Using the Windows Event Log
IN618 Security

September 8, 2014

Introduction

When we write software it is important that we include logging capability. Good logs are useful for debugging and other troubleshooting in addition to being necessary for proper security accounting.

It is typically neither necessary nor wise to write your own custom logging routines. Instead we use the built in logging functions supplied by the operating system. In this lab we will see how to write to the Windows Event Log from our application. We will extend the password checking program we wrote last week. If you do not have your code from that lab available, you can download sample source code from the week 7 section on Moodle.

1 Setting up logging

To make use of Windows event logging, you will need to add

```
using System.Diagnostics;
```

to your source code. Then, add an event log field to your Form1 class. We'll call ours `appEventLog`.

```
private System.Diagnostics.EventLog appEventLog;
```

In our `Form1_Load` function we set up the event log

```
    string source = "IN618 Example Application";
    string log = "IN618 Log";
        if (!System.Diagnostics.EventLog.SourceExists(source))
        {
            System.Diagnostics.EventLog.CreateEventSource(source,log);
        }                       }

    appEventLog = new System.Diagnostics.EventLog(log);
    appEventLog.Source = source;
```

This code will create the log if it does not exist already. This requires Administrator privileges, so in a real application this should be handled by the installer.

2 Writing log messages

With logging set up in our application, writing to he log is easy. For example, to log a failed login, add the following line at the appropriate point in your code:

```
 appEventLog.WriteEntry("Login failure, bad password", System.Diagnostics.EventLogEntryType.Information)
```

Notice that we set the log message type to “Information”. Other message types are available Add code to your application to log successful and failed logins.

3 Viewing logs

Now that we’re writing logs, let’s see how we can read them using the Event Viewer. Run your program and check a few passwords so that there will be an opportunity to view both failed and successful logins in the event log.

Open Event Viewer by clicking the Start button, clicking Control Panel, clicking Administrative Tools, and then double-clicking Event Viewer. Expand “Application and Services Logs” in the left-hand menu and select the “IN618 Log”. Open the log and select the event entries to inspect the details.