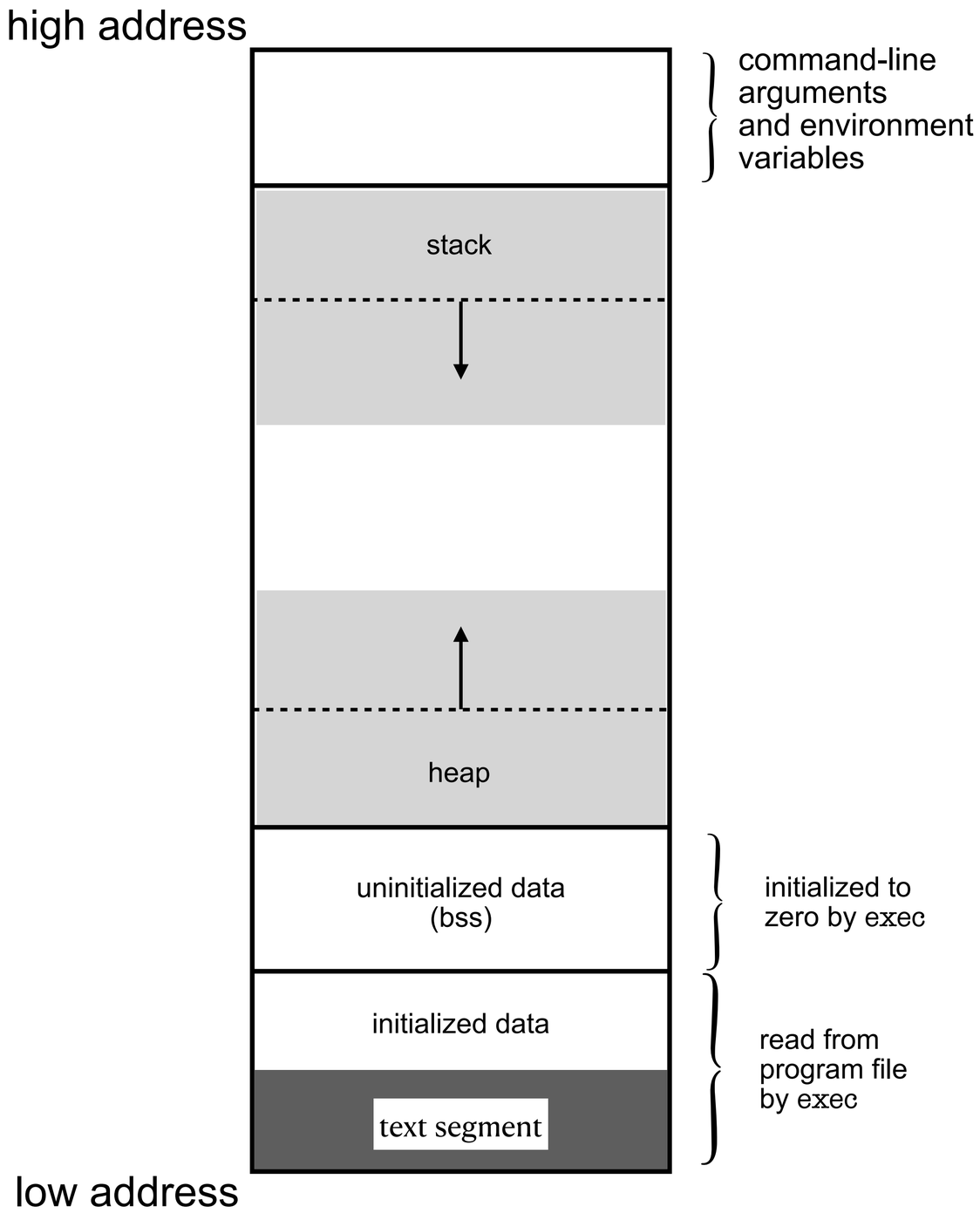
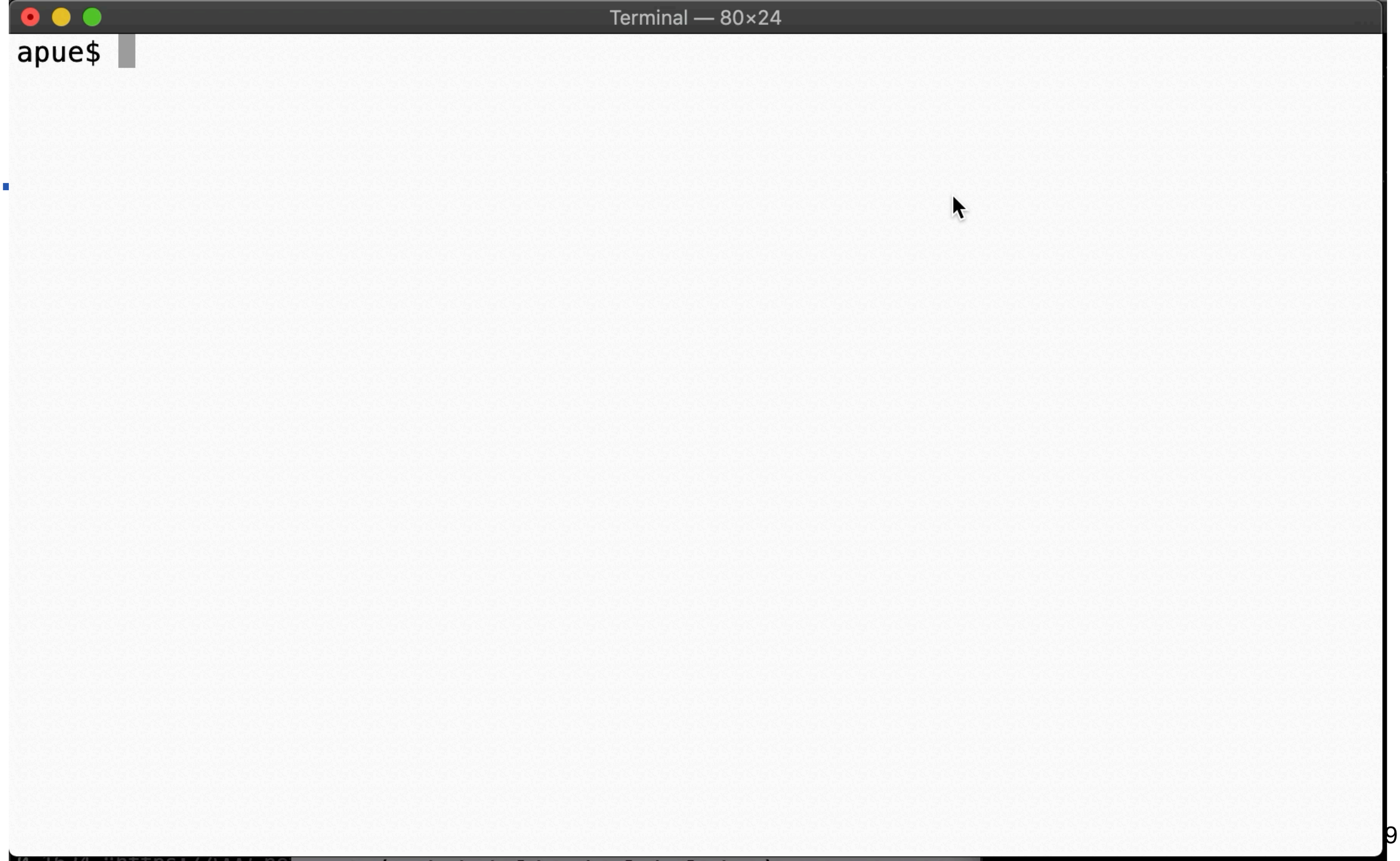
Advanced Programming in the UNIX Environment

