LUA Tools and Solutions Showdown

Windows Application Quality Team
Microsoft Corporation

The problem: "LUA bugs"

- "LUA bug" is:
  - Application or feature that works only with administrator (admin) privileges, and
  - Fails as normal ("LUA") user, and
  - No technical or business need for admin privileges
- "LUA bugs" are often the #1 cause of app compat problems.
- The bugs must be identified before they can be fixed.

The Solution … s?

Microsoft®
Application Compatibility Toolkit 5.0

Standard User Analyzer

Windows Sysinternals

Windows 7

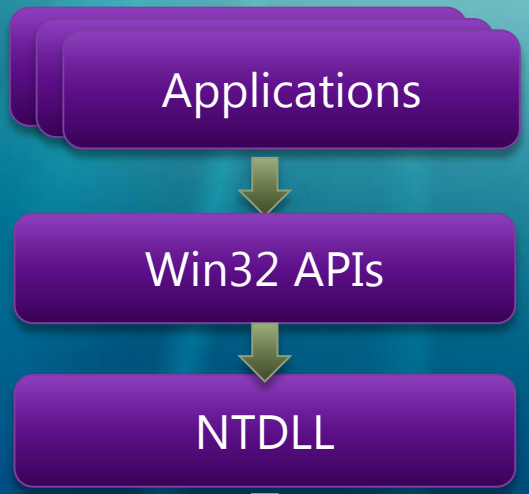
The Report Card

- Developers
- Administrators
- 2000/XP
- Vista
- Complex ACLs
- Less Common APIs
- Ease of Use
- Depth
- Breadth

Process Monitor

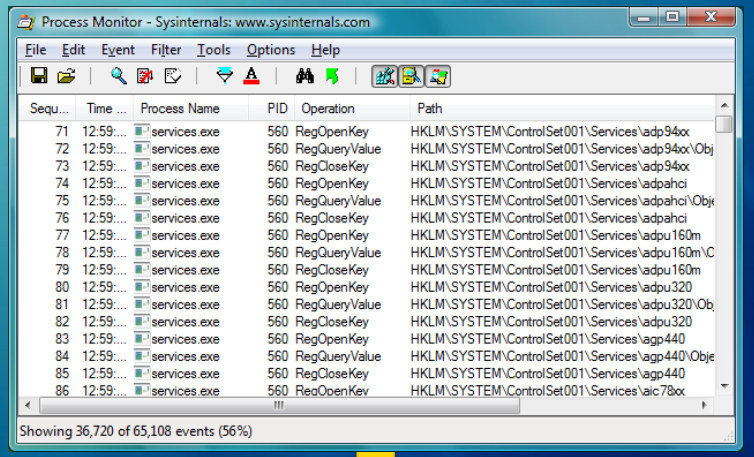
- Real-time file and registry activity
- Access denied with target credentials
- Full thread stack and symbol support

ProcMon Architecture



User mode

Kernel mode



Executive, Kernel, Drivers

File System mini-filter driver

Registry callbacks *

Kernel callbacks

ProcMon Driver

Windows 7

Process Monitor

demo

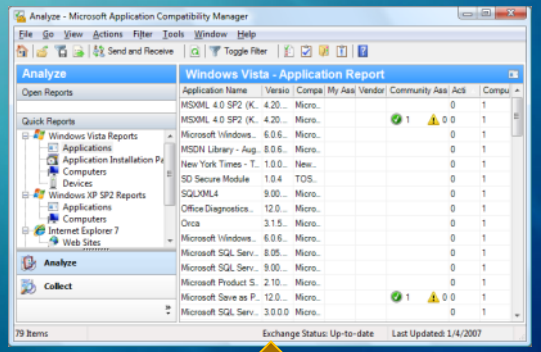
Report Card

	ProcMon	UACCE	SUA	LUA Buglight
Developers	C			
Administrators	C			
2000/XP	A			
Vista	A			
Complex ACLs	A			
Less Common APIs	F			
Ease of Use	C			
Depth	B			
Breadth	D			

UAC Compatibility Evaluator

- Shims a limited set of APIs
  - File
  - Registry
  - “Profile” (ini-file) APIs
  - Elevation detection
- Limited analysis (performance)

UACCE Architecture



Applications

UACCE Shim

Event Log

Log Processing Service

Windows API

Data Collection Service

ACT File Share

Windows 7

UACCE

demo

Report Card

	ProcMon	UACCE	SUA	LUA Buglight
Developers	C	D		
Administrators	C	D		
2000/XP	A	B		
Vista	A	B		
Complex ACLs	A	F		
Less Common APIs	F	F		
Ease of Use	C	A		
Depth	B	F		
Breadth	D	A		

