Speakers: Robin Sommers, Corelight/ICSI

A Tutorial on Writing Bro Plugins

Bro provides a powerful plugin API that facilitates a variety of extensions through external C\+\+ code, without requiring any changes to the core code base. Plugins have access to much of Bro's internal infrastructure and can, for example, provide new built-in functions to Bro scripts; implement additional protocol & file analyzers; and add new log writers or input readers. This talk will walk through writing a Bro plugin from scratch. We'll examine the main Bro APIs available to plugins, discuss some typical pitfalls to avoid, and learn how to make a custom plugin available to the Bro community by publishing it as a Bro package.