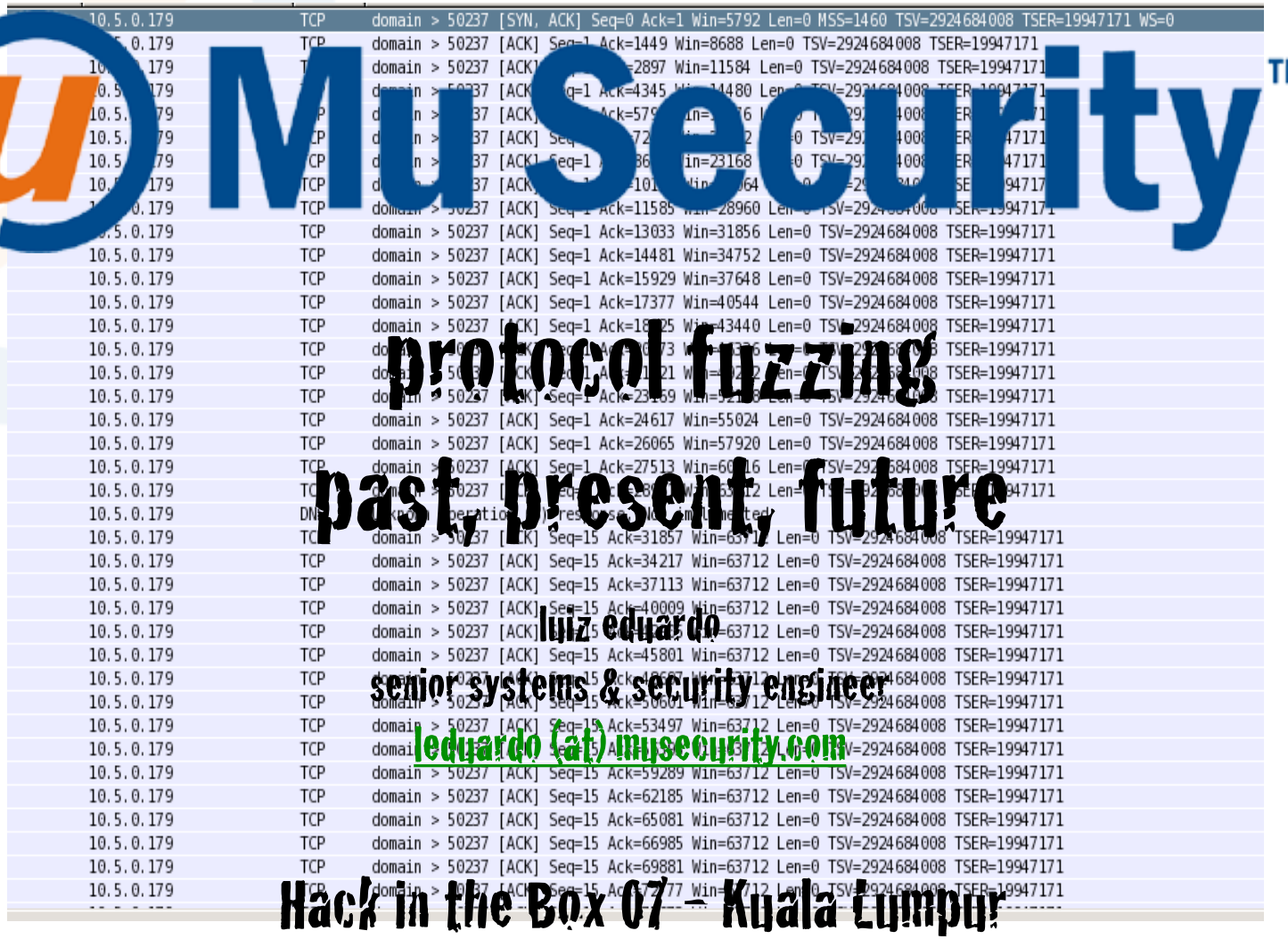


MuSecurity™

protocol fuzzing
past, present, future

luiz eduardo
senior systems & security engineer
leduardo (at) musecurity.com

Hack in the Box 07 – Kuala Lumpur

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

"hmmmmm... but... people are not supposed to send these packets"

