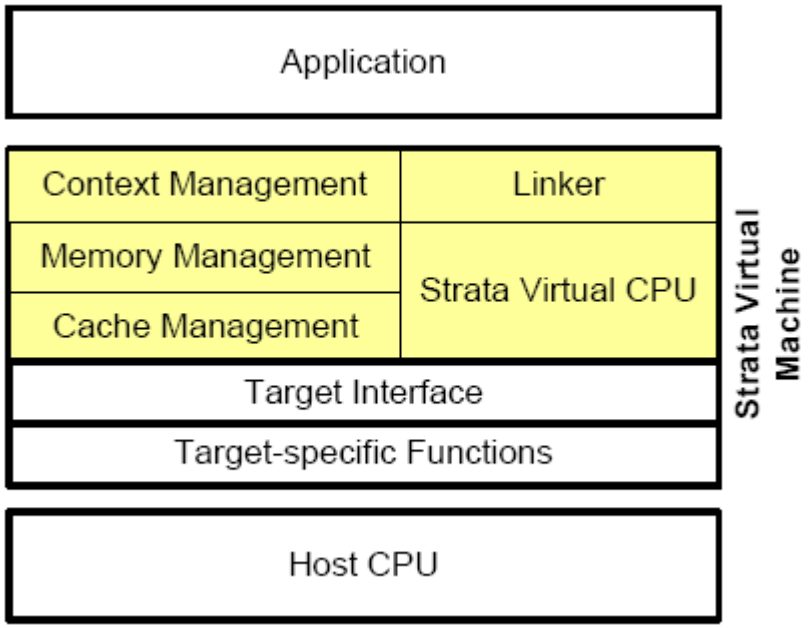
Dynamic Binary Translator
&
Randomized Instruction-Set Emulation