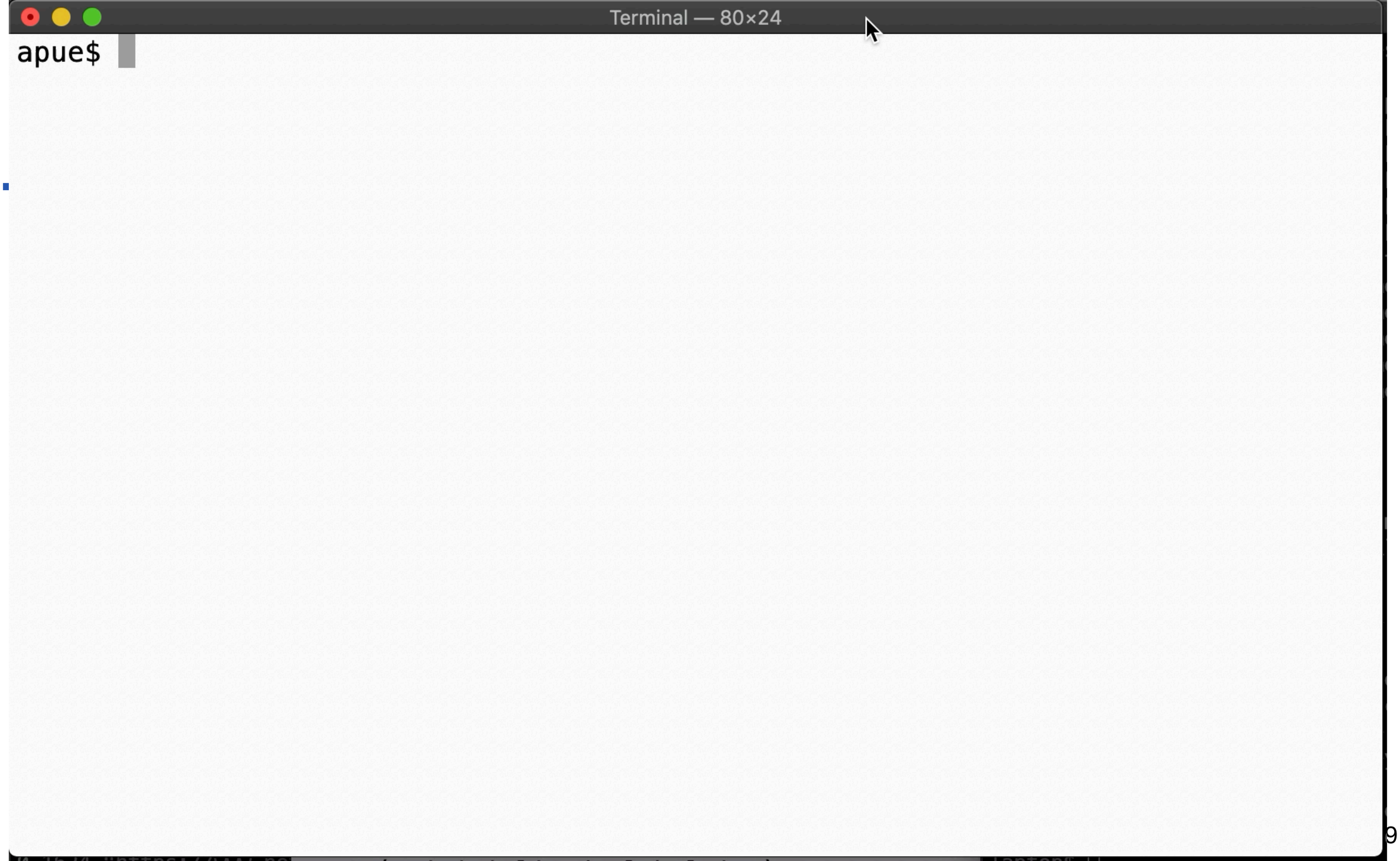
Week 06, Segment 1:
Memory Layout of a Process

Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/631/

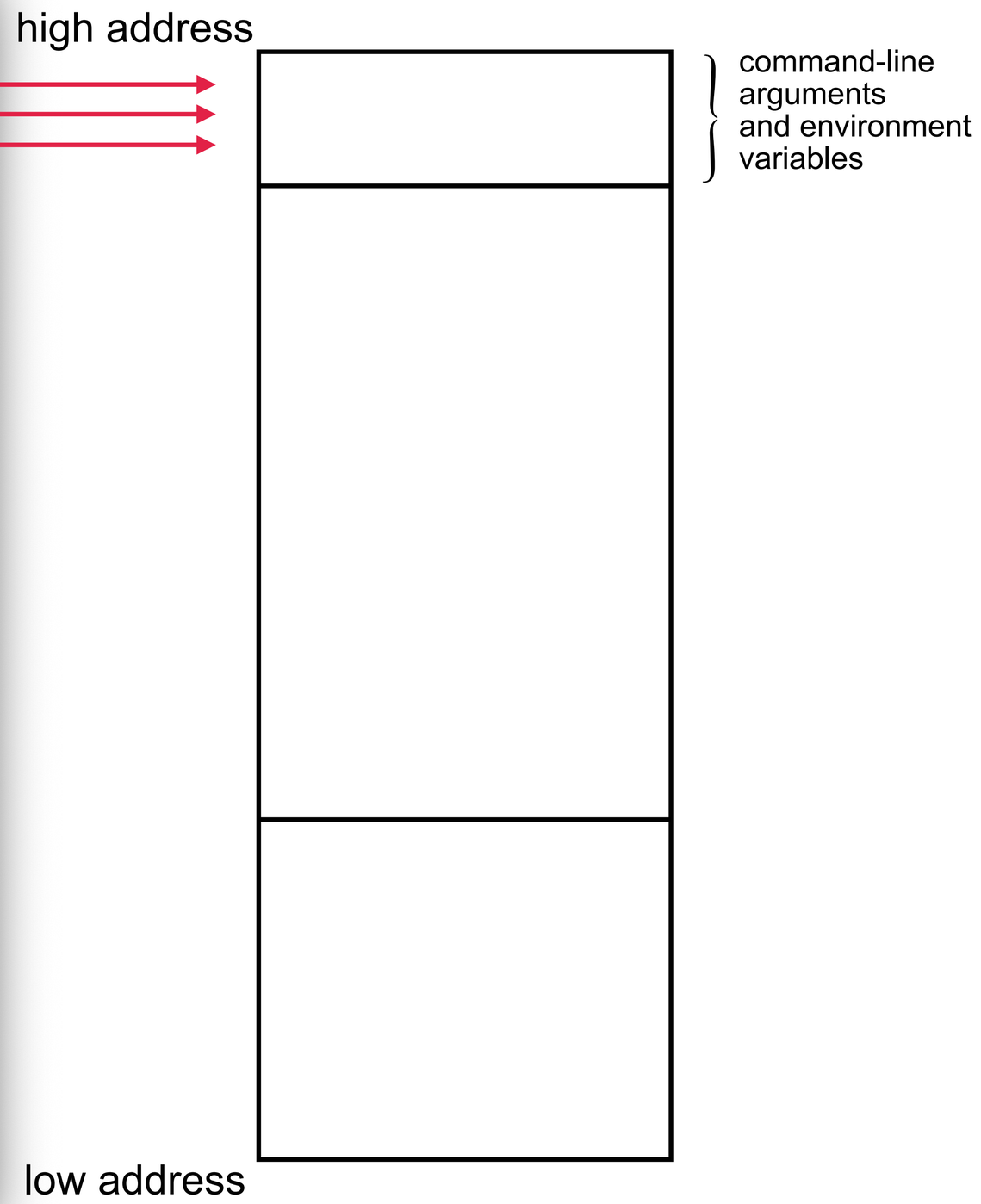

high address
command-line
arguments
and environment
variables
stack
heap
uninitialized data
(bss)
initialized to
zero by exec
initialized data
text segment
read from
program file
by exec
low address