Mu Security™

(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

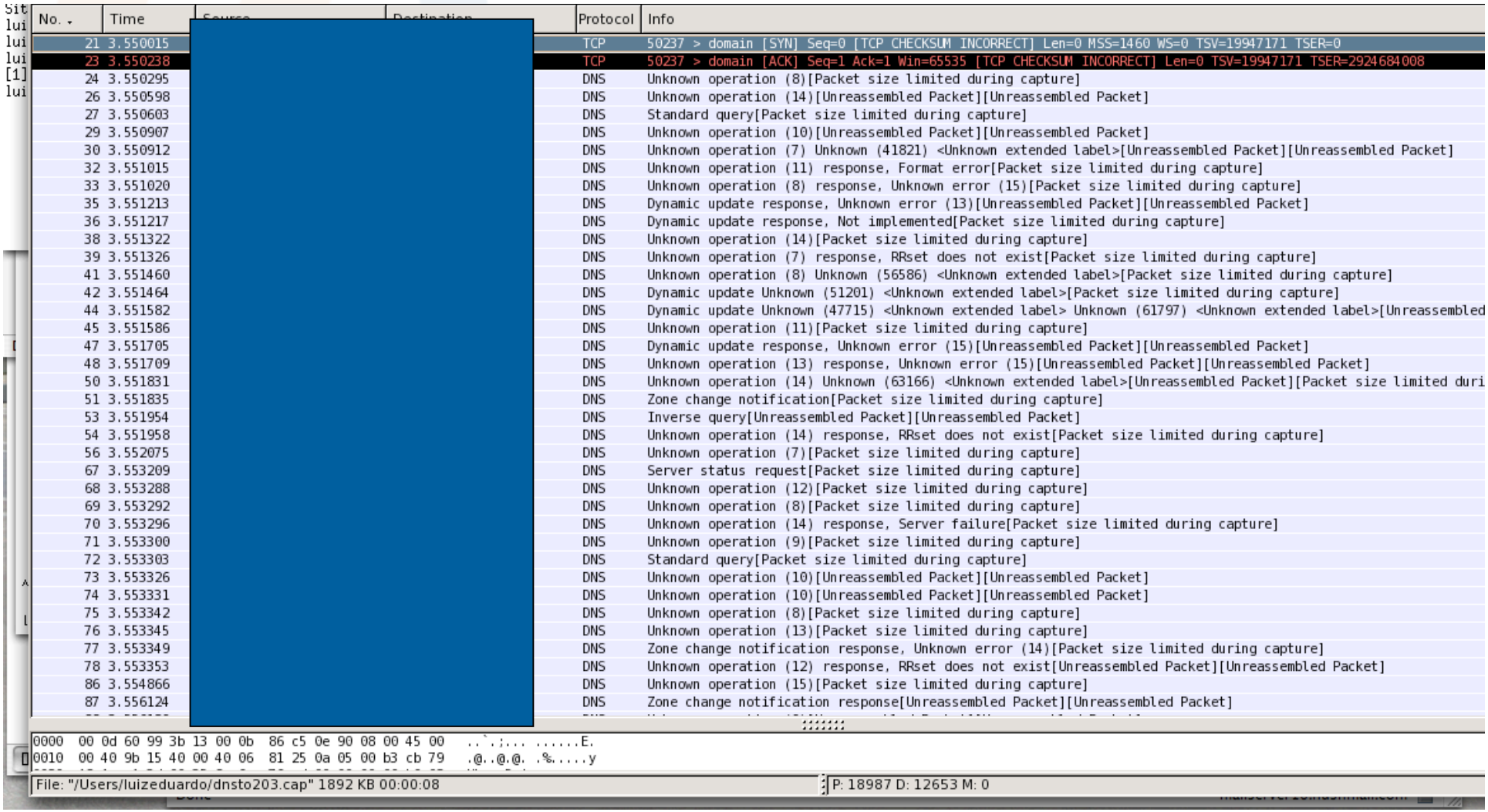
commercial

- 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



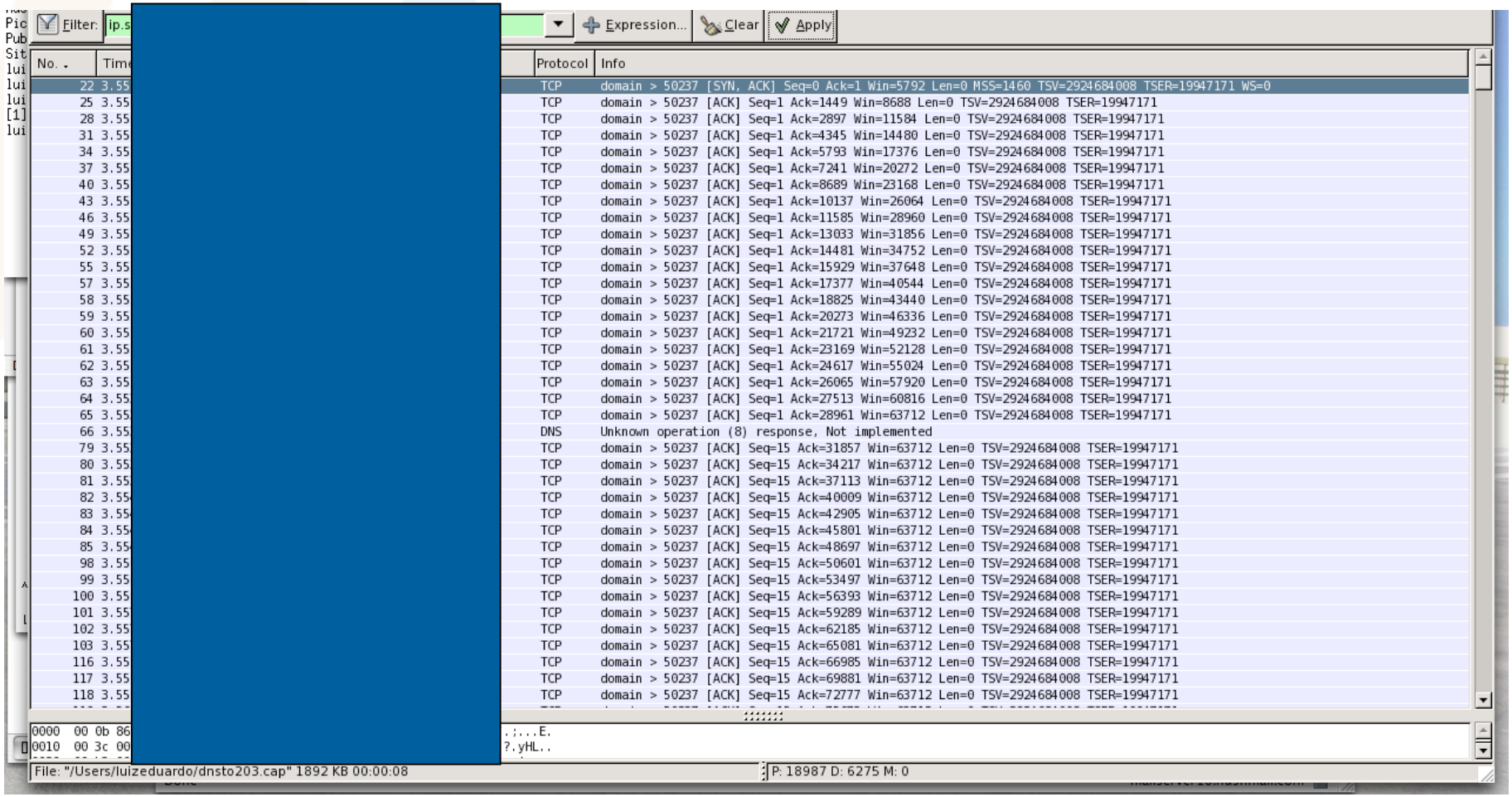
No.	Time	Source	Destination	Protocol	Info
21	3.550015	[redacted]		TCP	50237 > domain [SYN] Seq=0 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0 TSV=19947171 TSER=0
23	3.550238			TCP	50237 > domain [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=19947171 TSER=2924684008
24	3.550295			DNS	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
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][Packet size limited duri
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/luizeduardo/dnsto203.cap" 1892 KB 00:00:08 | P: 18987 D: 12653 M: 0

