ExpressLane v3.1.1
Test Plan and Test Procedures
April 2009

CL BY: 0986772
CL REASON: Section 1.5 c
DECL ON: X1
DRV FRM: EQU 19-82

Table of Contents

1 (U) Overview

(S))**:** OTS/i2c has a biometric collection system that is provided to liaison services around the world. The systems are provided to Liaison with the expectation for sharing of the biometric takes collected on the systems. Some of these biometric systems have already been given to the Liaison services. OTS/i2c plans to revisit these sites with the cover of upgrading the biometric software to perform a collection against the biometric takes.

2 (U) Purpose of Document

(S) This document defines the test steps and test procedures necessary to evaluate and establish a level of quality and operational fitness for the ExpressLane tool. The document records the results of the tests and identifies risks. If test results are satisfactory and the risks accepted, the test process verified in this document helps assure the successful performance of the IOC mission.

3 (U) Reference Documents

- IMIS Requirement 2009-1655 (S)

4 (U) Requirements

(S) The following requirements are from IMIS Requirements 2009-0555 and 2009-0182.

Num	Requirement	Source	Ref	Note
1.	3.1. (U) The execution of the tool shall look like an authentic Windows installation. 3.1.1. (U) It shall show a splash screen with a progress bar during installation. 3.1.2. (U) The executable shall be called MOBS_Upgrade.exe. 3.1.3. (S) The executable shall not be tied to any Crossmatch software. 3.1.3.1. (S) The executable shall be a separate script that does not install any Crossmatch software.	IMIS 2009-1655	3.1	
2.	3.2. (S) The collection shall begin during the execution of the installation. 3.2.1. (S) Activation of the collection software shall occur without removing/reinserting the	IMIS 2009-1655	3.2	

	thumb drive. 3.2.2. (S) Collection shall begin within one minute of the installation beginning.			
3.	3.3. (S) The tool shall collect *.eft, *.ldf and *.mdf files. 3.3.1. (S) *.eft files shall be collected first.	IMIS 2009-1655	3.3	
4.	3.4. (S) The directory listing of the system shall be collected during the execution of the installation	IMIS 2009-1655	3.4	
5.	3.5. (S) The collected files shall be uncompressed and encrypted.	IMIS 2009-1655	3.5	
6.	3.6. (S) The Trojan installation and the collection processes shall be decoupled to allow for flexibility in operation. 3.6.1. (S) The user shall be able to install the Trojan and run the collection process with the splash screen. 3.6.2. (S) The user shall be able to run just the collection process with the splash screen.	IMIS 2009-1655	3.6	
7.	3.7. (S) The kill switch date and size of the hidden partition shall be set through a separate GUI. 3.7.1. (S) The kill switch shall corrupt the MiltA.config file located in the following path: C:\Program Files\Cross Match Technologies\Configurations\MOBS MiltA. 3.7.2. (S) The tool shall corrupt the MOBS config file after the pre-set time elapses (MiltA.config). 3.7.3. (S) Date shall be able to be changed by inserting a watermarked thumb drive with a new kill date.	IMIS 2009-1655	3.7	
8.	3.8. (S) The tool shall allow the user to determine the amount of time the installation takes in advance. 3.8.1. (S) There shall be a GUI to pre-configure the installation time.	IMIS 2009-1655	3.8	
9.	3.9. (U) The installation shall replace the existing MiltA.ver, MiltA-Collect.ver, MiltA.config, and Country.ar.txt files on the system with new files. 3.9.1. (U) MiltA.ver, MiltA-Collect.ver, and MiltA.config are located in both: C:\Program Files\Cross Match Technologies\Configurations\MOBS MiltA\VerFiles and C:\Program Files\Cross Match Technologies\Configurations\MPBS\MiltA\Work spaces.	IMIS 2009-1655	3.9	

	3.9.2. (U) Country.ar.txt is located in: C:\Program Files\Cross Match Technologies\Configurations\Validation Files.			
10.	3.10. (S) Collection of data shall not change the date modified for the files.	IMIS 2009-1655	3.10	
11.	3.11. (S) The Trojan shall replace the old license file with a new license file for each system. 3.11.1. (S) The Trojan shall be packaged with a wrapper to allow user flexibility as to which license file is being installed.	IMIS 2009-1655	3.11	
12.	3.12. (S) ExpressLane v3.1 shall not be detectable by intrusion detection programs (Norton, McAfee, and Kaspersky), firewalls, and standard operating system features. (Note: no personal security products were installed on the system by OTS, but it is possible that liaison has installed one.)	IMIS 2009-1655	3.12	
13.	3.13. (S) ExpressLane v3.1 shall be compatible with Windows XP SP2 and run on a Panasonic CF-19. The target systems are provided to Liaison services by OTS/i2c with the hardware, Operating System, and biometric software, listed in the following table.			

