Minemu

The world's fastest taint tracker

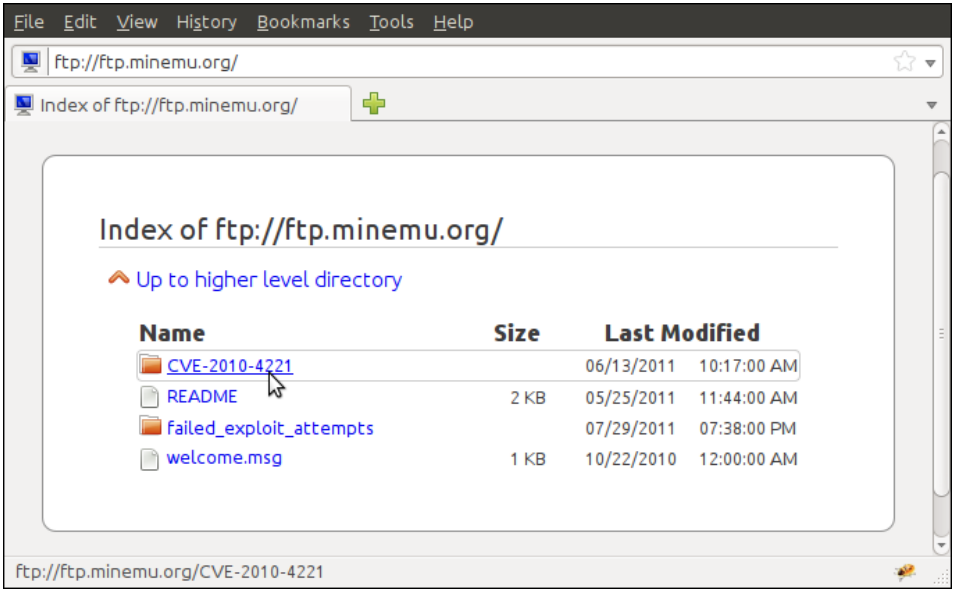
Attack detection aimed at production environments.

Erik Bosman, Asia Slowinska, and Herbert Bos

Challenge!

ftp://ftp.minemu.org runs Proftpd

vulnerable to CVE-2010-4221

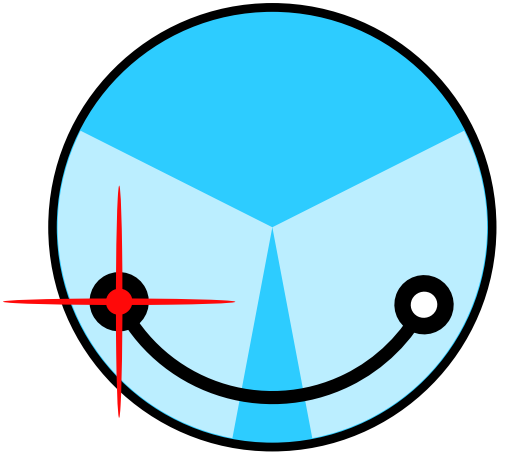


First exploiter gets a present!

Taint tracking: useful, but slow

Performance problems

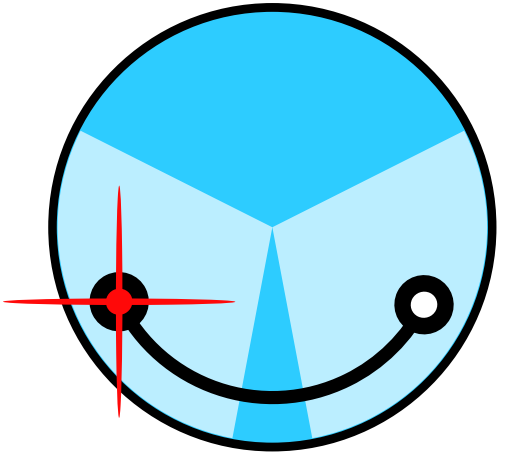
Is this slowness fundamental?



minemu

memory layout
use SSE registers to hold taint
fast emulator

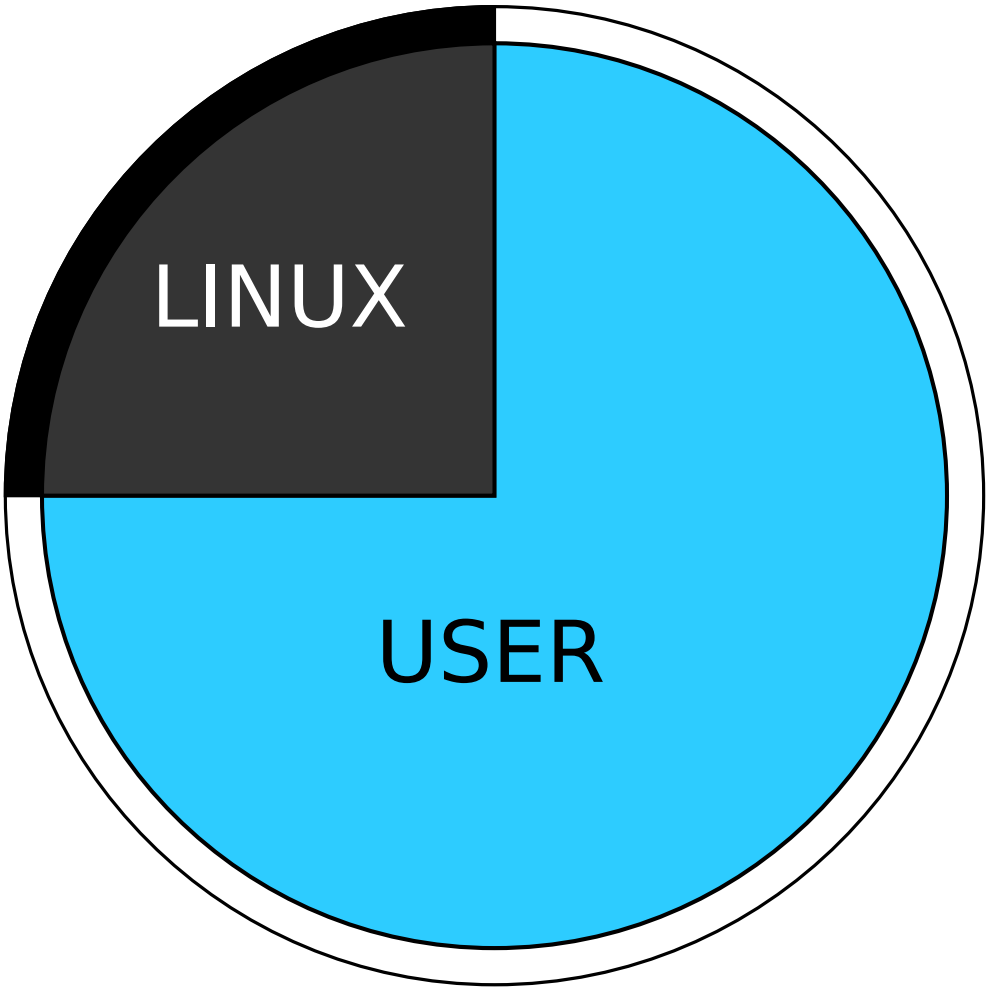
Is this slowness fundamental?



