Analysis, Design and Implementation of a Printing Stack for the Open-Source ReactOS Operating System

Bachelor Thesis Presentation

Colin Finck

Agenda

- Basics
  - The ReactOS Operating System
  - Technical Terms
  - Microsoft Windows Printing Stack
  - Remote Procedure Calls (RPC)
- Methods
  - Reverse Engineering Tools
- Implementation
  - Skip Lists

Basics

Goal: Open-Source Desktop Operating System for the Mass

- Fully compatible to applications and drivers written for Microsoft Windows
- Customizable
- Trustworthy

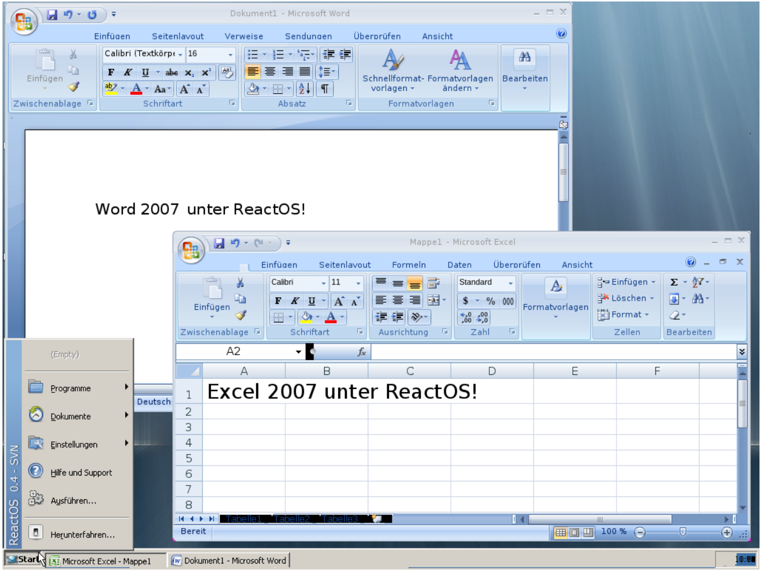
The ReactOS Operating System

Goal: Open-Source Desktop Operating System for the Mass

- Fully compatible to applications and drivers written for Microsoft Windows
- Customizable
- Trustworthy

But lacking Printing abilities prior to this work!

The ReactOS Operating System



Word 2007 unter ReactOS!

Excel 2007 unter ReactOS!

Technical Terms

- **API**

  Official and documented interface to let a software developer make use of a component

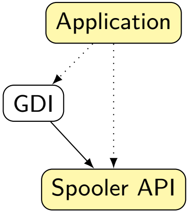
- **GDI**

  Windows component for drawing text and graphics on the screen and on paper

- **Spooler**

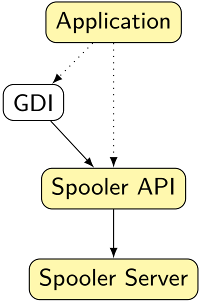
  Buffers concurrent print requests from multiple applications and sends them,
  one after another, to the Printer