Terminal — 80×24
apue$

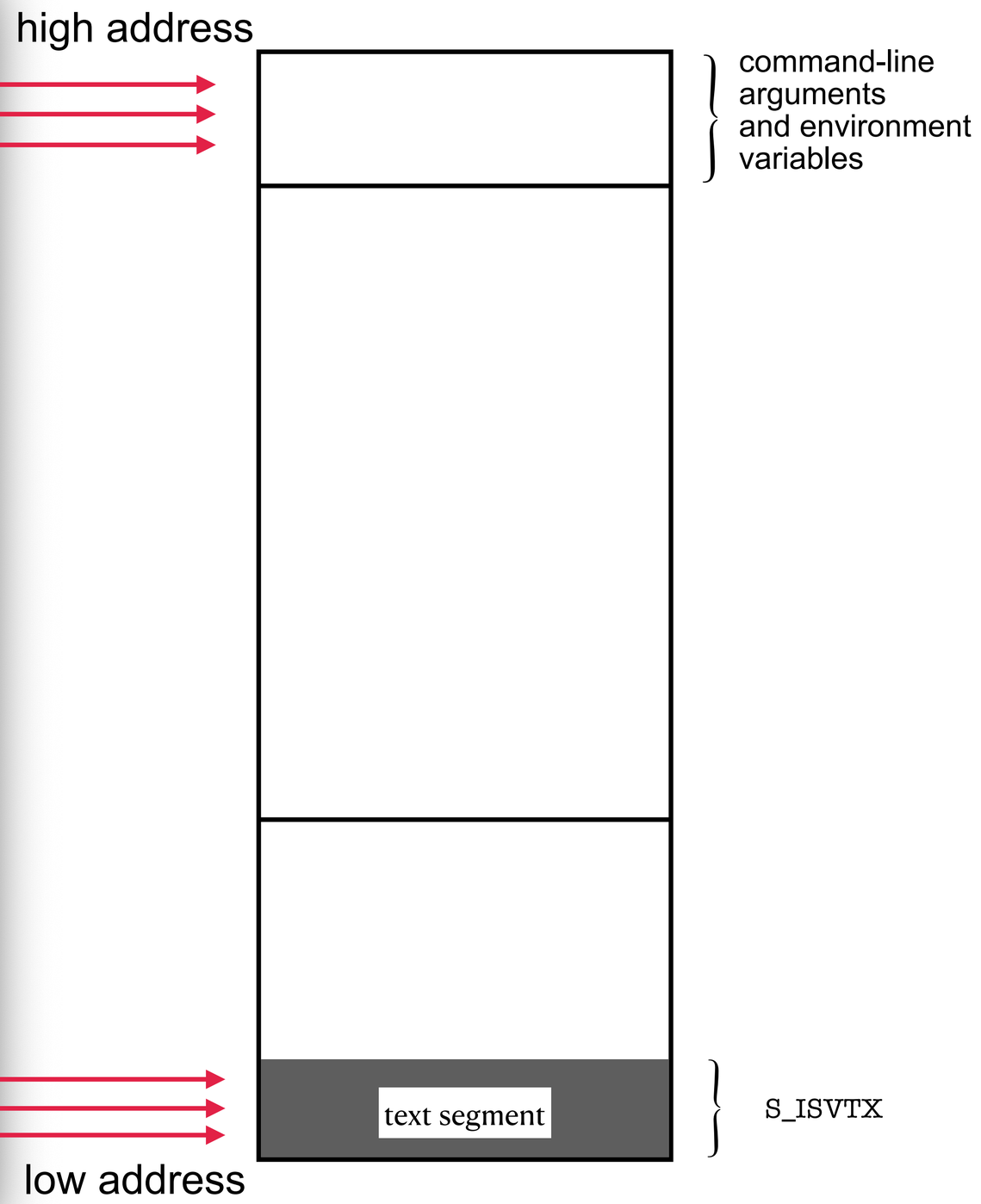

Terminal — 80×24
apue$

Terminal — 80×44

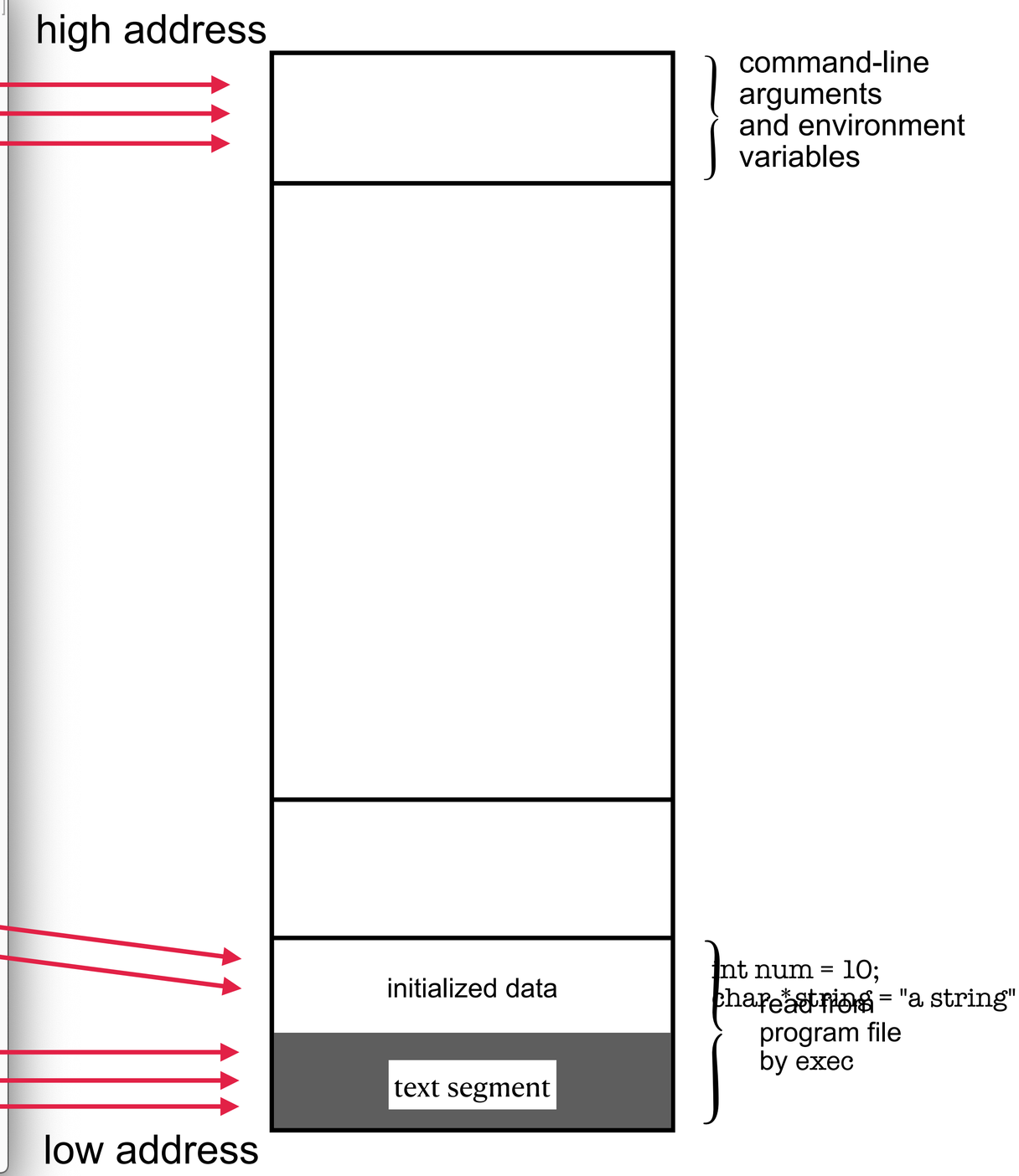
```
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                   : 0x7F7FFF8A82B8
last arg at                          argv[1]    : 0x7F7FFF8A82B0
first arg at                         argv[0]    : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                   : 0x7F7FFF8A8254
func_array[] ends at                            : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                         : 0x7F7FFF8A823C
argv at                                         : 0x7F7FFF8A8230
func2 (from main): frame at                     : 0x7F7FFF8A821C
func frame at                                   : 0x7F7FFF8A821C
static int n within func at                     : 0x      601A0C
func2 (from func): frame at                     : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                           : 0x76AC2C04B020
malloced area begins at                         : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                 : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at              : 0x      601A98
string2 (uninitialized global char *) at        : 0x      601A90
extern **environ at                             : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                 : 0x      601A08
string (initialized global char *) at           : 0x      601A00

Text Segment:
-------------
func2 (function) at                             : 0x      400E53
func (function) at                              : 0x      400E02
main (function) at                              : 0x      400B1A

apue$
```



