# ActiveX Fuzzing with Dranzer

## One Thousand Vulnerabilities Later

Will Dormann



© 2008 Carnegie Mellon University

# Outline

I. ActiveX Background

II. Fuzz Testing with Dranzer

III. Dranzer Results

IV. Automation

# Background – COM

Microsoft COM (Component Object Model) is a Windows technology that allows for communication between software components.

- Most Windows applications are built with COM objects as components.
- COM is present in Windows 95 and newer and Windows NT and newer.

# Background – ActiveX

Beginning with Internet Explorer 3, COM objects could be used in web pages.

- COM objects, referred to as ActiveX controls, could provide additional functionality to web pages.
- ActiveX controls are native code, as opposed to interpreted scripting languages, such as JavaScript and VBScript.

# ActiveX and Internet Explorer

Through use of the <OBJECT> HTML tag, Internet Explorer can utilize COM objects that reside on a Windows sytem.

```
<HTML>
<OBJECT ID="WMPlayer"
CLASSID="CLSID:6BF52A52-394A-11D3-B153-00C04f79FAA6">
</OBJECT>

</HTML>
```

# Attacking ActiveX with Internet Explorer

COM objects give Internet Explorer a large attack surface.

- Microsoft Windows XP comes with over 2500 COM objects pre-installed.
  - As more software is installed on a Windows computer, the number of installed COM objects will increase.
- Any COM object can by default be instantiated by any web page on the internet.
- A flaw in any single COM object may be exploitable, using Internet Explorer as an attack vector.
- Scripting technologies, such as JavaScript or VBScript give an attacker a better chance of exploiting flaws in COM objects.

# Outline

I. ActiveX Background

II. Fuzz Testing with Dranzer

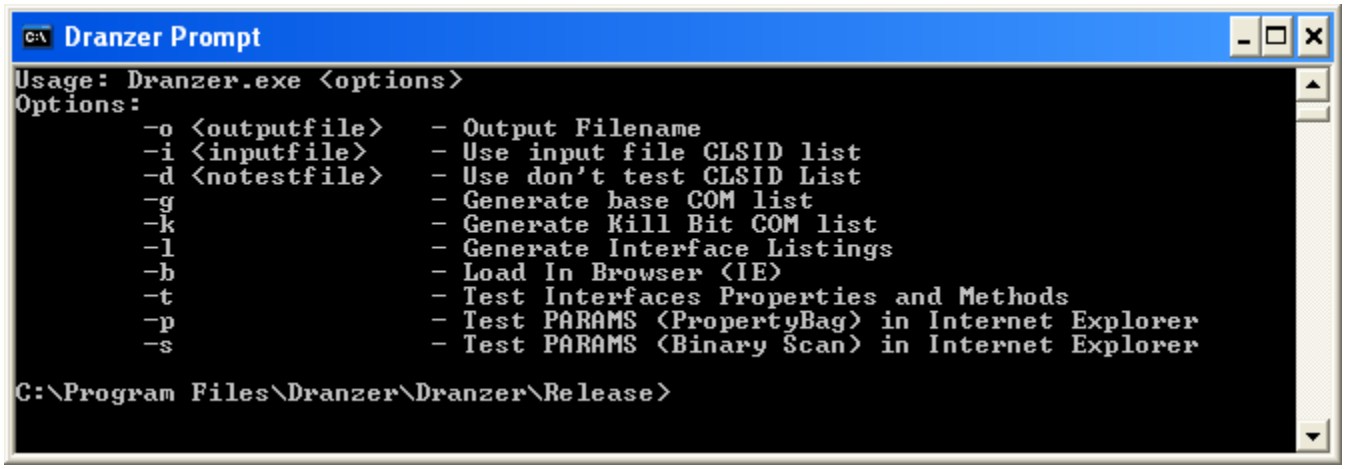
III. Dranzer Results

IV. Automation

# How To Discover Vulnerable Controls?

The Dranzer tool provides fast, automated fuzz testing of COM objects:

- Load Faults
- Properties and Methods
- Parameter Initialization
- Dangerous Methods



# Load Faults

COM objects that cause Internet Explorer to crash merely upon referencing the object.