Microsoft Windows Printing Stack



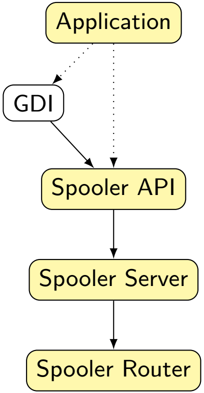
Implemented components in yellow

Microsoft Windows Printing Stack



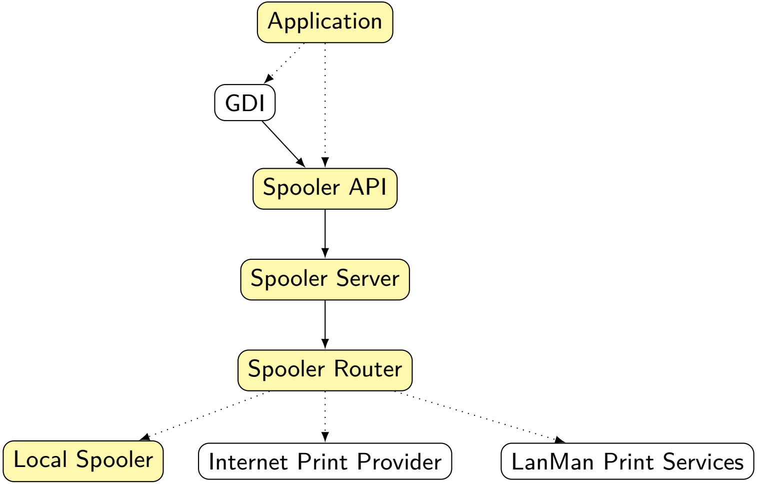
Implemented components in yellow

Microsoft Windows Printing Stack



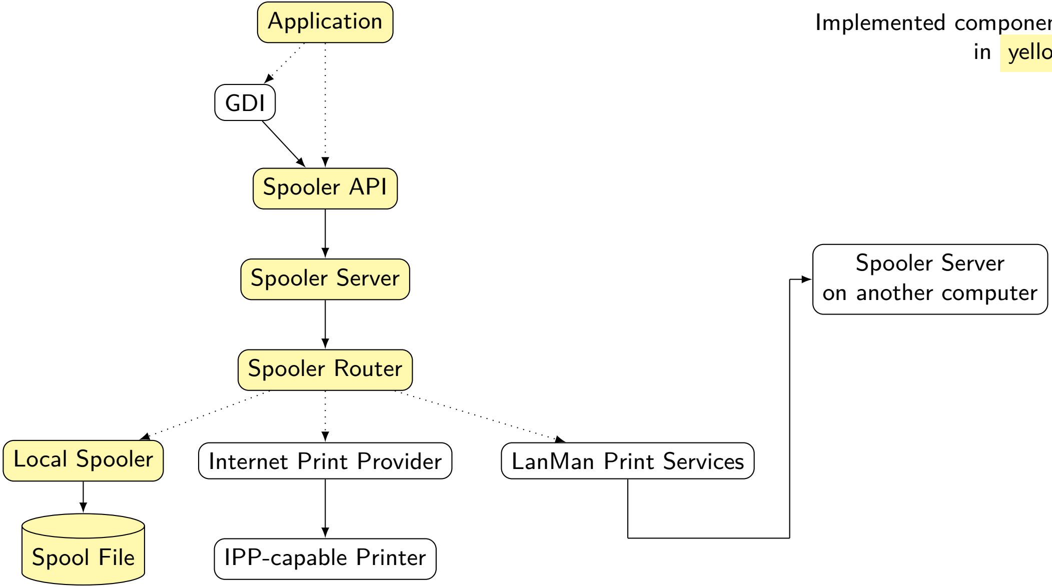
Implemented components in yellow

Microsoft Windows Printing Stack



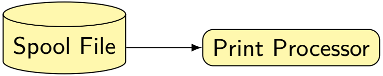
Implemented components in yellow

Microsoft Windows Printing Stack



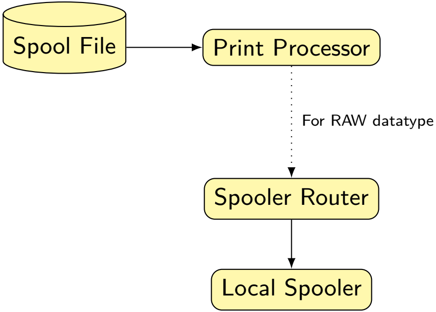
Implemented components in yellow

Microsoft Windows Printing Stack



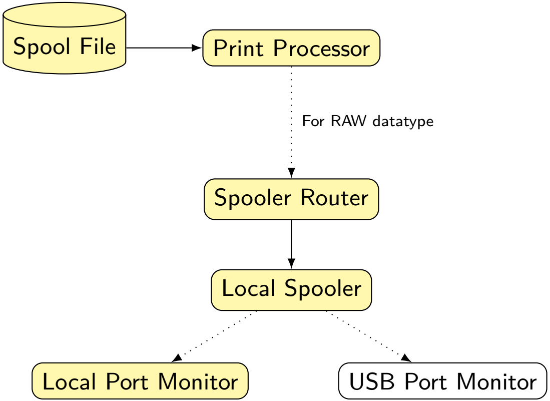
Implemented components in yellow

Microsoft Windows Printing Stack



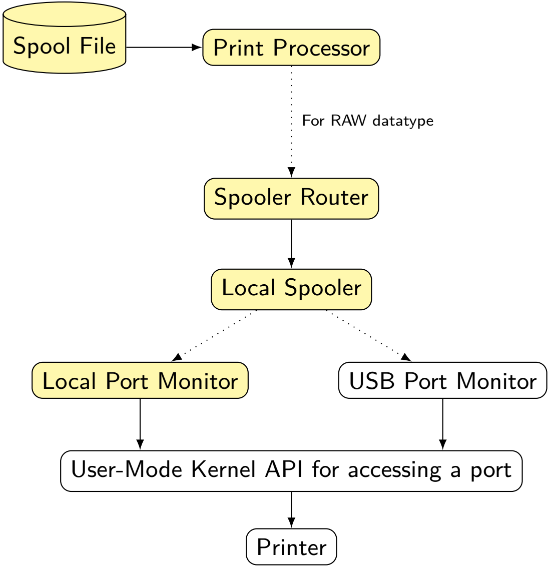
Implemented components in yellow

Microsoft Windows Printing Stack



Implemented components in yellow

Microsoft Windows Printing Stack



Implemented components in yellow

Remote Procedure Calls (RPC)

Call a function in another process, on another computer

Here used for Spooler API → Spooler Server communication.

- Function call and parameter information are transmitted over the network
- No network-specific code needs to be written

Remote Procedure Calls (RPC)