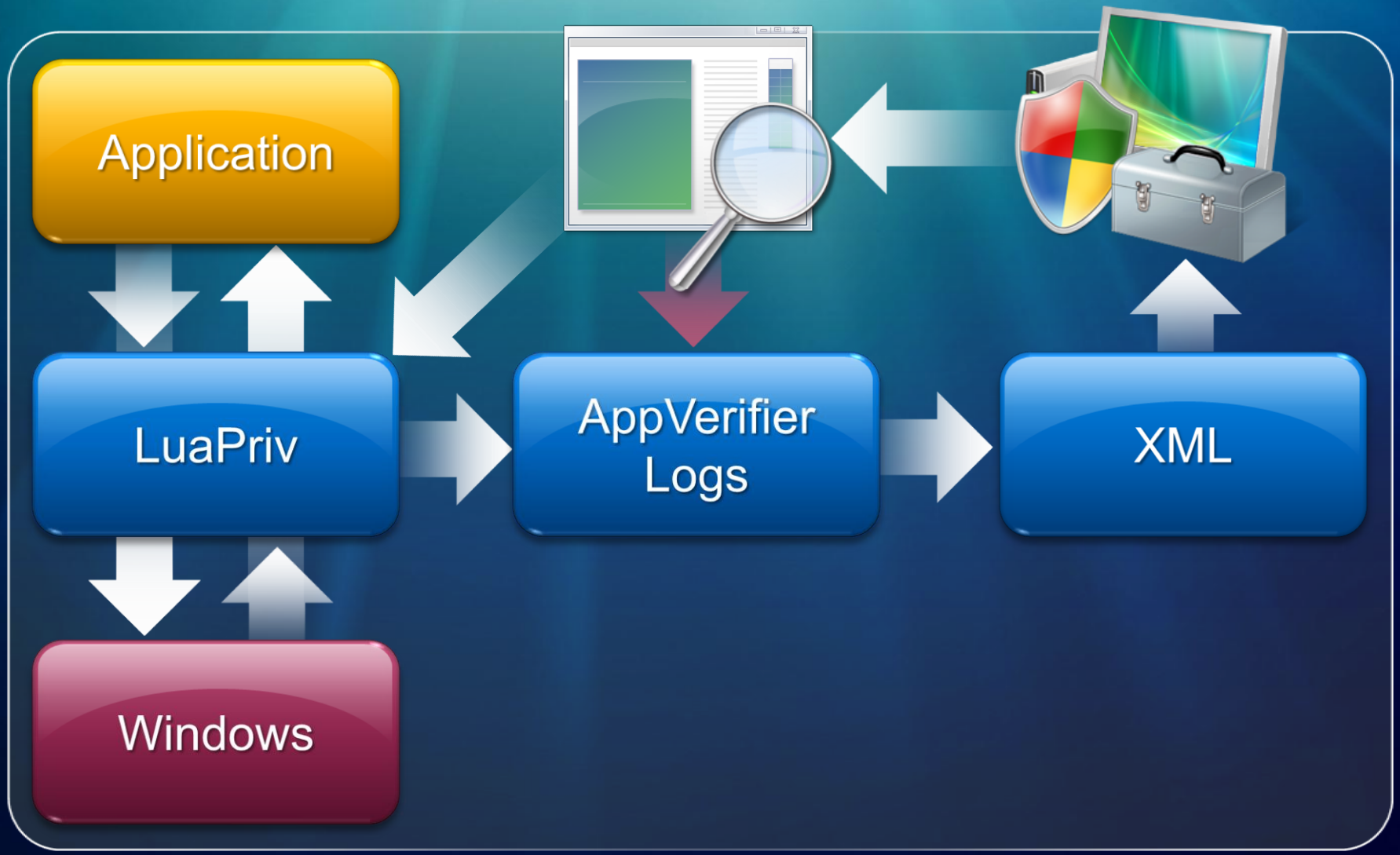
Standard User Analyzer

- Based on AppVerifier LUAPriv
- Predicts whether API calls fail for standard user
  - Predictive (elevated)
  - Diagnostic (non-elevated)
- Offers mitigations for selected issues

SUA API Coverage

- File system access
- Registry access
- INI WriteProfile
- Token checking
- Privilege
- Namespace
- Other securable objects
- Process creation

SUA Architecture



Standard User Analyzer

demo

Windows 7

Report Card

	ProcMon	UACCE	SUA	LUA Buglight
Developers	C	D	B	
Administrators	C	D	A	
2000/XP	A	B	A	
Vista	A	B	A	
Complex ACLs	A	F	D	
Less Common APIs	F	F	B	
Ease of Use	C	A	A	
Depth	B	F	A	
Breadth	D	A	C	

