



# agenda

- **history of fuzzing**
- **protocol fuzzing**
- **fuzzable or not?**
- **non-sense fuzzing**
- **session-based fuzzing / stateful-based fuzzing**
- **tools | techniques**
- **challenges**
- **getting creative**
- **packet fun**
- **predictions**
- **resources**

# fuzzing history

- **“born” @ university of madison in 1989 by professor barton miller and his crew**
- **why ?**
- **buzz word in the past few years**
- **sorta “hope” to find 0 days**
- **not just a http thing**
- **file format fuzzing**
- **application fuzzing**
- **and...**

## **(possible definition)/ terms/ keywords/ etc**

- **malformed / semi-malformed/ invalid input**
- **random**
- **target**
- **exception-handling**
- **mutations**
- **instrumentation**
- **art / creativity**
- **agents**
- **negative-testing**

**changed the mentality of: “but... that packet doesn’t follow the rfc spec”**

**or**

**“hmmmm... but... people are not supposed to send these packets”**



# (con)fuzzable or not?



## **“mainstreaming” fuzzing**

- **numerous bugs found in the past few years**
- **some of them make the news**
- **others probably not . . .**
- **growth in the number of specific tools**



## corporate fuzzing

- **again, nothing new. . . . but . . . if you don't fuzz, someone else will**
- **fuzzing became a “common practice” (regardless if it's done correctly or not)**
- **delivering products / services with “basic” testing is no longer acceptable**

## so... protocol fuzzing

- protocol abuse
- test robustness of the target
- from instability to crashes (or to remote code execution)
- if it's already hard for one to follow the rfc spec, how about the "anything but... " ?





ohhh

**fuzzers are not va scanners!**

# what to break in a protocol?

- **structure**
  - **state**
  - **semantics**
- **Buffer Overflow**
  - **Integer Overflow**
  - **Invalid Message**
  - **Format String**
  - **Fragmented Field**
  - **Invalid Header**
  - **Null Character**
  - **Wrong Encoding**
  - **Invalid Index**
  - **Invalid String**
  - **Recursion**
  - **Truncated**
  - **Underflow**
  - **Missing Field**
  - **Mixed Case**
  - **Out of Order**
  - **Self-Reference**
  - **Too Many Fields**
  - **Invalid Offset**

# what protocols to fuzz?

- all of them, of course
- but... what's the buzz? what's new? what's not mature?
- sip
- scada
- ipv6
- wireless
- bluetooth
- videogames

# non-sense fuzzing



## session-based fuzzing

- first you establish a channel with the target and then start fuzzing at that level

## stateful-based fuzzing

- **one step above establishing a session**
- **“on-the-fly” fuzzing**
- **(possible) better fault isolation**



## techniques

- random
- database
- (mix?)

## some of the challenges

- **fault isolation**
- **the “bug behind the bug”**
- **“slow” protocol implementations**
- **monitor the target (memory leaks/ cpu spikes/ some type of redundancy)**

## tools

- **human**
- **spike / written in c/ block-based approach**
- **protos / java / different fuzzers**
- **peach / python / “written while drinking beer at ph-neutral”**
- **antiparser / python/ fuzzer and fault injection tool**
- **dfuz / c**
- **sulley/ parallel fuzzing capabilities /legos**

## commercial

- **bestorm**
- **codenomicom**
- **hydra**
- **mu security**
- **thread-x**

## getting creative

- use different fuzzing tools
- use the same fuzzing tool (parallel fuzzing)
- use a framework to integrate other stuff (traffic gen, nmap, exploitation tools, etc)
- “ “ “ to integrate agents for monitoring
- well... use any tools available