Call a function in another process, on another computer

Here used for Spooler API → Spooler Server communication.

- Function call and parameter information are transmitted over the network
- No network-specific code needs to be written

Remote function call as easy as a local one!

Example:

```
_RpcOpenPrinter(L"\\\\Computer\\Printer", &hPrinter, Datatype, &DevMode, AccessRequired);
```

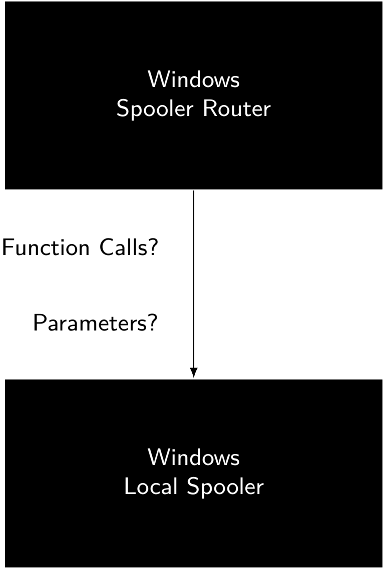
Remote Procedure Calls (RPC)

What's happening in the background:

1. **Marshalling:** Function name and parameters are packed into a message.
2. Message is transmitted over the network.
3. **Unmarshalling:** Function name and parameters are reconstructed out of the message.
4. The actual implemented function is called in the target application.

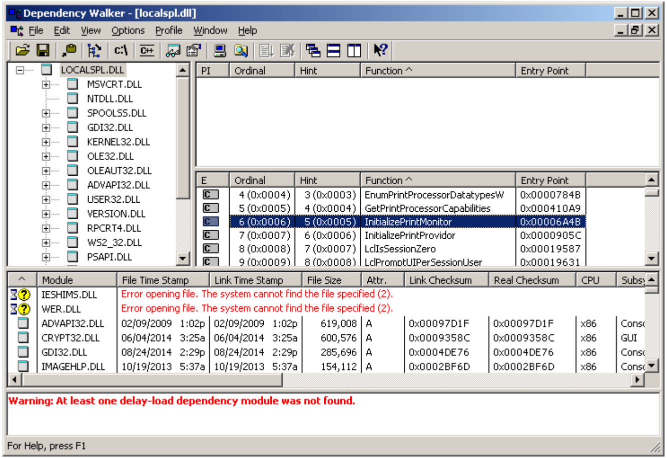
Methods

Reverse Engineering Tools



Dependency Walker

Reveals dependencies between modules and their imported and exported functions


Dependency Walker - [localspl.dll]
File Edit View Options Profile Window Help

LOCALSPL.DLL
- MSVCRT.DLL
- NTDLL.DLL
- SPOOLSS.DLL
- GDI32.DLL
- KERNEL32.DLL
- OLE32.DLL
- OLEAUT32.DLL
- ADVAPI32.DLL
- USER32.DLL
- VERSION.DLL
- RPCRT4.DLL
- WS2_32.DLL
- PSAPI.DLL

