода системы хранения паролей, обеспечивающей статичное подключение работников правительства области к системе:

Предположим, что в области N есть 5000 правительственных компьютеров и 50 городов (50 MAN). В центральном сервере всего хранится 5000, которые предназначены для осуществления входа в систему каждого работника. Однако также параллельно осуществляется хранение специальных 50 паролей, предназначенных для рассылки 100 пользователем.

Система рассылки специальных паролей работает следующим образом:

В начале рабочего дня работник, закрепленный за отдельным ПК, вводит свой пароль, который хранится на сервере и предназначенный только для его аутентификации. Затем, когда сервер убеждается в том, что за ПК есть человек, который сможет участвовать во 2 этапе аутентификации, она вносит его IP-адрес в специальную базу. В итоге после первого этапа аутентификации на сервере формируется база IP-адресов пользователей. Теперь из сервера выбирается один из специальных паролей и в случайном порядке шифруется последовательно 100 раз (в случае, если все 5000 работников готовы войти в систему). Далее пароль, зашифрованный 100 раз, отправляется пользователю, открытый пароль которого первым использовался во время шифрования. Пользователь вводит свой закрытый, нигде не хранимый, шифр (пароль №2). Расшифрованное им сообщение включает в себя часть с IP- или МАС – адресом того пользователя, которому необходимо переслать расшифрованное сообщение. В итоге специальный протокол рассылки паролей адресует расшифрованное сообщение следующему пользователю, к0торый получает начальное сообщение, зашифрованное уже 99 раз. В итоге 100 пользователь, применяя к сообщению, присланному ему 99 пользователем, свой скрытый пароль, получает в итоге конечное сообщение, пересылаемое протоколом на центральный сервер, сверяющий его достоверность.

Суть обеспечения именно такой рассылки паролей заключается в том, что если человек, не имеющий доступ к информационной системе правительства, имеет доступ к серверу, то ему известны все специальные пароли. Однако для того чтобы получить доступ к системе, ему нужно перехватить сообщение, которое будет отсылаться 100 пользователю, так как только в этом случае у него будет хорошая реальная возможность подобрать секретный шифр 100 пользователя N-ной MAN.

Теперь важно упомянуть про то, каким собственно способом шифруются пароли. При их шифровании будет использоваться схема Диффи-Хеллмана. Важно использовать именно подобную схему, потому что она реализует следующий принцип: при шифровании сообщения (пароля) открытым ключом его нельзя расшифровать повторным применением этого ключа. В итоге представляемый в статье протокол функционирования менеджмента паролей вместе с использованием схемы шифрования Диффи-Хеллмана обеспечивает высокий уровень безопасности системы. Однако если злоумышленнику, который уже получил доступ к серверу, повезет и он в какой-либо MAN области получит прямой доступ к компьютеру, который в цепи рассылки специальных паролей окажется последним, то сложится такая ситуация, что у злоумышленника будет то сообщение, которое ему прислал предпоследний пользователь одной из цепочек, и конечное сообщение (SP), которое он получил с сервера. И если все шифруется с применением схемы Диффи-Хеллмана, то возникает такая ситуация, что для того чтобы раскрыть секретный пароль конечного ПК цепочки, у злоумышленника есть 2 уравнения и 2 переменные:

M = (mod N)

N=p\*q

Однако система становится намного надежнее, чем просто аутентификация пользователей в 1 этап, так как если произошёл несанкционированный доступ к центральному серверу, то вероятность проникновения в систему не 100%, а 1/n, где n – количество ПК в 1 рассылке SP.

К тому же вряд ли человек станет рисковать угадывать, какой из ПК ему нужен, так как система оснащена системой оперативного реагирования на неверный ввод пароля.

