УДК 681.3.06

Е.Г.КАЧКО, канд. техн. наук, В.А. ЖЕЛЕЗНЯК

РАЗРАБОТКА КРИПТОПРОВАЙДЕРА. ИНТЕГРАЦИЯ КРИПТОПРОВАЙДЕРА В СИСТЕМУ

1. Введение

Человечество перешло к новой фазе своего развития – информационной, характеризующейся широким внедрением информационных технологий во все сферы его деятельности. Основной особенностью этой фазы является создание и коллективное использование массивов и баз данных, баз знаний, интенсивный обмен сообщениями, передача команд управления, широкое использование и распространение различного программного обеспечения. Одной из важнейших задач, возникающих при обмене информацией, является обеспечение ее целостности и конфиденциальности.

В связи со всеобщей стандартизацией все большее количество функций переходит от приложений к операционным системам (ОС). Например, до появления Windows, каждому приложению, работающему с принтером, было необходимо иметь в своем составе библиотеки для работы со всеми возможными видами принтеров. Аналогичная ситуация наблюдалась и для видеокарт, звуковых карт, а также коммуникационного оборудования – вообще любого оборудования. При стремительном росте ассортимента оборудования, начавшемся в 90х годах, такой способ перестал быть приемлемым. Появление сложных ОС позволило свести все драйвера оборудования под централизованное управление ОС и избежать ненужного дублирования. Однако процесс стандартизации не ограничился драйверами устройств – все большее количество функций, например, интерфейса с пользователем, ранее считавшихся прерогативой приложений, переходят к ОС.

В современных ОС, разработанных фирмой Microsoft был сделан еще один важный шаг к стандартизации – в ОС Windows теперь входят поддержка CryptoAPI – API, предоставляющего стандартизованный интерфейс для выполнения разнообразных криптографических операций, реализованная через криптопровайдеры (Cryptographic Service Provider, CSP) – особые DLL, интегрируемые в операционную систему. Интерфейс между приложениями и криптопровайдерами осуществляется через функции, реализованные в стандартном модуле AdvAPI32.DLL.

2. Постановка задачи

Многие, а в последнее время и большинство, программ требуют перед началом работы выполнить некоторую последовательность действий:

- копирование файлов на винчестер (возможно, с разархивированием);
- создание конфигурационного файла (файла настроек) или записей в реестре;

Обычно, все подготовительные операции выполняет специальная программа – ***инсталлятор***. В случае инсталляции криптопровайдера (Crypto Service Provider) рекомендованная Microsoft процедура состоит из следующих пунктов:

- копирование файлов провайдера в системную папку;
- создание записей в реестре;
- запись в реестр цифровой подписи (ЦП) провайдера.

Последний пункт является самым сложным, т.к. для получения цифровой подписи разрабатываемого провайдера необходимо обратиться в Государственный Департамент США, что невозможно по нескольким причинам.

Целью работы является исследование криптопровайдеров ОС WINDOWS, разработка пользовательского криптопровайдера и его инсталляция.

В данной работе решается проблема генерации ключа цифровой подписи для инсталлятора, встраивание открытого ключа в систему, генерация цифровой подписи длиной 1024 бита для метода RSA, инсталляция криптопровайдера таким образом, чтобы программы проверки целостности и подлинности «признали» эту программу, как свою.

3. Программная модель CryptoAPI

Microsoft Cryptographic Application Program Interface (CryptoAPI) – это набор функций для цифровой подписи и шифрования.

Все криптооперации реализованы с помощью независимых модулей, называемых криптопровайдерами (Cryptographic Service Provider, CSPs). По тем же причинам, по которым правильно разработанные приложения не вызывают напрямую драйвера графических устройств и аппаратуру, они не работают напрямую с криптопровайдерами и криптоаппаратурой.

Криптосистема Microsoft состоит из большого числа модулей. Три исполнимых части – непосредственно приложение, операционная система, и криптопровайдер.

Приложение связывается с ОС через функции, называемые программный интерфейс криптоприложения (Cryptographic Application Program Interface, CryptoAPI). ОС связывается с провайдерами через множество функций (Cryptographic Service Provider Interface, CryptoSPI). Как показали исследования, эти два набора функций практически идентичны: функция CryptoAPI CryptAcquireContext вызывает функцию CryptoSPI CPAcquireContext и т. д. Существующая разница, например, в списке параметров, обусловлена необходимостью изолировать область данных провайдера от приложений.