PI	Ordinal	Hint	Function ^	Entry Point

E	Ordinal	Hint	Function ^	Entry Point
C	4 (0x0004)	3 (0x0003)	EnumPrintProcessorDatatypesW	0x0000784B
C	5 (0x0005)	4 (0x0004)	GetPrintProcessorCapabilities	0x000410A9
C	6 (0x0006)	5 (0x0005)	InitializePrintMonitor	0x00006A4B
C	7 (0x0007)	6 (0x0006)	InitializePrintProvidor	0x0000905C
C	8 (0x0008)	7 (0x0007)	LclIsSessionZero	0x00019587
C	9 (0x0009)	8 (0x0008)	LclPromptUIPerSessionUser	0x00019631

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsy
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).							
?	WER.DLL	Error opening file. The system cannot find the file specified (2).							
	ADVAPI32.DLL	02/09/2009 1:02p	02/09/2009 1:02p	619,008	A	0x00097D1F	0x00097D1F	x86	Consc
	CRYPT32.DLL	06/04/2014 3:25a	06/04/2014 3:25a	600,576	A	0x0009358C	0x0009358C	x86	GUI
	GDI32.DLL	08/24/2014 2:29p	08/24/2014 2:29p	285,696	A	0x0004DE76	0x0004DE76	x86	Consc
	IMAGEHLP.DLL	10/19/2013 5:37a	10/19/2013 5:37a	154,112	A	0x0002BF6D	0x0002BF6D	x86	Consc

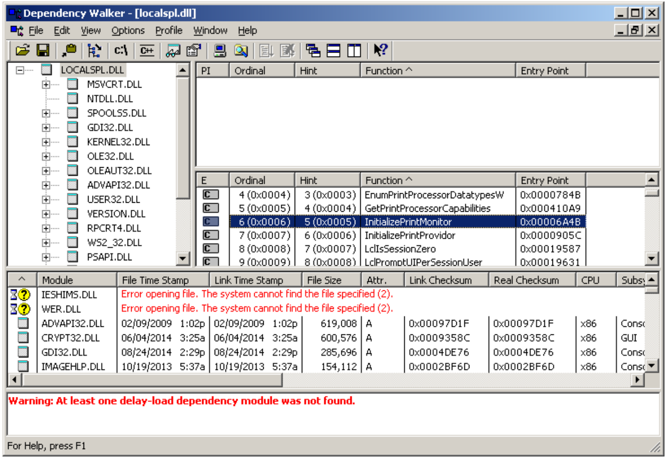
Warning: At least one delay-load dependency module was not found.

For Help, press F1

Dependency Walker

Reveals dependencies between modules and their imported and exported functions

Examining
Local Spooler



- LOCALSPL.DLL
  - MSVCRT.DLL
  - NTDLL.DLL
  - SPOOLSS.DLL
  - GDI32.DLL
  - KERNEL32.DLL
  - OLE32.DLL
  - OLEAUT32.DLL
  - ADVAPI32.DLL
  - USER32.DLL
  - VERSION.DLL
  - RPCRT4.DLL
  - WS2_32.DLL
  - PSAPI.DLL

PI	Ordinal	Hint	Function ^	Entry Point

E	Ordinal	Hint	Function ^	Entry Point
C	4 (0x0004)	3 (0x0003)	EnumPrintProcessorDatatypesW	0x0000784B
C	5 (0x0005)	4 (0x0004)	GetPrintProcessorCapabilities	0x000410A9
C	6 (0x0006)	5 (0x0005)	InitializePrintMonitor	0x00006A4B
C	7 (0x0007)	6 (0x0006)	InitializePrintProvidor	0x0000905C
C	8 (0x0008)	7 (0x0007)	LclIsSessionZero	0x00019587
C	9 (0x0009)	8 (0x0008)	LclPromptUIPerSessionUser	0x00019631