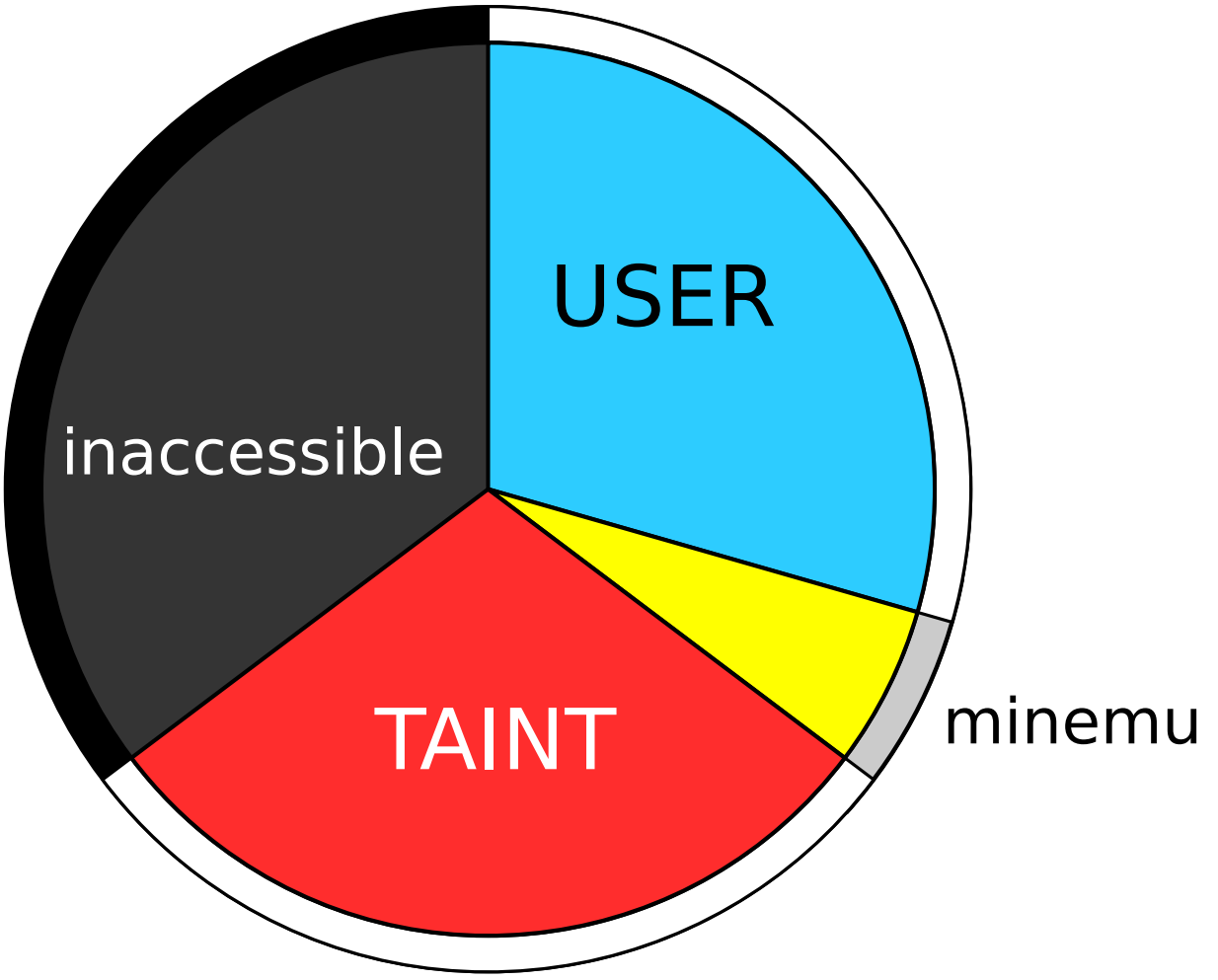
minemu

- memory layout
  use SSE registers to hold taint
  fast emulator

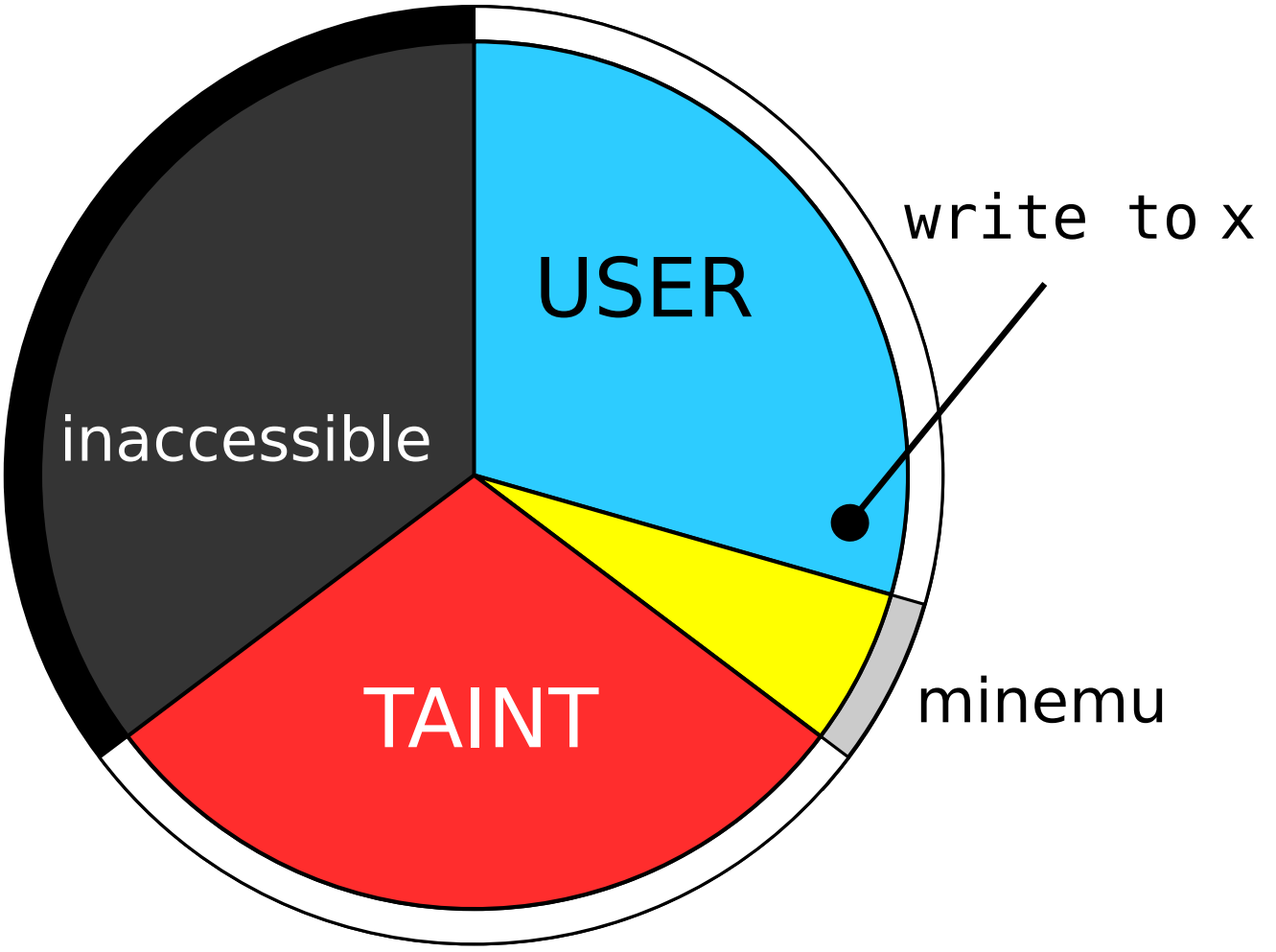
