Background

- Reliability is an important aspect of any application.
- Fault injection techniques are used for assessing the reliability of applications.
- NFTAPE is a tool developed for performing automated fault injections to evaluate the reliability of applications.

Fig 1: NFTAPE Architecture

- Increased vulnerabilities of Windows applications created the need to do reliability assessment and thereby take corresponding measures to improve the performance of the application.
- Windows Injector can be used for assessing reliability of Windows applications.

Goals

- Design a fault injector for Windows applications that is capable of injecting faults to the text, data, and stack segments of an application.
- Make the injector compatible with the NFTAPE architecture.
- Automate the injection process.
- Store the results of injections performed on an application.

Fundamental Questions/Challenges

- How to:
  - Attach to a target application.
  - Access the attached application’s address space.
  - Control the injection:
    - When should the injection be done?
    - Where should it be done?
    - What should be injected?
    - How should it be injected?
  - Automate the fault injection process.

Research Plan

- Understand the working of NFTAPE Linux and Solaris Injectors.
- Get familiar with the usage of Windows APIs.
- Design a Basic Debugger for Windows applications.
- Modify the Debugger to function as a fault injector.

Research Results

- Input format of Injector:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Breakpoint Address</th>
<th>Destination Address</th>
<th>Injection Type</th>
<th>Mask Function</th>
<th>Mask Size</th>
<th>Mask Data</th>
<th>Wait Time (milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack.exe</td>
<td>0x401291</td>
<td>0x404070</td>
<td>Text/Data/Stack</td>
<td>OverWrite/Add/BitFlip</td>
<td>0x401291</td>
<td>Value (&gt;1000)</td>
<td></td>
</tr>
</tbody>
</table>

- A fault injector for Windows applications that is able to inject faults to the text, data, and stack segments of the target application.

Fig 2: Win32 Fault Injector

- Automated injection process.

Fig 3: Flow Chart of Automation

Related Work

- Information regarding Windows APIs is available in the Microsoft Developer Network site: http://msdn.microsoft.com/en-us/library/ms