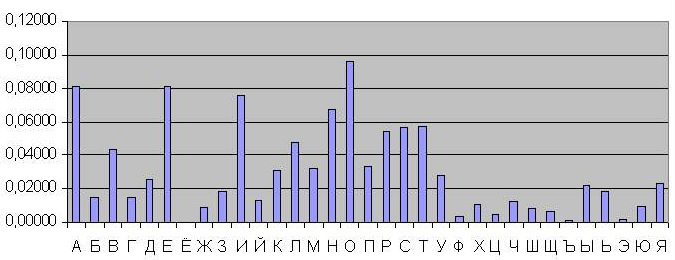
Суть метода шифрования, представляемого в данной статье, основывается на исключении возможности применения злоумышленником метода лингвистического анализа к зашифрованному сообщению. Соответственно, иные методы дешифрования, которые злоумышленник может попытаться применить, не принесут результата (кроме перебора, который реализовать при современных мощностях ЗВМ невозможно).

Описание функционирования программы, которая будет осуществлять шифрование данным способом:

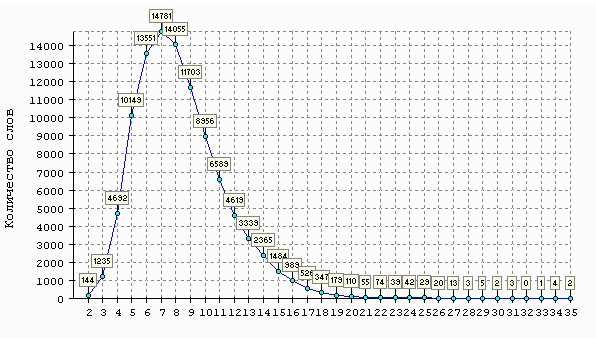
1) Берется какой-либо правительственный документ, и каждой букве/цифре произвольно присваивается какой-то символ, не совпадающий с этой буквой/цифрой.

2) Далее программа производит подсчет каждой буквы и определяет, какой символ встречается чаще всего.

3) На третьем этапе программа создает некую базу из символов (которые представляют собой зашифрованные буквы), количество которых в этой базе определяется следующим образом: “Число, показывающее, сколько раз представлен чаще всего встречающийся символ в тексте” - “Число, показывающее, сколько раз представлен данный символ в тексте”. Это делается как раз для того, чтобы злоумышленник не смог воспользоваться при расшифровке данным графиком:



4) Далее в этой базе (база представляет из себя какой-либо текстовый документ) формируются «слова» (т.е. некий набор символов, разделенный с остальными буквами пробелами). Количество букв в слове формируется на основе средней частоты встречаемости слов конкретной длины в текстах. Программа при прохождении данного этапа может использовать следующую статистику:



Также очень важно, чтобы образованное «слово» не имело никакого смысла, так что программа во время своего функционирования должна использовать специальную библиотеку со словарем русского языка.

5) На последнем этапе программа добавляет собственные сформированные «слова» в текст, распределение которых происходит также случайно.

Выше была описана работа программы-шифратора.

Теперь опишем то, как функционирует программа-дешифратор:

Программа-дешифратор, получив зашифрованное сообщение, сначала расшифровывает его на основе транскрипции символов шифра в буквы по созданному правилу, а затем отбрасывает слова, которые не находит в словаре русского языка.

Огромным плюсом данного метода является то, что для расшифрования такого сообщения злоумышленником, у него есть только вариант перебора букв, которые соответствуют какому-то символу. А это получается, что всего на перебор к него 33! вариантов, что означает, что для расшифровки такого сообщения современных мощностей не хватает.