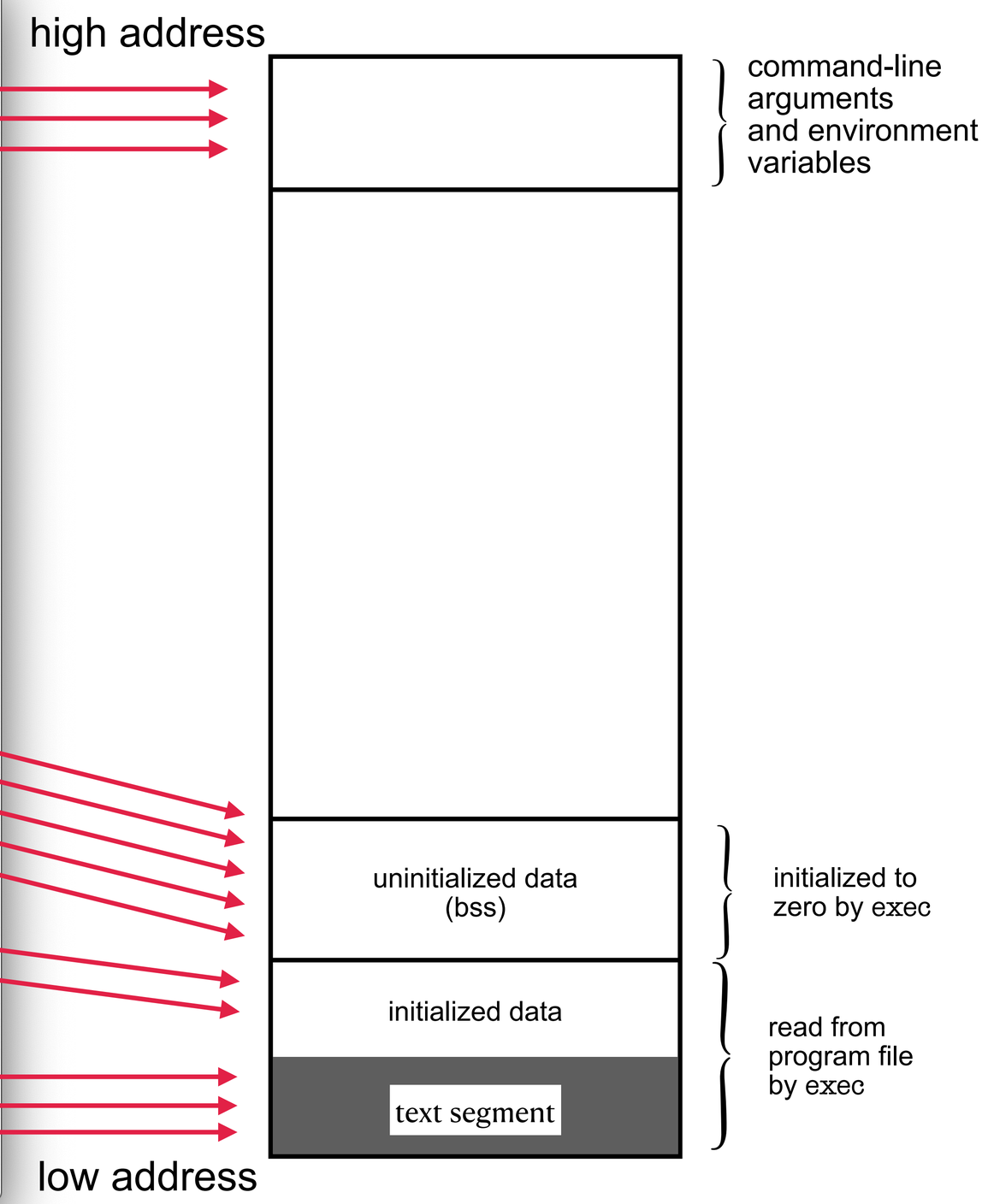
```
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```



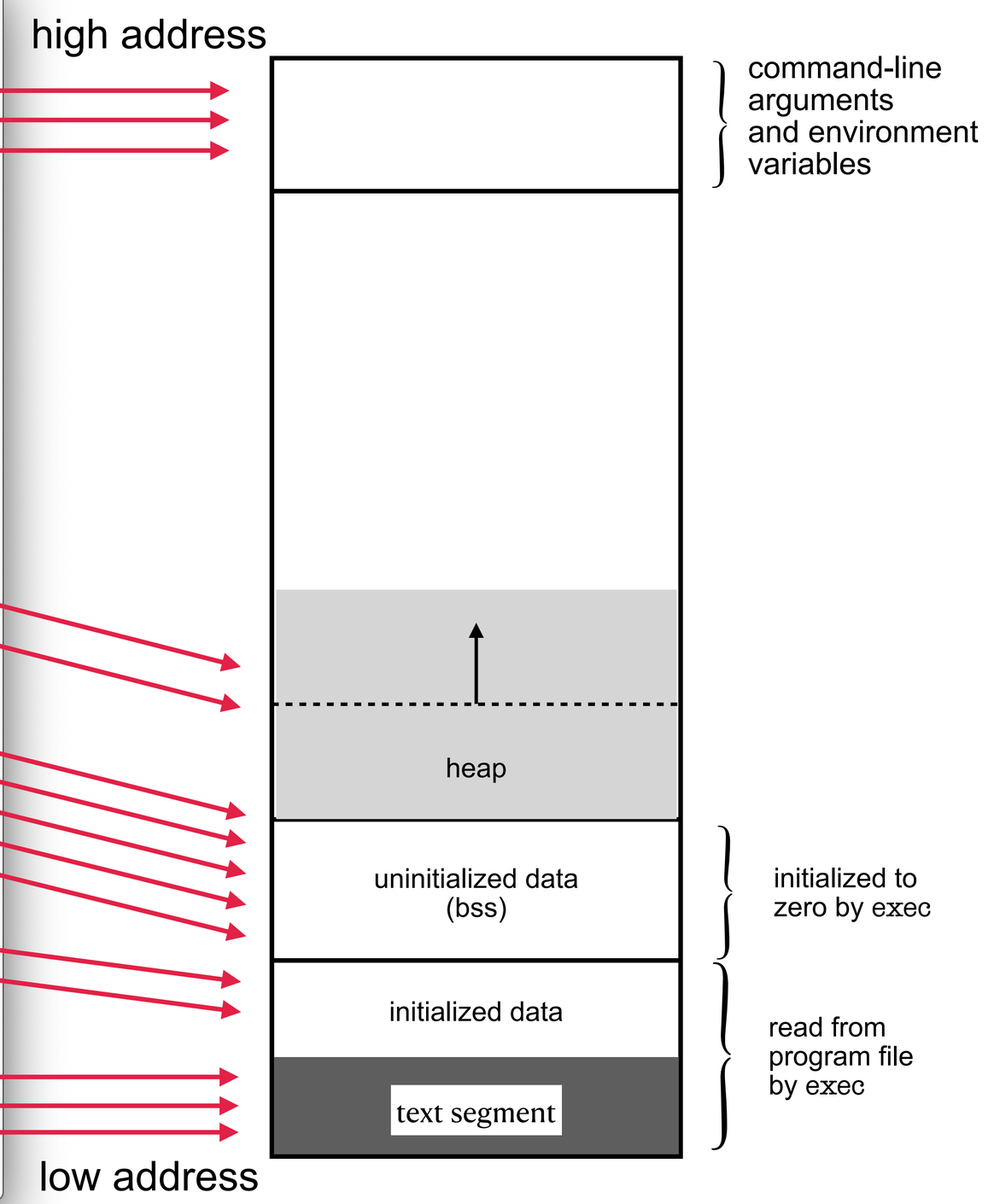
```
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```



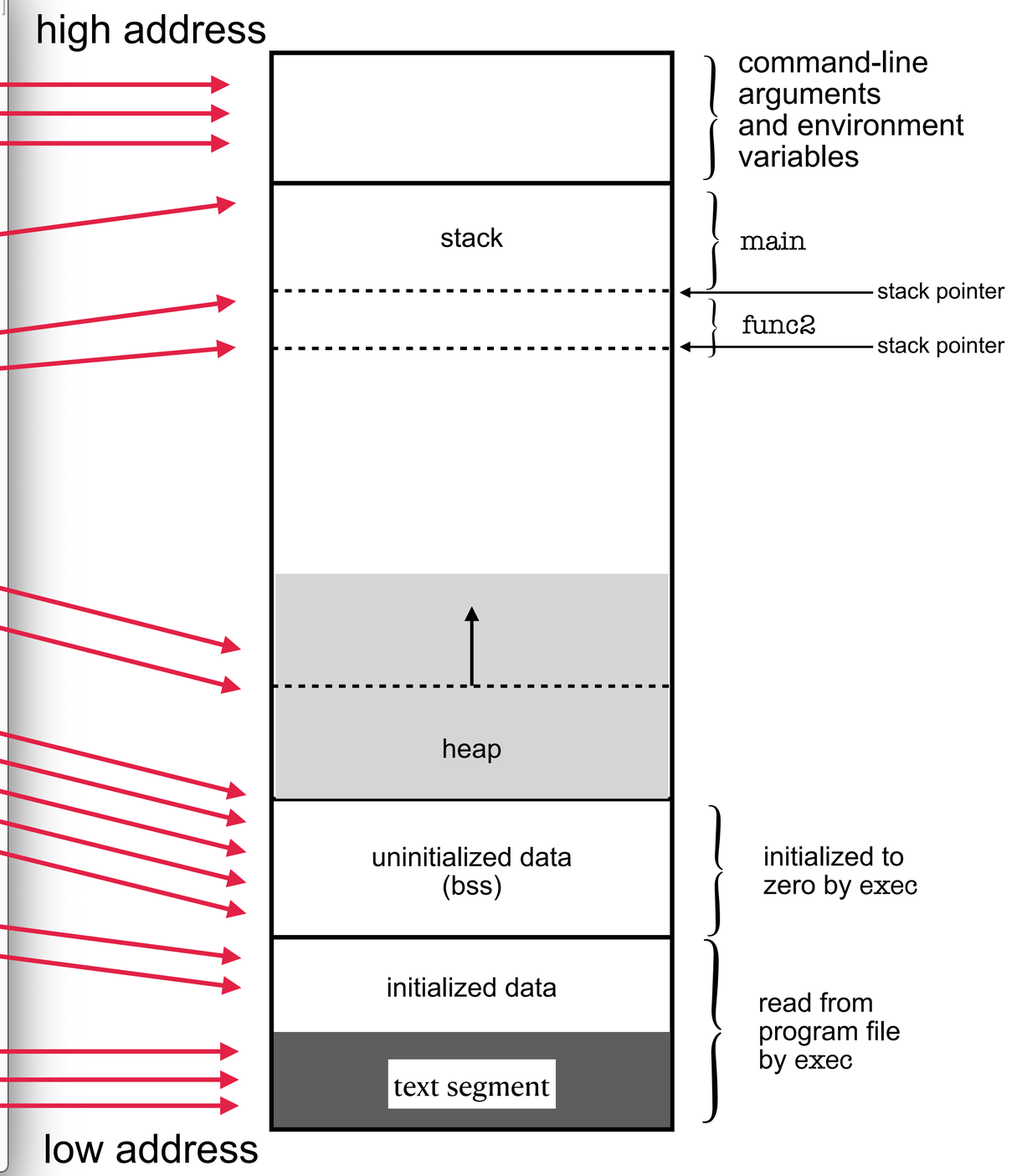
```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):                                  ARRAY_SIZE = 16
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```



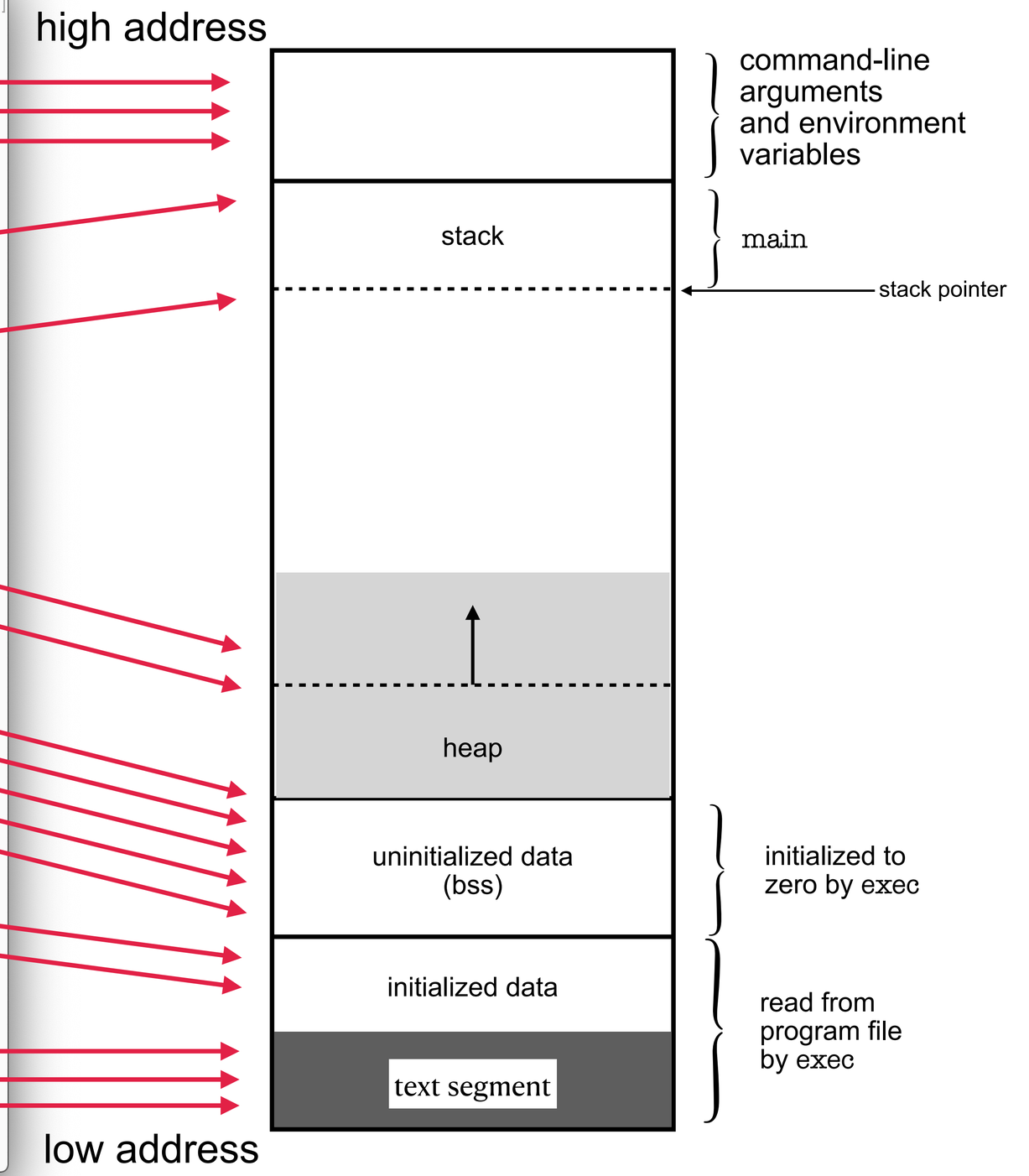
```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:                                                      MALLOC_SIZE = 32
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```



