Protected USB dongle with integrated browser for online banking

Customer

Swiss company specializing in Internet solutions for e-commerce and client-bank systems.

Objective

To develop a hardware and software solution for secure transaction between a bank and its clients when unsecure computer terminal is used.

The product must provide the following functionality:

- Tamper (Secure) storage of user identification information
- User identification information should have restricted knowledge based algorithm. Identification information shouldn't have a sense without user know component (like PIN)
- User-know component should have possibility to change without any re-encrypting user files
- Secured execution client software at unsecured PC
- Integrity checking of client software to detect attacker modification
- Guaranteed secure update, checking for substitution by fishing site
- Online possibility booking client software
- Encrypting / decrypting user private files
- Encrypting / decrypting downloading data
- Sign/check sign of user data
- Secure delete operation
- Client software should work under Microsoft(c) Windows XP(c), Microsoft(c) Windows Vista(c)

Solution

As the hardware platform was selected USB smart drive by SanDisk supporting U3 technology. SanDisk Extreme Contour is an extremely rugged and smart USB flash drive. It is built with Liquidmetal® casing that is crash-resistant to over 2,000 lbs. SanDisk Extreme Contour also includes U3 smart technology which deals with security functions.

1. Hardware

A U3 flash drive presents itself to the host system as a USB hub with a CD drive and standard USB mass storage device.

This configuration causes Windows disk management to show two drives:

- A read-only ISO9960 volume on an emulated CD-ROM drive with an autorun configuration to execute the U3 LaunchPad
- A standard flash drive (FAT formatted) that includes a hidden "SYSTEM" folder with installed applications

Table 1. SanDisk Extreme Contour flash drive specification

Capacities	4GB, 8GB, 16GB, 32GB and 64GB
Read and write performance	Up to 25MB/sec read and 18MB/sec write
Password protection	Supported in Windows(c) XP and Windows(c) Vista
AES encryption	Supported in Windows(c) XP and Windows(c) Vista
USB port	Hi-Speed USB 2.0

2. Software

Software consists from four independent parts:

- Launcher software, to provide all security operation and controlling algorithms
- Mozilla Firefox customized browser to provide user web interface for interaction with banks account
- Secure token library, connected to Mozilla Firefox browser and provided PKCS#11 functionality

Launcher software developed for:

- Quick access to functionality
- Providing software AES 256 encryption of client files
- Integrity checking of internal components and Mozilla Firefox components
- Getting secure update from customer
- Online activation software by booking number

All user private identification information and data are stored in encryption partition. Launcher software used u3dapi library interface to get SanDisk U3 AES 256 encryption algorithm and tamper storage.

Launcher user interface have a progress bar with display of integrity checks current state. If malware try to made changes, user notification is present immediate and session would be security destroyed.

The secure delete algorithm makes impossible to recover deleted data from stick.

Mozilla Firefox browser customized for increase security:

- Launching from portable device – no temporary files stored on local HDD
- Excluded build-in object token – no possibility to add or change objects by malware
- Developed Mozilla Firefox download extension – prevent creating plaintext temporary file
- Minimized plugins and extension loading – no possibility to attach malware module

Secure token library attached to Mozilla Firefox browser as PKCS#11 library and provide:

- Getting certificate object from client software – no possibilities to add or substitute certificate authority
- Performs AES encryption
- Performs RSA encrypting and key distribution
- Provides external random generator to OpenSSL

Firefox browser has ability to download files to encrypted temporary storage thus preventing fishing of Firefox downloadable extensions.

Advantages

- Portable browser solution has an integrity checking to prevent fake substitution of malicious components
- Portable browser customized for bank interaction, substitution of bank page cause a security error
- Protected file storage for user data files
- Hidden and unreadable user identification data
- Secure delete algorithm to prevent recovery user deleted files

Programming languages	C++, JS
Interfaces	USB 2.0
Development tools	MSVC2005, MinGW
Project management tools	dotProject, SVN
Project duration	5 months