Speakers: Alan Commike, Reservoir Labs

The Ins and Outs of Developing a new Bro protocol analyzer in BinPAC

Reservoir Labs developed a Financial Interchange Format (FIX) analyzer for Bro* using BinPAC. This talk discusses some of the details required to develop this analyzer with a walkthrough of code and concepts. We tailored the development of the analyzer towards real-world use cases were the notion of simply identifying a protocol can sometimes be sufficient. We will discuss the three stages of analyzer development with the notions of Identification, Verification, and Extraction. The talk will highlight a small change to BinPAC that was required to enable the parsing of ASCII protocols that use arbitrary line breakers (as is the case with FIX) and some of the design decisions that went into analyzer development. We will end with a discussion of some of the limitations of the Bro analyzer framework during Bro startup and other limitations with long running sessions and how to mitigate them with proper tuning of Bro.