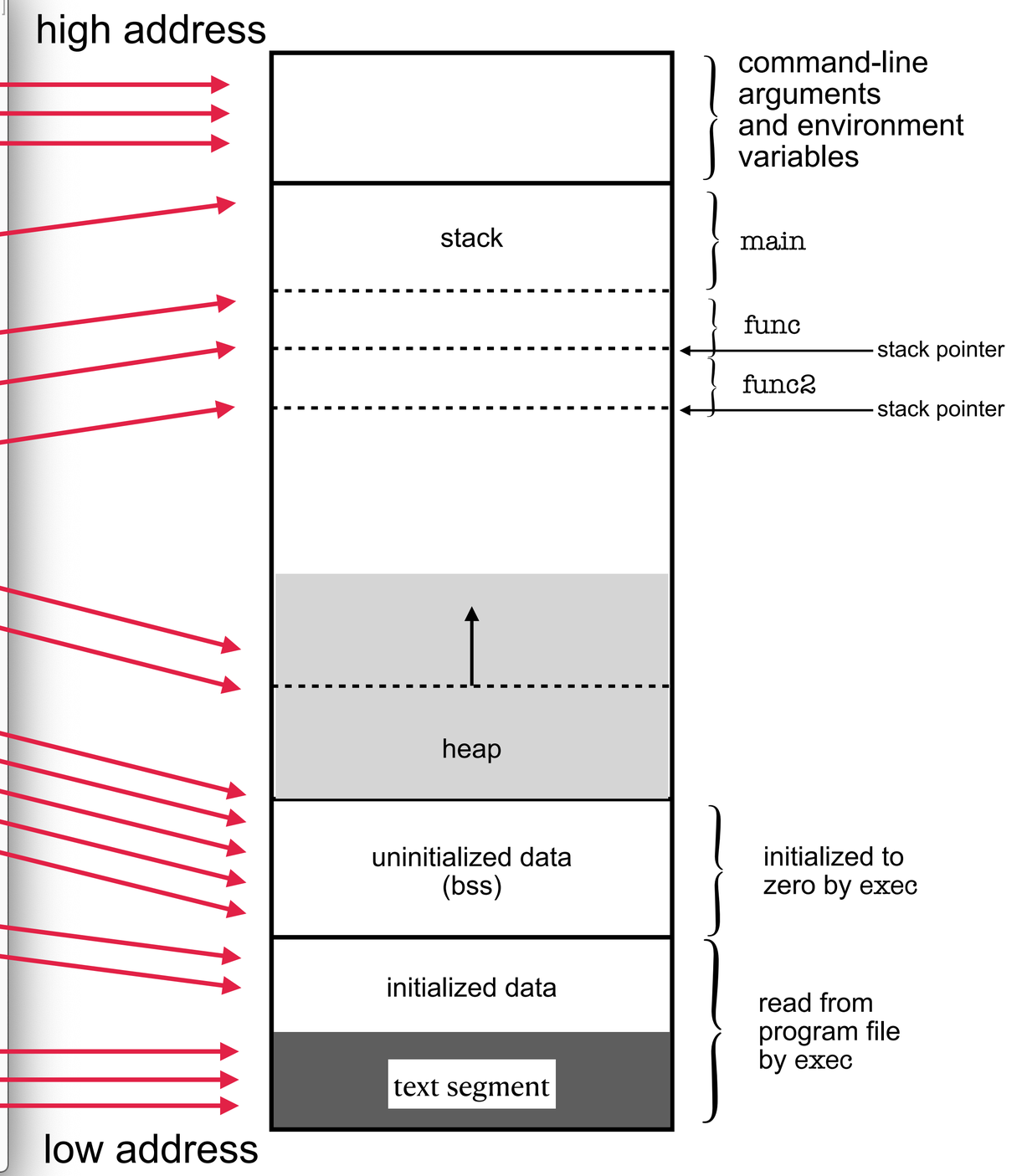
```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------                                                     ARRAY_SIZE = 16
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```