(U) Requirement 13 enumeration

Item/Vendor	Media Description	Ver. #	License Number	Media Format
MSFT	Windows XP-Operating system	XP w/ SP2	Machine-specific	Preloaded
Cross Match	MOBS- Software Application (Collection)	1.4.0.0045	n/a	Download (FTP)
Cross Match	MILTA-Configuration File	1.4.0.0045	n/a	Download (FTP)
Cross Match	EMS- Watchlist Application (Enrollment and Identification)	R1.10	Machine-specific	Download (FTP)
Cross Match	ID Trak- Watchlist Viewer	1.0.0.16	n/a	Download (FTP)
Panasonic Toughbook	Panasonic	N/A	N/A	CF-19
I-Scan 2 Dual Iris Scanner	Crossmatch	N/A	N/A	ISCAN2
Guardian Finger Print	Crossmatch	N/A	N/A	Ruggedized Version

Item/Vendor	Media Description	Ver. #	License Number	Media Format
Scanner				
Digital Camera (Powershot)	Canon	N/A	N/A	PSA640
IS MRZ Passport Reader	Access	N/A	N/A	Asses-IS
NiMH Rechargeable Battery	Matthew Associates	N/A	N/A	BB-390A/U
NiMH Rechargeable Battery	BenTronics	N/A	N/A	BB-390B/U 6140-01-490-4317

5 (U) Approach

(U) The Independent Verification and Validation (IV&V) team will obtain requirements from the developer and, where gaps exist, will identify additional tests. The requirements will be validated through functional testing that executes part or all of the system to determine if the requirement has been satisfied. Each requirement will be specifically addressed in a detailed test procedure. Functional and performance testing will determine if the client component operates as expected.

6 (U) Test Environment

(S) The test environment consists of a developer-provided Panasonic CF-19 Toughbook laptop configured with Windows XP Professional w/SP2 and pre-installed biometric applications that produce target test data and ExpressLane USB drives. Security application characterization was conducted on two Dell Optiplex 330 machines with Windows XP, SP2 installed.

7 (U) Test Procedures**

(U) **Note: The test procedures have been refined to alleviate redundancy.

1.1 (S) Test Set 1 – ExpressLane

7.1.1 (U) Test Procedure 1.1 – Windows XP Professional w/SP2 Operating Systems Testing

(S) The following test procedure tests the operation of the ExpressLane client to covertly capture biometric data files, with or without the cover application splash screen, from a target computer when the operator has physical access to the computer to install a cover application.

(S) Setup steps:

1. Receive target Panasonic CF-19 Toughbook laptop equipped with various biometric applications and Windows XP Professional, SP2 provided by the customer.
2. The same laptop is used for pre-processing, target attack and post-processing activity.

(S) Testing steps:

Step	Action	Expected Result	Req
1.	Run **strings.exe** on all ExpressLane file and associated USB drives (overt and covert sides).	No suspicious text was observed on either side. The covert side was not accessible.	1
2.	Run Advanced Registry Tracer on the Target and compare with a previous scan; then save to a log file.	Registry changes were saved to file on the desktop.	1
3.	Using **createpartition.exe**, allocate 10% of a commercial USB drive to a hidden partition and set the time for installation to 5 minutes.	A hidden partition was created on the commercial USB drive.	7, 8
4.	Using MOBS_UPGRADE.exe on the cover application CD, install the cover application on the target computer. Restart the target computer.	**mobslangsvc.exe** service is running on the target computer after the restart.	1, 2
5.	Remove the USB drive from the target laptop once hard drive activity ceases.	Hard drive will indicate activity for several minutes while target files are copied to the hidden partition on the USB drive.	2
6.	Re-insert the USB drive into the target laptop. Execute **exitramp.exe** to retrieve captured files from the USB drive.	Once the process is completed, captured eft, ldf, and mdf files are visible in the designated output directory.	3, 4
7.	Install McAfee Total Protection 2009 on the target laptop.	Appropriate security application is active on the target laptop.	12
8.	Repeat steps 3 through 6 on the target laptop.	ExpressLane is not detected by the security application.	12
9.	Uninstall the security application from the target laptop.	Security application has been uninstalled.	12
10.	Install Norton Internet Security 2009 on the target laptop.	Appropriate security application is active on the target laptop.	12
11.	Repeat steps 3 through 6 on the target laptop.	ExpressLane is not detected by the security application.	12
12.	Uninstall the security application from the target laptop.	Security application has been uninstalled.	12
13.	Install Kaspersky 8.0 on the target laptop.	Appropriate security application is	12