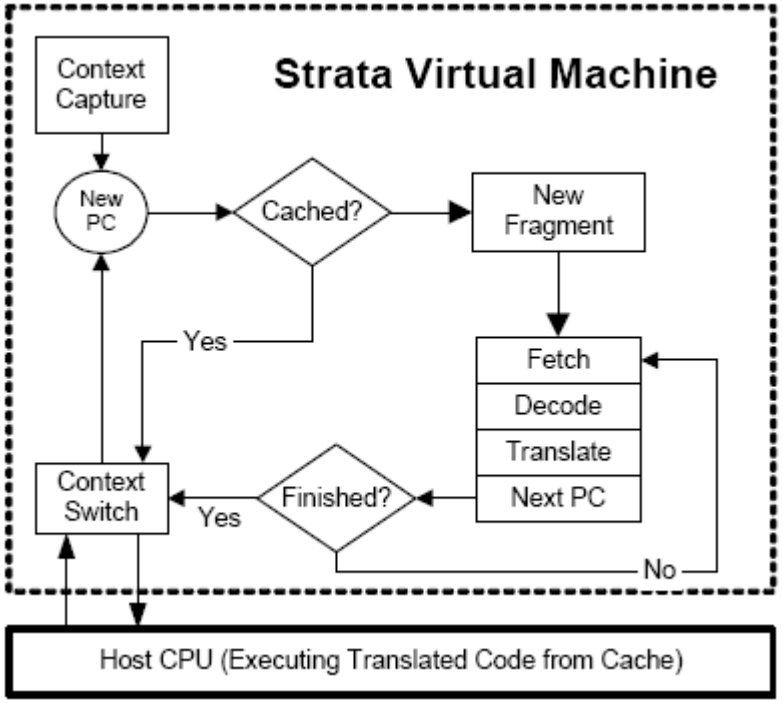
SoC 최적화연구실 권용인

Introduction

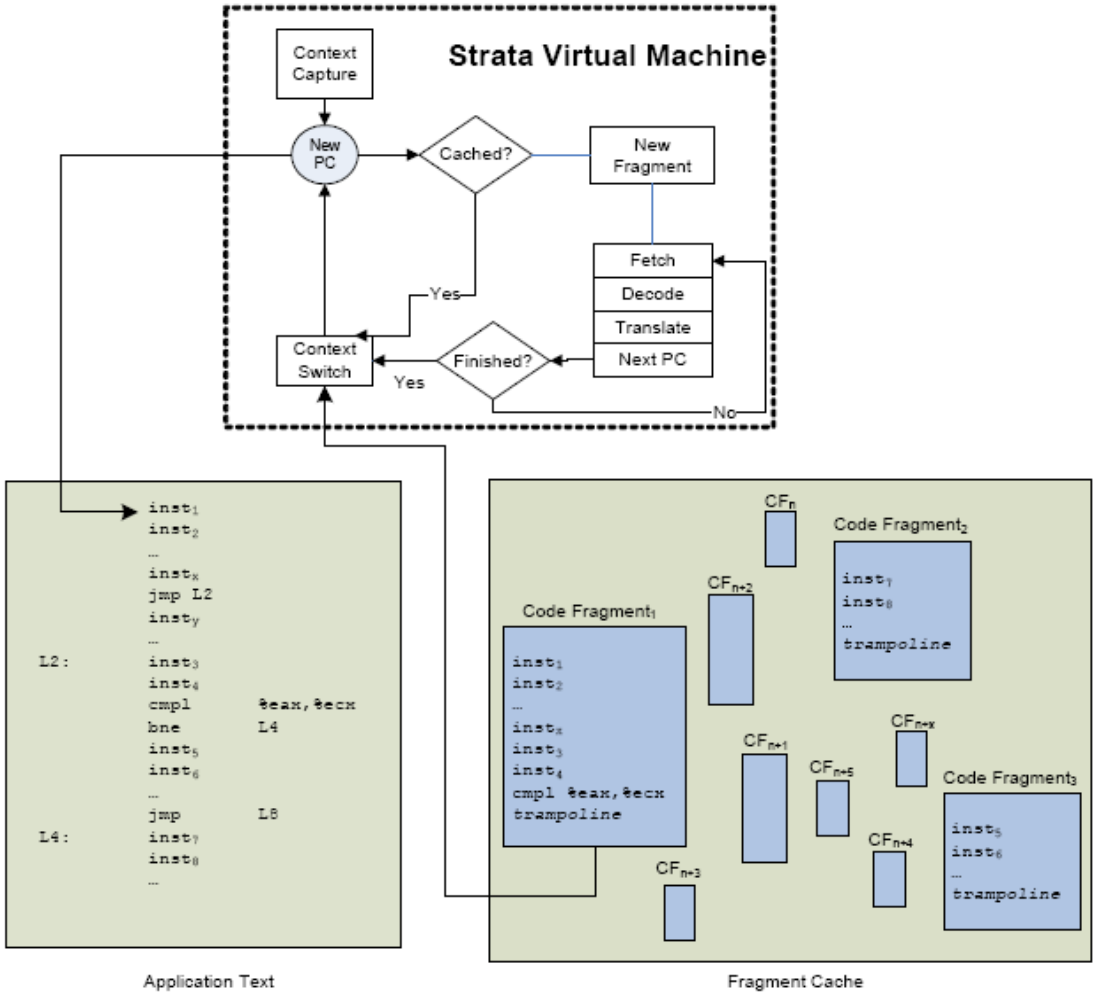
- Dynamic Binary Translation(Software Dynamic Translation) is the alteration of a running program to achieve a specific objective.
  - Shade [Cmelik and Keppel 1994]
  - Embra [Witchel and Rosenblum 1996]
  - Dynamo [Bala et al. 2000]
  - Strata [Kevin Scott and Jack Davidson 2002]
- virtualize aspects of the host execution environment by interposing a layer of software between program and CPU.

