Windows Feedback & Reliability

Vince Orgovan – November 12, 2008
Dev Manager, Windows Reliability Analysis Team
Windows Core Operating System Division
Windows Reliability Topics

• Windows Reliability Feedback & Telemetry Systems
  – Windows Error Reporting (WER) for operating system crashes
  – Windows Error Reporting for application crashes and hangs
  – AutoBug automated Windows bug filing
  – Customer Experience Improvement Program
  – Winqual partner portal

• Samples of what we are learning
  – What causes operating system crashes?
  – What are the trends in system failures?

• What are our results?
WER for Operating System Crashes

- Started in 2001 with Windows XP
- Current back-end is significantly over-provisioned to accommodate spikes
- Customer opt-in rate is ~20% for XP, ~80% for Vista
- OS crash minidump is collected with each CAB, which is analyzed in real-time with customer response (2-3 secs)
- CAB meta-data is saved in 1.7 TB analysis database with 300+ tables
- Debugging symbol server indexes 308 million binary files in 1.3 TB database
- Analysis web portals for both internal and winqual users
!analyze is a Windows debugger extension that identifies the component most likely responsible for the failure

- Uses bugcheck or verifier code as initial input
- Weighted stack frames
- Uses additional data about known problems provided by developers
- Checks for memory and pool corrupting drivers
- Checks for obsolete drivers or buckets that should be split by OEM or device

!analyze found a single bit error in the instruction stream: expected 0x45, but found 0xc5

!analyze classified the crash as MEMORY_CORRUPTION_ONE_BIT; the response recommends running a memory diagnostic
WER for Application Crashes & Hangs

- Started in 2001 with Office XP
- Current back-end is significantly over-provisioned to accommodate spikes
- Report contains app name, app version, module name, mod version, offset which define a crash/hang bucket
- CABs with minidumps are collected for popular buckets
- CABs are processed offline to populate analysis databases with failureIDs
- WatsonDb does bucket analysis with 4.6 TB and 150 tables
- WERAnalysis does failureID analysis with 0.5 TB and 120 tables
- Analysis web portals for both internal and winqual users
App hang occurs when a user clicks the close button on a Window that hasn’t processed key/mouse events for 5+ seconds

If hang is on RPC to a local process, WER collects the local process too

If hang is on device I/O, WER collects an OS kernel mini dump too

!analyze detects deadlocks
AutoBug - Automated Bug Filing

- Automated bug triage via rules, e.g. “open a bug if there are 5+ CABs from 2+ machines running WinMain builds from the last 30 days”
- Automated assignment to the correct developer using mappings in the CompCentral database
- Bug includes !analyze output and link to the internal web portal for additional data & WER reports
- Automated regression monitoring for WER reports from builds after the fix is made

➤ Reliability feedback is completely integrated into the Windows development process
Customer Experience Improvement Program

- Opt-in program to collect very rich reliability telemetry
- CEIP collects every boot, standby, resume, shutdown, crash, hang, driver install, resource exhaustion along with rich configuration data
- CEIP allows Microsoft to calculate true failure rates
- CEIP allows Microsoft to calculate failure prevalence, i.e. the percent of machines affected by a particular failure
- Hundreds of thousands of worldwide Vista SP1 machines send real-time telemetry
Winqual Partner Portal

- Provides access to WER reports to OEMs, hardware vendors and software vendors who support the WER data collection policy
- ISVs and IHVs can register products/files, receive WER CABs, and create WER responses
- OEMs get a view of all the WER reports coming from their models
- Microsoft’s partner engagement efforts leverage this data for all top issues
- Our long term goal is to allow partners to completely integrate reliability feedback into their own development processes
# Learning: OS Crash Causes

## Top 500 Vista SP1 OS crash causes* for Sep 2008

<table>
<thead>
<tr>
<th>Category</th>
<th>% Crashes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>12.5%</td>
<td>Most are power mgmt; fix distribution slow</td>
</tr>
<tr>
<td>Display</td>
<td>9.4%</td>
<td>Mostly video card; first time display &lt; 10%</td>
</tr>
<tr>
<td>OS Core</td>
<td>8.6%</td>
<td>Kernel is 3.3%; USB is 3.3%</td>
</tr>
<tr>
<td>Application Drivers</td>
<td>6.5%</td>
<td>Antivirus 3.6%; Malware 1.1%; Firewall 0.5%</td>
</tr>
<tr>
<td>Hardware</td>
<td>6.3%</td>
<td>2.7% is general, 2.2% is memory, 1.4% is disk</td>
</tr>
<tr>
<td>Triage</td>
<td>5.7%</td>
<td>These are not well classified today</td>
</tr>
<tr>
<td>Corruption</td>
<td>5.1%</td>
<td>These cannot be well classified</td>
</tr>
<tr>
<td>Storage</td>
<td>5.0%</td>
<td>Mostly RAID controllers, some IDE/Atapi</td>
</tr>
<tr>
<td>Peripherals</td>
<td>2.6%</td>
<td>Mostly personal media players, now fixed</td>
</tr>
<tr>
<td>Imaging</td>
<td>1.7%</td>
<td>Camera drivers, USBvideo</td>
</tr>
<tr>
<td>Streaming Media</td>
<td>0.8%</td>
<td>Third party cameras and TV tuners</td>
</tr>
<tr>
<td>Audio</td>
<td>0.6%</td>
<td>Audio cards and HD drivers</td>
</tr>
<tr>
<td>Input</td>
<td>0.5%</td>
<td>Third party mice</td>
</tr>
<tr>
<td>Issues Beyond Top 500</td>
<td>34.6%</td>
<td>Haven't looked at many of these</td>
</tr>
</tbody>
</table>

* Excludes causes where no crash dump is created like power failures or system hangs
Learning: Trends in System Failures

- Our telemetry has identified over 390,000 unique devices attached to Vista systems
- 25 new drivers seen each day on avg, plus 100 others revised
- Older drivers persist a long time, so fix distribution is a focus
- Display drivers are increasingly complex but improving
- Malware is growing
- CD/DVD burning, USB, antivirus are getting better
- Huge variation in OEM models: the best models average 30X longer between OS crashes than the poorest
- Large variations between locales: the best locales average 4X longer between OS crashes than the poorest
Result: Improving OS Crash Rate

Time since Vista Launch

Crash Rate

Vista RTM

Vista SP1
Thank you for attending ISSRE!

Members of the Windows reliability team are here for the next ~hour to hear your suggestions and answer your questions.