		active on the target laptop.	
14.	Repeat steps 3 through 6 on the target laptop.	ExpressLane is not detected by the security application.	12
15.	Uninstall the security application from the target laptop.	Security application has been uninstalled.	12
16.	Watermark the USB drive using createpartition.exe**.**	Drive is now water marked.	1
17.	Insert the USB drive in the target machine, but do not execute the cover application.	Collection begins and completes successfully	1

1.2 (S) Test Set 2 – ExpressLane (Kill Switch)

7.2.1 (U) Test Procedure 2.1 – Windows XP Professional, SP2 Operating Systems Testing

(S) The following test procedure tests the ability of ExpressLane to covertly corrupt the license files of the biometric application which will force a visit to re-install the software.

(S) Setup steps:

1. Receive target Panasonic CF-19 Toughbook laptop equipped with various biometric applications and Windows XP Professional, SP2 provided by the customer.

(S) Testing steps:

Step	Action	Expected Result	Req
1.	Using **MOBS_UPGRADE.exe** on the cover application USB drive, install the cover application on the target computer. Restart the target computer.	**mobslangsvc.exe** service is running on the target computer after the restart.	1, 2, 6
2.	Use **createpartition.exe**, to allocate 50% of a commercial USB drive to a hidden partition and set the install time to 5 minutes.. Set the Kill date to 1day earlier. (Yesterdays Date) Use "View Partition" to verify that the kill data has been set and that the USB drive now is 50% smaller than what it originally was.	A hidden partition was created on the commercial USB drive.	7, 8
3.	Using a hex editor, view the USB drive and look for the expiration date that you set with the utility **createPartition.exe**.	Expiration date is not found in plain text or numeric data.	1
4.	On the target computer, open the license files and copy the license line to a text file so that you can preserve the original and reference it.		11
5.	Insert the USB drive into the target computer. After 30 seconds the light on the USB drive will begin to show disk activity. Remove the USB drive from the system at this point.	No pop up should occur.	2
6.	Check the license files, they should have been modified and will no longer match the original license files.	Both license files were modified.	9, 10, 11
7.	Cut and copy the original license files back into	License files are restored back to their	10

	the original license files and restart the system.	original state	
8.	Reinsert the USB drive back into the target computer and let it collect all the EFT files on the system.		2, 6
9.	Remove the USB drive from the target laptop once hard drive activity ceases.	Hard drive will indicate activity for several minutes while target files are copied to the hidden partition on the USB drive.	2
10.	Insert the USB drive into the post processing laptop. Execute “exitramp.exe” to retrieve captured files from the USB drive.	Once the process is completed, captured and encrypted eft. Ldf and mdf files are visible in the designated output directory along with the directory scan.	3, 4, 5

8 (U) Test Report

8.1 (U) Requirements Verification Matrix

(U) The Requirements Verification Matrix below displays six different letter keys to signify how well the tool meets the user requirement. The meaning of each letter key is shown adjacent to each letter.

Identifier	Meaning
p	The tool meets the requirement
I	The tool meets the requirement but there is an issue
F	The tool fails to meet the requirement
C	The tool failed to meet the requirement for a specific configuration
n	The requirement could not be tested
T	The requirement was tested by other means

Table 8.1.1 (U) Requirements Verification Matrix Letter Keys

	Requirement Number												
Test Identifier		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
	7.1.1	p	p	p	p			p	p				p	p
	7.2.1	p	p	p	p	p	p	p	p	p	p	p		

Table 8.1.2 (U) Requirements Verification Matrix for Requirements 1-10

8.2 (U) Findings

(U) None.

8.3 (U) Observations and Comments (Security Characterization)

1. McAfee – all three versions had a single low level alert stating that the installation modified a registry entry.
2. Norton Internet Security - both versions were non-alerting.
3. Kaspersky –All alerts were low level and were related to the installation.
4. The accessed date and timestamp for the files collected are modified during the collection process.