# packets

No.	Time	Source	Destination	Protocol	Info
21	3.550015			TCP	50237 > domain [SYN] Seq=0 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0 TSV=19947171 TSER=0
23	3.550238			TCP	50237 > domain [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=19947171 TSER=2924684008
24	3.550295			DNS	Unknown operation (8)[Packet size limited during capture]
26	3.550598			DNS	Unknown operation (14)[Unreassembled Packet][Unreassembled Packet]
27	3.550603			DNS	Standard query[Packet size limited during capture]
29	3.550907			DNS	Unknown operation (10)[Unreassembled Packet][Unreassembled Packet]
30	3.550912			DNS	Unknown operation (7) Unknown (41821) <Unknown extended label>[Unreassembled Packet][Unreassembled Packet]
32	3.551015			DNS	Unknown operation (11) response, Format error[Packet size limited during capture]
33	3.551020			DNS	Unknown operation (8) response, Unknown error (15)[Packet size limited during capture]
35	3.551213			DNS	Dynamic update response, Unknown error (13)[Unreassembled Packet][Unreassembled Packet]
36	3.551217			DNS	Dynamic update response, Not implemented[Packet size limited during capture]
38	3.551322			DNS	Unknown operation (14)[Packet size limited during capture]
39	3.551326			DNS	Unknown operation (7) response, RRset does not exist[Packet size limited during capture]
41	3.551460			DNS	Unknown operation (8) Unknown (56586) <Unknown extended label>[Packet size limited during capture]
42	3.551464			DNS	Dynamic update Unknown (51201) <Unknown extended label>[Packet size limited during capture]
44	3.551582			DNS	Dynamic update Unknown (47715) <Unknown extended label> Unknown (61797) <Unknown extended label>[Unreassembled Packet]
45	3.551586			DNS	Unknown operation (11)[Packet size limited during capture]
47	3.551705			DNS	Dynamic update response, Unknown error (15)[Unreassembled Packet][Unreassembled Packet]
48	3.551709			DNS	Unknown operation (13) response, Unknown error (15)[Unreassembled Packet][Unreassembled Packet]
50	3.551831			DNS	Unknown operation (14) Unknown (63166) <Unknown extended label>[Unreassembled Packet][Unreassembled Packet]
51	3.551835			DNS	Zone change notification[Packet size limited during capture]
53	3.551954			DNS	Inverse query[Unreassembled Packet][Unreassembled Packet]
54	3.551958			DNS	Unknown operation (14) response, RRset does not exist[Packet size limited during capture]
56	3.552075			DNS	Unknown operation (7)[Packet size limited during capture]
67	3.553209			DNS	Server status request[Packet size limited during capture]
68	3.553288			DNS	Unknown operation (12)[Packet size limited during capture]
69	3.553292			DNS	Unknown operation (8)[Packet size limited during capture]
70	3.553296			DNS	Unknown operation (14) response, Server failure[Packet size limited during capture]
71	3.553300			DNS	Unknown operation (9)[Packet size limited during capture]
72	3.553303			DNS	Standard query[Packet size limited during capture]
73	3.553326			DNS	Unknown operation (10)[Unreassembled Packet][Unreassembled Packet]
74	3.553331			DNS	Unknown operation (10)[Unreassembled Packet][Unreassembled Packet]
75	3.553342			DNS	Unknown operation (8)[Packet size limited during capture]
76	3.553345			DNS	Unknown operation (13)[Packet size limited during capture]
77	3.553349			DNS	Zone change notification response, Unknown error (14)[Packet size limited during capture]
78	3.553353			DNS	Unknown operation (12) response, RRset does not exist[Unreassembled Packet][Unreassembled Packet]
86	3.554866			DNS	Unknown operation (15)[Packet size limited during capture]
87	3.556124			DNS	Zone change notification response[Unreassembled Packet][Unreassembled Packet]

0000 00 0d 60 99 3b 13 00 0b 86 c5 0e 90 08 00 45 00 .....E.  
0010 00 40 9b 15 40 00 40 06 81 25 0a 05 00 b3 cb 79 .@.@.@.%....y

File: "/Users/luizduardo/dnst0203.cap" 1892 KB 00:00:08 | P: 18987 D: 12653 M: 0



# packets (cont)

The screenshot shows a network traffic analysis tool interface. At the top, there is a filter bar with 'ip.s' and buttons for 'Expression...', 'Clear', and 'Apply'. Below this is a table with columns for 'No.', 'Time', 'Protocol', and 'Info'. The table contains a list of network packets, primarily TCP acknowledgments (ACK) and a DNS response. A large blue rectangle obscures the left side of the table. At the bottom, there is a hex dump showing the raw data of the selected packet.

