CUBRO
NETWORK VISIBILITY

DPI SDK APPLICATION

APPLICATION NOTE

FEBRUARY 2020

Reduce time, cost, and complexity of adding traffic intelligence to your solution.

Cubro DPI SDK

Cubro's single pass traffic scanner ensures extreme performance with minimal memory use, allowing it to perform on the smallest embedded device or scale to the largest multi-core server.

Embedded DPI vendors have traditionally designed their products around protocol inspectors, trackers, or analyzers. Signatures are commonly represented in code, authored in general purpose programming languages. These naive methods have the advantage of a minimal initial technology investment; however, they result in high maintenance costs, increasing code complexity, and mediocre performance.

An alternative solution involves representing signatures in data. These solutions typically load state machines in memory. These state machines are in theory very fast but in practice lack the flexibility to deal with the complexities of modern traffic identification. They also suffer from an exponential blowup issue which consumes memory and impacts performance. To remedy these challenges, vendors may slice their automata up, which unfortunately defeats much of the performance edge they should have over the naive approach.

In contrast, Cubro's SDK includes a purpose built environment for high performance stream scanning and traffic identification using a proprietary hybrid single pass DFA along side an execution environment. The design ensures network stream scanning and traffic identification is easy, performant, and safe.

Rapid, Safe Signature Development

Signatures are expressed in a specialized, domain specific, language with powerful primitives for pattern matching and limited room for errors. Our proprietary compiler is able to catch many signature quality issues at compile time, driving quality up and costs down, benefits that we pass on to our customers.

Advanced traffic intelligence

Easy integration measured in hours or days, not weeks or months.
Minimal API and direct access to underlying data. At Cubro, we strive for simplicity and speed.

Memory Sandbox
Safe and performant memory allocation as requests to allocate or free memory are only made during startup or teardown, and made with external functions only.

Single Pass
We do not slice or partition its stream scanning, which allows stream data to pass through the runtime just once. This gives our runtime a large performance advantage.

Content Extraction
A simple yet powerful callback subscription provides the integration access to published values. These values can represent anything from fields in the stream the integration would like extracted, protocol header fields, synthetic values (such as assembling a URL from a host header and URI), or detected events.

Hitless Updates
Transition from one signature bundle to another with one simple function without interruption in scanning. Unknown connections in progress will continue to use the old signatures until they have been identified, while new connections will start using the new bundle right away.

Expected Flows
Uses the information gathered from one flow to improve classification accuracy in related flows. In order to correlate several distinct but related flows, the runtime maintains a lookup table for traffic events that are expected to occur. This table works in concert with signatures to provide a reliable framework for correlation.

Endpoint Telemetry
Our runtime intelligently monitors endpoint DNS traffic to increase classification confidence where encryption or payload obfuscation impede pattern matching and to associate traffic to the proper application even when traffic is delivered via CDNs.

Connection Tracking
Our SDK provides optional packet hashing and connection state management which implements a finite state machine to appropriately manage connection state as segments traverse the network.

Highly Portable
Supported on x86, ARM, MIPS Linux user-space

Runtime Scanner

This library hosts a runtime environment for high performance stream scanning for pattern matching programs compiled by he signature compiler. It provides methods to scan network streams for the purpose of device, protocol, and application dentification.

Network Flow Engine

This library provides methods to decode and hash packets, create and retrieve connection state, and directly accepts Ethernet, IP, IP6, and encapsulations like LAN, GRE, GTP, L2TP and IP-in-IP

Performance Tools & Sample Source Code

To demonstrate an integration, the SDK includes the source to a multi-threaded packet analysis tool called pcapscan. The sample application is simple and provides basic reference integration. In addition, it demonstrates the performance and scaling characteristics of protocol handling, onnection tracking and pattern matching capabilities of the SDK.