(U) Note: For additional information on observation 4, see Appendix A Forensic Examination Results

Appendix A: (U) Forensic Examination Results

(U) Tool Name: Express Lane v3.1.1
(U) Date of Report: 28 Apr 2009

(U) Reference Documents

- (S) IMIS Req #: 2009-1655
- (S) Live Examination Checklist V1.doc
- (S) Post Mortem Analysis Checklist V1.doc

S:\DO\IOC\EDG ALL\Front Office\EDG Systems Engineering\IVV\Forensics\Checklists

(U) Executive Summary:
(S/NF) Though the tool does not change the modified date/time for the collected files, the accessed date and times are changed. Table 1 contains a list of files and/or directories containing evidence of tool activity categorized by operating system. Details of the evidence discovered in each file can be found in the Examination Results section of this report.

Table 1. (S) Files/Directories Containing Evidence

Windows XP Pro SP2 32-bit
*.eft
*.ldf
*.mdf

(U) Subject Computers and Media Examined:

Subject A. Dell Vostro 200 with Windows XP Professional SP2 64 Bit installed

(U) Examination Procedure:
(S) This examination was conducted in accordance with established IV&V checklists and procedures. Supporting documentation can be found on the CWE Share at the following path:

S:\DO\IOC\EDG ALL\Front Office\EDG Systems Engineering\IVV\Forensics

(U) Examination Results:

(U) Findings

(S/NF) In accordance with COG Requirement #2009-1655 from the IMIS requirement documentation, the following statement below is categorized as a finding:

(S/NF) 1. None.

(U) Observations

(S/NF) 1. The accessed date and time for the files collected are modified during the collection process.

(U) Live State Examination

(U) A live state examination was not conducted.

(U) Post-Mortem Examination:

(S/NF) The following artifacts were retrieved from a forensic image of the Subject following the installation and utilization of the tool:

(U) Subject A: Dell Vostro 200 with Windows XP Professional SP2 64 Bit installed

(S/NF) A1. The tool modifies the accessed date and time for the files collected. Table A2 lists the filenames with modified accessed date and time.

(U) Table A2**.** Accessed Files
(S/NF) Path: Varies

Name	File Created
*.eft	04/24/09 08:31:42 AM – 08:32:59 AM
*.ldf	04/24/09 08:31:42 AM – 08:32:59 AM
*.mdf	04/24/09 08:31:42 AM – 08:32:59 AM

Appendix B: (U) Forensic Terms

$MFT - Master File Table is a relational database of all files, folders, and system structures contained on an NTFS volume. In NTFS, everything on a volume is a file. The $MFT is the master index for the entire volume.

$MFT Records - Each $MFT entry contains information about a file or directory. There are three types of records: File records, Directory Records, and Metadata Records. File Records store information about files. Directory Records store and index file names. Metadata Records contain system and file structure information. Each record is a series of attributes.

$MFTMirr - $MFT Mirror File is a copy of the first four $MFT records used for recovery purposes. It provides an alternate means of accessing the essential volume structures should the $MFT become damaged. The mirror file contains $MFT records for the $MFT, MFTMirr, $LogFile, and $Volume files.

$LogFile - Log File is used to protect critical system data not user data. NTFS uses a transaction based checkpoint logging system to track any changes to the volume structure. A transaction is any operation that alters a file on an NTFS volume. The $LogFile is a database containing RCRD and RSTR records. The RSTR records contain information needed in the event that the files system needs to be recovered. RSTR are referred to as Re-do and Un-do information. The RCRD are called infinite logging records since they are continually reused. RCRD contain transaction information until committed to disk. Fragments of data are commonly found in the $LogFile.

$Volume - $Volume record contains the volume name and volume attributes.

$AttrDef - Attribute Definitions is a file that lists the NTFS attributes supported on the current volume, including additional information about each attribute.

$Bitmap -$Bitmap file is a simple cluster map showing which clusters are allocated and which clusters are not.

$Boot - Boot Sector is the Volume Boot Record for the volume. $Boot points to the boot sector VBR.

$Badclus - Bad Cluster Map maps the location of any known bad clusters on the disk.

$Secure - $Secure is an NTFS database containing security information for all files and directories in the volume. The security descriptors database is maintained in a series of alternate data streams, $SDS Data Stream, $SDH Index, and $SII Index.

$UpCase - $UpCase is a file that contains a map of lowercase Unicode characters and the uppercase equivalents.

$Extend - $Extend is a directory containing the location of extended metadata files, $Quota, $ObjID, SReparse, and $UsnJrnl.