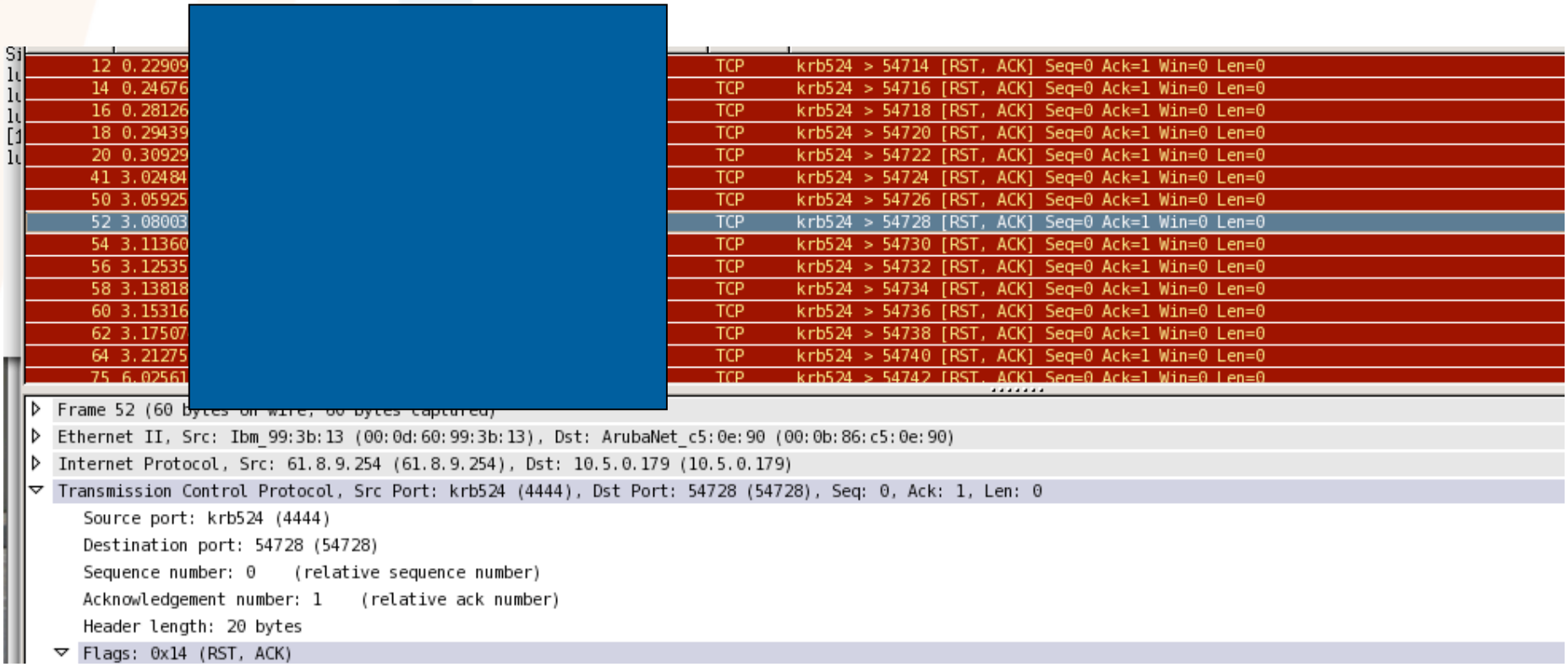
Mu Security™

packets (cont)