Memory layout



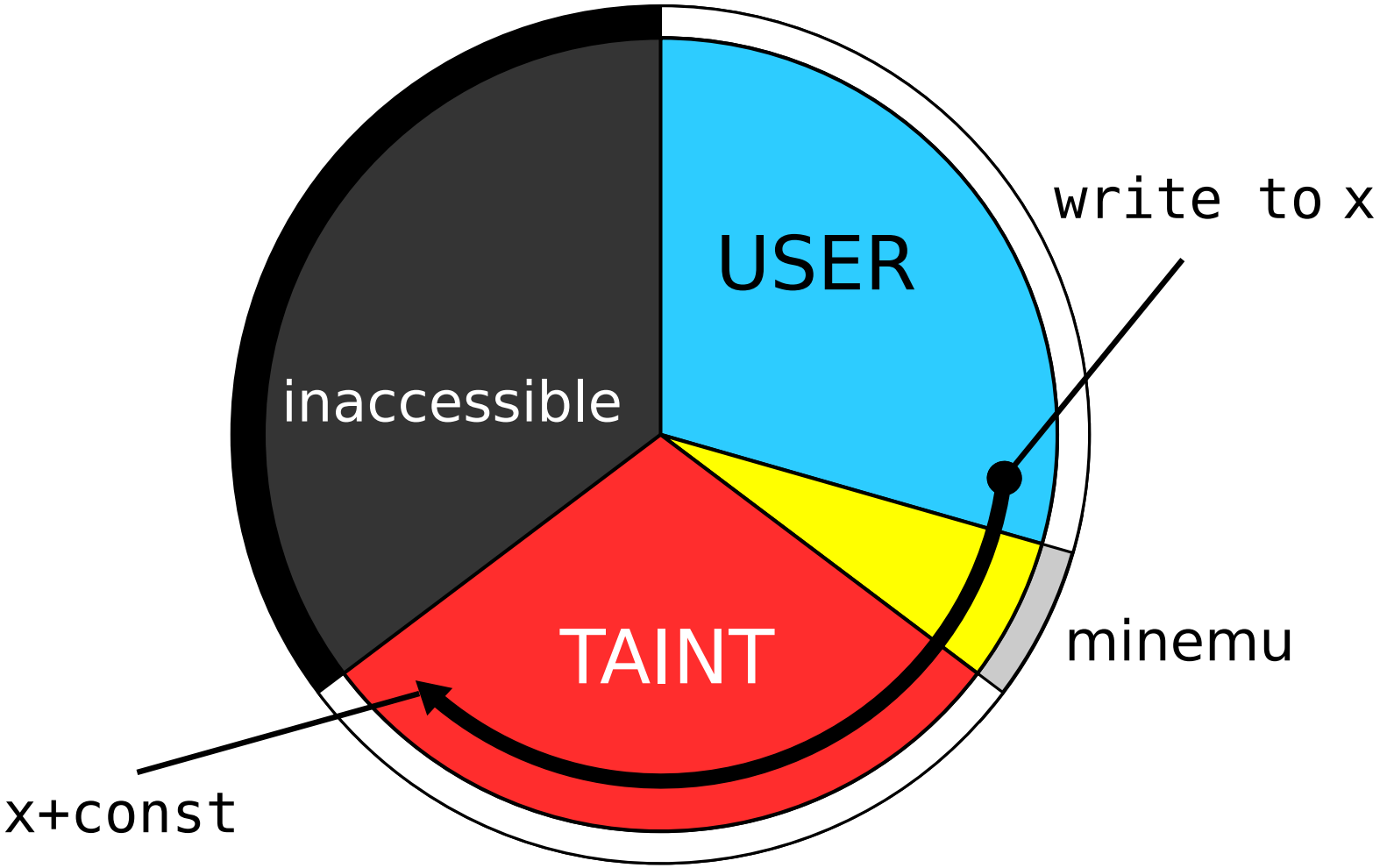
Memory layout (minemu)



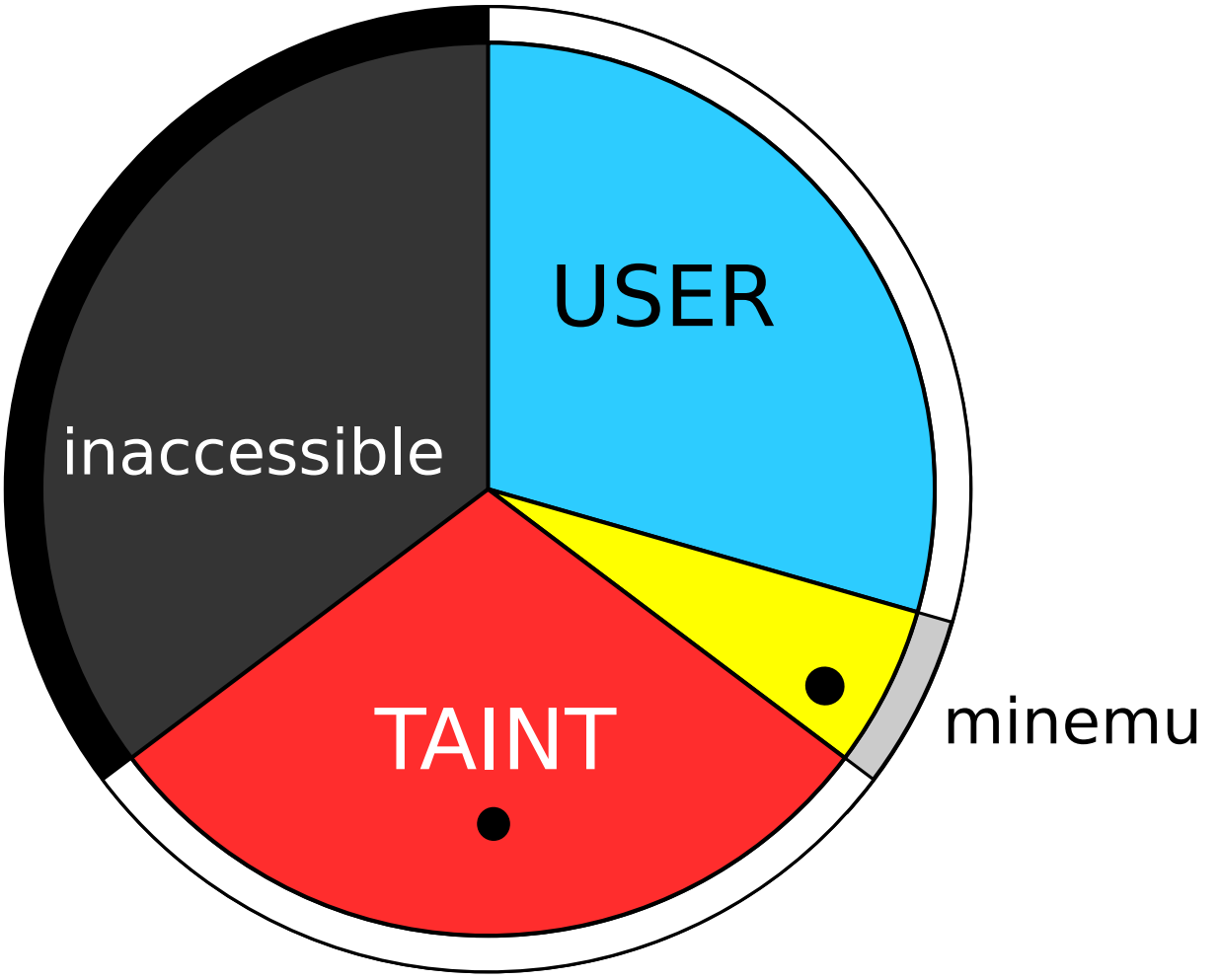
Memory layout (minemu)



