



Contribution ID: 172

Type: **not specified**

Enhancing User Defined Tracepoints

Thursday, November 15, 2018 2:20 PM (20 minutes)

BPF trace tools such as `bcc/trace` and `bpfftrace` can attach to Systemtap USDT (user application statically defined tracepoints) probes. These probes can be created by a macro imported from `"sys/sdt.h"` or by a provider file. Either way, Systemtap will register those probes as entries in the note section of the ELF file with the name of the probe, its address and the arguments as assembly locations. This approach is fairly simple, easy to parse and non-intrusive. Unfortunately, it is also obsolete and lacks features such as typed arguments and built-in dynamic instrumentation. Since BPF tools are growing in popularity, it makes sense to create a new enhanced format to fix these shortcomings.

We can discuss and make decisions about the future of USDT probes used by BPF trace tools. Some possible alternatives are: extend Systemtap USDT to introduce these new features or extend kernel tracepoints so that user applications can also register them.

Presenter: MARCHINI, Matheus (Sthima)

Session Classification: BPF MC