Example:

Vulnerability Note VU#898241

Microsoft BlnMgr Proxy (blnmgrps.dll) COM object fails to implement required methods

# Properties and Methods

COM objects that crash when passed “unexpected” values to methods or properties.

Example:

Vulnerability Note VU#649289

Retro64 / Miniclip CR64Loader ActiveX control buffer overflow

# Parameter Initialization

COM objects that crash when passed unexpected values to initialization parameters.

Example:

Vulnerability Note VU#225217

Sky Software FileView ActiveX control buffer overflow vulnerability

# Dangerous Methods

COM objects that expose methods that are inherently dangerous, but fail to restrict access by 3rd parties. (Repurposing)

Example:

Vulnerability Note VU#221700

Acer LunchApp ActiveX Control fails to properly restrict access to methods

# Dranzer vs. Other ActiveX Fuzzers

| | Dranzer | axfuzz | COMRaider | AxMan |
|---|---|---|---|---|
| Time to test object | **1 sec.** | 4 sec. | 140 sec. | 660 sec. |
| Exceptions found | **3** | 2 | **3** | 1 |
| Vulnerability classes covered: | | | | |
| Class I | **yes** | no | no | no |
| Class II (methods) | **yes** | **yes** | **yes** | **yes** |
| Class II (params) | **yes** | no | no | no |
| Class III | **yes** | no | no | no |
| Output | text | text | **database** | none |
| User interaction required | **none** | medium | high | very high |
| Test multiple objects | **yes** | **yes** | no | **yes** |
| Test sequences | **yes** | **yes** | no | **yes** |
| Crash details reported | **yes** | no | **yes** | no |

# Outline

I. ActiveX Background

II. Fuzz Testing with Dranzer

III. Dranzer Results

IV. Automation

# Example Dranzer Output

```
*****************************************************************************
{288C5F13-7E52-4ADA-A32E-F5BF9D125F99}-CR64Loader Object
ERROR - Access violation (0xc0000005)
*****************************************************************************
*****************************************************************************
Testing COM Object - {288C5F13-7E52-4ADA-A32E-F5BF9D125F99} CR64Loader Object
*****************************************************************************
COM Object Filename : C:\miniclipGameLoader.dll
Major Version       : 1
Minor Version       : 0
Build Number        : 0
Revision Number     : 1
Product Version     : 1.0.0.1
Product Name        : TODO: <Product name>
Company Name        : TODO: <Company name>
Legal Copyright     : TODO: (c) <Company name>.  All rights reserved.
Comments            : not found
File Description    : TODO: <File description>
File Version        : 1.0.0.1
Internal Name       : retro64_loader.dll
Legal Trademarks    : not found
Private Build       : not found
Special Build       : not found
Language            : not found
*****************************************************************************
```

# Example Dranzer Output (cont.)

```
*****************************************************************************
Invoking Property Get           - IR64Loader::BSTR filename()
*****************************
***   Access Violation    ***
*****************************
Invoked - VariantClear 1
Access violation at 0x77124874 :Bad read on 0xFFFFFFFF
*****************************
Invoking Property Put           - IR64Loader::void filename([in] BSTR<"xxxx.....{10240}">)
*****************************
***   Access Violation    ***
*****************************
Invoked Property Put            - IR64Loader::void filename([in] BSTR<"xxxx.....{10240}">)
Access violation at 0x008E134E :Bad write on 0x008FE000
*****************************
*****************************
***   Access Violation    ***
*****************************
Access violation at 0x008E8749 :Bad read on 0x78787880
*****************************
*****************************************************************************
Number of COM Objects                    1
Number of COM Objects With Kill Bit      0
Number of COM Objects Without Kill Bit   1
Number of COM Objects Not Script Safe    0
Number of COM Objects Passed Test        0
Number of COM Objects Failed Test        1
Number of COM Objects Hung During Test   0
Number of COM Objects with No Type Info  0
Number of COM Objects Misc Errors        0
*****************************************************************************
```

# Vulnerability Verification

http://xcat.mallab.cert.org/tools/activex/ - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://xcat.mallab.cert.org/tools/activex/ Go Links

