

Historical Perspectives

The dynamic binary modification systems detailed in this text are by no means the first of their kind (nor are they likely to be the last). The three systems were chosen as the focus of this book because at the time of its writing, they were widely used and readily available.

In the 1990's, several other dynamic binary modifiers were developed, including Shade for SPARC/Solaris (Cmelik and Keppel [1994]), DynInst for a variety of platforms (Buck and Hollingsworth [2000]), Vulcan for x86/Windows (Edwards et al. [2001]), Wiggins/Redstone for Alpha (Deaver et al. [1999]), and Dynamo for HPUX/PA-RISC (Bala et al. [1999]).

Later on, numerous other dynamic binary instrumentation frameworks appeared, including Strata (Scott et al. [2003]), DELI (Desoli et al. [2002]), which is a descendent of Dynamo for the LX architecture, DIOTA for x86/Linux (Maebe et al. [2002]), Mojo for x86/Windows (Chen et al. [2000]), Walkabout for SPARC/Solaris (Cifuentes et al. [2002]), and HDTrans (Sridhar et al. [2006]). In addition, the three focus systems from this book (Pin, DynamoRIO, and Valgrind) appeared during that first decade of 2000.

Other tools served a similar purpose to one of more of the applications of dynamic binary modification, such as simulation or dynamic translation. Hardware simulators or emulators include Embra (Witchel and Rosenblum [1996]) and Simics (Magnusson et al. [2002]). Dynamic binary translators include DAISY (Ebcioğlu and Altman [1997]), Crusoe (Dehnert et al. [2003]), and Rosetta (Apple).

Outside of dynamic binary modification, there are a wide variety of static instrumentation tools dating back several decades. For instance, the ATOM toolkit from Digital (Srivastava and Eustace [1994]) formed the basis for the look-and-feel of the Pin API, and indeed there were several developers in common. Meanwhile, other systems included Etch (Romer et al. [1997]), EEL (Larus and Schnarr [1995]), and Morph (Zhang et al. [1997]).