STRATA


Application
Context Management
Linker
Memory Management
Strata Virtual CPU
Cache Management
Target Interface
Target-specific Functions
Host CPU
Strata Virtual Machine


Context Capture
Strata Virtual Machine
New PC
Cached?
New Fragment
Yes
Fetch
Decode
Translate
Next PC
Context Switch
Yes
Finished?
No
Host CPU (Executing Translated Code from Cache)

STRATA


Strata Virtual Machine
Context Capture
New PC
Cached?
New Fragment
Fetch
Decode
Translate
Next PC
Finished?
Context Switch
Yes
Yes
No
inst1
inst2
…
instx
jmp L2
insty
…
L2: inst3
inst4
cmpl %eax,%ecx
bne L4
inst5
inst6
…
jmp L8
L4: inst7
inst8
…
Application Text
CFn
Code Fragment2
inst7
inst8
…
trampoline
CFn+2
Code Fragment1
inst1
inst2
…
instx
inst3
inst4
cmpl %eax,%ecx
trampoline
CFn+1
CFn+5
CFn+x
Code Fragment3
inst5
inst6
…
trampoline
CFn+4
CFn+3
Fragment Cache

Performance of Strata

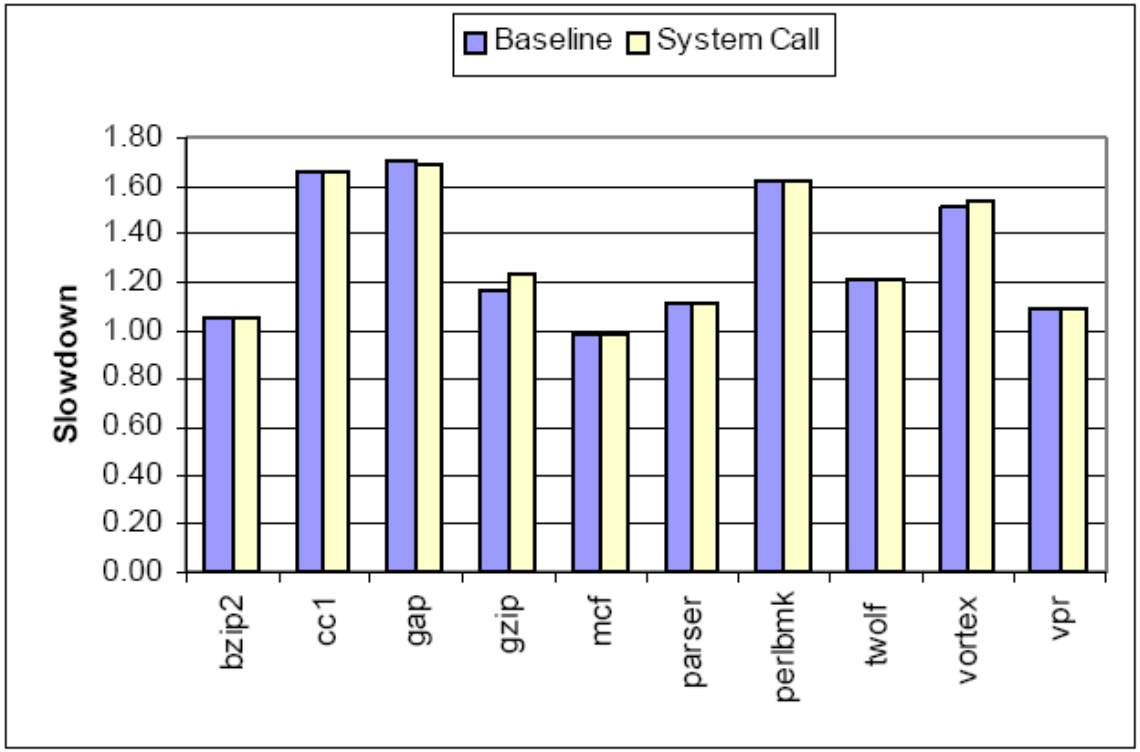
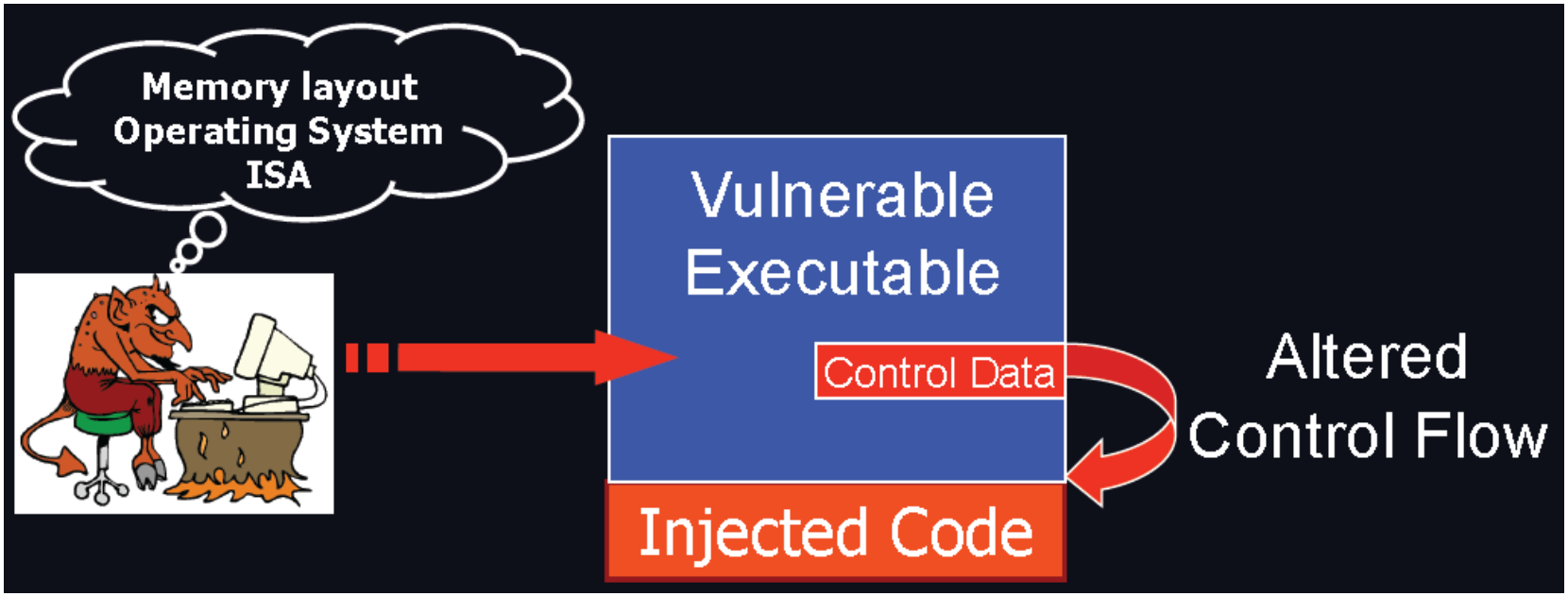