$Quota - $Quota file is a directory containing a list of users and files saved under their quota restraints.

$Objid - Object Identifier is part of the NTFS Link Tracking Service (LTS). This service enables Windows to keep track of a file or directory even when the name or location is changed.

$Reparse - Reparse Points are similar in function to a link or shortcut file. A reparse point can be used as a mount point for volumes, directories, or files. $Reparse is an index containing a list of reparse points in use on the volume.

$Usnjrnl - Change Journal is designed to keep track of any changes made to $MFT records. It provides a persistent log of changes made to files on a volume. When any file or folder is created, modified, or deleted, NTFS adds a record to the change journal for the volume. The change journal is turned off by default.

BIOS - BIOS stands for Basic Input Output System. It is a combination of low-level software and drivers that function as the interface, intermediary, or layer between a computer's hardware and its operating system. They load into RAM from the motherboard ROM (ROM BIOS), an adapter card ROM, or from disk in the form of disk drivers.

Cluster - Cluster is the smallest allocation unit on a hard drive. It can be the size of one sector. A cluster is normally comprised of many sectors.

File System - File System is a method of storing and retrieving data on a computer system that allows for a hierarchy of directories, subdirectories, and files.

File Slack - File Slack is the area from the end of the logical file until the end of the cluster.

hiberfil.sys - hiberfile.sys is a file that allows Windows to hibernate. The machine powers off, goes to sleep, and can be brought back to the precise point where it went to sleep. To accomplish this, the entire contents of RAM must be written to a file, hiberfile.sys.

Hives - Hives are the component files that make up the registry. There are five hives in the registry: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG.

HKEY_CLASSES_ROOT - HKCR contains information about file extension associations. One of the five hives of the Windows registry.

HKEY_CURRENT_USER - HKCU contains user information, preferences, and settings for the currently logged in user. One of the five hives of the Windows registry.

HKEY_LOCAL_MACHINE - HKLM contains information specific to the computer. One of the five hives of the Windows registry.

HKEY_USERS - HKU contains user information from the user currently logged in and the default profile. The user information here is an alias to HKCU. One of the five hives of the Windows registry.

HKEY_CURRENT_CONFIG - HKCC is dynamically created during the boot process and contains information associated with the hardware configuration.

INFO2 - INFO2 file contains a single record for each deleted file or folder in Windows.

Junctions - Junctions are similar to volume mount points. Junctions are directory mount points that point a folder to another folder.

NTUSER.DAT - NTUSER.DAT is a file that contains user specific registry settings such as personal configuration, preferences, and program settings.

NTUSER.DAT.log - NTUSER.DAT.log is a log file that records changes made to the User registry hives within the NTUSER.DAT file.

Prefetch File - Prefetch Files are trace files that enable expedient loading of previously launched applications into memory.

Page file - A file on disk that is used to cache RAM memory. It is also called a swap file.

pagefile.sys - Pagefle.sys is a file on disk that is used to cache RAM memory. Windows NT based operating systems use the pagefile.sys as temporary storage for data dumped from primary memory (RAM). The pagefile is often used to store unused memory pages when all existing space within physical RAM is full.

Partition - Partition is a collection of consecutive sectors within a volume and is a container for a file system, with specific boundaries and properties.

Registry - Registry is a hierarchal database in Windows that contains system and user specific data.

ROM - Read Only Memory holds data permanently. It is nonvolatile.

RAM - Random Access Memory is a temporary workspace for storing data, code, settings, and so forth.

Ram Slack - Ram Slack or Sector Slack is the area of space after the data until the end of

that sector. It is the space after the logical file until the end of the last written to sector.

Sector - Sector is a contiguous group of bytes. It is the smallest number of bytes that can be addressed or written to on a drive. One sector = 512 bytes.

Sector Slack - Sector Slack or Ram Slack is the area of space after the data until the end of that sector. It is the space after the logical file until the end of the last written to sector.

Swap file - A file on disk that is used to cache RAM memory. It is also called a page file.

Unallocated Clusters - Unallocated Clusters are areas of data storage that are not allocated. They may or may not have data in them. When a file is deleted by the user, the clusters allocated to that file are released by the operating system to be used again. Data remains in the cluster until overwritten. Files and data fragments may be retrieved from unallocated clusters.

USBSTOR - USBSTOR is a registry key that records information about USB storage devices plugged into the computer.

Volume - Volume is a collection of addressable sectors that are used by an operating system or application to store data. It may be a single partition, multiple partitions, or physical hard drives.