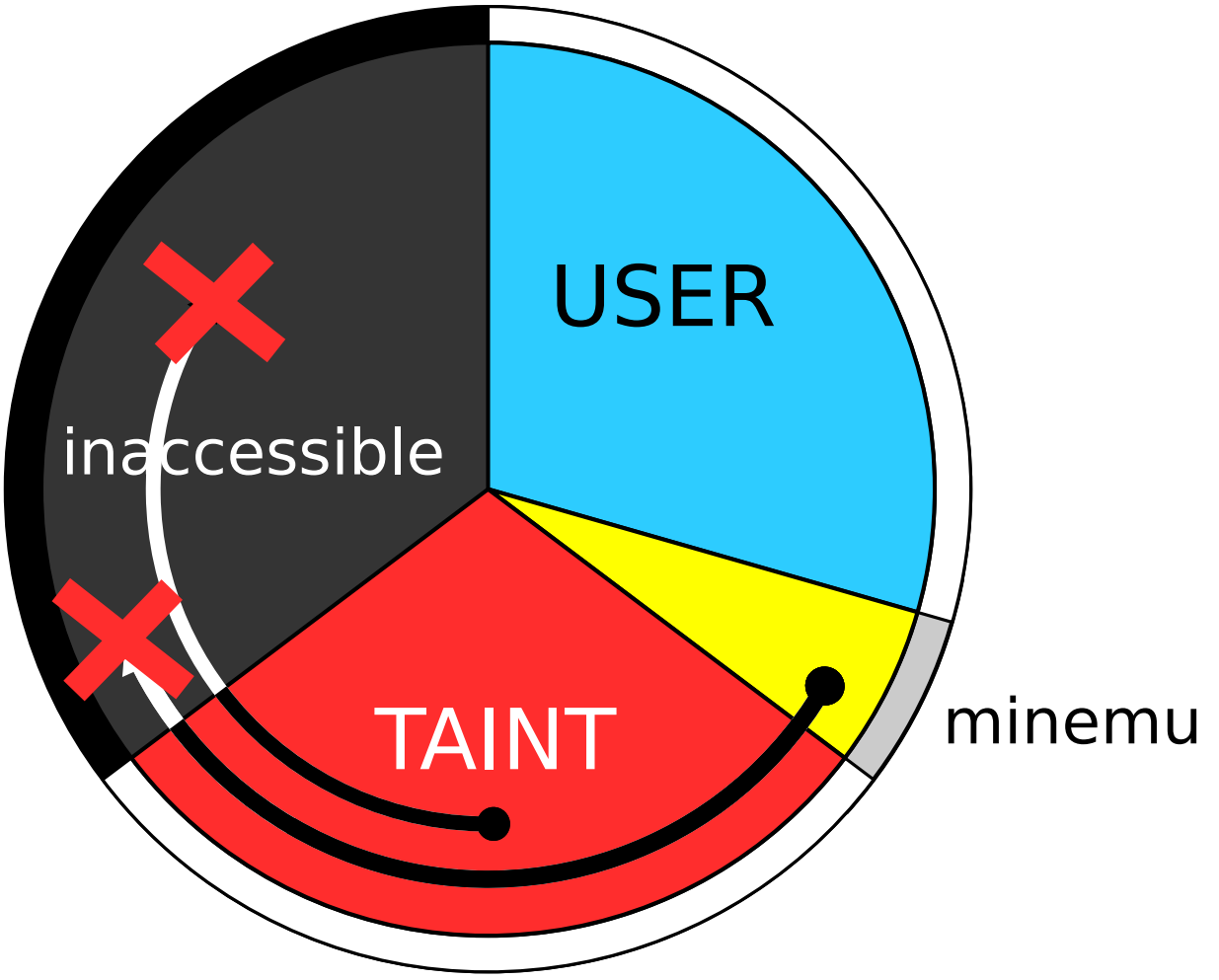
Memory layout (minemu)



Memory layout (minemu)



Memory layout (minemu)



Addressing shadow memory

```
mov EAX, (EDX)
```

Addressing shadow memory

```
mov EAX, (EDX)

address:

    EDX
```

Addressing shadow memory

```
mov EAX, (EDX)

address:

    EDX

taint:

    EDX+const
```

Addressing shadow memory

```
mov EAX, (EDX+EBX*4)
```

Addressing shadow memory

```
mov EAX, (EDX+EBX*4)

address:

    EDX+EBX*4
```

Addressing shadow memory

```
mov EAX, (EDX+EBX*4)

address:

    EDX+EBX*4

taint:

    EDX+EBX*4+const
```

Addressing shadow memory

```
push ESI
```

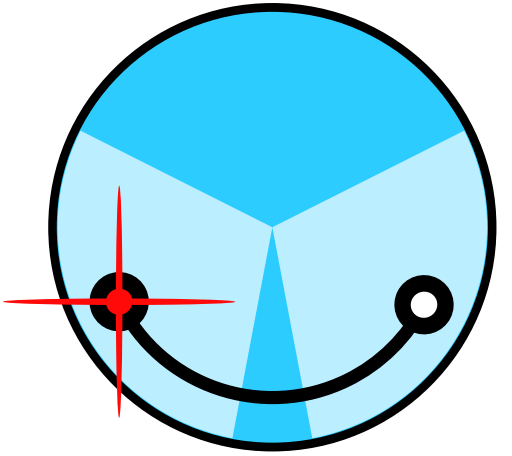
Addressing shadow memory

```
push ESI

address:

    ESP
```

Addressing shadow memory

```
push ESI

address:

    ESP

taint:

    ESP+const
```