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsy
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).							
?	WER.DLL	Error opening file. The system cannot find the file specified (2).							
	ADVAPI32.DLL	02/09/2009 1:02p	02/09/2009 1:02p	619,008	A	0x00097D1F	0x00097D1F	x86	Cons
	CRYPT32.DLL	06/04/2014 3:25a	06/04/2014 3:25a	600,576	A	0x0009358C	0x0009358C	x86	GUI
	GDI32.DLL	08/24/2014 2:29p	08/24/2014 2:29p	285,696	A	0x0004DE76	0x0004DE76	x86	Cons
	IMAGEHLP.DLL	10/19/2013 5:37a	10/19/2013 5:37a	154,112	A	0x0002BF6D	0x0002BF6D	x86	Cons

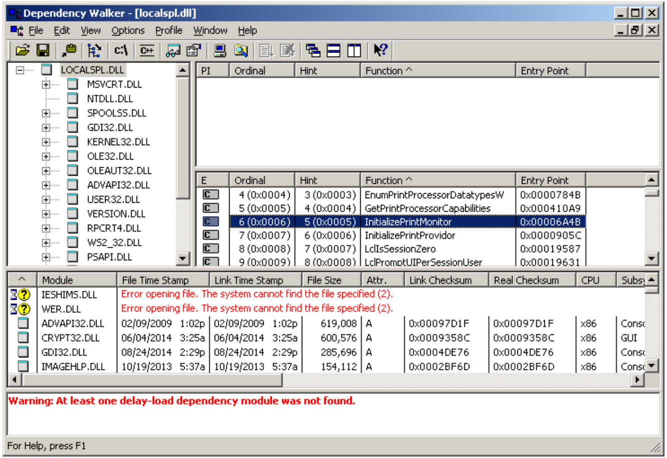
Warning: At least one delay-load dependency module was not found.

For Help, press F1

Dependency Walker

Reveals dependencies between modules and their imported and exported functions

Examining
Local Spooler


Dependency Walker - [localspl.dll]
File Edit View Options Profile Window Help

LOCALSPL.DLL
- MSVCRT.DLL
- NTDLL.DLL
- SPOOLSS.DLL
- GDI32.DLL
- KERNEL32.DLL
- OLE32.DLL
- OLEAUT32.DLL
- ADVAPI32.DLL
- USER32.DLL
- VERSION.DLL
- RPCRT4.DLL
- WS2_32.DLL
- PSAPI.DLL

PI	Ordinal	Hint	Function ^	Entry Point

E	Ordinal	Hint	Function ^	Entry Point
C	4 (0x0004)	3 (0x0003)	EnumPrintProcessorDatatypesW	0x0000784B
C	5 (0x0005)	4 (0x0004)	GetPrintProcessorCapabilities	0x000410A9
C	6 (0x0006)	5 (0x0005)	InitializePrintMonitor	0x00006A4B
C	7 (0x0007)	6 (0x0006)	InitializePrintProvidor	0x0000905C
C	8 (0x0008)	7 (0x0007)	LclIsSessionZero	0x00019587
C	9 (0x0009)	8 (0x0008)	LclPromptUIPerSessionUser	0x00019631

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsy
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).							
?	WER.DLL	Error opening file. The system cannot find the file specified (2).							
	ADVAPI32.DLL	02/09/2009 1:02p	02/09/2009 1:02p	619,008	A	0x00097D1F	0x00097D1F	x86	Cons
	CRYPT32.DLL	06/04/2014 3:25a	06/04/2014 3:25a	600,576	A	0x0009358C	0x0009358C	x86	GUI
	GDI32.DLL	08/24/2014 2:29p	08/24/2014 2:29p	285,696	A	0x0004DE76	0x0004DE76	x86	Cons
	IMAGEHLP.DLL	10/19/2013 5:37a	10/19/2013 5:37a	154,112	A	0x0002BF6D	0x0002BF6D	x86	Cons