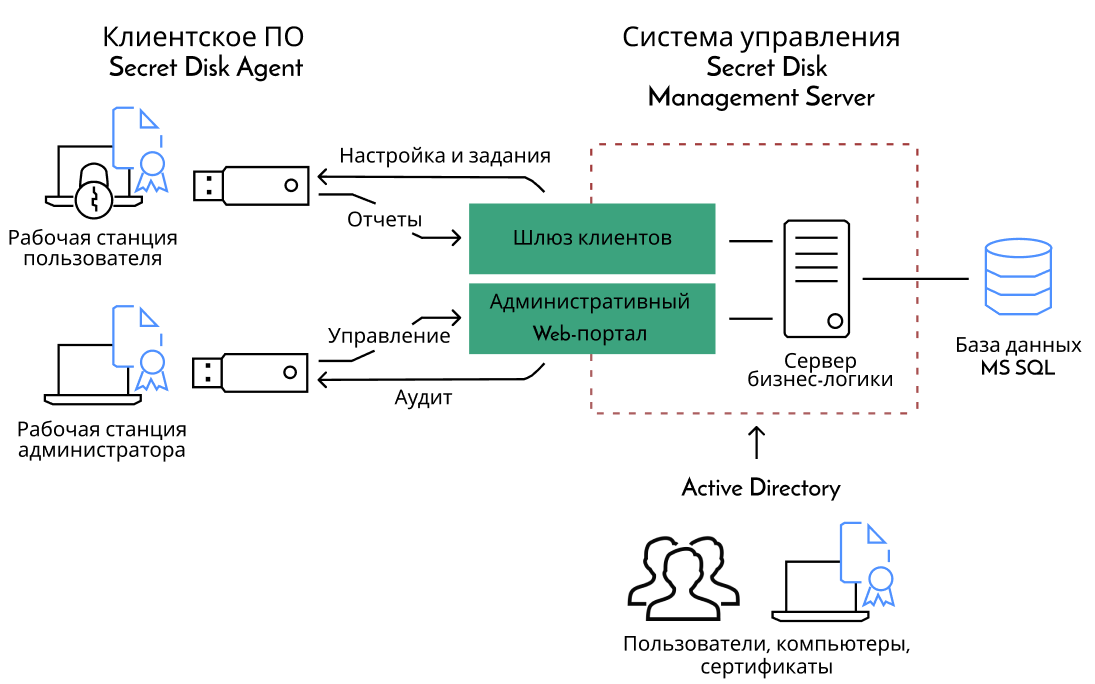
Решение задачи единой системы администрирования средств криптографической защиты информации. Для решения вопроса наша команда предлагает внедрение продукта для криптографической защиты хранимых данных Secret Disk Enterprise, поскольку он многофункционален, не предъявляет высоких требований к системе, с его помощью централизованно обеспечивается защита любых ресурсов, а самое главное он имеет сертификат Лицензия ФСБ России № 12632H от 20.12.2012. Secret Disk Enterprise построен по технологии клиент-сервер. Клиентская часть представлена приложением Secret Disk Agent, выполняемым на рабочих станциях пользователей. Серверная часть состоит из трех основных компонентов:

сервер бизнес-логики;