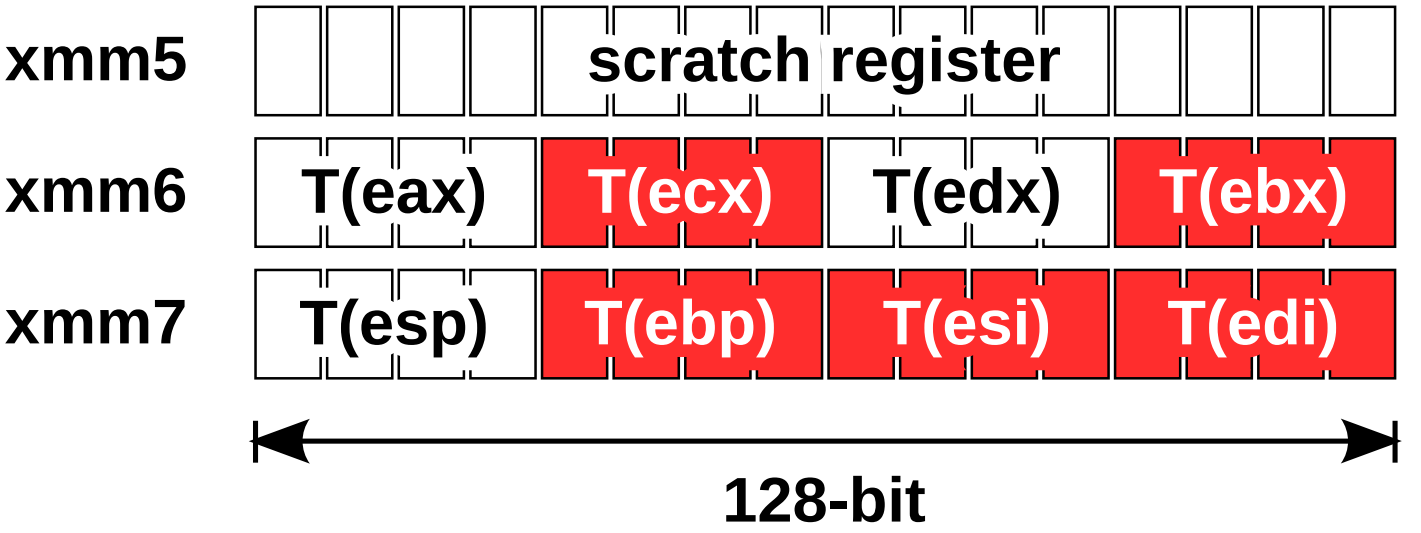
Is this slowness fundamental?



minemu

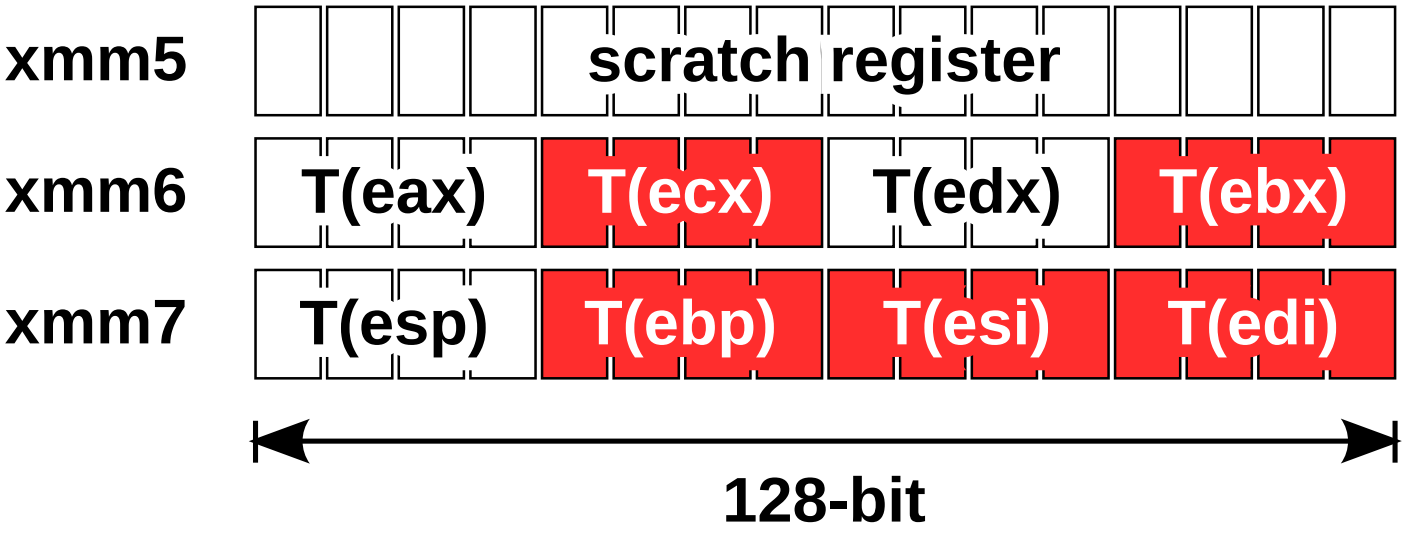
- memory layout
- use SSE registers to hold taint
- fast emulator

Taint propagation in SSE registers



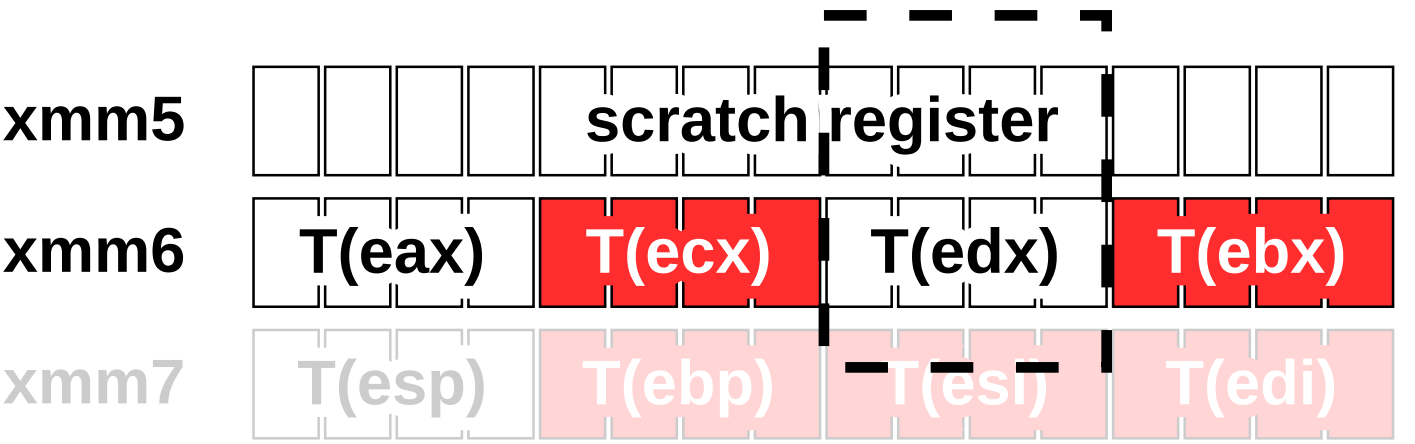
Taint propagation in SSE registers

```
add EDX, x
```



