**Flow Detector Environment Setup**

Before you start to get the FlowDetector code from SVN, you need first to download and install the following programs:

* Microsoft Network Monitor link: <http://www.microsoft.com/en-us/download/details.aspx?id=4865> for both the FlowDector client and server.
* For the FlowDetectorServer .Net MySql Connector (DB Driver) link: <http://dev.mysql.com/downloads/connector/net/>
* Microsoft Visual Studio 2010 (C#) any edition would be fine even the free express one. Link to Visual Studio 2010 Express: <http://www.microsoft.com/visualstudio/en-us/products/2010-editions/express>
* For SVN any SVN client would work e.g. TortoiseSVN link: <http://tortoisesvn.net/>

After checking out the code from the SVN server, open the solution with Visual Studio 2010; you should find three projects as illustrated in Figure 1.



**Figure 1**

The DecisionTree project is a class library (DLL). The FlowDetector is the client (sniffer and feature extractor). The FlowDetectorServer is the decision maker that uses the DecisionTree to decide on the flow if malicious or not and stores alerts to a MySQL DB.

Make sure that the MySQL DB is installed and configured correctly to accept connections from the machine that the FlowDetectorServer will run on.

**In order to configure the MySQL DB you can do the following:**

* Download and install MySQL DB from <http://dev.mysql.com/downloads/mysql/>, download the community server edition (the free one).
* Download MySQL Workbench from <http://dev.mysql.com/downloads/workbench/5.2.html>
* Run the MySQL Workbench; copy and paste the following in the Query Editor to create the DB: delimiter $$

CREATE DATABASE `detectorplugindb` /\*!40100 DEFAULT CHARACTER SET latin1 \*/$$

* Run the following in the Query Editor to create the first table:

delimiter $$

CREATE TABLE `alertsbuffer` (

`ID` int(11) NOT NULL AUTO\_INCREMENT,

`FLD\_LOGGERIDENTITY` varchar(45) DEFAULT NULL,

`FLD\_TIMESTAMP` varchar(45) DEFAULT NULL,

`FLD\_APL` double DEFAULT NULL,

`FLD\_PV` double DEFAULT NULL,

`FLD\_PX` double DEFAULT NULL,

`FLD\_PPS` double DEFAULT NULL,

`FLD\_FPS` double DEFAULT NULL,

`FLD\_DPL` double DEFAULT NULL,

`FLD\_FLOWTYPE` varchar(45) DEFAULT NULL,

`FLD\_SOURCEIP` int(11) DEFAULT NULL,

`FLD\_SOURCEPORT` int(11) DEFAULT NULL,

`FLD\_SOURCEMAC` varchar(45) DEFAULT NULL,

`FLD\_DESTINATIONIP` int(11) DEFAULT NULL,

`FLD\_DESTINATIONPORT` int(11) DEFAULT NULL,

`FLD\_DESTINATIONMAC` varchar(45) DEFAULT NULL,

`FLD\_TRASPORTTYPE` varchar(45) DEFAULT NULL,

PRIMARY KEY (`ID`),

UNIQUE KEY `ID\_UNIQUE` (`ID`)

) ENGINE=InnoDB AUTO\_INCREMENT=141440 DEFAULT CHARSET=latin1$$

* Run the following in the Query Editor to create the second table:

delimiter $$

CREATE TABLE `flowtypetable` (

`id` int(11) NOT NULL AUTO\_INCREMENT,

`name` varchar(45) NOT NULL COMMENT 'Malicious flow type name.',

`label` varchar(45) NOT NULL,

PRIMARY KEY (`id`),

UNIQUE KEY `id\_UNIQUE` (`id`)

) ENGINE=InnoDB AUTO\_INCREMENT=5 DEFAULT CHARSET=utf8 COMMENT='Describe the flow type by the MAC marker'$$

* Use the following insert statements to create entries in the “flowtypetable” that match the signature file used by the FlowDetectorServer:

INSERT INTO `flowtypetable` VALUES(1, "SMTPSpam", "AA:AA:AA:AA:AA:AA");

INSERT INTO `flowtypetable` VALUES(2, "UDPStorm", "BB:BB:BB:BB:BB:BB");

INSERT INTO `flowtypetable` VALUES(3, "Zeus", "CC:CC:CC:CC:CC:CC");

INSERT INTO `flowtypetable` VALUES(4, "ZeusControl", "CC:CC:CC:DD:DD:DD");

