PCap com filtragem orientada ao processo

Nuno Martins[1] e Vítor Duarte[2]

[1] nuno.m.g.martins@gmail.com
[2] vad@di.fct.unl.pt
CITI — Departamento de Informática,
Faculdade de Ciências e Tecnologia,
Universidade Nova de Lisboa, Portugal

Resumo A monitorização do comportamento dos processos é uma das melhores formas de compreender, detectar erros e avaliar o seu desempenho durante a sua execução real, ainda mais se não for possível aceder ao seu código fonte. No entanto, o impacto no desempenho e comportamento pode ser bastante significativo. O caso das interacções via rede não é excepção, sendo o PCap um dos sistemas mais populares para monitorizar/capturar o tráfego de rede ao nível do SO. Este trabalho baseia-se nesse sistema e no suporte dado pelo núcleo Linux, para permitir capturar as interacções via rede de processos específicos, procurando também limitar o impacto negativo desta monitorização. Pretende-se que sem conhecer *à priori* quais os portos que irão ser utilizados pelo processo, e sem necessitar de capturar todo o tráfego que circula pela rede obter apenas os pacotes referentes ao processo alvo. Para tal, foi criada uma forma de filtragem no *bpf-filters*, usados pelo pcap que, dinamicamente, através da monitorização das chamadas ao sistema do processo, permite manter os endereços e portos em utilização pelo processo alvo e capturar apenas o seu tráfego. Deste modo é possível obter apenas os dados relevantes, diminuir o volume de dados transferidos entre o núcleo de sistema e a ferramenta que monitoriza/analisa o processo, assim como um menor número de trocas de contexto, com vantagens funcionais e de desempenho.

Palavras chave: Instrumentação, KProbes, Linux Kernel, Monitorização, Núcleo do Linux, PCap