Еще раз отметим, что приложение не связывается с криптопровайдерами напрямую. Вместо этого, все обращения к криптографическим функциям выполняются через операционную систему. Параметр для каждой CryptoAPI функции указывает для операционной системы который CSP использовать, чтобы выполнить фактическую криптографическую операцию. Подробнее этот вопрос обсуждается в разделе 3.

Примечание: При попытке одновременного вызова двух криптофункций из разных потоков одного приложения вызов одной из них будет задержан до выхода из другой.

Криптопровайдеры - это независимые модули, которые и выполняют реальную криптоработу. В идеале они написаны полностью независимо от любого приложения, так что любое приложение выполняется с множеством провайдеров. На самом деле, некоторые приложения могут иметь очень специфические требования, которые потребуют заказного CSP.

CSP состоит, как минимум, из DLL и подписи файла. Подпись файла необходима, чтобы ОС распознала CSP. Операционная система проверяет правильность этой сигнатуры периодически, чтобы гарантировать, что CSP не модифицирован. Подробнее этот вопрос рассматривается в 1.4.

В Windows NT операционная система[1)] может просмотреть область данных провайдера. Можно, конечно, не хранить ключи в открытом виде и раскрывать их непосредственно перед использованием, но поскольку в любой момент может произойти передача управления другому процессу, то такой метод сам по себе не применим. Возможно, решением будет разработка своего драйвера – работа драйверов не может быть прервана;

В Windows 95/98, не только система, но и любой процесс, применив специальные методы, может просмотреть любую область памяти. В данной работе проблема защиты от несанкционированного доступа не решалась.

При реализации криптопровайдера следует иметь в виду, что изоляция ключей и централизация криптографических операций в аппаратных средствах безопасней программной реализации.

Проверка целостности и подлинности провайдера. Проверка осуществляется по следующему алгоритму [1]:

1) Вычисляется сжатый образ проверяемого провайдера по алгоритму MD5;

2) из системной библиотеки AdvAPI32.Dll берется значение основного открытого ключа и модуля криптопреобразований. Т. к. эти данные хранятся в зашифрованном виде, то предварительно производится декодирование (сложение по модулю 2 с константой);

3) сигнатура из реестра дешифруется на открытом ключе;

4) сверяются значения, полученные в 1) и 3). В случае равенства целостность и подлинность файла провайдера считаются доказанными;

5) в случае, если проверка не удалась, то берется дополнительный ключ и повторяются 3) и 4).

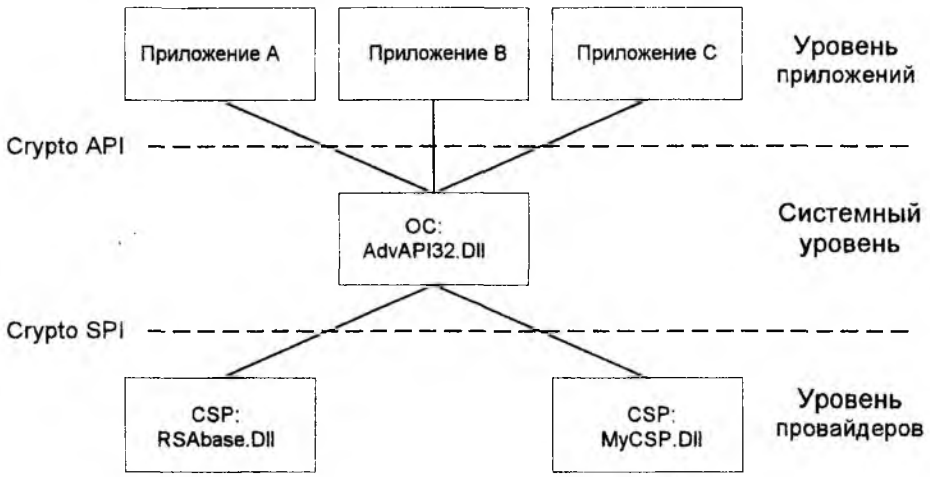
Необходимо добавить, что заменив один байт[2)] в теле AdvAPI32, целостность которой нигде не проверяется, можно добиться полного отключения проверки.

