

List of the ITDB Installation Files

This document contains information about installing the ITDB. The information includes the database, the DLL files, and set of executables, including their names, their function, and their directories.

The list is categorized into the following parts:

1. The Credit Card Application
2. The ITDB Components
3. The DLLs
4. The Database
5. The Others

1. The Credit Card Application

Executable Filename:

Poci.exe

Function:

Manually simulate a transaction of the credit card application to ITDB

Directory:

./ITDB/The Credit Card Application/

2. The ITDB components

2.1 The Mediator

Executable Filename :

Mediate.exe

Function:

1. Provide services to clients for accessing the database.
2. Capture most of the information about transactions' behavior.
3. Identify the type of each incoming transaction.
4. Enforce some important intrusion tolerance policies such as isolation and damage containment.

Directory:

./ITDB/ITDB Components/The Mediator/

Related Files:

1. TranPatt.ctl
This text file keeps information about the transaction's patterns that are used for identifying the type of each incoming transaction. This file has to be stored in the same directory as the Mediator.
2. OCIMEDIATE.HLP
The Mediator's Help File.
3. SQL Script files
The script files are called by the Mediator while performing the isolation process.

2.2 The Intrusion Detector

Executable Filename :

ID.exe

Function:

Detects suspicious or malicious transactions and reports the malicious transaction_id to the Repair Manager and the Mediator.

Directory:

./ITDB/ITDB Components/The Intrusion Detector/

Related Files:

See Part 3 the DLLs for ID

2.3 The Damage Container and Damage Uncontainer

Executable Filename :

Medaite.exe, DCM.exe

Function:

The Damage Container uses the multi-phase damage containment approach which first instantly contains the damage the might have been caused by an intrusion as soon as the intrusion is identified. The Damage Container is developed as a part of the Mediator.

The Damage Uncontainer tries to uncontain the objects that are previously contained by mistake.

Directory:

1. The Damage Container (Mediate.exe):
./ITDB/ITDB Components/The Mediator/
2. The Damage Uncontainer (DCM.exe):
./ITDB/ITDB Components/The Damage Uncontainer/

Related Files:

1. TrnsType_Log.txt
The text file keeps information that is used for building the transaction type graph. Th file has to be stored in the same directory as the Damage Uncontainer (DCM.exe).

2.4 The Isolation Manager

Executable Filename :

Mediate.exe

Function:

Isolate the set of suspicious transactions and merge the updates back to the database if an isolated user turns out to be innocent. The Isolation Manager is developed as a part of the Mediator (Mediate.exe).

Directory:

./ITDB/ITDB Components/The Mediator/

2.5 The Repair Manager

Executable Filename :

Repair.exe

Function:

Assess the damage caused by the intrusion and performs on-the-fly damage repair.

Directory:

./ITDB/ITDB Components/The Repair Manager/

2.6 The SSM

Executable Filename :

SSM.exe

Function:

Dynamic ally reconfigure the other ITDB components based on the current situation of the damage, the attacks, the workload, the ITDB performance, the ITDB effectiveness, and the cost in such a way that a stabilized level of data integrity can be provided to applications in a cost effective way.

Directory:

./ITDB/ITDB Components/The SSM/

Related Files:

See Part 3 the DLLs for SSM

2.7 The Transaction Simulator

Executable Filename :

AutoTrns - Usr xx.exe

Function:

Simulate transactions to the database (via the Mediator). The simulator randomly updates the 'acc_balance' field in the Accounts table. There are five different simulators:

1. AutoTrns - Usr 4.exe
The simulator logs in as user 'test4' and randomly simulates both innocent and suspicious transactions.
2. AutoTrns - Usr 5.exe
The simulator logs in as user 'test5' and randomly simulates both innocent and suspicious transactions.
3. AutoTrns - Usr 11.exe
The simulator logs in as user 'test11' and randomly simulates both innocent and suspicious transactions.
4. AutoTrns - Inct Usr 1.exe
The simulator logs in as user 'test1' and always simulates the innocent transactions.
5. AutoTrns - Inct Usr 2.exe
The simulator logs in as user 'test2' and always simulates the innocent transactions.

Directory:

./ITDB/ITDB Components/The Transaction Simulators/

3. The DLLs

3.1 DLLs for ID

Filename:

1. IDrule.dll
2. Rule2.dll
3. MFC42D.DLL
4. MSVCP60D.DLL
5. MSVCRTD.DLL

Function:

The IDrule.dll and Rule2.dll keep rules, which are used by the Intrusion Detector to identify the suspicious or malicious transactions. The IDrule.dll has to be stored in the

'C:\itdbms\IDrule\Debug\' also the rule2.dll has to be stored in the 'C:\itdbms\rule2\Debug\' folder.

MFC42D.DLL, MSVCP60D.DLL, and MSVCRTD.DLL are Microsoft run time library. If your machine does not install the MS VC++, you need to copy these files into the same directory as the Intrusion Detector (ID.exe).

Directory:

./ITDB/The DLLs/DLLs for ID/

3.2 DLLs for SSM

Filename:

MFCO42D.DLL

Function:

MFCO42D.DLL is the Microsoft dynamic link library. If your machine does not install the MS VC++, you need to copy this file into the same directory as the SSM (SSM.exe).

Directory:

./ITDB/The DLLs/DLLs for SSM/

4. The Database

Filename:

EntireDB_Final.DMP

Function:

The database export file which is exported from the ITDB latest version. The file includes all users' objects such as data and table structures.

Directory:

./ITDB/The Database/

5. The others

5.1 The SQL Scripts

Filename:

1. Itdbms_capture.sql
2. cuz_sys_user.sql
3. cuz_itsys_user.sql
4. cuz_test_user.sql
5. cuz_rpmgr_user.sql

Function:

These SQL scripts must have been run in order from (1) to (5) after finishing import the database and configure the SQL net. (See details in the installation manual)

Directory:

./ITDB/The Others/SQL Scripts/

5.2 The CORBA Testing Program

Filename:

CorbaTest.exe

Function:

This utility program is used for testing if the client can communicate with the CORBA server by sending a command from client to make a 'beep' sound in the server (the Mediator).

Directory:

./ITDB/The Others/CORBA Testing Program/