Distr.
GENERAL

CES/SEM.47/13 (Summary)
30 January 2002

RUSSIAN
Original: ENGLISH

СТАТИСТИЧЕСКАЯ КОМИССИЯ и ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ

КОНФЕРЕНЦИЯ ЕВРОПЕЙСКИХ СТАТИСТИКОВ

КОМИССИЯ ЕВРОПЕЙСКИХ СООБЩЕСТВ

ЕВРОСТАТ

Совместный семинар ЕЭК ООН/Евростата по интегрированным статистическим информационным системам и связанным с ними вопросам (ИСИС-2002)
(17-19 апреля 2002 года, Женева, Швейцария)

Тема II: Надежные средства связи и конфиденциальность данных

ШИФРОВАНИЕ НА ПЕРЕНОСНЫХ ПК

Вспомогательный документ

Представлен Статистическим управлением Швеции[1]

Резюме

1. Сегодняшний мир требует все большей мобильности, и переносные ПК используются более чем когда-либо. Оставленный без присмотра переносной ПК рискует исчезнуть в мгновение ока. Что может случиться, если похититель заинтересован не в перепродаже вашего компьютера, а в деликатности информации, хранящейся на его жестком диске? Цель настоящего исследования заключается в обзоре существующих на рынке средств шифрования, определении продукта, который будет удовлетворять потребностям Статистического управления Швеции, и реализации избранного решения.

2. В основе всех проблем безопасности лежит деликатная информация, которая обычно хранится в виде незащищенных файлов на вашем жестком диске.

[1] Автор: Бехзад Панахи (behzad.panahi@scb.se).

3. Статистическое управление Швеции ведет большое число различных секретных регистров, таких как:

- регистры, содержащие секреты национальной обороны
- национальные регистры, охватывающие все население, все предприятия и объекты недвижимости
- секреты компаний
- различные наблюдения (состояние здоровья, доходы, планирование семьи)
- регистры, охватывающие подвергшихся жесткому обращению детей, лиц, злоупотребляющих наркотиками, и преступников. Следует также учитывать тот факт, что граждане с доверием относятся к статистике и информации ЦСУ Швеции.

Переносные ПК широко используются в Статистическом управлении Швеции, в связи с чем необходимость шифрования является вполне очевидной.

4. Криптография используется уже на протяжении тысяч лет для обеспечения секретности информации. Существует два типа криптографии: асимметричная криптография и симметричная криптография. Симметричная криптография опирается на принцип преобразования (шифрования) скрытого текста (исходных данных) в зашифрованный текст (защищенные данные) таким образом, чтобы сделать невозможным обратимость процесса без полного знания функции преобразования. Асимметричная криптография или криптография открытого ключа также трансформирует открытый текст в зашифрованный текст с использованием определенного алгоритма и ключа. Различие заключается в использовании другого ключа для дешифрования, откуда и происходит название "асимметричная".

5. Ключ дешифрования (секретный) и ключ шифрования (открытый) связаны друг с другом, однако первый не может быть определен на основании второго. С учетом этого ключ шифрования не обязательно хранить в тайне, и он может быть открытым. Однако при этом пользователи открытого ключа должны быть уверены в том, что данный ключ не принадлежит конкретному владельцу. Решением этой проблемы служит процесс сертификации. Безопасность обеспечивается за счет сохранения в тайне секретного ключа.

Подход к проблемам безопасности в Статистическом управлении Швеции

6. В основе подхода лежат следующие соображения, что:

- противниками являются отдельные лица, а не иностранные державы;
- политика компании опирается на продукты Microsoft;
- компания имеет контракты также с фирмой IBM.

7. С учетом неопределенности относительно сроков службы и будущего использования средств безопасности было принято взаимосогласованное решение о том, что система шифрования файлов (EFS) для Windows 2000 будет тщательно изучена и надлежащим образом устанавливаться на переносных ПК.

Система шифрования файлов (EFS) для Windows 2000

8. Система шифрования файлов для Windows 2000 позволяет избежать следующих проблем:

- ручного шифрования и дешифрования в каждом отдельном случае: сервисы шифрования являются нетранспарентными для пользователей в большинстве программных средств. Пользователь должен дешифровывать файл перед каждым использованием и зашифровывать его снова после окончания работы с ним;

- утечки информации из временных файлов и файлов страничного обмена: эти временные файлы остаются незашифрованными на диске, даже если исходный документ является зашифрованным, что облегчает хищение данных;

- низкого уровня безопасности: ключи разрабатываются на основе паролей, состоящих из одного или нескольких слов. Попытки регистрации путем перебора имен по словарю способны легко преодолеть этот вид защиты, если используются легкие для запоминания пароли;

- отсутствия возможности восстановления данных: многие продукты не имеют сервисов по восстановлению данных.

Принципы работы системы шифрования файлов

9. Система шифрования файлов опирается на шифрование открытым ключом с использованием CryptoAPI. Каждый файл шифруется с использованием случайно

генерируемого ключа, называемого *ключом шифрования файла*, который не зависит от пары открытый/секретный ключ пользователя; это обеспечивает защиту от многих форм атак на зашифрованные файлы с использованием криптографического анализа.

10. Если исходный файл является зашифрованным, то программа шифрует и его временные копии при передаче атрибутов в ходе создания файла. Программа расположена в ядре Windows 2000 и использует область памяти, не подлежащую страничному обмену, для хранения ключей шифрования файлов, чтобы обеспечить невозможность их передачи в файл страничного обмена.

11. Шифрование и дешифрование производятся на пофайловой основе или на основе всего каталога. Шифрование каталога является транспарентно-принудительным.

12. Система шифрования файлов автоматически обнаруживает зашифрованный файл и локализует сертификат пользователя и соответствующий закрытый ключ в сертификате пользователя и хранилищах ключей.

Выводы

13. Был сделан вывод о том, что Windows 2000 обеспечивает приемлемый уровень шифрования, соответствующий потребностям Статистического управления Швеции. Было принято решение о том, что все новые переносные компьютеры, позволяющие сделать это, должны быть переведены на Windows 2000, что даст пользователям возможность применять шифрование на этих компьютерах.