Spray Heap ◉ Tiny ○ Small ○ Med ○ Big ○ Huge slide char: 0x 90 0x02_____ - 0x09_____

**Enter COM object ClassID:** ☐ Initialize with parameter?

{288C5F13-7E52-4ADA-A32E-F5BF9D125F99}

Create Object

**Method:** filename

**Parameter(s):** 1 Change number of parameters: - +

☑ bigstring

(Character:0x 06 Size: 10240 )

☑ property put

☐ property get

◉ JavaScript ○ VBscript

ScriptMe

Exploit template Killbit generator

The object {288C5F13-7E52-4ADA-A32E-F5BF9D125F99}:

Spray size: 150, slide: 90

Done Internet

# Outline

I. ActiveX Background

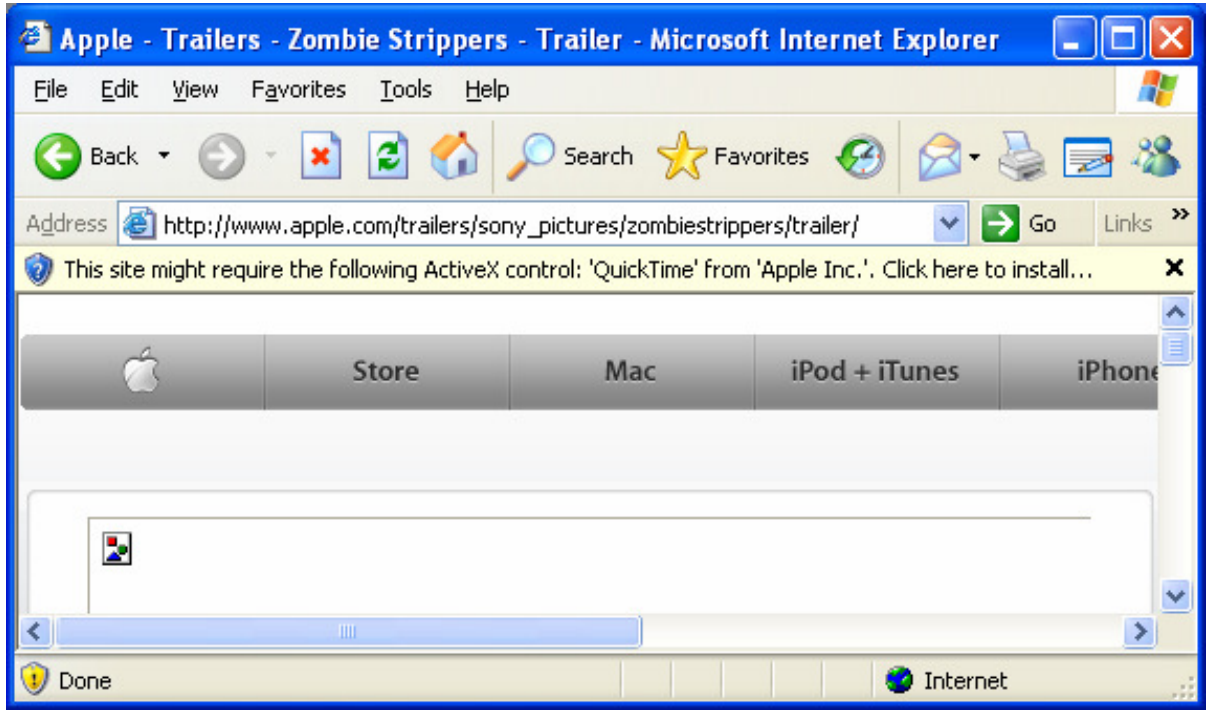
II. Fuzz Testing with Dranzer

III. Dranzer Results

IV. Automation

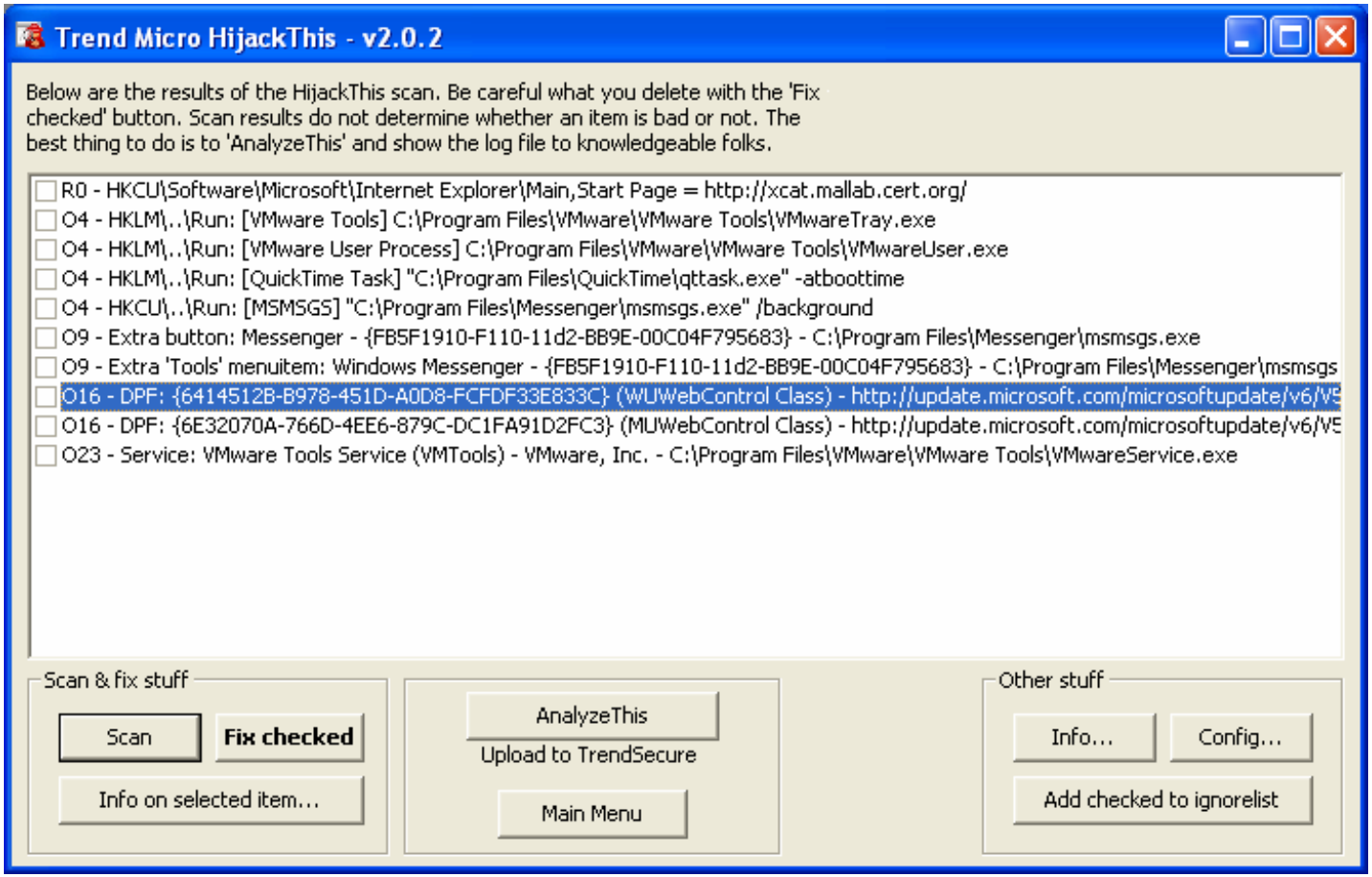
# Sources of ActiveX Controls

- Installed with Windows applications
  - Requires user interaction
- Installed by a web page in IE
  - Automatable

