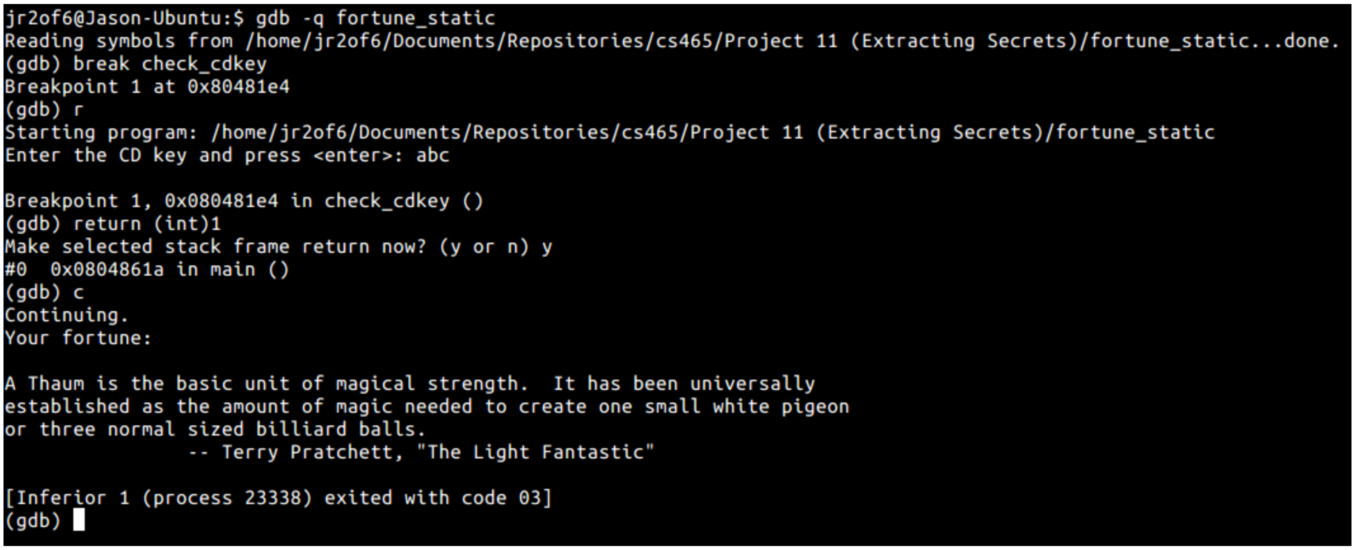
Jason Rasmussen
December 5, 2013

Project 11 (Extracting Secrets)

How did you use the debugger to bypass the password mechanism? What variables were modified? Please include a screenshot of the debugger in the report.

In order to bypass the password mechanism I put a breakpoint in the ‘check_cdkey’ method, and then forced it to ‘return (int)1’. This (I believe) caused the method to return true. Thus, modifying the return value of the function, I could type any cdkey and it would yield a fortune. Below is a screenshot that shows this.

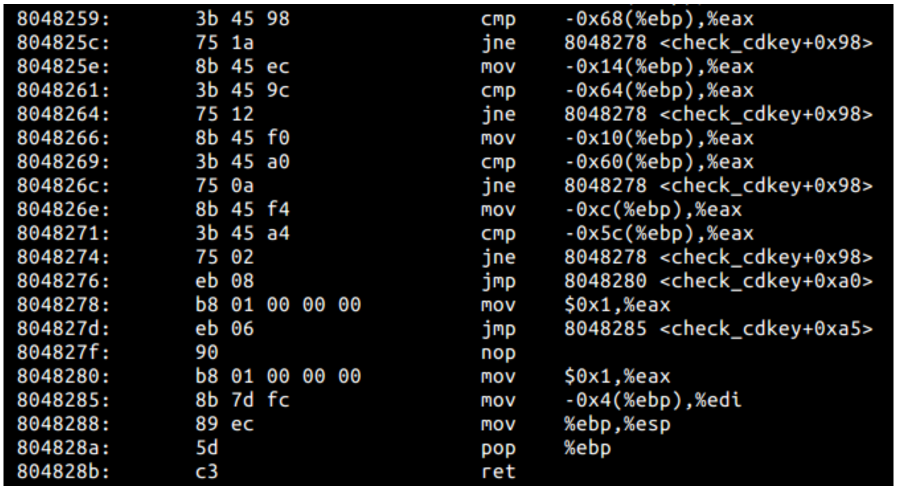


```
jr2of6@Jason-Ubuntu:$ gdb -q fortune_static
Reading symbols from /home/jr2of6/Documents/Repositories/cs465/Project 11 (Extracting Secrets)/fortune_static...done.
(gdb) break check_cdkey
Breakpoint 1 at 0x80481e4
(gdb) r
Starting program: /home/jr2of6/Documents/Repositories/cs465/Project 11 (Extracting Secrets)/fortune_static
Enter the CD key and press <enter>: abc

Breakpoint 1, 0x080481e4 in check_cdkey ()
(gdb) return (int)1
Make selected stack frame return now? (y or n) y
#0  0x0804861a in main ()
(gdb) c
Continuing.
Your fortune:

A Thaum is the basic unit of magical strength.  It has been universally
established as the amount of magic needed to create one small white pigeon
or three normal sized billiard balls.
                -- Terry Pratchett, "The Light Fantastic"

[Inferior 1 (process 23338) exited with code 03]
(gdb) 
```