Figure 2. Performance of Strata-based system call monitor.

Code-injection attack

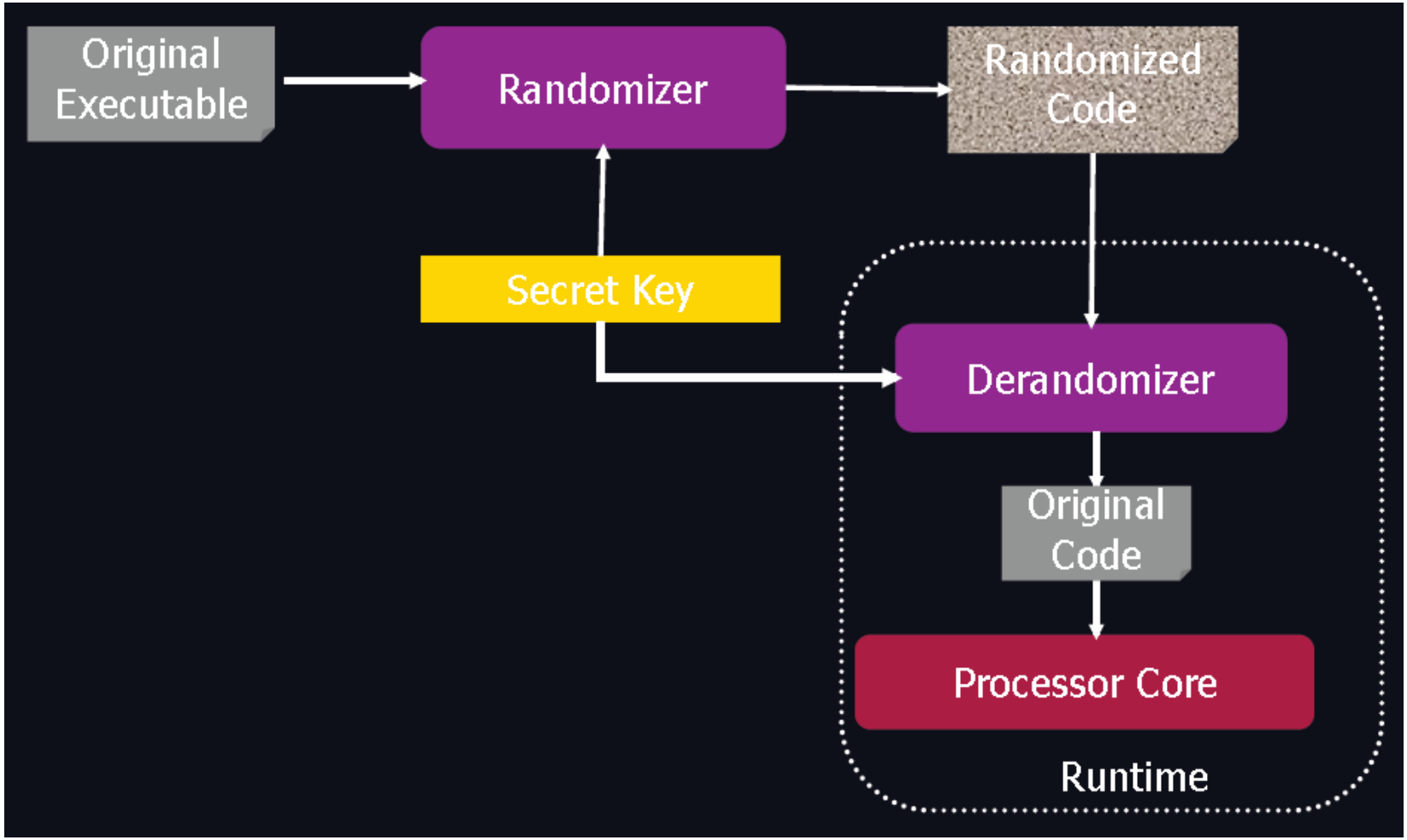
- In 2004, the Department of Homeland Security reported 323 buffer overflow vulnerabilities
- The most common attack : code-injection attack



