шифрование с открытым и закрытым ключом и архитектуру CryptoAPI. EFS может использовать любой симметричный алгоритм шифрования файлов, однако первоначальная версия использует только DES. В Северной Америке используются 128-битные ключи, а за ее пределами - 40-битные ключи.

В настоящее время закладываются предпосылки для унификации и стандартизации средств шифрования, что в свою очередь позволяет встраивать криптографическую защиту в программы и операционные системы на более высоком уровне.

Литература:

1. Schneier, Bruce. Applied Cryptography. John Wiley & Sons, 1996.
2. http://www.bdv.newmail.ru/
3. RSA Laboratories, a division of RSA Data Security, Inc., RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), Copyrightc 1991-1993.

СИСТЕМА АУТЕНТИФИКАЦИИ KERBEROS.

А.И. Галабурда
(БГТУ, г. Минск)

Используемые некогда лишь в правительственных учреждениях, таких как Агентство национальной безопасности и военные организации, алгоритмы шифрования сегодня нашли применение в коммерческом ПО брандмауэров. Этот процесс в значительной степени стимулируется распространением электронной коммерции, виртуальных частных сетей и растущим числом мобильных сотрудников. Сейчас улучшению защиты данных, передаваемых между узлами Internet, уделяется самое пристальное внимание.

Особую роль в вопросе унификации и стандартизации играют различные стандарты и протоколы, а также продукты на их основе.

Одним из нововведений Windows 2000 является система распределения ключей Kerberos 5.0. Kerberos – протокол аутентификации, основанный на распределении секретной информации, т.е. пользователь и ЦРК знают пароль пользователя. Кроме клиента и сервера применяется третий участник системы обмена ключевой информацией – ЦРК, которому «доверяют» и клиент и сервер. Протокол предполагает серию передач информации между клиентами, ЦРК, и серверами для получения и использования «билетов» kerberos.

Процесс аутентификации происходит следующим образом: клиент посылает запрос на сервер аутентификации(ЦРК) на предмет получения подключения к определенному серверу. Сервер аутентификации зашифровывает информацию, необходимую для подключения, клиентским ключом и передает клиенту. Информация по подключению содержит «билет» для сервера и временный ключ шифрования, называемый сессионным ключом. Клиент передает «билет», содержащий информацию уникальную для данного клиента, и однозначно идентифицирующую его, и копию сессионного ключа, зашифрованные ключом сервера, на сервер. Сессионный ключ с этого момента разделяем между клиентом и сервером и служит для аутентификации клиента, и может использоваться для аутентификации сервера. Он также может использоваться для шифрования передаваемой информации и для обмена новыми сессионными ключами.

Когда пользователь производит операцию входа в Windows, сервиспровайдер Kerberos получает первоначальный «билет» из шифрованного значения хеш функции, для которой данными служит пароль пользователя. Операционная система сохраняет «билет» на компьютере пользователя. Когда пользовательская программа пытается получить доступ к сетевым ресурсам, kerberos проверяет хранилище ключей на предмет подходящего сессионного ключа для сервера. Если такого не оказалось «билет» отправляется по запросу на ЦРК для получения сессионного ключа, который бы позволил получить доступ к серверу. В свою очередь этот «билет» также сохраняется для последующего использования с этим сервером. Срок действия ключа может истечь, тогда процедура аутентификации повторяется. Срок действия ключа определяется доменной политикой.

Windows 2000 реализует ЦРК, как сервис аутентификации, в каждом контроллере домена. Клиент kerberos реализован как провайдер безопасности, основанный на SSPI. Первоначальная аутентификация kerberos интегрирована в загрузку системы, реализованную как архитектура единичной подписи. Сервер kerberos ЦРК интегрирован в существующие сервисы безопасности Windows, работающие на контроллере домена. Он использует службу каталога Active Directory как хранилище информации о аккаунтах пользователей.

Протокол аутентификации kerberos улучшает базовые сервисы безопасности Windows:

- Быстрая процедура аутентификации во время установления соединения.
- Делегирование прав при мультисерверной архитектуре.
- Поддержка политика доверия прав при междоменной аутентификации.

Литература:

1. RFC1510
2. http://msdn.microsoft.com/

ВЫЧИСЛЕНИЕ ХАРАКТЕРИСТИК ХАОТИЧЕСКОЙ ДИССИПАТИВНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ

Н.В. Маньяков
(БГТУ, Брест)

Диссипативные динамические системы характеризуются притяжением всех траекторий, проходящих через некоторую область фазового пространства, к геометрическому объекту, называемому аттрактором. В то же время хаотические динамические системы обладают чувствительностью к заданию начальных условий. Т.е. две близкие в некоторый момент времени траектории через небольшой промежуток времени будут значительно отставать одна от другой. Значит в одних направлениях происходит притяжение, а в других разбегание траекторий. Но учитывая диссипацию весь n-мерный объем необходимо должен сокращаться.

Характеристиками изменения этого объема служат показатели Ляпунова, положительные в некоторых направлениях в случае расходимости траекторий, что характеризует хаотичность системы. Причем сумма всего спектра показателей должна быть отрицательна, что необходимо для диссипации.

Метод вычисления всех показателей Ляпунова основан на вычислении логарифма изменения n-мерного объема в направлениях собственных векторов матрицы Якоби фазового потока динамической системы [1]. В случае, если известны только временные ряды изменения фазовых переменных системы на небольшом промежутке времени, а не система уравнений этой системы, это сделать очень сложно.

Для преодоления этого предлагается использовать нейронную сеть (многослойный персептрон) [2]. Использование ее основано на предложенном