

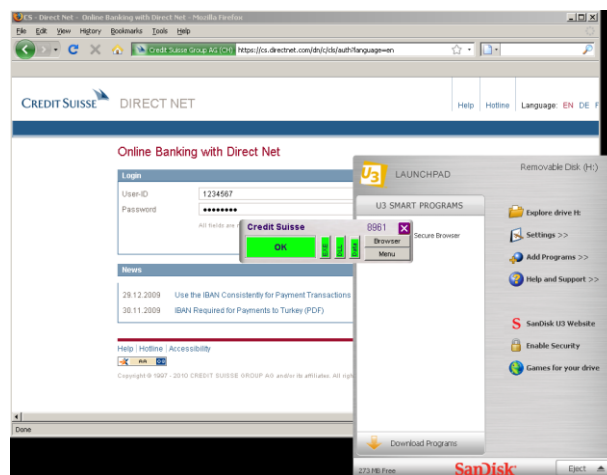
Заказчик

Швейцарская компания, которая специализируется в области интернет-решений для систем клиент-банк.

Задача

Разработка программно-аппаратного комплекса для обеспечения безопасной работы клиента и банка на небезопасном терминальном компьютере.

Изделие должно обеспечивать следующую функциональность:



- Безопасное хранение идентификационной информации пользователя.
- Идентификационная информация должна использоваться только в паре с известным пользователю пин-кодом.
- Известный пользователю пин-код можно изменять без повторного шифрования файлов пользователя.
- Безопасная работа клиентского ПО на небезопасном ПК.
- Целостная проверка клиентского ПО на наличие модификаций, внесенных вредоносными программами.
- Гарантированное безопасное обновление. Проверка на подмену / замещение посредством фишинговых сайтов.
- Возможность онлайн-блокирования клиентского ПО.
- Шифрование / дешифрование личных файлов пользователя.
- Шифрование / дешифрование загружаемых данных.
- Подпись / проверка подписи данных пользователя (электронно-цифровая подпись).
- Операция безопасного удаления.
- Клиентское ПО должно работать под Microsoft Windows XP, Microsoft Windows Vista.

Решение

В качестве аппаратной платформы выбран USB-накопитель от компании SanDisk с поддержкой U3. SanDisk Extreme Contour является чрезвычайно прочным USB Smart флеш-накопителем. Он выполнен в корпусе Liquidmetal®,



который устойчив к давлению свыше 900 килограмм. SanDisk Extreme Contour также включает смарт-технологии U3.

Аппаратное обеспечение

Флеш-накопитель U3 определяется узловой системой как USB-хаб с CD-приводом и включенным стандартным устройством USB mass-storage. Такая конфигурация обуславливает тот факт, что менеджер устройств ОС Windows определяет данный флеш-накопитель как два устройства:



- том ISO9960 на эмулированном приводе CD-ROM с конфигурационным файлом autorun для запуска U3 LaunchPad (только для чтения);
- стандартный флеш-накопитель (форматированный под файловую систему FAT), который включает скрытую папку SYSTEM с установленными приложениями.

Спецификация флеш-накопителя SanDisk Extreme Contour.

| Возможные объемы | 4 Гб, 8 Гб, 16 Гб, 32 Гб и 64 Гб |
|------------------|--|
| Чтение и запись | До 25MB/sec скорость чтения и 18MB/sec скорость записи |
| Защита паролем | Поддерживается в Windows XP и Windows Vista |
| AES-шифрование | Поддерживается в Windows XP и Windows Vista |
| USB-порт | USB 2.0 |

Программное обеспечение

ПО состоит из четырех независимых частей:

- ПО для запуска приложений для обеспечения всех секретных операций и контролирующих алгоритмов;
- настроенный браузер Mozilla Firefox для предоставления пользовательского веб-интерфейса для взаимодействия с банковским счетом;
- библиотека подключаемая к браузеру Mozilla Firefox и предоставляющая функциональность PKCS#11 (криптографический стандарт открытого ключа).



ПО запускающей программы (лаунчера) разработано для:

- быстрого доступа к функциональным элементам;
- предоставления шифрования файлов клиента (ПО AES 256);
- полной проверки собственных компонентов и компонентов Mozilla Firefox;
- получение безопасных обновлений от клиента;
- онлайн-активации ПО посредством пин-кода

Вся личная идентификационная информация пользователя и данные хранятся в зашифрованном разделе. ПО лаунчера использует интерфейс библиотеки u3dapi для получения на флеш-накопитель SanDisk u3 алгоритма шифрования AES 256 и безопасного хранения.

Пользовательский интерфейс лаунчера имеет индикатор проверки текущего состояния. Если вредоносное ПО попытается внести изменения, мгновенно появляется предупреждение для пользователя и сессия безопасно завершается.

Алгоритм безопасного удаления делает невозможным восстановление удаленных данных.

Браузер Mozilla Firefox имеет дополнительные настройки для увеличения безопасности:

- при запуске с мобильного устройства временные файлы не сохраняются на локальном HDD;
- включает встроенный объект токена – отсутствует возможность добавления или изменения объектов посредством вредоносного ПО;
- разработанная Mozilla Firefox загрузка дополнений предотвращает создание незашифрованных временных файлов;
- минимизация загрузки плагинов и дополнений – нет возможности установить вредоносный модуль.

Токен-библиотека подключается к браузеру Mozilla Firefox как библиотека PKCS#11. Она предоставляет следующие возможности:

- получение объекта сертификата с клиентского ПО – нет возможности добавить или заменить сертификат авторизации;
- выполнение AES-шифрования;
- выполнение RSA-шифрования и генерации ключей;
- предоставляет openSSL, внешний генератор случайных чисел, который усложняет порчу встроенного генератора.

Javascript-загрузка дополнений для браузера Mozilla Firefox предоставляет загрузку файлов во временные зашифрованные файлы, что усложняет подмену дополнения.

Преимущества



- Разработанный мобильный браузер имеет полную проверку для предотвращения несанкционированной замены.
- Браузер настроен для взаимодействия с конкретным банком, подмена страницы сайта банка вызовет ошибку безопасности.
- Безопасное файловохранилище для пользовательских данных.
- Скрытые и нечитаемые пользовательские идентификационные данные.
- Алгоритм безопасного удаления для предотвращения восстановления удаленных пользовательских файлов.

| | |
|------------------------------|-----------------|
| Языки программирования | C++, JS |
| Интерфейсы | USB 2.0 |
| Средства разработки | MSVC2005, MinGW |
| Средства управления проектом | dotProject, SVN |
| Срок выполнения проекта | 5 месяцев |