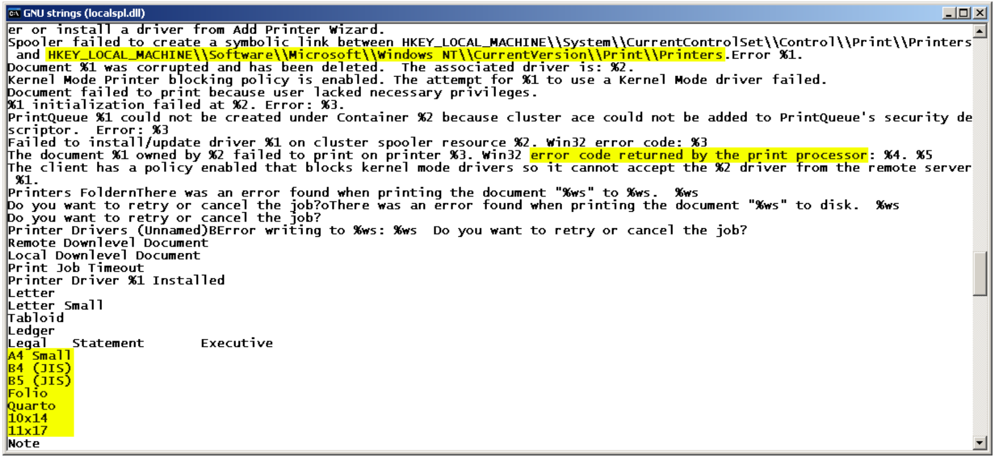
Warning: At least one delay-load dependency module was not found.

For Help, press F1

Found function
InitializePrintMonitor

GNU strings

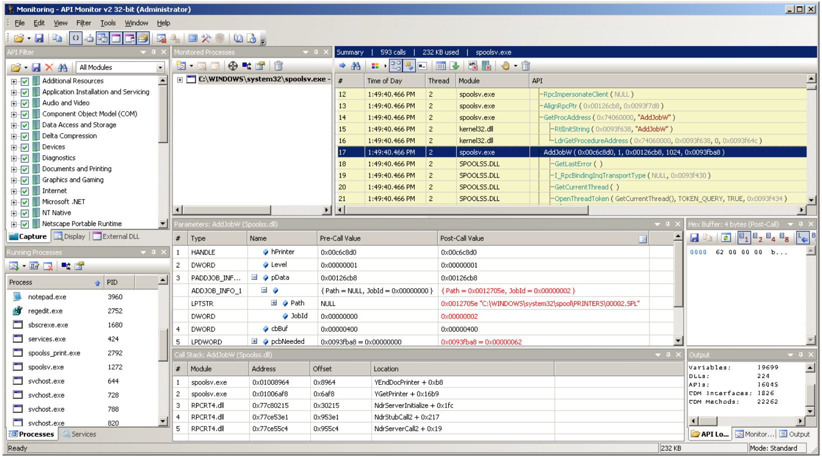
Outputs all strings found in a binary file



```
er or install a driver from Add Printer Wizard.
Spooler failed to create a symbolic link between HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Control\\Print\\Printers
 and HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Print\\Printers.Error %1.
Document %1 was corrupted and has been deleted.  The associated driver is: %2.
Kernel Mode Printer blocking policy is enabled. The attempt for %1 to use a Kernel Mode driver failed.
Document failed to print because user lacked necessary privileges.
%1 initialization failed at %2. Error: %3.
PrintQueue %1 could not be created under Container %2 because cluster ace could not be added to PrintQueue's security de
scriptor.  Error: %3
Failed to install/update driver %1 on cluster spooler resource %2. Win32 error code: %3
The document %1 owned by %2 failed to print on printer %3. Win32 error code returned by the print processor: %4. %5
The client has a policy enabled that blocks kernel mode drivers so it cannot accept the %2 driver from the remote server
 %1.
Printers FoldernThere was an error found when printing the document "%ws" to %ws.  %ws
Do you want to retry or cancel the job?oThere was an error found when printing the document "%ws" to disk.  %ws
Do you want to retry or cancel the job?
Printer Drivers (Unnamed)BError writing to %ws: %ws  Do you want to retry or cancel the job?
Remote Downlevel Document
Local Downlevel Document
Print Job Timeout
Printer Driver %1 Installed
Letter
Letter Small
Tabloid
Ledger
Legal   Statement       Executive
A4 Small
B4 (JIS)
B5 (JIS)
Folio
Quarto
10x14
11x17
Note
```

API Monitor

Monitors all calls done to system functions and their parameters



Process	PID
notepad.exe	3960
regedit.exe	2752
sbscrexe.exe	1680
services.exe	424
spoolss_print.exe	2792
spoolsv.exe	1272
svchost.exe	644
svchost.exe	728
svchost.exe	788
svchost.exe	820