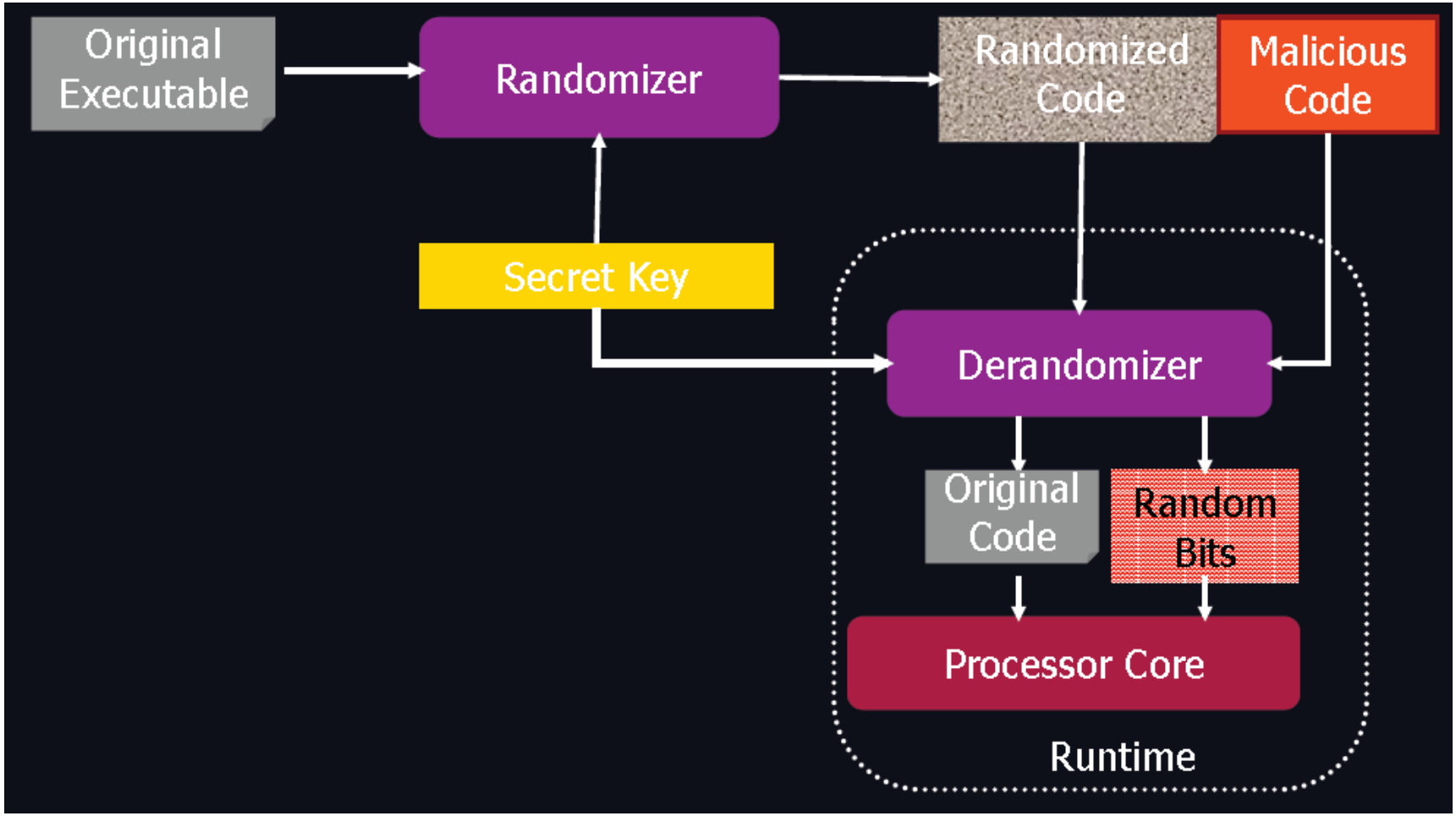
RISE

- Randomized Instruction-Set Emulation(RISE)
- A theoretically strong approach to defending against any type of code-injection attack
- Create and use a process-specific instruction set created by a randomization algorithm
- Code injected by attacker will be invalid