```
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```

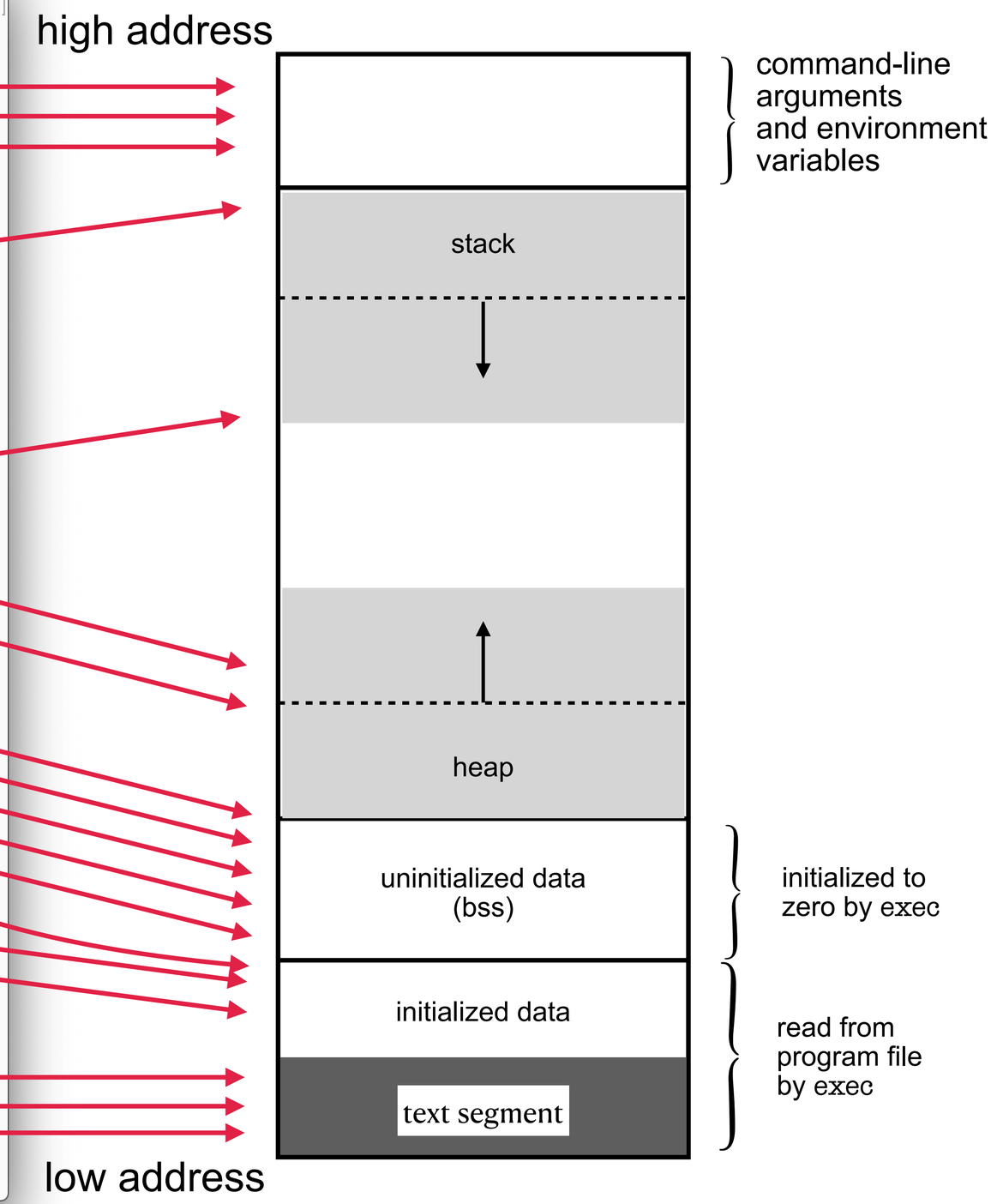


```
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```

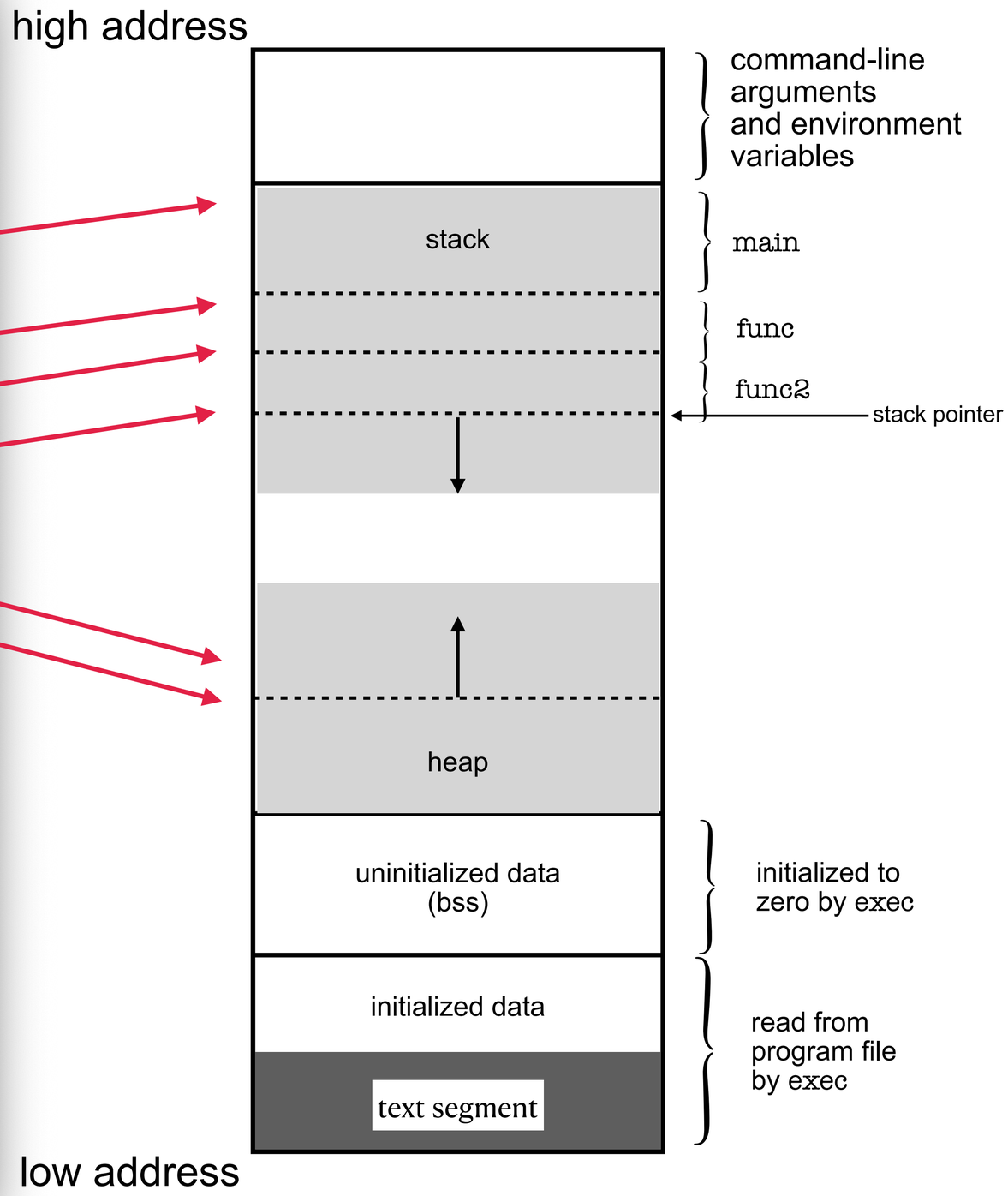


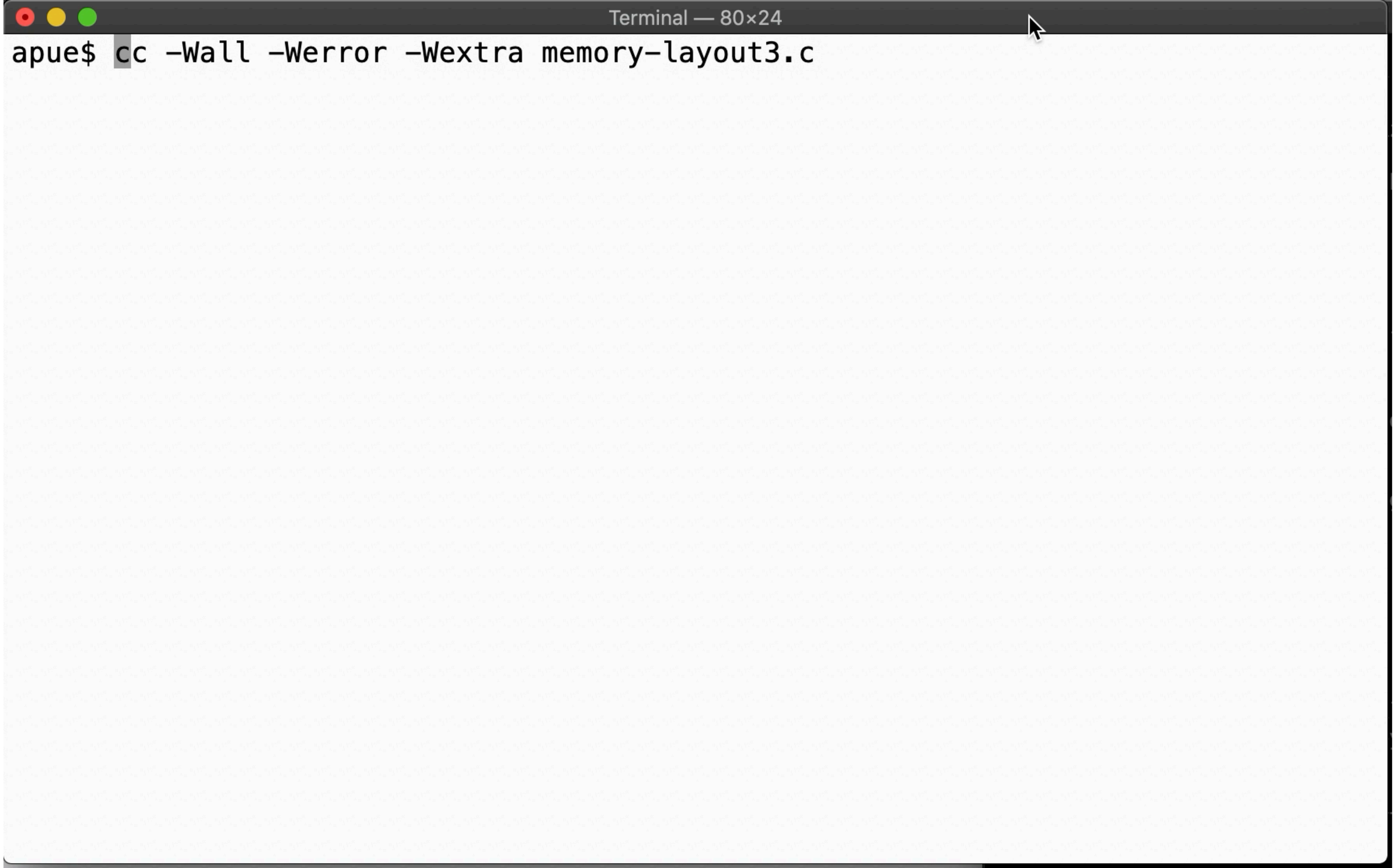
Terminal — 80×44

```
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A81EC
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81EC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```