#	Time of Day	Thread	Module	API
12	1:49:40.466 PM	2	spoolsv.exe	RpcImpersonateClient (NULL)
13	1:49:40.466 PM	2	spoolsv.exe	AlignRpcPtr (0x00126cb8, 0x0093f7d8)
14	1:49:40.466 PM	2	spoolsv.exe	GetProcAddress (0x74060000, "AddJobW")
15	1:49:40.466 PM	2	kernel32.dll	RtlInitString (0x0093f638, "AddJobW")
16	1:49:40.466 PM	2	kernel32.dll	LdrGetProcedureAddress (0x74060000, 0x0093f638, 0, 0x0093f64c)
17	1:49:40.466 PM	2	spoolsv.exe	AddJobW (0x00c6c8d0, 1, 0x00126cb8, 1024, 0x0093fba8)
18	1:49:40.466 PM	2	SPOOLSS.DLL	GetLastError ( )
19	1:49:40.466 PM	2	SPOOLSS.DLL	I_RpcBindingInqTransportType (NULL, 0x0093f430)
20	1:49:40.466 PM	2	SPOOLSS.DLL	GetCurrentThread ( )
21	1:49:40.466 PM	2	SPOOLSS.DLL	OpenThreadToken (GetCurrentThread(), TOKEN_QUERY, TRUE, 0x0093f434)

Parameters: AddJobW (Spoolss.dll)

#	Type	Name	Pre-Call Value	Post-Call Value
1	HANDLE	hPrinter	0x00c6c8d0	0x00c6c8d0
2	DWORD	Level	0x00000001	0x00000001
3	PADDJOB_INF...	pData	0x00126cb8	0x00126cb8
	ADDJOB_INFO_1		{ Path = NULL, JobId = 0x00000000 }	{ Path = 0x0012705e, JobId = 0x00000002 }
	LPTSTR	Path	NULL	0x0012705e "C:\WINDOWS\system32\spool\PRINTERS\00002.SPL"
	DWORD	JobId	0x00000000	0x00000002
4	DWORD	cbBuf	0x00000400	0x00000400
5	LPDWORD	pcbNeeded	0x0093fba8 = 0x00000000	0x0093fba8 = 0x00000062

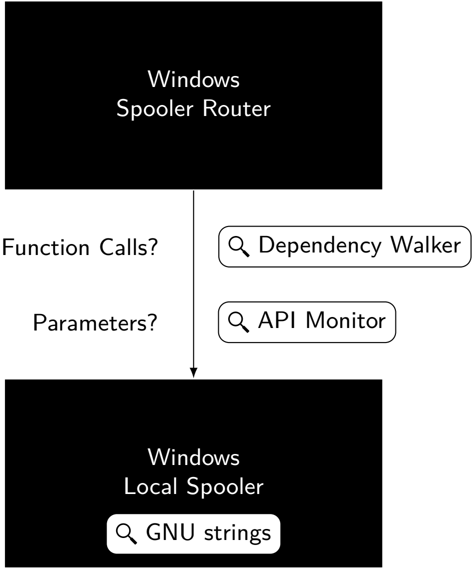
Call Stack: AddJobW (Spoolss.dll)

#	Module	Address	Offset	Location
1	spoolsv.exe	0x01008964	0x8964	YEndDocPrinter + 0xb8
2	spoolsv.exe	0x01006af8	0x6af8	YGetPrinter + 0x16b9
3	RPCRT4.dll	0x77c80215	0x30215	NdrServerInitialize + 0x1fc
4	RPCRT4.dll	0x77ce53e1	0x953e1	NdrStubCall2 + 0x217
5	RPCRT4.dll	0x77ce55c4	0x955c4	NdrServerCall2 + 0x19