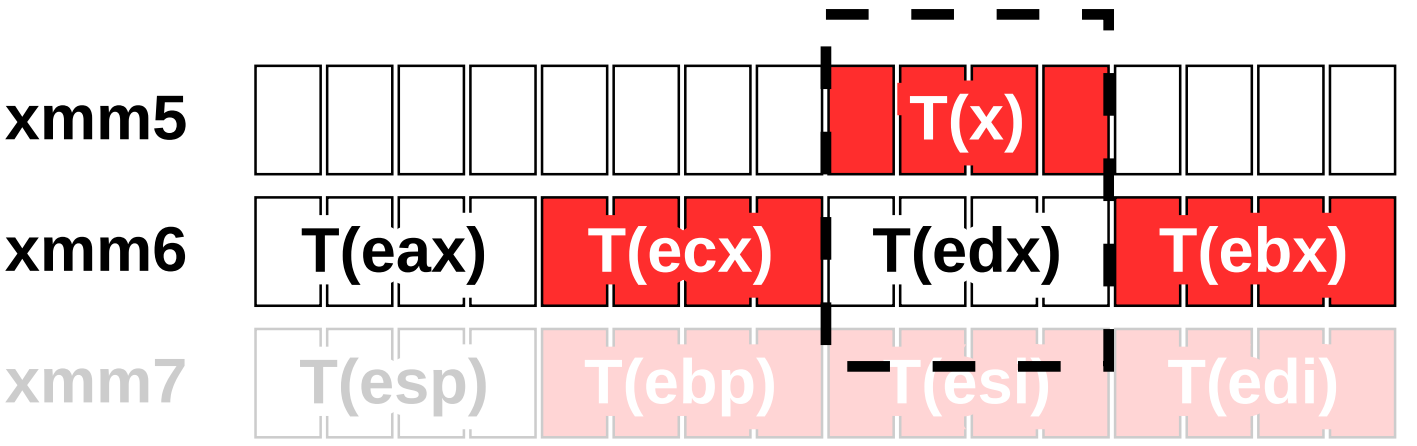
Taint propagation in SSE registers

```
add EDX, x
```



Taint propagation in SSE registers

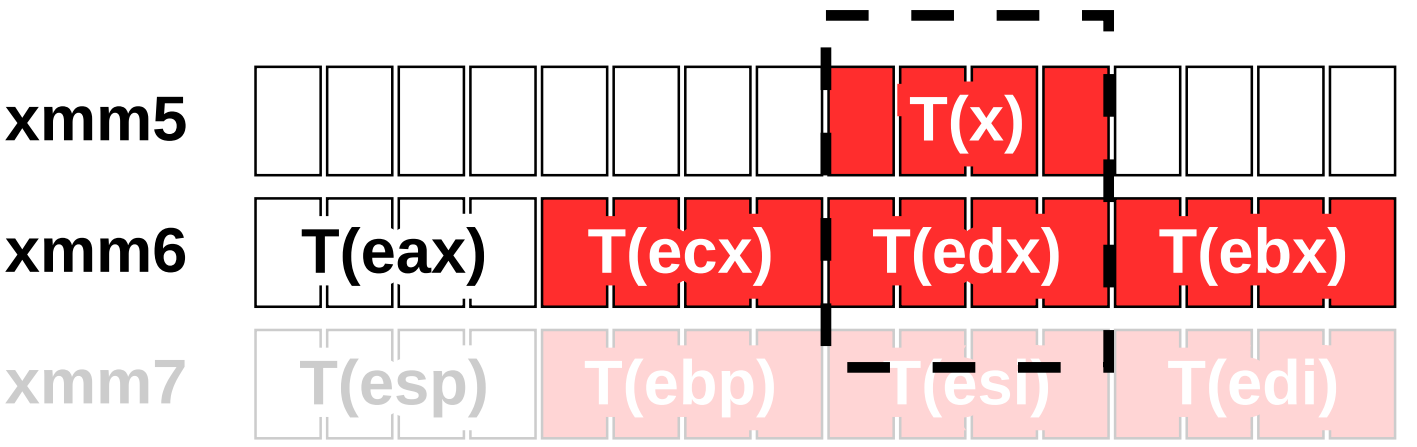
`add EDX, x`



`vector insert`

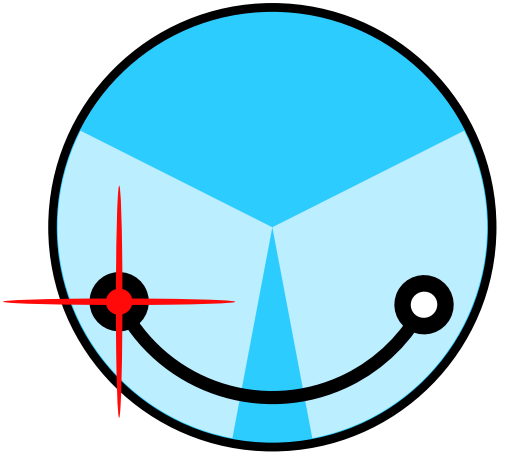
Taint propagation in SSE registers

```
add EDX, x
```



or

Is this slowness fundamental?



minemu

- memory layout
- use SSE registers to hold taint
- fast emulator

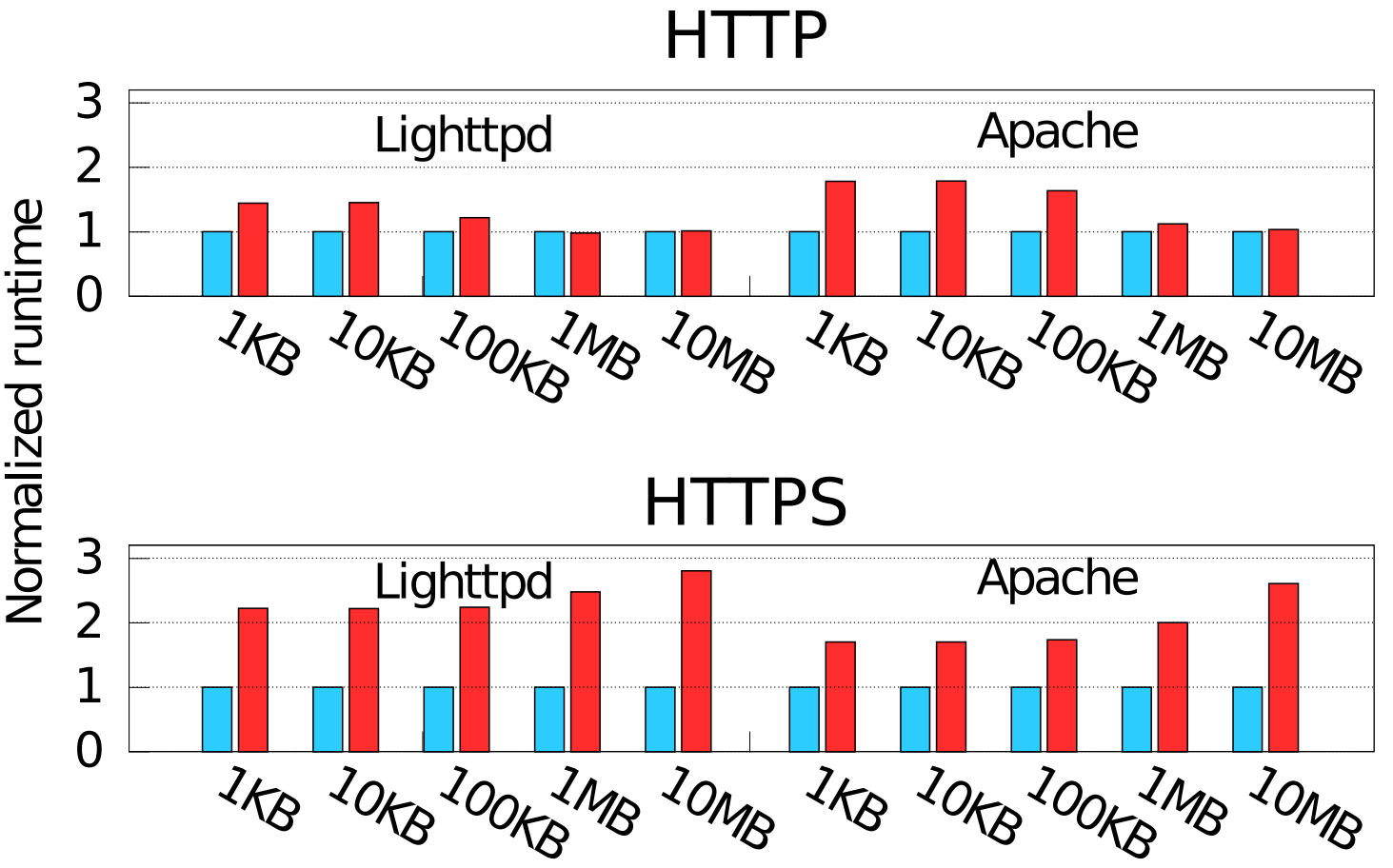
Emulator

- translates large code chunks
- keeps register state the same
- aggressive caching