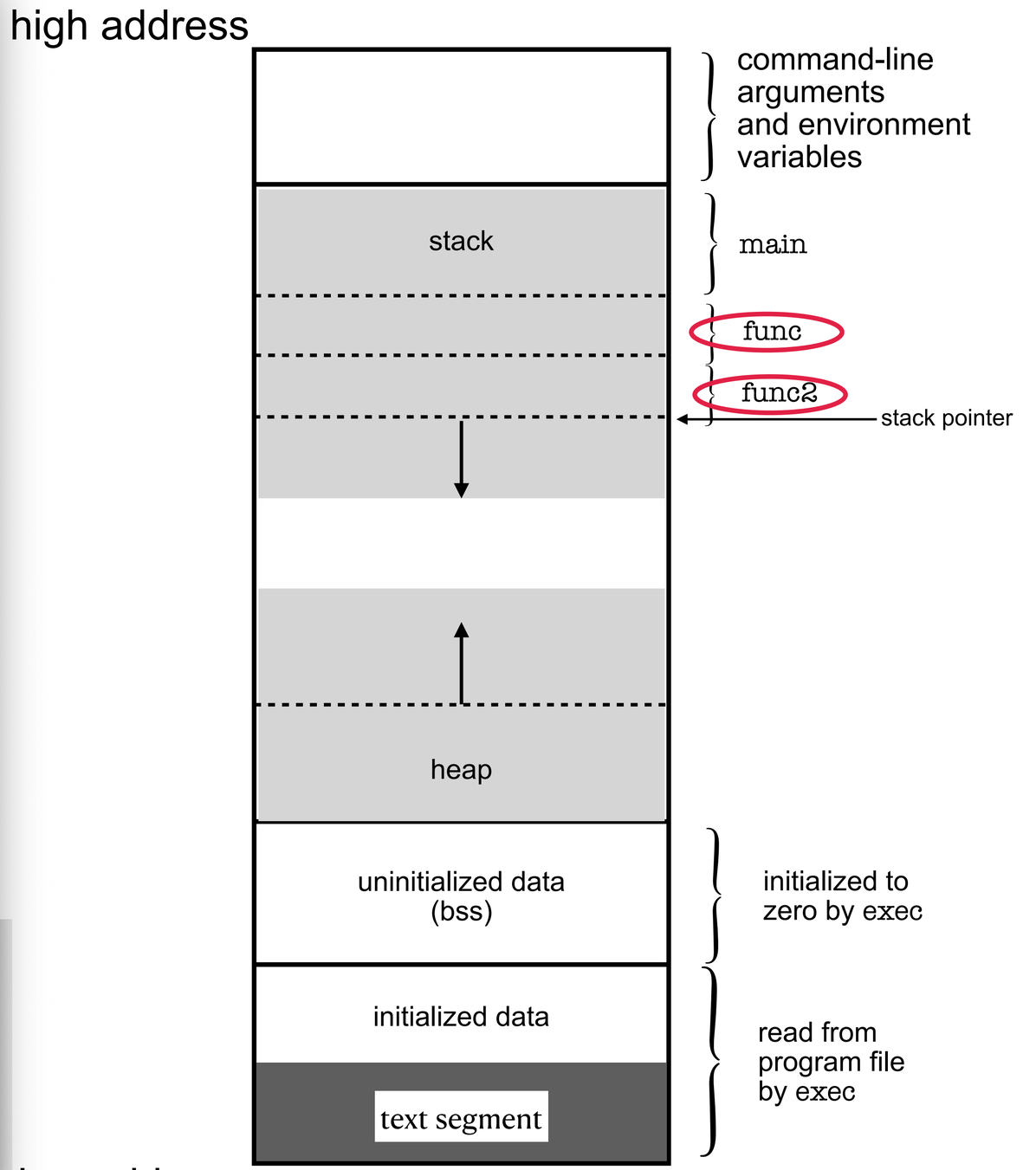


```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF8A82B8
last arg at                                            : 0x7F7FFF8A82B0
first arg at                                           : 0x7F7FFF8A82A8

Stack:
------
First variable inside main at                          : 0x7F7FFF8A8254
func_array[] ends at                                   : 0x7F7FFF8A8250
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF8A8240
argc at                                                : 0x7F7FFF8A823C
argv at                                                : 0x7F7FFF8A8230
func2 (from main): frame at                            : 0x7F7FFF8A821C
func frame at                                          : 0x7F7FFF8A821C
static int n within func at                            : 0x      601A0C
func2 (from func): frame at                            : 0x7F7FFF8A81FC

Heap:
-----
malloced area ends at                                  : 0x76AC2C04B020
malloced area begins at                                : 0x76AC2C04B000

Uninitialized Data (BSS):
-------------------------
array[] ends at                                        : 0x      601AB0
array[] (uninitialized, fixed-size char * on BSS) from : 0x      601AA0
num2 (uninitialized global int) at                     : 0x      601A98
string2 (uninitialized global char *) at               : 0x      601A90
extern **environ at                                    : 0x      601A80

Initialized Data:
-----------------
num (initialized global int) at                        : 0x      601A08
string (initialized global char *) at                  : 0x      601A00

Text Segment:
-------------
func2 (function) at                                    : 0x      400E53
func (function) at                                     : 0x      400E02
main (function) at                                     : 0x      400B1A

apue$
```