Output

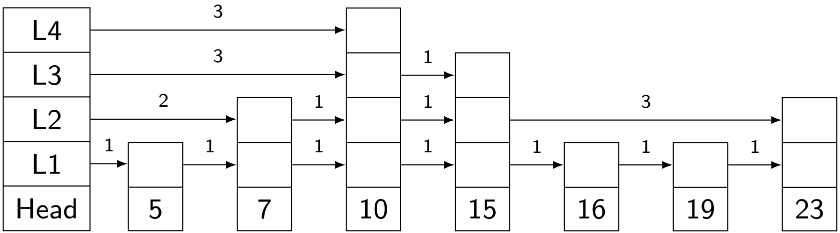
```
Variables:      19699
DLLs:           224
APIs:           16045
COM Interfaces: 1826
COM Methods:    22262
```

Reverse Engineering Tools



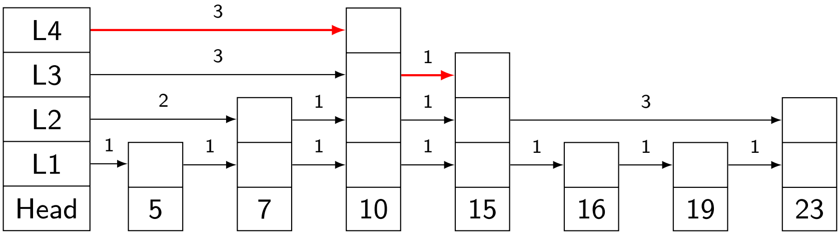
Implementation

Skip Lists



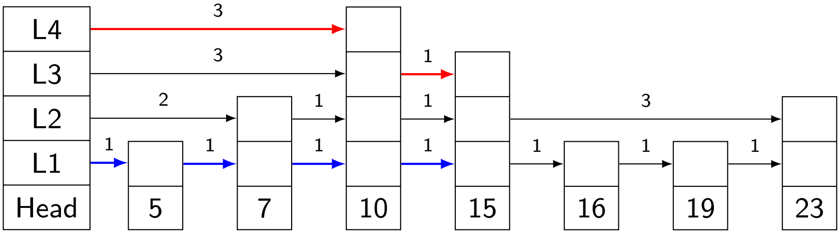
- Fast insertions, deletions and lookups, $\mathcal{O}(\log n)$ on average
- Easy to implement
- Extensible

Skip Lists



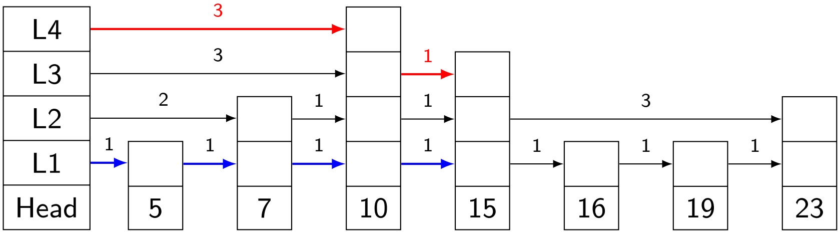
- Fast insertions, deletions and lookups, $\mathcal{O}(\log n)$ on average
- Easy to implement
- Extensible

Skip Lists



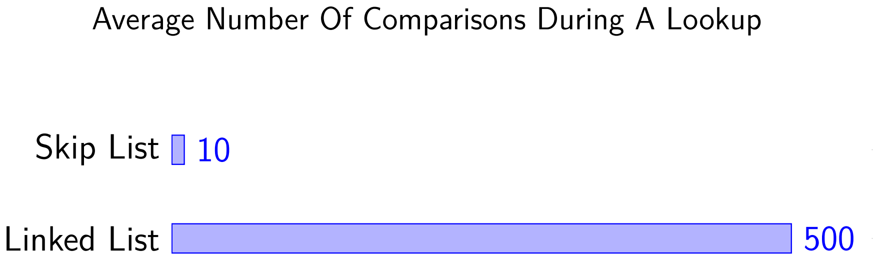
- Fast insertions, deletions and lookups, $\mathcal{O}(\log n)$ on average
- Easy to implement
- Extensible

Skip Lists



- Fast insertions, deletions and lookups, $\mathcal{O}(\log n)$ on average
- Easy to implement
- Extensible

Example: Data Structure with 1000 Elements



Thank you for your kind attention!

Colin Finck – colin.finck@rwth-aachen.de

Institute for Automation of Complex Power Systems
E.ON Energy Research Center, RWTH Aachen University
Mathieustraße 10
52074 Aachen

www.eonerc.rwth-aachen.de