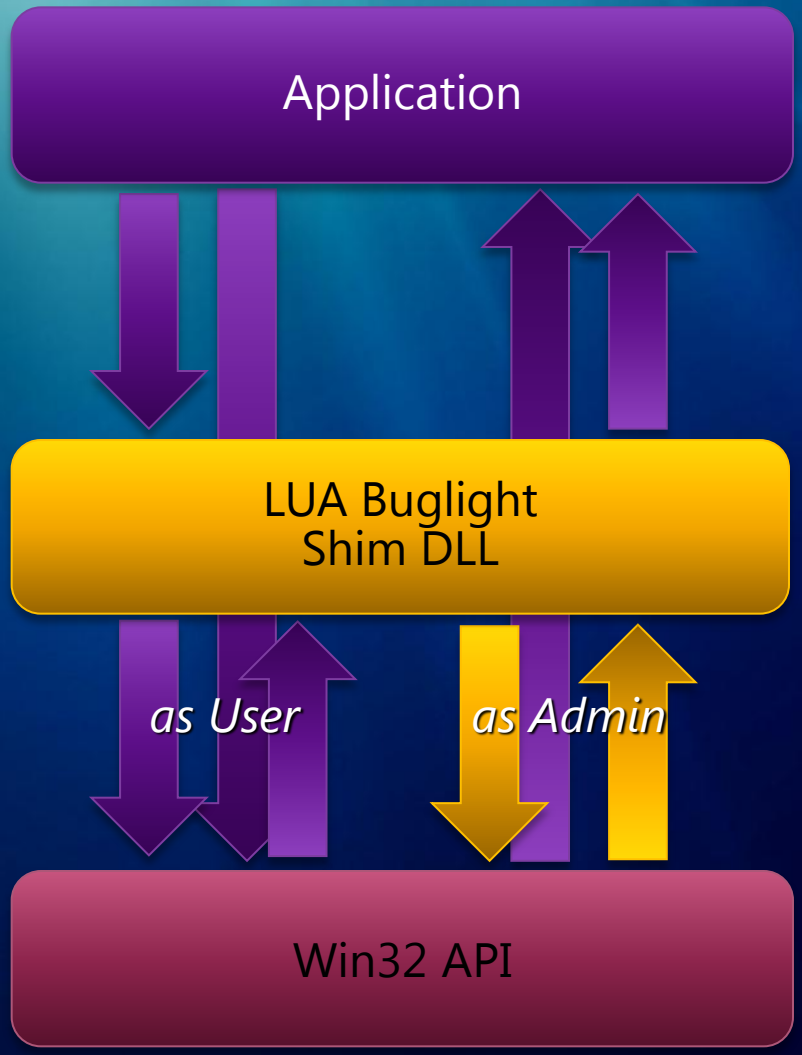
LUA Buglight

- App runs as the regular user
  - As defined by customer environment
- LUA Buglight injects:
  - DLL to intercept API calls
  - Token representing same user as admin
- When API call gets “access denied”:
  - Try again with elevated token
  - Log if retry succeeds

LBL Architecture

- App calls Win32 API
- Shim calls actual API
- If “access denied”…
  - Call again as admin
  - If it works, log it
- Return result to app

App works, but all admin use logged



LBL API Coverage

- Over 200 APIs intercepted, including:
  - Registry
  - File System
  - INI File APIs
  - Services
  - Event Log
  - Hard Admin Checks
  - Token Manipulation
  - Privilege Use

Target Audience

- Information technology (IT) professionals
  - Minimum set of changes to allow app to work
- Developers
  - Symbol information point to line of source

System Requirements

- Windows XP® (SP2 or higher), or
- Windows Server® 2003, or
- Windows Vista®
- That's it!
  - Self-contained
  - No additional/upgraded components needed
  - No installation: leaves no artifacts
  - Can run from CD
- The Report Viewer requires Microsoft® .NET 2.0

Report Card

	ProcMon	UACCE	SUA	LUA Buglight
Developers	C	D	B	A
Administrators	C	D	A	C
2000/XP	A	B	A	A
Vista	A	B	A	A
Complex ACLs	A	F	D	A
Less Common APIs	F	F	B	B
Ease of Use	C	A	A	A
Depth	B	F	A	A
Breadth	D	A	C	C

Code Coverage

- These tools analyze runtime behavior
  - Can't just analyze exe files on disk.
- Be sure all areas of the app are tested
  - SME or script

Making sense of the output

- "Access denied" does not always mean "bug"
- Is it a true LUA bug?
- How does the app respond?
  - "Fire and forget"? Not a LUA bug!
  - Gracefully degrade? Not a LUA bug!
  - Failure? That's a bug!

Tools

- Application Compatibility Toolkit 5.0
  http://go.microsoft.com/fwlink/?LinkId=82101
- LUA Buglight
  http://go.microsoft.com/fwlink/?LinkId=75605
- Process Monitor
  http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

Resources

- Windows Vista Application Development Requirements for User Account Control Compatibility
  http://www.microsoft.com/downloads/details.aspx?FamilyID=ba73b169-a648-49af-bc5e-a2eebb74c16b&DisplayLang=en
- Teach Your Apps To Play Nicely With Windows Vista User Account Control
  http://msdn.microsoft.com/msdnmag/issues/07/01/UAC/default.aspx
- Problems of Privilege: Find and Fix LUA Bugs
  http://www.microsoft.com/technet/technetmag/issues/2006/08/LUABugs/
- Application Compatibility Cookbook
  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnlong/html/AppComp.asp
- Advanced Windows Troubleshooting with SysInternals Process Monitor
  http://www.microsoft.com/emea/itsshowtime/sessionh.aspx?videoid=346

Microsoft®

Your potential. Our passion.™

Windows 7