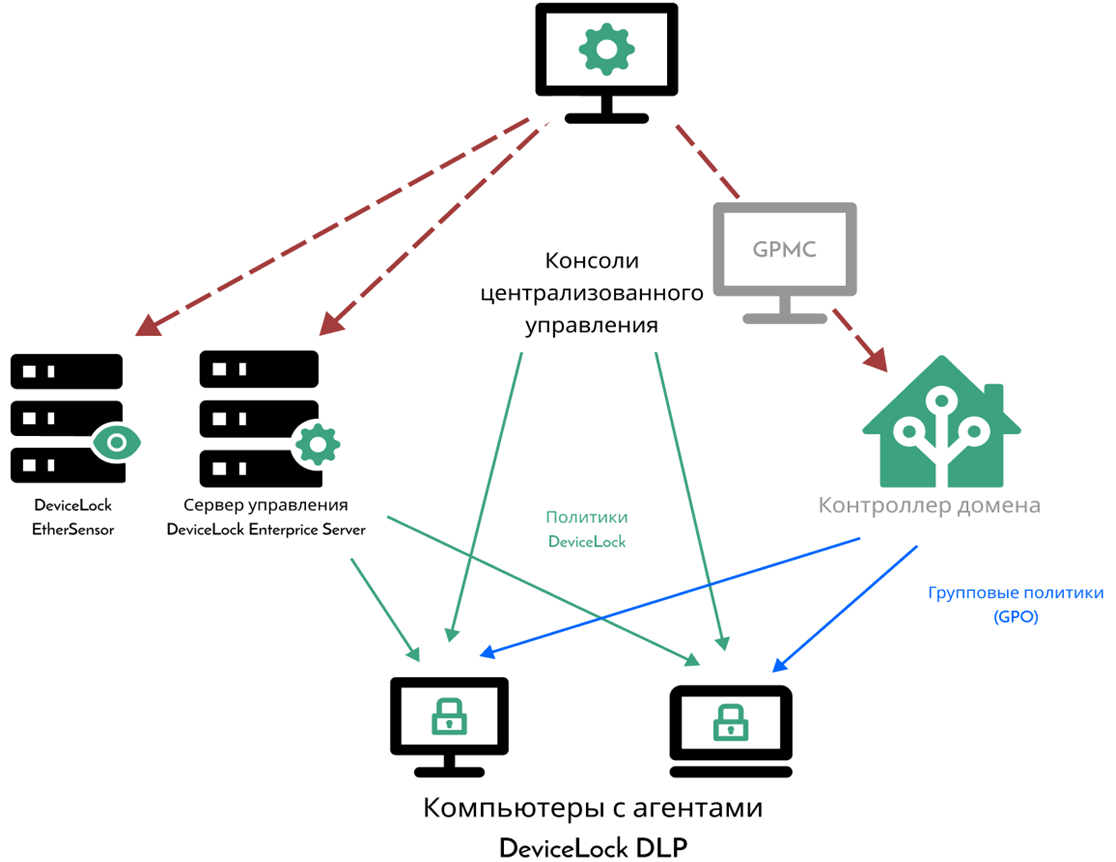
шлюз клиентов;

административный Web-портал.

На основе анализа работы продукта Secret Disk Enterprise мы спроектировали схему взаимодействия компонентов: сервер бизнес-логики обеспечивает работу всех процессов; шлюз клиентов - модуль реализации канала связи; административный web-портал для администрирования системы; база данных – хранение всей служебной информации; модуль синхронизации с Active Directory – синхронизация данных о пользователях; Модуль сертификации — компонент для выпуска сертификатов; Secret Disk Agent — клиентское приложение, непосредственно осуществляющее криптографические преобразование и защиту хранимых данных на рабочих местах, серверах и съемных накопителях; Secret Disk Reader — утилита для доступа к зашифрованным данным вне защищенной инфраструктуры.



Второе - решение проблемы единой системы выявления инцидентов информационной безопасности. Для решения данной задачи необходима организация внедрения сторонней, либо разработка собственной DLP-системы. Однако разработка может оказаться намного затратнее, чем приобретение уже готовой системы. Наша команда предлагает внедрение программного комплекса DeviceLock DLP. Он имеет действующий сертификат соответствия ФСТЭК России № 3465 от 05.11.2015 г. Мы выбрали данный продукт, поскольку он предлагает наиболее рациональный и удобный подход к управлению DLP-системой – с использованием объектов групповых политик домена Microsoft Active Directory и интегрированной в редактор групповых политик Windows. При этом политики DeviceLock DLP автоматически распространяются средствами директории как интегральная часть ее групповых политик на все компьютеры домена, а также виртуальные среды. Такое решение позволяет службе информационной безопасности централизованно и оперативно управлять DLP-политиками в масштабах всей организации, а их исполнение распределенными агентами DeviceLock обеспечивает точное соответствие между бизнес-функциями пользователей и их правами на передачу и хранение информации на рабочих компьютерах.

Аналогично составлена схема продукта DeviceLock DLP. Агент. DeviceLock который устанавливается на каждый компьютер и требуется для обеспечения контроля устройств и сетевых сервисов, защищая от утечки конфиденциальной информации. Сервер. Компонент, который служит для централизованного сбора данных и работы с журналом аудита. Консоль управления DeviceLock Enterprise Manager инструмент администратора безопасности, который позволяет производить удаленное администрирование системой

Что касаемо реализации решения, то

Сроки. Внедрение происходит в течение месяца.