No.	Time	Protocol	Info
22	3.55	TCP	domain > 50237 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2924684008 TSER=19947171 WS=0
25	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=1449 Win=8688 Len=0 TSV=2924684008 TSER=19947171
28	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=2897 Win=11584 Len=0 TSV=2924684008 TSER=19947171
31	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=4345 Win=14480 Len=0 TSV=2924684008 TSER=19947171
34	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=5793 Win=17376 Len=0 TSV=2924684008 TSER=19947171
37	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=7241 Win=20272 Len=0 TSV=2924684008 TSER=19947171
40	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=8689 Win=23168 Len=0 TSV=2924684008 TSER=19947171
43	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=10137 Win=26064 Len=0 TSV=2924684008 TSER=19947171
46	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=11585 Win=28960 Len=0 TSV=2924684008 TSER=19947171
49	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=13033 Win=31856 Len=0 TSV=2924684008 TSER=19947171
52	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=14481 Win=34752 Len=0 TSV=2924684008 TSER=19947171
55	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=15929 Win=37648 Len=0 TSV=2924684008 TSER=19947171
57	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=17377 Win=40544 Len=0 TSV=2924684008 TSER=19947171
58	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=18825 Win=43440 Len=0 TSV=2924684008 TSER=19947171
59	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=20273 Win=46336 Len=0 TSV=2924684008 TSER=19947171
60	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=21721 Win=49232 Len=0 TSV=2924684008 TSER=19947171
61	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=23169 Win=52128 Len=0 TSV=2924684008 TSER=19947171
62	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=24617 Win=55024 Len=0 TSV=2924684008 TSER=19947171
63	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=26065 Win=57920 Len=0 TSV=2924684008 TSER=19947171
64	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=27513 Win=60816 Len=0 TSV=2924684008 TSER=19947171
65	3.55	TCP	domain > 50237 [ACK] Seq=1 Ack=28961 Win=63712 Len=0 TSV=2924684008 TSER=19947171
66	3.55	DNS	Unknown operation (8) response, Not implemented
79	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=31857 Win=63712 Len=0 TSV=2924684008 TSER=19947171
80	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=34217 Win=63712 Len=0 TSV=2924684008 TSER=19947171
81	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=37113 Win=63712 Len=0 TSV=2924684008 TSER=19947171
82	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=40009 Win=63712 Len=0 TSV=2924684008 TSER=19947171
83	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=42905 Win=63712 Len=0 TSV=2924684008 TSER=19947171
84	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=45801 Win=63712 Len=0 TSV=2924684008 TSER=19947171
85	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=48697 Win=63712 Len=0 TSV=2924684008 TSER=19947171
98	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=50601 Win=63712 Len=0 TSV=2924684008 TSER=19947171
99	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=53497 Win=63712 Len=0 TSV=2924684008 TSER=19947171
100	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=56393 Win=63712 Len=0 TSV=2924684008 TSER=19947171
101	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=59289 Win=63712 Len=0 TSV=2924684008 TSER=19947171
102	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=62185 Win=63712 Len=0 TSV=2924684008 TSER=19947171
103	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=65081 Win=63712 Len=0 TSV=2924684008 TSER=19947171
116	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=66985 Win=63712 Len=0 TSV=2924684008 TSER=19947171
117	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=69881 Win=63712 Len=0 TSV=2924684008 TSER=19947171
118	3.55	TCP	domain > 50237 [ACK] Seq=15 Ack=72777 Win=63712 Len=0 TSV=2924684008 TSER=19947171

File: "/Users/luizduardo/dnst0203.cap" 1892 KB 00:00:08 P: 18987 D: 6275 M: 0

# packets (again)

12	0.22909	TCP	krb524	>	54714	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
14	0.24676	TCP	krb524	>	54716	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
16	0.28126	TCP	krb524	>	54718	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
18	0.29439	TCP	krb524	>	54720	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
20	0.30929	TCP	krb524	>	54722	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
41	3.02484	TCP	krb524	>	54724	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
50	3.05925	TCP	krb524	>	54726	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
52	3.08003	TCP	krb524	>	54728	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
54	3.11360	TCP	krb524	>	54730	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
56	3.12535	TCP	krb524	>	54732	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
58	3.13818	TCP	krb524	>	54734	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
60	3.15316	TCP	krb524	>	54736	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
62	3.17507	TCP	krb524	>	54738	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
64	3.21275	TCP	krb524	>	54740	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0
75	6.02561	TCP	krb524	>	54742	[RST, ACK]	Seq=0	Ack=1	Win=0	Len=0