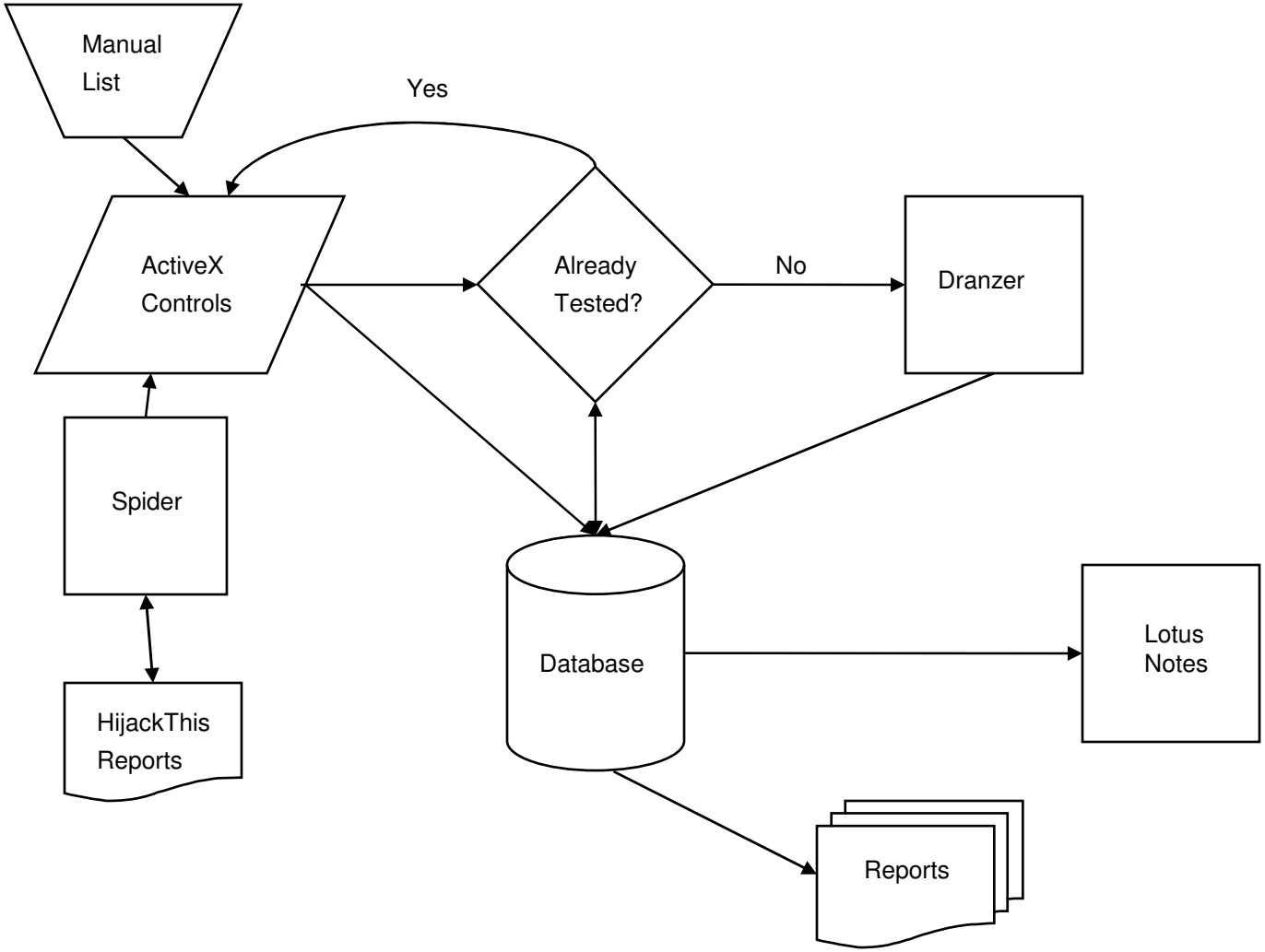


# Finding Downloadable ActiveX Controls

HijackThis



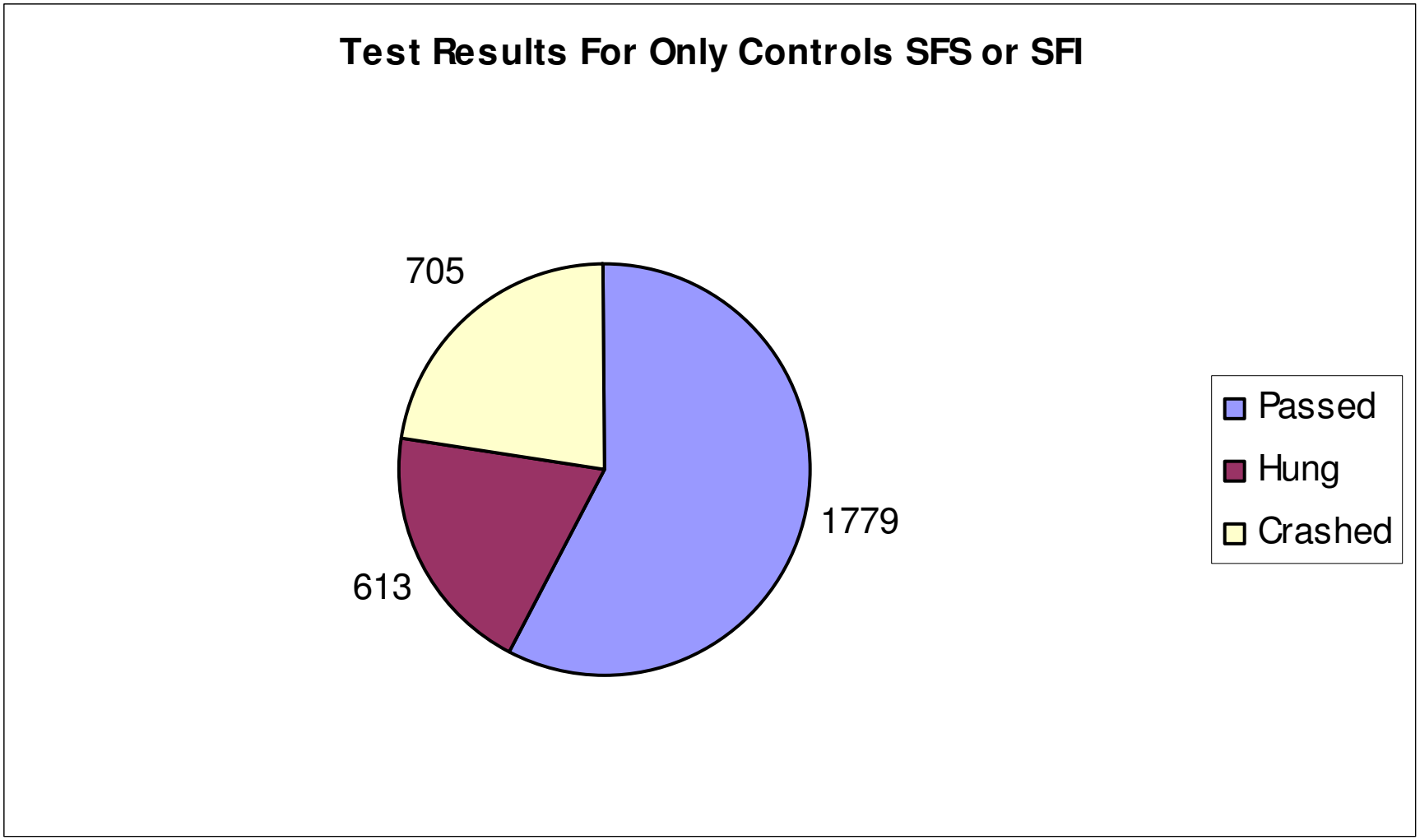
# Automation


Manual
List
Yes
ActiveX
Controls
Already
Tested?
No
Dranzer
Spider
Database
Lotus
Notes
HijackThis
Reports
Reports

# Automation Results

| | SFS or SFI | Percent |
|---|---|---|
| Total | 3097 | 100.00% |
| Passed | 1779 | 57.44% |
| Hung | 613 | 19.79% |
| Crashed | 705 | 22.76% |

# Automation Results



# Automation Demonstration

(Videos)

# Live Dranzer Demo

(Demo)

# Questions?

**Email:** cert@cert.org

**Phone:** +1 412 268 7090 (24 hour hotline)

**Fax:** +1 412 268 6989

**Postal address:**

CERT
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
U.S.A.