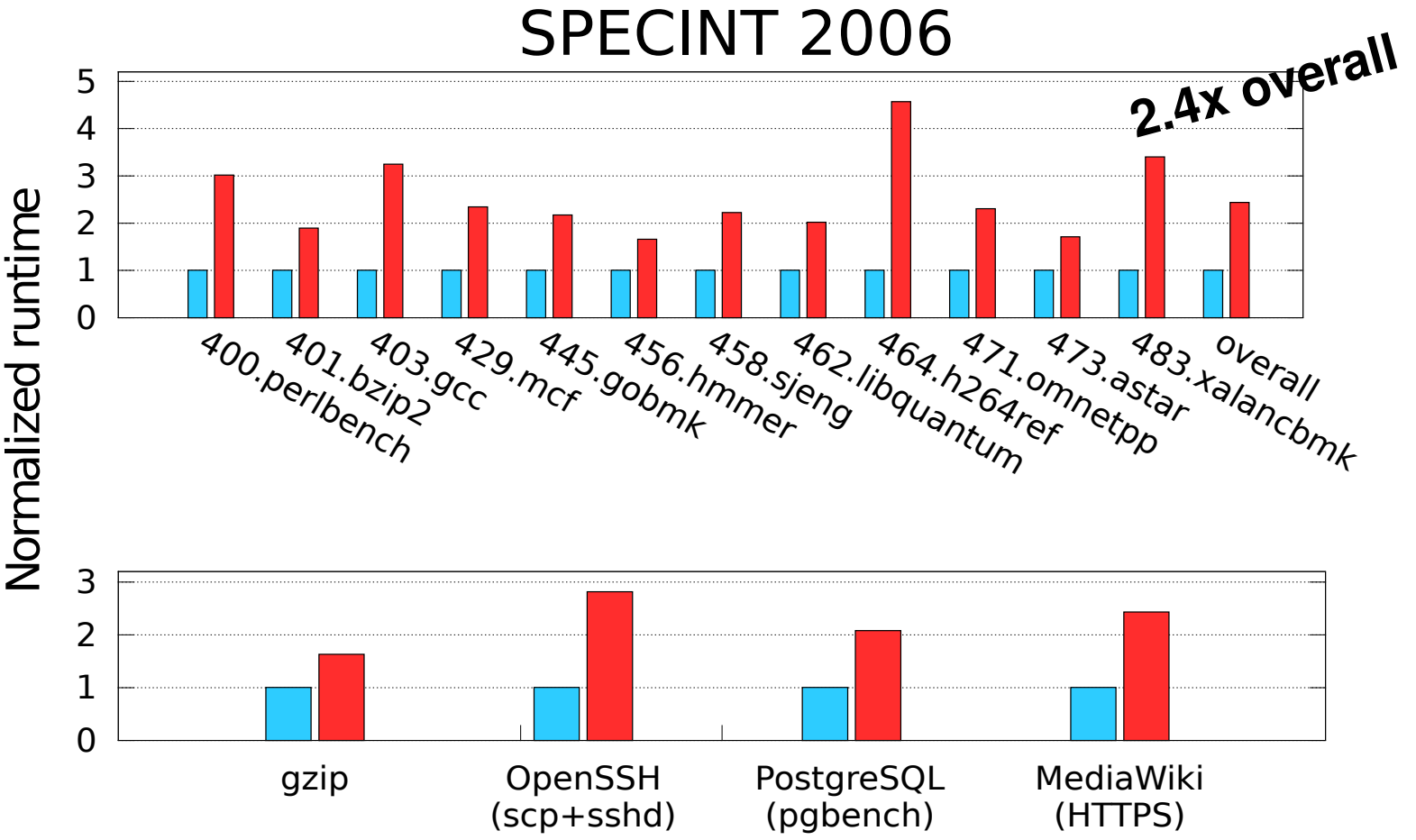
Effectiveness

Application	Type of vulnerability	Security advisory
Snort 2.4.0	Stack overflow	CVE-2005-3252
Cyrus imapd 2.3.2	Stack overflow	CVE-2006-2502
Samba 3.0.22	Heap overflow	CVE-2007-2446
Nginx 0.6.32	Buffer underrun	CVE-2009-2629
Memcached 1.1.12	Heap overflow	CVE-2009-2415
Proftpd 1.3.3a	Stack overflow	CVE-2010-4221
Samba 3.2.5	Heap overflow	CVE-2010-2063
Ncompress 4.2.4	Stack overflow	CVE-2001-1413
Iwconfig V.26	Stack overflow	CVE-2003-0947
Aspell 0.50.5	Stack overflow	CVE-2004-0548
Htget 0.93	Stack overflow	CVE-2004-0852
Socat 1.4	Format string	CVE-2004-1484
Aeon 0.2a	Stack overflow	CVE-2005-1019
Exim 4.41	Stack overflow	EDB-ID#796
Htget 0.93	Stack overflow	
Tipxd 1.1.1	Format string	OSVDB-ID#12346