INSERT INTO `flowtypetable` VALUES(5, "IRCBot", "EE:EE:EE:EE:EE:EE");

**Before building the server and client, you need to change the configuration parameters:**

* Configure the FlowDetectorServer to use the right IP of the MySQL DB server, Name of the DB, UserName and Password:
* Open the solution in Visual Studio 2010.
* Open the FlowDetectorServer Project (double click).
* Double click the app.config file of the project.
* Scroll down to the end of the file.
* Make the necessary modifications as illustrated in Figure 2.
* **It is important to note that, all of these modifications can later on be altered by editing FlowDetectorServer.exe.Config XML file. You can find the file in the same location of the FlowDetectorServer.exe executable file. Also the application must be restarted for the changes to take effect.**



**Figure 2: app.config file**

* The explanation of each of the configuration parameters is as follows:
* Version: version of the program
* SignatureFile: the signature file to be used by the FlowDetectoServer
* TrainingPercentage: The percentage of the training file to be used for training, this parameter should always be 1 unless you want to train the detector with a subset of the training file.
* DataSvcPort: the port number the server uses to listen to the connections from the client.
* DBSvrAddr: The IP address of the MySQL DB
* DBUser: the user name to the DB
* DBPwd: the password of the DB
* DBSchema: the name of the DB; it should be consistent with the one we created when we configured the MySQL DB.
* DBInstance: Don’t worry about this one
* ErrorLog: the name of the log file.
* TimeWindow: the time window the server uses to extract the features, this number is in seconds, so one minute is 60 sec and so on.
* For the client, the configuration of the parameters are the same:
* Open the FlowDetector project.
* Double click the app.config file
* Make the necessary changes as illustrated in Figure 3.
* **It is important to note that all of these modifications can later on be altered by editing FlowDetector.exe.Config XML file. You can find the file in the same directory of the FlowDetector.exe executable file. Also the application must be restarted for the changes to take effect.**



**Figure 3: FlowDetector Configuration**

* The explanation of the parameters:
* Version: version of the program
* CaptureWindow: capture window in seconds.
* ErrorLog: Error log file
* ServerAddr: the IP address of the FlowDetectorServer
* ServerPort: the port number the FlowDetectorServer is listening on.

After building both the Client and Server you can simply run them, however you must run them as Administrator, in order to do that you can right click on the exe and select run as Administrator from the pop-up menu as shown in Figure 4.



**Figure 4: Run as Administrator**

When you run the client you will find a calculator icon in the windows system tray. Right clicking the icon and you will get a context menu like shown in Figure 5. Clicking the “**Config Server Address”** will show a form to change the configuration for the server IP address and port number as shown in Figure 6. **You must restart the client for the changes to take effect.**



**Figure 5: Config Server Address**



**Figure 6: Configure Server Address Form**

The FlowDetectorServer.exe must be run “as Administrator” like the client. Right Click the exe file and select run as Administrator just like we did at Figure 5. When you right click on the magnifying glass icon in the system tray you get the context menu in Figure 7.



**Figure 7: Signature Generation and Offline detection**

Selecting “Generate Signature“ will prompt the user with Windows open file dialog to choose a network trace file (pcap/cap) for the signature generation. The resulted signature file will be created in the same directory of the exe file. The signature file is a serialization of the decision tree in XML format. You can configure the FlowDetectorServer to use the newly created file by editing the FlowDetectorServer.exe.Config xml file. At anytime the user can cancel the signature generation by right clicking the system tray icon and clicking “Cancel signature generation”.

Selecting “Start Offline Detection” will prompt the user with Windows open file dialog to select a network trace file (pcap/cap) for offline detection. While the offline detection is executing hovering over the system tray icon will prompt the user with a cloud pop-up about the percentage of the file being processed. At anytime the user can cancel the offline detection by right clicking the system tray icon and selecting “Cancel offline detection” as illustrated in Figure 8.



**Figure 8: Cancelling Offline Detection**

**Trouble Shooting Windows XP:**

* In order for the FlowDetector Client to work on Windows XP, a registry value must be created as follows:
* The default threading mode of the Windows XP and Windows Server 2003 driver is single-threaded. This can be changed using registry settings, but may cause side-effects as the driver may be shared by other applications. Be careful when making this kind of change. To change the threading model in the Windows XP registry, under **My Computer\HKCR\CLSID\{425882B0-B0BF-11CE-B59F-00AA006CB37D}\InProcServer32**, add a string called **ThreadingModel**, if it is not already there, and set its value to **Both**.