

Using NetZob for Active protocol reverse engineering

Onur Catakoglu , Bastien Drouot, Paul Germouty, Florent Tardif

November 2, 2017

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields
- 4 Characterizing Fields
- 5 Finding Protocol Behaviour
- 6 Experiments demonstration
- 7 Future Work

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields
- 4 Characterizing Fields
- 5 Finding Protocol Behaviour
- 6 Experiments demonstration
- 7 Future Work

Objectives-Attack Model

- Reverse engineering transmission protocols
⇒ characterize protocols' structure
- Client-owning Model
⇒ possibility to discuss with the server with the protocol

Passive framework for analysing transmission

- symbol
- *Format.splitAligned(s)*
- *Format.splitStatic(s)*
- *Format.splitDelimiter(s,Raw(listofbytes))*

Attack Model

1

Introduction

2

RoadMap

3

Reconstructing Fields

4

Characterizing Fields

5

Finding Protocol Behaviour

6

Experiments demonstration

7

Future Work

Road Map of GoodGuy ReverseIngBoy

Getting Information

getting pcap

Divide and Conquer

sorting client server

sorting type of request (s7: co, rm, wm, dc)

recognize field (delimiters approach, Shaping to split aligns)

Analysing Shape

IDK what is left i guess

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields**
- 4 Characterizing Fields
- 5 Finding Protocol Behaviour
- 6 Experiments demonstration
- 7 Future Work

getting pcap and sorting

delimiters
shaping to split

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields
- 4 Characterizing Fields**
- 5 Finding Protocol Behaviour
- 6 Experiments demonstration
- 7 Future Work

static/dyn?
bin/text?
nb

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields
- 4 Characterizing Fields
- 5 Finding Protocol Behaviour**
- 6 Experiments demonstration
- 7 Future Work

Stateless, relations

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields
- 4 Characterizing Fields
- 5 Finding Protocol Behaviour
- 6 Experiments demonstration**
- 7 Future Work

- 1 Introduction
- 2 RoadMap
- 3 Reconstructing Fields
- 4 Characterizing Fields
- 5 Finding Protocol Behaviour
- 6 Experiments demonstration
- 7 Future Work**