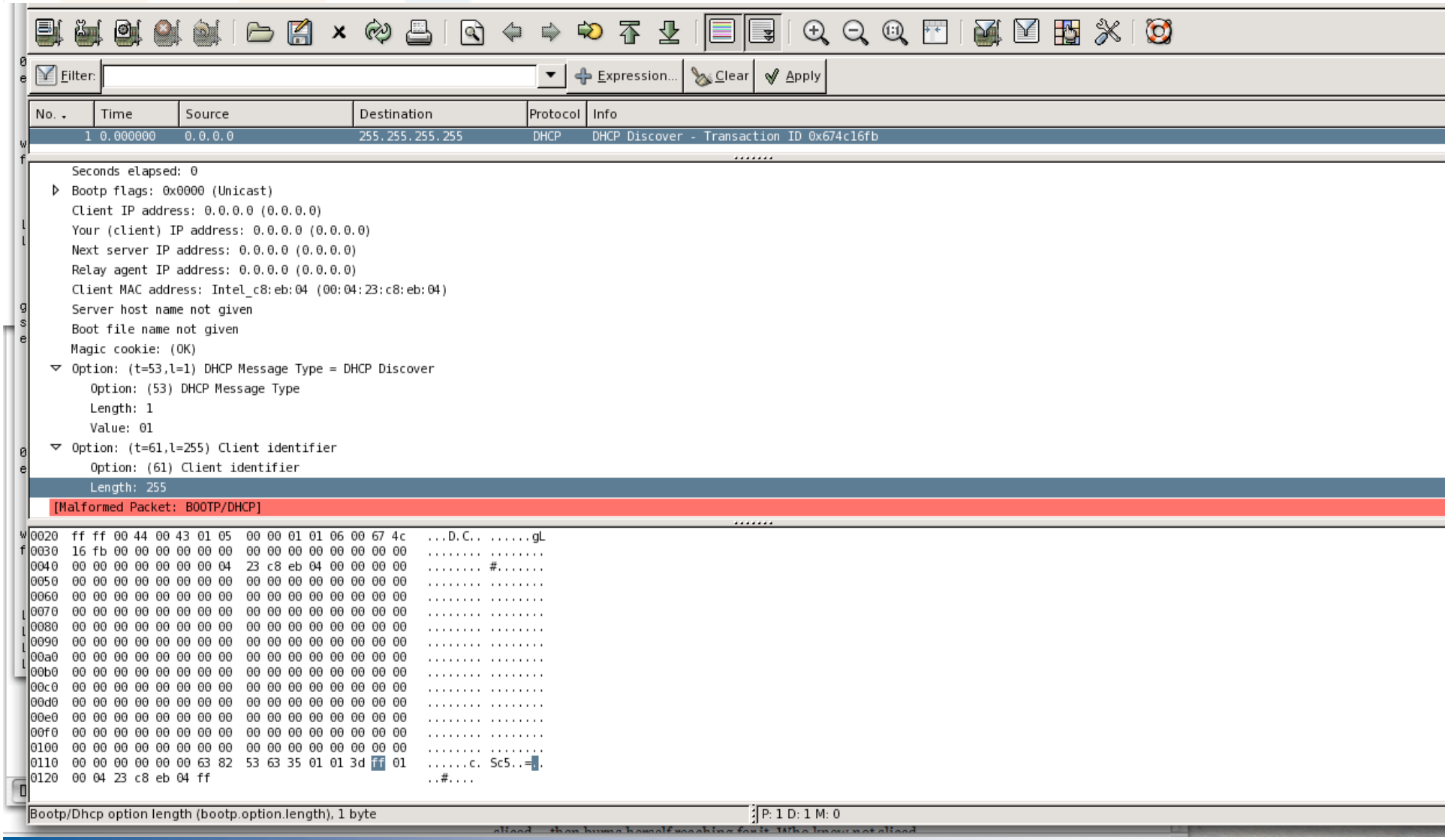
Mu Security™

packets (again)



