Using NetZob for Active protocol reverse engineering

Onur Catakoglu , Bastien Drouot, Paul Germouty, Florent Tardif

November 2, 2017

Objectives-Attack Model

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

Previous Work **Netzob**

Passive framework for analysing transmission

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

Attack Model

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

getting pcap and sorting

delimiters
shaping to split

static/dyn?
bin/text?
nb

Stateless, relations