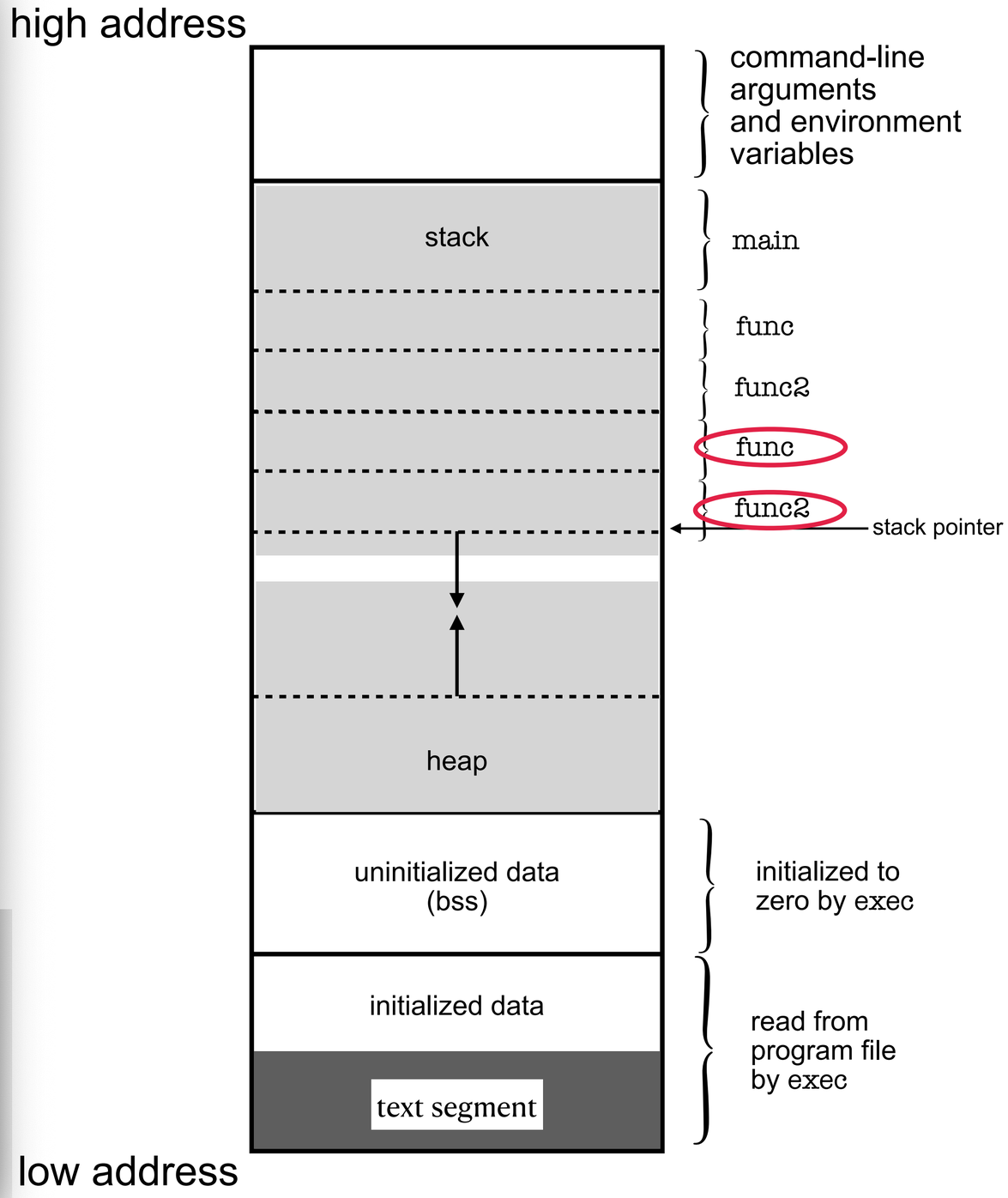



Terminal — 80×24
apue$ cc -Wall -Werror -Wextra memory-layout3.c

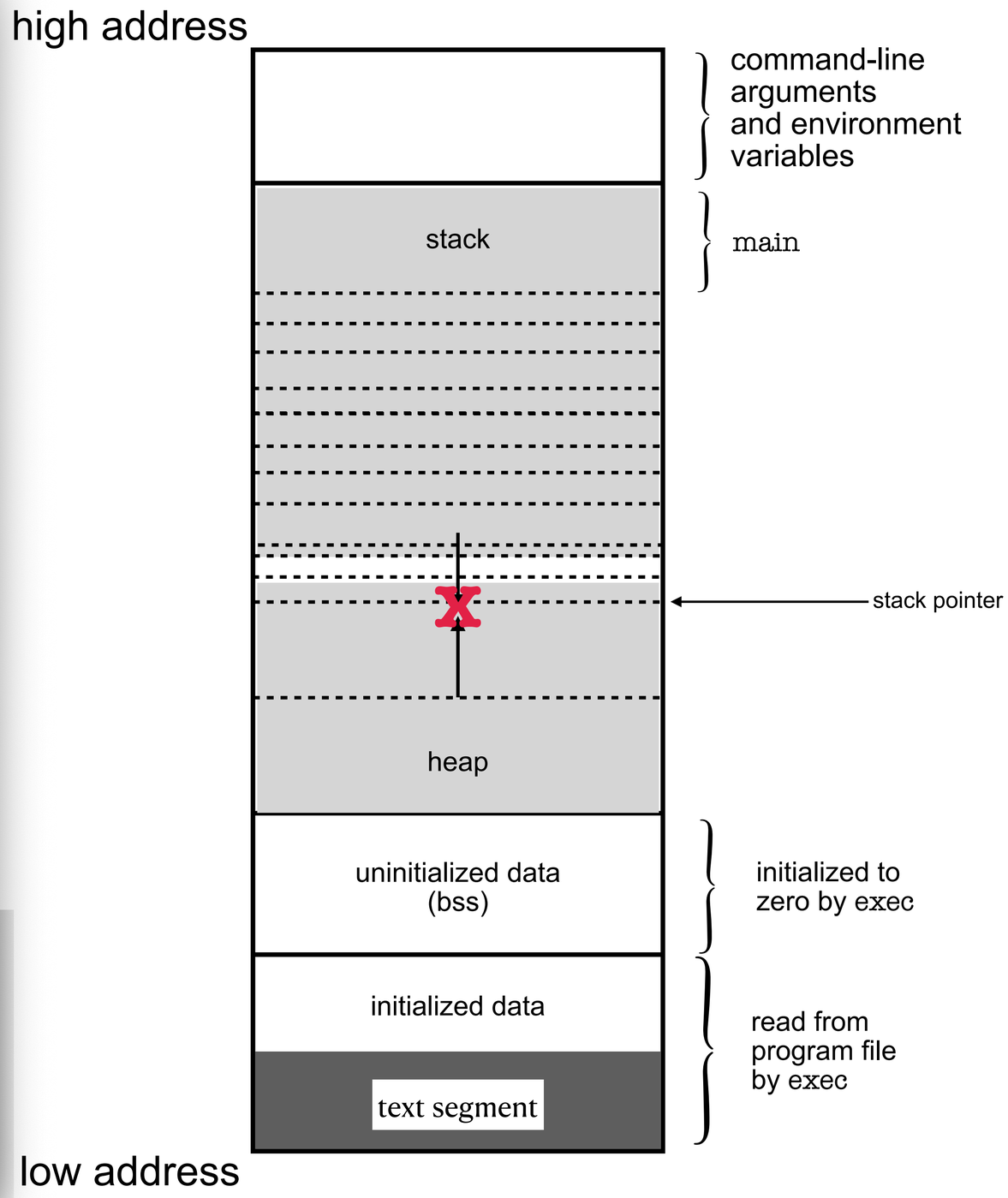
```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF3346A8
last arg at                                            : 0x7F7FFF3346A0
first arg at                                           : 0x7F7FFF334698

Stack:
------
First variable inside main at                          : 0x7F7FFF334644
func_array[] ends at                                   : 0x7F7FFF334640
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF334630
argc at                                                : 0x7F7FFF33462C
argv at                                                : 0x7F7FFF334620
func2 (from main): frame at                            : 0x7F7FFF33460C
static int n within func at                            : 0x      601A3C
func (called     1 times): frame at                    : 0x7F7FFF3345D4
func2 (recursive): frame at                            : 0x7F7FFF3345AC
static int n within func at                            : 0x      601A3C
func (called     2 times): frame at                    : 0x7F7FFF334574
func2 (recursive): frame at                            : 0x7F7FFF33454C
static int n within func at                            : 0x      601A3C
func (called     3 times): frame at                    : 0x7F7FFF334514
func2 (recursive): frame at                            : 0x7F7FFF3344EC
static int n within func at                            : 0x      601A3C
func (called     4 times): frame at                    : 0x7F7FFF3344B4
func2 (recursive): frame at                            : 0x7F7FFF33448C
static int n within func at                            : 0x      601A3C
func (called     5 times): frame at                    : 0x7F7FFF334454
func2 (recursive): frame at                            : 0x7F7FFF33442C

      ...

func (called 43633 times): frame at                    : 0x7F7FFEF35BD4
func2 (recursive): frame at                            : 0x7F7FFEF35BAC
static int n within func at                            : 0x      601A3C
func (called 43634 times): frame at                    : 0x7F7FFEF35B74
func2 (recursive): frame at                            : 0x7F7FFEF35B4C
static int n within func at                            : 0x      601A3C
func (called 43635 times): frame at                    : 0x7F7FFEF35B14
func2 (recursive): frame at                            : 0x7F7FFEF35AEC
[1]   Segmentation fault (core dumped) ./a.out
apue$
```



```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF3346A8
last arg at                                            : 0x7F7FFF3346A0
first arg at                                           : 0x7F7FFF334698

Stack:
------
First variable inside main at                          : 0x7F7FFF334644
func_array[] ends at                                   : 0x7F7FFF334640
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF334630
argc at                                                : 0x7F7FFF33462C
argv at                                                : 0x7F7FFF334620
func2 (from main): frame at                            : 0x7F7FFF33460C
static int n within func at                            : 0x      601A3C
func (called     1 times): frame at                    : 0x7F7FFF3345D4
func2 (recursive): frame at                            : 0x7F7FFF3345AC
static int n within func at                            : 0x      601A3C
func (called     2 times): frame at                    : 0x7F7FFF334574
func2 (recursive): frame at                            : 0x7F7FFF33454C
static int n within func at                            : 0x      601A3C
func (called     3 times): frame at                    : 0x7F7FFF334514
func2 (recursive): frame at                            : 0x7F7FFF3344EC
static int n within func at                            : 0x      601A3C
func (called     4 times): frame at                    : 0x7F7FFF3344B4
func2 (recursive): frame at                            : 0x7F7FFF33448C
static int n within func at                            : 0x      601A3C
func (called     5 times): frame at                    : 0x7F7FFF334454
func2 (recursive): frame at                            : 0x7F7FFF33442C

      ...

func (called 43633 times): frame at                    : 0x7F7FFEF35BD4
func2 (recursive): frame at                            : 0x7F7FFEF35BAC
static int n within func at                            : 0x      601A3C
func (called 43634 times): frame at                    : 0x7F7FFEF35B74
func2 (recursive): frame at                            : 0x7F7FFEF35B4C
static int n within func at                            : 0x      601A3C
func (called 43635 times): frame at                    : 0x7F7FFEF35B14
func2 (recursive): frame at                            : 0x7F7FFEF35AEC
[1]   Segmentation fault (core dumped) ./a.out
apue$
```



```
Terminal — 80×44
apue$ ./a.out
High address (args and env):
----------------------------
environ[0] at                                          : 0x7F7FFF3346A8
last arg at                                            : 0x7F7FFF3346A0
first arg at                                           : 0x7F7FFF334698

Stack:
------
First variable inside main at                          : 0x7F7FFF334644
func_array[] ends at                                   : 0x7F7FFF334640
func_array[] (like 'array[]', but on stack) begins at  : 0x7F7FFF334630
argc at                                                : 0x7F7FFF33462C
argv at                                                : 0x7F7FFF334620
func2 (from main): frame at                            : 0x7F7FFF33460C
static int n within func at                            : 0x      601A3C
func (called     1 times): frame at                    : 0x7F7FFF3345D4
func2 (recursive): frame at                            : 0x7F7FFF3345AC
static int n within func at                            : 0x      601A3C
func (called     2 times): frame at                    : 0x7F7FFF334574
func2 (recursive): frame at                            : 0x7F7FFF33454C
static int n within func at                            : 0x      601A3C
func (called     3 times): frame at                    : 0x7F7FFF334514
func2 (recursive): frame at                            : 0x7F7FFF3344EC
static int n within func at                            : 0x      601A3C
func (called     4 times): frame at                    : 0x7F7FFF3344B4
func2 (recursive): frame at                            : 0x7F7FFF33448C
static int n within func at                            : 0x      601A3C
func (called     5 times): frame at                    : 0x7F7FFF334454
func2 (recursive): frame at                            : 0x7F7FFF33442C

      ...

func (called 43633 times): frame at                    : 0x7F7FFEF35BD4
func2 (recursive): frame at                            : 0x7F7FFEF35BAC
static int n within func at                            : 0x      601A3C
func (called 43634 times): frame at                    : 0x7F7FFEF35B74
func2 (recursive): frame at                            : 0x7F7FFEF35B4C
static int n within func at                            : 0x      601A3C
func (called 43635 times): frame at                    : 0x7F7FFEF35B14
func2 (recursive): frame at                            : 0x7F7FFEF35AEC
[1]    Segmentation fault (core dumped) ./a.out
apue$
```



Memory Layout of a Process

See also:

- `/proc/self/map`
- `pmap(1)` / `pmap(9)`

- "Smashing The Stack For Fun And Profit":
  https://insecure.org/stf/smashstack.html
- "`stdarg` And The Case Of The Forgotten Registers":
  https://www.netmeister.org/blog/stdarg.html