Frame 52 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: Ibm\_99:3b:13 (00:0d:60:99:3b:13), Dst: ArubaNet\_c5:0e:90 (00:0b:86:c5:0e:90)

Internet Protocol, Src: 61.8.9.254 (61.8.9.254), Dst: 10.5.0.179 (10.5.0.179)

Transmission Control Protocol, Src Port: krb524 (4444), Dst Port: 54728 (54728), Seq: 0, Ack: 1, Len: 0

- Source port: krb524 (4444)
- Destination port: 54728 (54728)
- Sequence number: 0 (relative sequence number)
- Acknowledgement number: 1 (relative ack number)
- Header length: 20 bytes

Flags: 0x14 (RST, ACK)

# packets (cont)

The image shows a Wireshark network traffic analysis interface. The top toolbar contains various icons for file operations, navigation, and analysis. Below the toolbar is a filter bar with a dropdown menu and buttons for 'Expression...', 'Clear', and 'Apply'. The main display area is divided into several sections:

- Packet List:** A table with columns 'No.', 'Time', 'Source', 'Destination', 'Protocol', and 'Info'. The first entry is: 1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x674c16fb
- Packet Bytes:** A detailed view of the selected packet. It shows the following information:
  - Seconds elapsed: 0
  - Bootp flags: 0x0000 (Unicast)
  - Client IP address: 0.0.0.0 (0.0.0.0)
  - Your (client) IP address: 0.0.0.0 (0.0.0.0)
  - Next server IP address: 0.0.0.0 (0.0.0.0)
  - Relay agent IP address: 0.0.0.0 (0.0.0.0)
  - Client MAC address: Intel\_c8:eb:04 (00:04:23:c8:eb:04)
  - Server host name not given
  - Boot file name not given
  - Magic cookie: (OK)
  - Option: (t=53,l=1) DHCP Message Type = DHCP Discover
    - Option: (53) DHCP Message Type
    - Length: 1
    - Value: 01
  - Option: (t=61,l=255) Client identifier
    - Option: (61) Client identifier
    - Length: 255
- Malformed Packet:** A red bar indicates a malformed packet: [Malformed Packet: BOOTP/DHCP]
- Hex Dump:** A table showing the raw bytes of the packet. The first few lines are:
  - 0020 ff ff 00 44 00 43 01 05 00 00 01 01 06 00 67 4c ...D.C. ....gL
  - 0030 16 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  - 0040 00 00 00 00 00 00 00 04 23 c8 eb 04 00 00 00 00 .....
- Packet Details:** A section at the bottom showing the structure of the packet, including 'Bootp/Dhcp option length (bootp.option.length), 1 byte' and 'P: 1 D: 1 M: 0'.

# packets (last one)

Filter:  + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x906c2c87

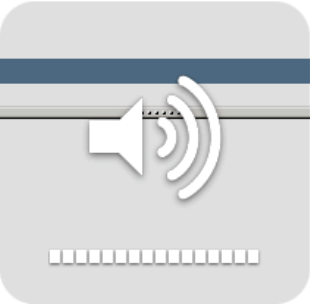
▶ Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0 (0.0.0.0)  
Your (client) IP address: 0.0.0.0 (0.0.0.0)  
Next server IP address: 0.0.0.0 (0.0.0.0)  
Relay agent IP address: 0.0.0.0 (0.0.0.0)  
Client MAC address: Intel\_c8:eb:04 (00:04:23:c8:eb:04)  
Server host name not given  
Boot file name not given  
Magic cookie: (OK)

▼ Option: (t=53,l=1) DHCP Message Type = DHCP Discover  
Option: (53) DHCP Message Type  
Length: 1  
Value: 01