Стоимость внедрения. 2 134 000 рублей.

Порядок внедрения. В первую очередь следует внедрить Secret Disk Enterprise, поскольку внедрение DLP-системы займет больше времени за счет обучения персонала.

Проект.

Суть метода системы хранения паролей, обеспечивающей статичное подключение работников правительства области к системе:

Предположим, что в области N есть 5000 правительственных компьютеров и 50 городов (50 MAN). В центральном сервере всего хранится 5000, которые предназначены для осуществления входа в систему каждого работника. Однако также параллельно осуществляется хранение специальных 50 паролей, предназначенных для рассылки 100 пользователем.

Система рассылки специальных паролей работает следующим образом:

В начале рабочего дня работник, закрепленный за отдельным ПК, вводит свой пароль, который хранится на сервере и предназначенный только для его аутентификации. Затем, когда сервер убеждается в том, что за ПК есть человек, который сможет участвовать во 2 этапе аутентификации, она вносит его IP-адрес в специальную базу. В итоге после первого этапа аутентификации на сервере формируется база IP-адресов пользователей. Теперь из сервера выбирается один из специальных паролей и в случайном порядке шифруется последовательно 100 раз (в случае, если все 5000 работников готовы войти в систему). Далее пароль, зашифрованный 100 раз, отправляется пользователю, открытый пароль которого первым использовался во время шифрования. Пользователь вводит свой закрытый, нигде не хранимый, шифр (пароль №2). Расшифрованное им сообщение включает в себя часть с IP- или МАС – адресом того пользователя, которому необходимо переслать расшифрованное сообщение. В итоге специальный протокол рассылки паролей адресует расшифрованное сообщение следующему пользователю, к0торый получает начальное сообщение, зашифрованное уже 99 раз. В итоге 100 пользователь, применяя к сообщению, присланному ему 99 пользователем, свой скрытый пароль, получает в итоге конечное сообщение, пересылаемое протоколом на центральный сервер, сверяющий его достоверность.

Суть обеспечения именно такой рассылки паролей заключается в том, что если человек, не имеющий доступ к информационной системе правительства, имеет доступ к серверу, то ему известны все специальные пароли. Однако для того чтобы получить доступ к системе, ему нужно перехватить сообщение, которое будет отсылаться 100 пользователю, так как только в этом случае у него будет хорошая реальная возможность подобрать секретный шифр 100 пользователя N-ной MAN.

Теперь важно упомянуть про то, каким собственно способом шифруются пароли. При их шифровании будет использоваться схема Диффи-Хеллмана. Важно использовать именно подобную схему, потому что она реализует следующий принцип: при шифровании сообщения (пароля) открытым ключом его нельзя расшифровать повторным применением этого ключа. В итоге представляемый в статье протокол функционирования менеджмента паролей вместе с использованием схемы шифрования Диффи-Хеллмана обеспечивает высокий уровень безопасности системы. Однако если злоумышленнику, который уже получил доступ к серверу, повезет и он в какой-либо MAN области получит прямой доступ к компьютеру, который в цепи рассылки специальных паролей окажется последним, то сложится такая ситуация, что у злоумышленника будет то сообщение, которое ему прислал предпоследний пользователь одной из цепочек, и конечное сообщение (SP), которое он получил с сервера. И если все шифруется с применением схемы Диффи-Хеллмана, то возникает такая ситуация, что для того чтобы раскрыть секретный пароль конечного ПК цепочки, у злоумышленника есть 2 уравнения и 2 переменные:

M = (mod N)

N=p\*q

Однако система становится намного надежнее, чем просто аутентификация пользователей в 1 этап, так как если произошёл несанкционированный доступ к центральному серверу, то вероятность проникновения в систему не 100%, а 1/n, где n – количество ПК в 1 рассылке SP.

К тому же вряд ли человек станет рисковать угадывать, какой из ПК ему нужен, так как система оснащена системой оперативного реагирования на неверный ввод пароля.