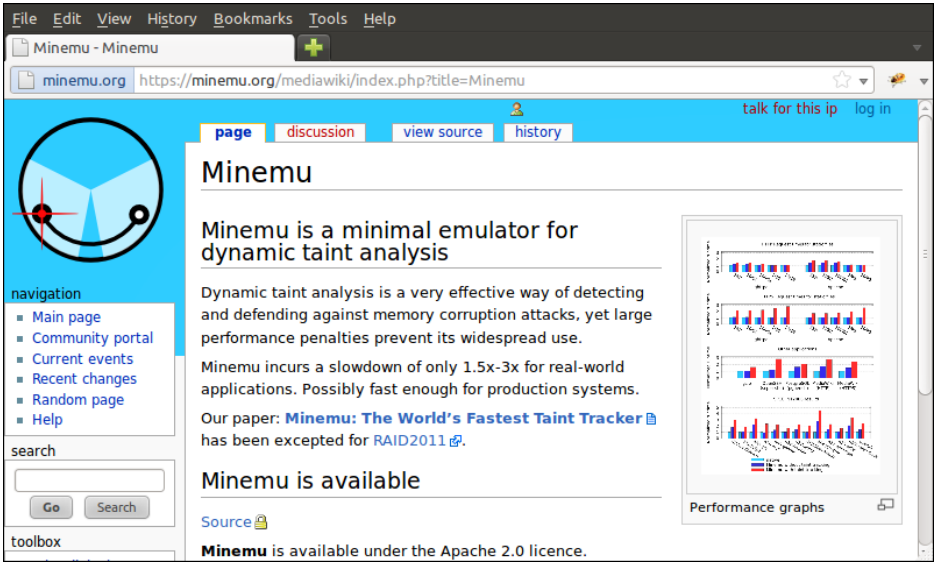
Performance



Performance



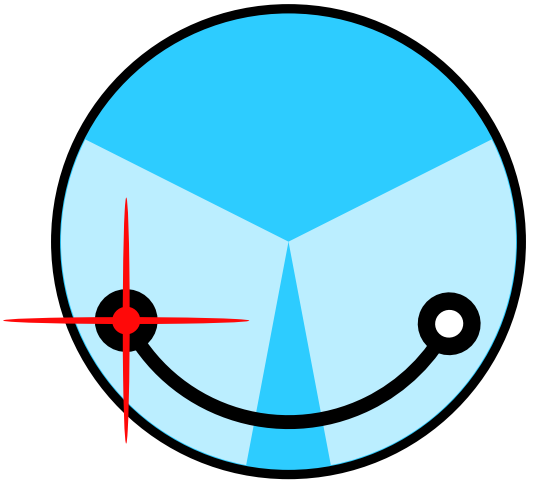
Minemu is available now



website runs on minemu

source code is available

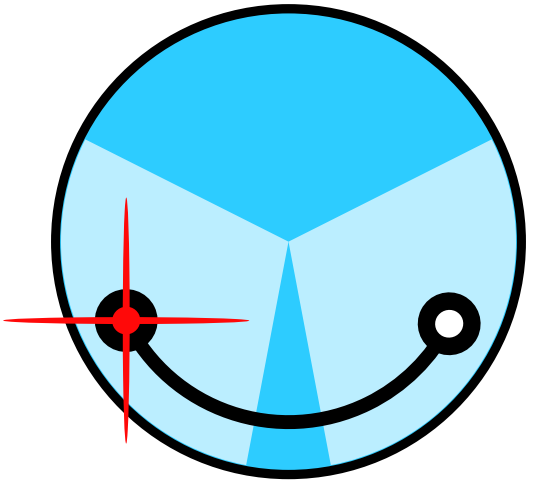
Apache 2.0 licenced



Minemu

`https://minemu.org/`

The world's fastest taint tracker

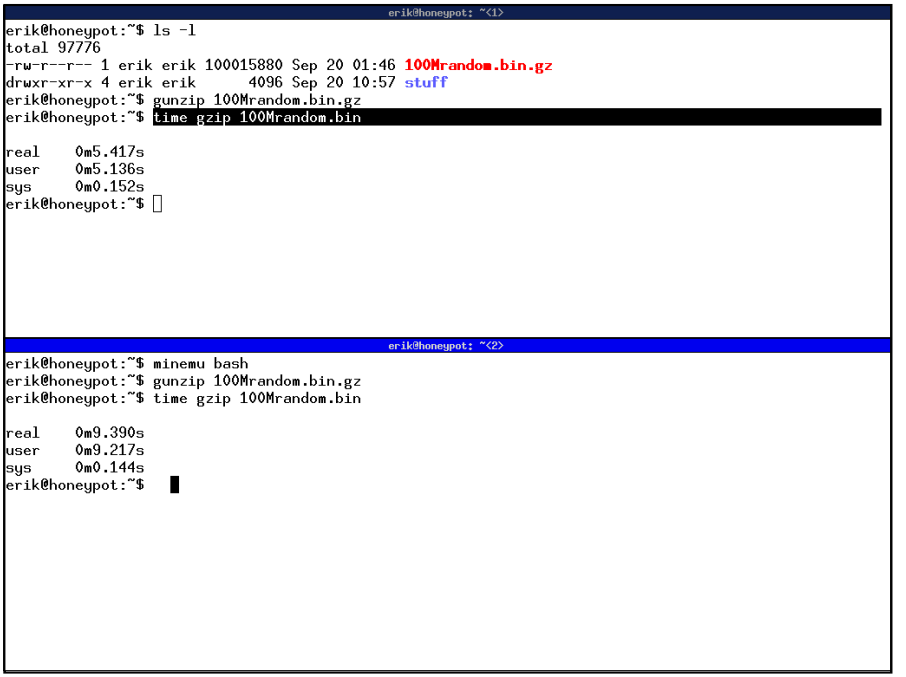


Minemu

`https://minemu.org/`

The world's fastest taint tracker (until the next conference?)

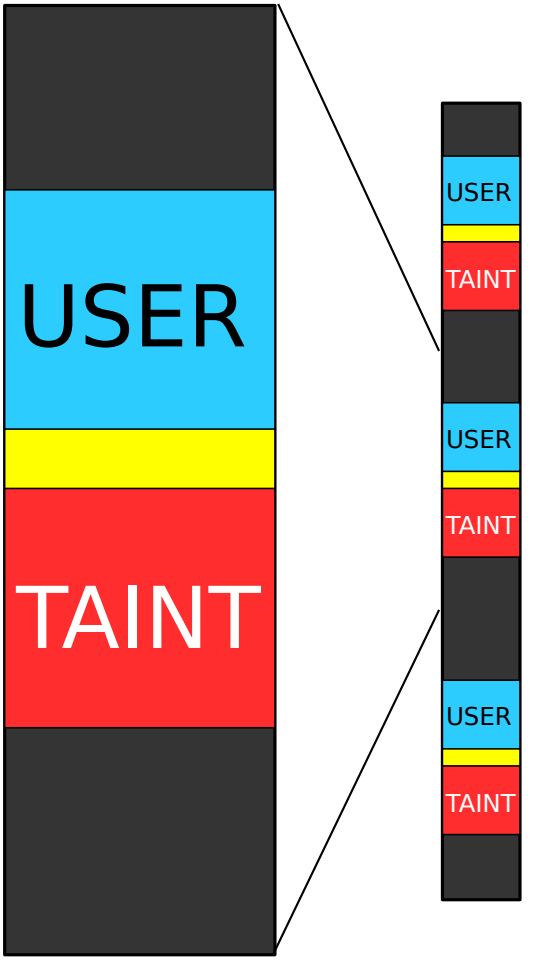
Demo


erik@honeypot: ~<1>
erik@honeypot:~$ ls -l
total 97776
-rw-r--r-- 1 erik erik 100015880 Sep 20 01:46 100Mrandom.bin.gz
drwxr-xr-x 4 erik erik   4096 Sep 20 10:57 stuff
erik@honeypot:~$ gunzip 100Mrandom.bin.gz
erik@honeypot:~$ time gzip 100Mrandom.bin
real   0m5.417s
user   0m5.136s
sys   0m0.152s
erik@honeypot:~$
erik@honeypot: ~<2>
erik@honeypot:~$ minemu bash
erik@honeypot:~$ gunzip 100Mrandom.bin.gz
erik@honeypot:~$ time gzip 100Mrandom.bin
real   0m9.390s
user   0m9.217s
sys   0m0.144s
erik@honeypot:~$

Threads

- duplicate cache structures
- keep cache base address in SSE
- code-deletion corner case

Memory layout (64 bit)



Memory layout (minemu)