▼ Option: (t=61,l=255) Client identifier  
Option: (61) Client identifier  
Length: 255  
Value: DF1DCAC2093C61E3DAB2D2D4F96337A6870784807EB72893...  
End Option

0110 00 00 00 00 00 00 63 82 53 63 35 01 01 3d ff df .....c. Sc5...=.  
0120 1d ca c2 09 3c 61 e3 da b2 d2 d4 f9 63 37 a6 87 .....ea. ....C7.  
0130 07 84 80 7e b7 28 93 e7 b9 4d 3d e5 fe f3 17 79 ..... (. .M=...y  
0140 cf 41 1a eb 17 60 7c d8 7f f1 10 a3 32 63 a1 63 .....A...|. ....2c.c  
0150 09 06 0d 2b db d8 89 6c 1c 5d ed ac ab 51 50 b4 .....+. .l .) .OP.  
0160 c9 04 18 e4 51 e5 9f ab 65 e1 22 6b a5 68 e9 40 .....Q... e."k.h@  
0170 e8 72 f5 5c 3f e6 8a 40 8e 87 08 54 b2 eb b2 66 .....r.\?..@ ...T...f  
0180 20 36 31 f1 0a 9c 06 b7 16 49 c6 e9 47 0c f7 9e .....61.... .I.G...  
0190 a6 42 9e 5c d8 96 89 d2 57 b5 91 e4 f5 e9 9a 93 .....B.\... W...  
01a0 bd 76 a8 28 4f ba 9e ea 3a b9 03 0e 6b 7b 29 ba .....v.(0... .k{).  
01b0 d4 47 9a 5a 29 f5 02 27 0a 51 13 43 e3 00 ce 0d .....G.Z)... .Q.C....  
01c0 fa 18 06 97 b9 b4 68 4b 5e 19 05 d8 9a 00 08 2c .....hK ^.....  
01d0 50 4b 9b bb f4 47 4d 3f 20 fa 1a 6e 04 1a 61 d9 .....PK...GM? ..n..a.  
01e0 41 f2 bf b7 ee ad 60 96 88 7b fb 7c 54 12 6c e8 .....A... ..{. [T.L.  
01f0 23 a8 7f 9f 04 6f 01 ac bc d8 74 5b d7 24 7c 37 .....#. .o. . .t[. \$]7  
0200 b1 6d 45 25 5d a7 45 ae 31 a2 b6 b2 28 f3 33 c4 .....mE%.E. 1... (.3.  
0210 da ab 88 77 89 df ab fd e5 82 3e 5d 9b 23 ff .....w.... .>].#.

Bootp/Dhcp option value (bootp.option.value), 255 bytes P: 1 D: 1 M: 0



## **(con)fuzzing state of the security community**

- **“bad” security in depth implementations (dos?)**
- **again. . . lots of security is based on known attacks**
- **critical infrastructure (?)**
- **roj**
- **fuzzing is just one of the tools, but certainly has helped changing the way people think**

# predictions / crazy thoughts

- **most people already got fuzzing**
- **more intelligence has to be incorporated to protocol fuzzing**
  - **protocol/ application “adaptation”**
  - **offline protocol fuzzing/ protocol correlation**
  - **redundant system testing**
  - **fuzzing through tunnels**
  - **proxy-fuzzing (not a-la spike proxy)**
  - **fuzz through/ on/ with non-standard media types (traffic shapers, etc)**
- **creativity is key : use the brain, for anything**
- **better integration with other tools**
- **anything is fuzzable**



## resources

- fuzzing mailing list by gadi evron  
<http://www.whitestar.linuxbox.org/mailman/listinfo/fuzzing>
- book: fuzzing: brute force vulnerability discovery: pedram et al  
<http://fuzzing.org>
- <http://labs.musecurity.com>
- <http://www.hacksafe.com.au/blog/2006/08/21/fuzz-testing-tools-and-techniques/>
- [http://www.immunitysec.com/downloads/advantages\\_of\\_block\\_based\\_analysis.pdf](http://www.immunitysec.com/downloads/advantages_of_block_based_analysis.pdf)



**questions?**

**leduardo (at) musecurity.com**