Актуальность применения способа шифрования текстовой информации, представленного в статье, обусловлена тем, что на сегодняшний день нельзя с уверенностью сказать, что ЭВМ не смогут дойти до такой степени развития, которая позволила бы им эффективно дешифровать информацию, зашифрованную с помощью схемы Диффи-Хеллмана (так как протокол, который представлен в первой статье, основывается именно на шифровании этим способом).

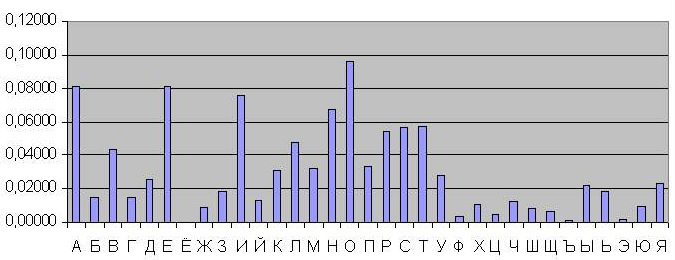
Суть метода шифрования, представляемого в данной статье, основывается на исключении возможности применения злоумышленником метода лингвистического анализа к зашифрованному сообщению. Соответственно, иные методы дешифрования, которые злоумышленник может попытаться применить, не принесут результата (кроме перебора, который реализовать при современных мощностях ЗВМ невозможно).

Описание функционирования программы, которая будет осуществлять шифрование данным способом:

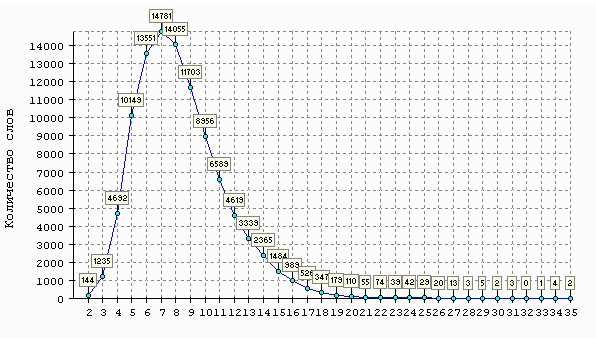
1) Берется какой-либо правительственный документ, и каждой букве/цифре произвольно присваивается какой-то символ, не совпадающий с этой буквой/цифрой.

2) Далее программа производит подсчет каждой буквы и определяет, какой символ встречается чаще всего.

3) На третьем этапе программа создает некую базу из символов (которые представляют собой зашифрованные буквы), количество которых в этой базе определяется следующим образом: “Число, показывающее, сколько раз представлен чаще всего встречающийся символ в тексте” - “Число, показывающее, сколько раз представлен данный символ в тексте”. Это делается как раз для того, чтобы злоумышленник не смог воспользоваться при расшифровке данным графиком:



4) Далее в этой базе (база представляет из себя какой-либо текстовый документ) формируются «слова» (т.е. некий набор символов, разделенный с остальными буквами пробелами). Количество букв в слове формируется на основе средней частоты встречаемости слов конкретной длины в текстах. Программа при прохождении данного этапа может использовать следующую статистику:



Также очень важно, чтобы образованное «слово» не имело никакого смысла, так что программа во время своего функционирования должна использовать специальную библиотеку со словарем русского языка.

5) На последнем этапе программа добавляет собственные сформированные «слова» в текст, распределение которых происходит также случайно.

Выше была описана работа программы-шифратора.

Теперь опишем то, как функционирует программа-дешифратор:

Программа-дешифратор, получив зашифрованное сообщение, сначала расшифровывает его на основе транскрипции символов шифра в буквы по созданному правилу, а затем отбрасывает слова, которые не находит в словаре русского языка.

Огромным плюсом данного метода является то, что для расшифрования такого сообщения злоумышленником, у него есть только вариант перебора букв, которые соответствуют какому-то символу. А это получается, что всего на перебор к него 33! вариантов, что означает, что для расшифровки такого сообщения современных мощностей не хватает.