TaintScope:A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection

Tielei Wang, Tao Wei, Guofei Gu, Wei Zou

Motivating Example

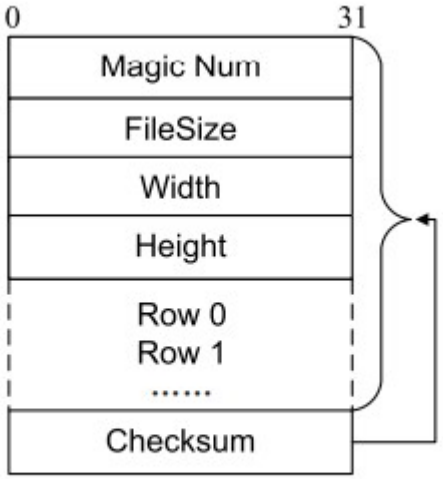

Figure 2. Example input format

```
1  void decode_image(FILE* fd){
2   ...
3   int length            = get_length(fd);
4   int recomputed_chksum = checksum(fd, length);
5   int chksum_in_file    = get_checksum(fd);
    //line 6 is used to check the integrity of inputs
6   if(chksum_in_file != recomputed_chksum)
7     error();
8   int Width    = get_width(input_file);
9   int Height   = get_height(input_file);
10  int size = Width*Height*sizeof(int); //integer overflow
11  int* p   = malloc(size);
12  ...
13  for(i=0; i<Height;i++){// read ith row to p
14    read_row(p + Width*i, i, fd); //heap overflow
```

Figure 3. Example Code

System Overview

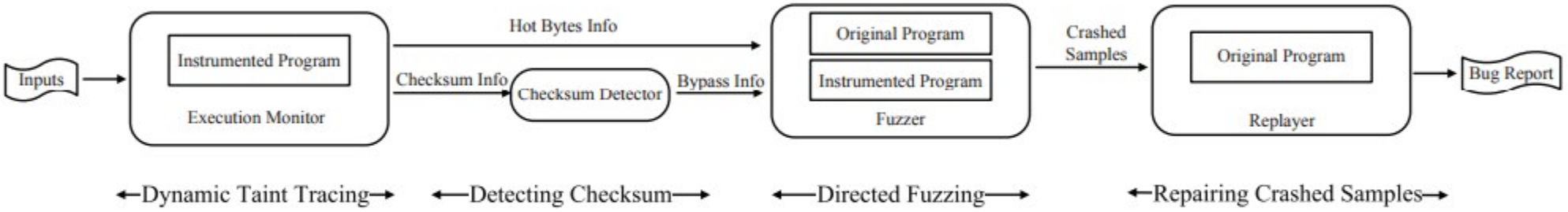

Figure 4. TaintScope System Overview

Dynamic Taint Tracing

- Which input bytes pollute the arguments of specified API
  - Malloc, realloc, strcpy, strcat
- Which input bytes pollute each conditional jump instruction depends on

- Examples
  - 0x8048d5b: invoking malloc: [0x8, 0xf]
  - 0x8048d4f: JZ: 1024: [0x0, 0x3ff]

Detecting Checksum Check Points

- Identifying Potential Checksum Check Points
  - Conditional jump instructions
  - Eflags: predefined threshold
- Refinement Procedure
  - Well-formed inputs
    - P1(conditional jump take); P0 (conditional jump not take)
  - Malformed inputs
    - P’1(conditional jump take); P’0(conditional jump not take)
  - (P1∩P’0)U(P0 ∩P’1)
- Checksum Field Identification
  - Reconmputed_chksum == attached_chksum

Directed and Checksum-aware Fuzzing

- Directed Fuzzing
  - Hot bytes->memory allocation functions
- Checksum-aware Fuzzing
  - Dynamically change the code flags in eflags
  - Modify the binary

Repairing Test Cases

- Treats the checksum fields as symbolic values
- Dynamically collect the trace
- Use STP to solve the constraint

Evaluation

Category	Application	Version	OS	Category	Application	Version	OS
Image Viewer	Google Picasa	3.1.0	Windows	Media Player	MPlayer	SVN-28979	Linux
	Adobe Acrobat	9.1.3	Windows		Gstreamer	0.10.15	Linux
	ImageMagick	6.5.2-7	Linux		Winamp	5.552	Windows
	Microsoft Paint	5.1	Windows	Other	libtiff	3.8.2	Linux
Web Browser	Amaya	11.1	Windows		XEmacs	21.4.22	Linux
	Dillo	2.1.1	Linux		wxWidgets	2.8.10	Linux