How did you edit the program to bypass the cdkey mechanism?

I modified the program to bypass the cdkey by having it return 1 regardless of whether or not the cdkey passed the tests or not.

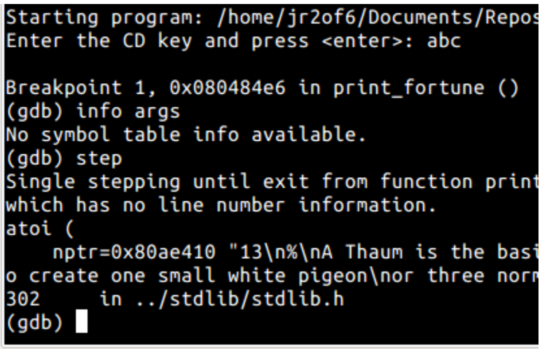
The addresses 0x80482559-0x8048274 perform checks and either copy a 0 or a 1 into %eax, before returning. I simply changed 0x8048278 to copy a 1 (like address 0x8048278) instead of one copying a 0. By doing so I was able to run my program and get a fortune regardless of the cd key I entered.



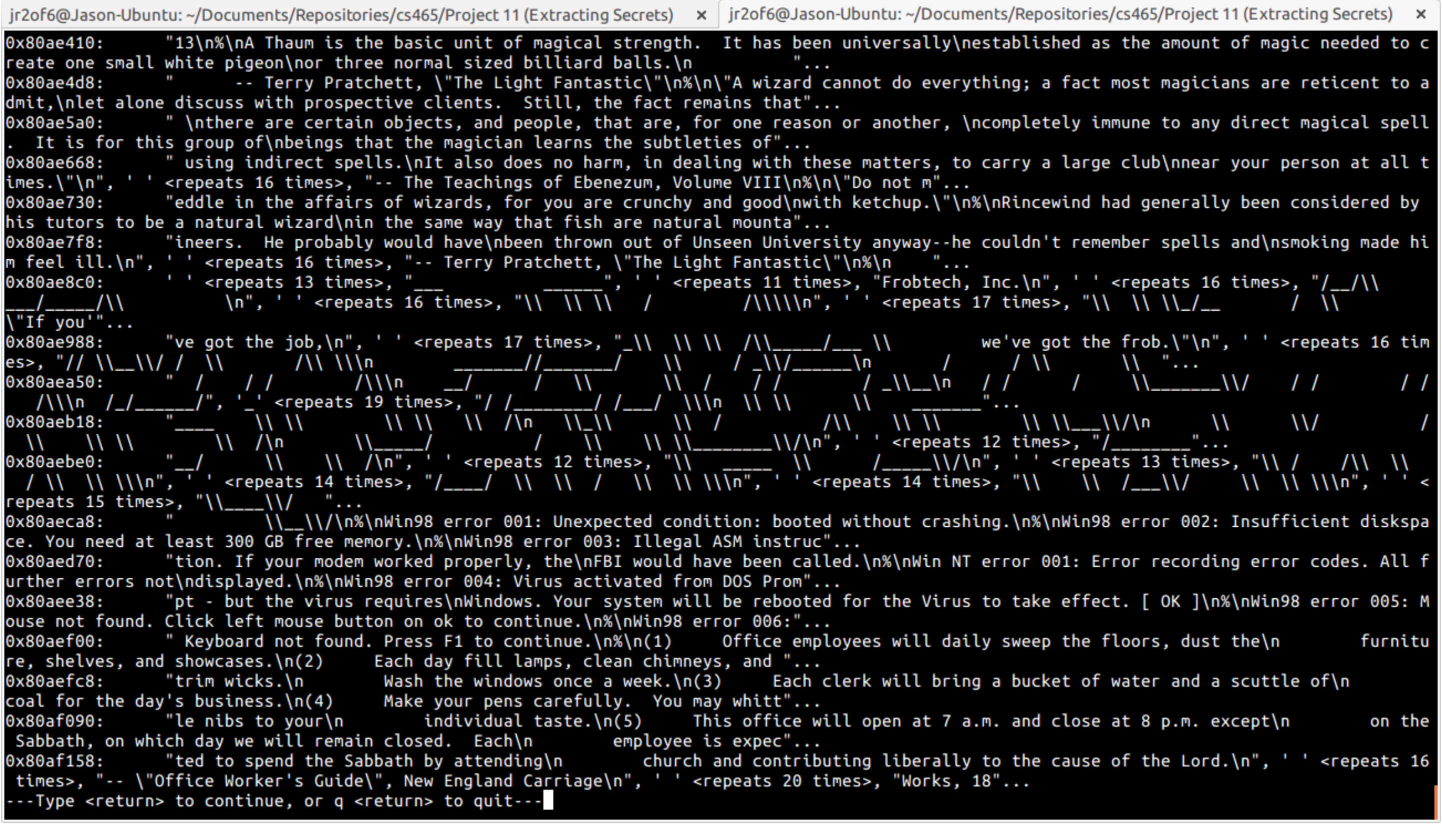
```
8048259:       3b 45 98                cmp    -0x68(%ebp),%eax
804825c:       75 1a                   jne    8048278 <check_cdkey+0x98>
804825e:       8b 45 ec                mov    -0x14(%ebp),%eax
8048261:       3b 45 9c                cmp    -0x64(%ebp),%eax
8048264:       75 12                   jne    8048278 <check_cdkey+0x98>
8048266:       8b 45 f0                mov    -0x10(%ebp),%eax
8048269:       3b 45 a0                cmp    -0x60(%ebp),%eax
804826c:       75 0a                   jne    8048278 <check_cdkey+0x98>
804826e:       8b 45 f4                mov    -0xc(%ebp),%eax
8048271:       3b 45 a4                cmp    -0x5c(%ebp),%eax
8048274:       75 02                   jne    8048278 <check_cdkey+0x98>
8048276:       eb 08                   jmp    8048280 <check_cdkey+0xa0>
8048278:       b8 01 00 00 00          mov    $0x1,%eax
804827d:       eb 06                   jmp    8048285 <check_cdkey+0xa5>
804827f:       90                      nop
8048280:       b8 01 00 00 00          mov    $0x1,%eax
8048285:       8b 7d fc                mov    -0x4(%ebp),%edi
8048288:       89 ec                   mov    %ebp,%esp
804828a:       5d                      pop    %ebp
804828b:       c3                      ret
```

