Beyond the PDP-11: Architectural support for a memory-safe C abstract machine

David Chisnall, Colin Rothwell, Robert N.M. Watson,
Jonathan Woodruff, Munraj Vadera, Simon W. Moore,
Michael Roe,
(University of Cambridge)

Brooks Davis, Peter G. Neumann
(SRI International)

ASPLOS 2015

Motivation

- C memory model was originally designed close to what PDP-11 could do, and is still close to that.
- Obviously (some) memory safety would be nice.
- CWE/SANS top 25 most dangerous software errors (2011) has buffer overflows on place three.
- Goal: Describe an (abstract) machine that runs existing C-code memory safe(r).

Difficult idioms

Program	Deconst	Container	Sub	II	Int	IA	Mask	Wide	LoC
ffmpeg	150	0	800	4	0	0	4	0	693,010
libX11	117	0	19	9	1	0	0	5	120,386
FreeBSD libc	288	0	216	2	13	50	184	17	136,717
bash	43	0	207	11	0	0	15	4	109,250
libpng	20	0	175	1	0	0	0	0	50,071
tcpdump	579	0	9	1299	0	0	0	0	66,555
perf	575	151	46	0	53	151	31	4	52,033
pmc	2	0	0	0	18	0	0	0	8,886
pcre	98	0	52	0	0	0	0	0	70,447
python	494	0	358	1	109	0	131	8	383,813
wget	55	0	61	0	3	0	1	10	91,710
zlib	4	0	24	0	0	0	0	0	21,090
zsh	29	0	267	0	0	0	5	5	98,664
Total	2491	151	2236	1557	197	201	371	53	1,902,632