Hot Bytes Identification

Executable	Package	Input Format	Input Size (Bytes)	# Hot Bytes	# X86 Instrs	Run Time
Display	ImageMagick	TIFF	5778	18	191,759,211	2m53s
			2,020	18	82,640,260	1m30s
		PNG	5,149	9	19,051,746	1m54s
			1,250	29	47,246,043	1m8s
		JPEG	6,617	11	48,983,897	1m13s
			6,934	9	48,823,905	1m11s
PicasaPhotoViewer.exe	Google Picasa	GIF	3,190	14	304,993,501	1m25s
			6,529	43	536,938,567	2m57s
		PNG	2,730	18	712,021,776	5m16s
			1,362	16	660,183,239	4m8s
		BMP	3,174	8	310,909,256	1m21s
			7,462	19	468,273,580	2m35s
Acrobat.exe	Adobe Acrobat	BMP	1,440	6	658,370,048	4m25s
			3,678	6	663,923,080	5m2s
		PNG	770	21	297,492,758	3m8s
			1,250	12	354,685,431	4m31s
		JPEG	1,012	13	328,365,912	4m14s
			2,356	4	356,136,453	4m36s

Checksum Check Points Identification

Executable	Package (Version)	File Format	Checksum Algorithm	$\lvert\mathcal{A}\rvert$	$\lvert(\mathcal{P}_1 \cap \mathcal{P}'_0) \cup (\mathcal{P}_0 \cap \mathcal{P}'_1)\rvert$	Detected?
PicasaPhotoViewer	Google Picasa (3.1)	PNG	CRC32	830	1	√
Acrobat	Adobe Acrobat (9.1.3)			5,805	1	√
Snort	snort (2.8.4.1)	PCAP	TCP/IP checksum	2	2	√
tcpdump	tcpdump (4.0.0)			5	2	√
sigtool	clamav (0.95.2)	CVD	MD5	2	1	√
vcdiff	open-vcdiff (0.6)	VCDIFF	Adler32	1	1	√
Tar	GNU Tar (1.22)	Tar Archive	Tar checksum	9	1	√
objcopy	GNU binutils (2.17)	Intel HEX	Intel HEX checksum	62	1	√

Table III
CHECKSUM IDENTIFICATION RESULTS

Checksum Fields Repair

Executable	File Format	# fields	|field|	Repaired?	Time (s)
display	PNG	4	4	√	271.9
tcpdump	PCAP	8	2	√	455.6
tar	Tar Archive	3	8	√	572.8
objcopy	Intel HEX	4	2	√	327.1

Fuzzing Results

Package	Vuln-Type	# Vulns	Checksum-aware?	Advisory	Severity Rating
Microsoft Paint	Memory Corruption	1	N	CVE-2010-0028	Moderate
Google Picasa	Infinite loop	1	N	pending	N/A
	Integer Overflow	1		SA38435	Moderate
Adobe Acrobat	Infinite loop	1	N	CVE-2009-2995	Extremely critical
	Memory Corruption	1	N	CVE-2009-2989	Extremely critical
ImageMagick	Integer Overflow	1	N	CVE-2009-1882	Moderate
CamlImage	Integer Overflow	3	**Y**	CVE-2009-2660	Moderate
LibTIFF	Integer Overflow	2	N	CVE-2009-2347	Moderate
wxWidgets	Buffer Overflow	2	N	CVE-2009-2369	Moderate
	Double Free	1	**Y**		
IrfanView	Integer Overflow	1	N	CVE-2009-2118	High
GStreamer	Integer Overflow	1	**Y**	CVE-2009-1932	Moderate
Dillo	Integer Overflow	1	**Y**	CVE-2009-2294	High
XEmacs	Integer Overflow	3	**Y**	CVE-2009-2688	Moderate
	Null Dereference	1	N	N/A	N/A
MPlayer	Null Dereference	2	N	N/A	N/A
PDFlib-lite	Integer Overflow	1	**Y**	SA35180	Moderate
Amaya	Integer Overflow	2	**Y**	SA34531	High
Winamp	Buffer Overflow	1	N	SA35126	High
Total		27			