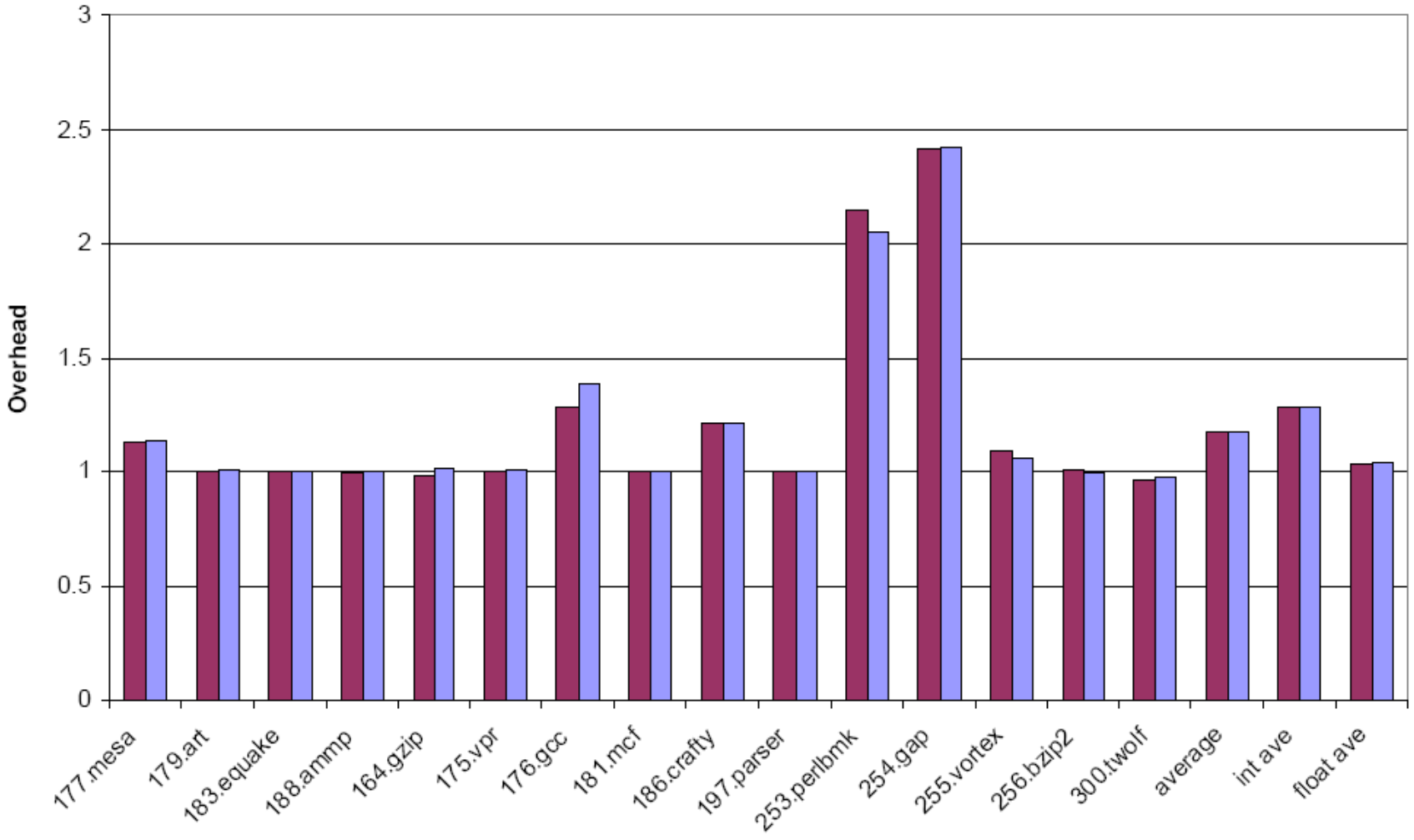
RISE using STRATA



RISE Defuses Injected Code



Performance of RISE using STRATA



Overhead of RISE using STRATA

Table 2: Disk image overhead (Kilobytes).

	BIND				Apache			
	Native	**SDT-only**	**SDT-based ISR**	**SDT-based ISR Expansion**	**Native**	**SDT-only**	**SDT-based ISR**	**SDT-based ISR Expansion**
Disk image	1811	1872	2731	1.51x	916	987	1617	1.77x
text	1786	1838	2690	1.51x	875	939	1566	1.79x
data	23	28	32	1.39x	34	39	43	1.26x
bss	13	32	41	3.15x	166	186	194	1.17x

Future work

- Dynamic Binary Translation on mobile devices
- Secure execution on mobile devices
- Minimize disk overhead of RISE on mobile devices
- Maximize performance of RISE on mobile devices