4. Интерфейс между приложениями, ОС и криптопровайдерами

Всякая работа приложений с функциями криптопровайдеров осуществляется не непосредственно, а через вызовы системных функций (рисунок)

[1)] В т.ч. и драйвера, а до установки ServicePack 3, и любой процесс

[2)] Код условного перехода на код безусловного



Для начала работы приложение вызывает функцию CryptAcquireContext (AdvAPI32.Dll) дл получения уникального контекста провайдера (аналогично вызову GetDC в функциях графическо подсистемы). Переданные параметры содержат имя требуемого криптопровайдера, идентификато алгоритма, а также параметры этого алгоритма.

При вызове CryptAcquireContext Windows предпринимает следующие действия:

- По переданному имени провайдера и записям в реестре (HKLM\ SOFTWARE\ Microsoft Cryptography\ Defaults\ Provider Types\ ..., HKLM\ SOFTWARE\ Microsoft\ Cryptography\ Defaults Provider\...) определяет путь и имя DLL провайдера;
- Проверяет целостность этой DLL – по коду DLL, сигнатуре в реестре (HKLM\ SOFTWARE Microsoft\ Cryptography\ Defaults\ Provider\ Signature) по алгоритмам MD5 и RSA. Заменой одного байт в AdvAPI32.DLL, целостность которой нигде не проверяется, можно добиться отключения проверки целостности;
- Загружает DLL провайдера и создает массив указателей на экспортируемые функции. Есл хотя бы одна из этих функций реализована не будет – выход с ошибкой;
- Вызывает CPAcquireContext из DLL провайдера

5. Интеграция нового провайдера в ОС

При установке нового провайдера должны выполняться следующие действия:

- Копирование файла (DLL) провайдера в системный каталог Windows;
- запись в реестр имени провайдера и полного имени соответствующей DLL;
- запись в реестр цифровой подписи (ЦП) провайдера.

На последнем пункте следует остановиться более подробно: для получения подпис провайдера необходимо обратиться в Microsoft, что неприемлемо по причине нарушени суверенных прав Украины.

В ходе исследований было найдено два способа решения этой проблемы – можно ил отключить ее вышеописанным методом или сгенерировать сигнатуру для нового провайдера Способ отключения проверки, однако, неприемлем, т.к. приводит к отключению проверк целостности одновременно всех провайдеров, в т.ч. и стандартных, следовательно, дл разработанного инсталлятора был выбран второй метод.

Алгоритм генерации ЦП:

1) по алгоритму RSA генерируются ключи для ЦП;

2) осуществляется подпись провайдера;

3) открытый ключ и модуль шифруются сложением по модулю 2 с константой;

4) клиенту передаются: зашифрованные открытый ключ и модуль ЦП, а также ЦП и D провайдера;

5) в системе клиента записывается в реестр ЦП и заменяется резервный ключ в AdvAPI32.

Заключение

Несмотря на то, что на данный момент функции CryptoAPI используются сравнительно редко, в будущем они, судя по всему, станут более распространены. Например, в Windows 2000 на базе CryptoAPI будет реализована новая файловая система - Encrypted File System (EFS), обеспечивающая, в отличие от FAT и NTFS, реальное шифрование данных на винчестере. Т.к. за пределы США и Канады будет экспортироваться только версия, поддерживающая ключи ограниченной длины, то разработка провайдеров приобретает вдвойне большее значение.

В рамках дальнейшей работы необходимо более тщательно исследовать механизмы проверки целостности и подлинности в ОС Windows 98 и Windows NT, а также разработать и реализовать механизмы более надежной защиты целостности и подлинности провайдеров и ключей.

Список литературы. 1. *Железняк В.А.* Разработка криптопровайдера. Интеграция криптопровайдера в систему. Материалы 3-го международного молодежного форума «Радиоэлектроника и молодежь в XX1 веке», 20-23 апреля 1999 г. Харьков, 1999, с. 489 – 490

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 15.03.2000