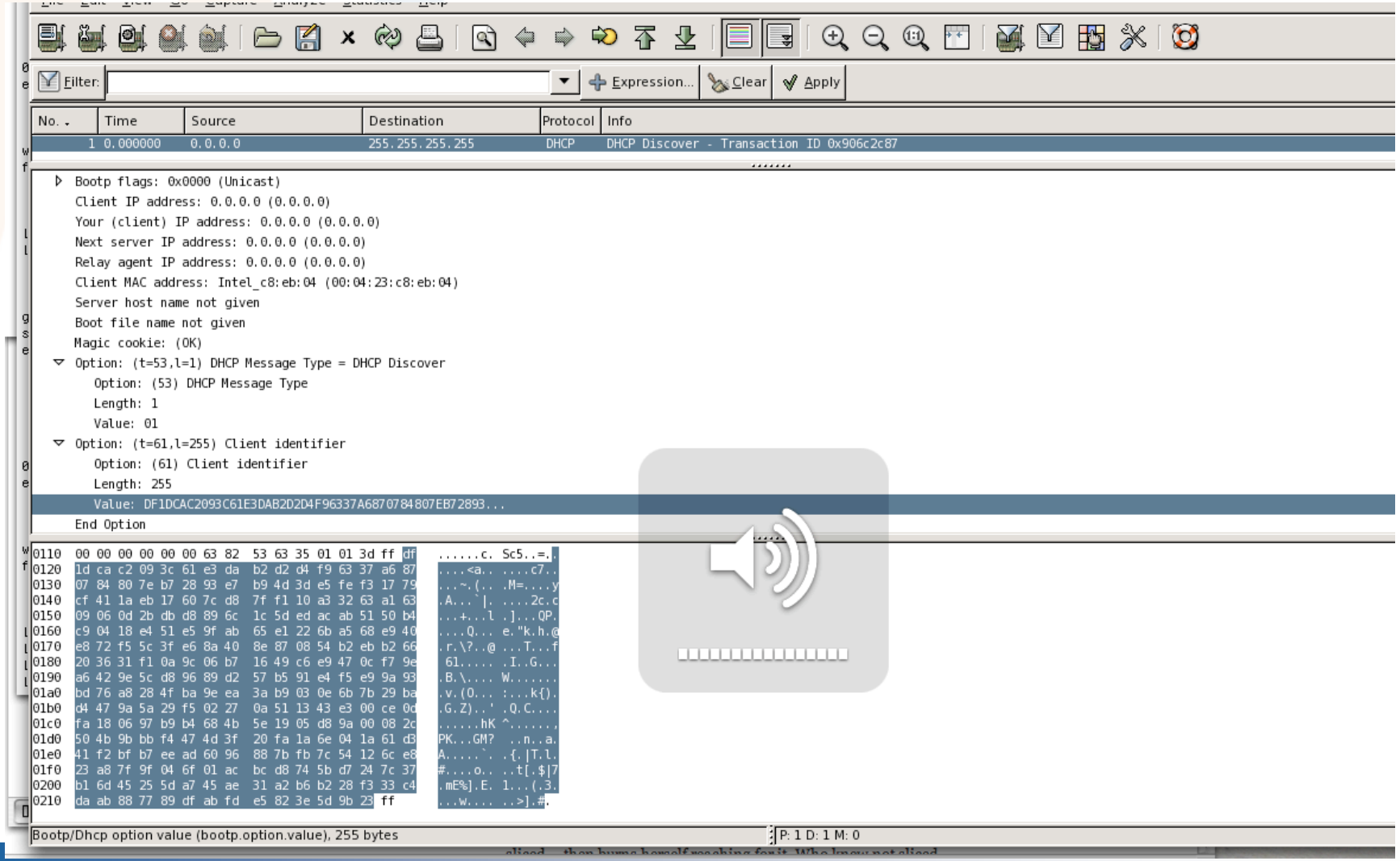
Mu Security™

packets (cont)



Mu Security™

packets (last one)



Mu Security™

(con)fuzzing state of the security community

- "bad" security in depth implementations (dos?)
- again. . .. lots of security is based on known attacks
- critical infrastructure (?)
- roi
- 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 incoporated 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

questions?

leduardo (at) musecurity.com