How did you obtain all the fortunes from the encrypted file?

I was able to obtain all the fortunes by putting a breakpoint in print_fotrunes and then printing out information about the variables in the function. I was able to find a pointer to the location in memory with the fortunes. ('nptr=0x80ae410'). Using this address and the string print method in gdb I was able to view all the fortunes in memory.



```
Starting program: /home/jr2of6/Documents/Repos
Enter the CD key and press <enter>: abc

Breakpoint 1, 0x080484e6 in print_fortune ()
(gdb) info args
No symbol table info available.
(gdb) step
Single stepping until exit from function print
which has no line number information.
atoi (
    nptr=0x80ae410 "13\n%\nA Thaum is the basi
o create one small white pigeon\nor three norm
302     in ../stdlib/stdlib.h
(gdb) 
```


jr2of6@Jason-Ubuntu: ~/Documents/Repositories/cs465/Project 11 (Extracting Secrets) ×
jr2of6@Jason-Ubuntu: ~/Documents/Repositories/cs465/Project 11 (Extracting Secrets) ×

```
0x80ae410:      "13\n%\nA Thaum is the basic unit of magical strength.  It has been universally\nestablished as the amount of magic needed to c
reate one small white pigeon\nor three normal sized billiard balls.\n         "...
0x80ae4d8:      "       -- Terry Pratchett, \"The Light Fantastic\"\n%\n\"A wizard cannot do everything; a fact most magicians are reticent to a
dmit,\nlet alone discuss with prospective clients.  Still, the fact remains that"...
0x80ae5a0:      " \nthere are certain objects, and people, that are, for one reason or another, \ncompletely immune to any direct magical spell
.  It is for this group of\nbeings that the magician learns the subtleties of"...
0x80ae668:      " using indirect spells.\nIt also does no harm, in dealing with these matters, to carry a large club\nnear your person at all t
imes.\"\n", ' ' <repeats 16 times>, "-- The Teachings of Ebenezum, Volume VIII\n%\n\"Do not m"...
0x80ae730:      "eddle in the affairs of wizards, for you are crunchy and good\nwith ketchup.\"\n%\nRincewind had generally been considered by
his tutors to be a natural wizard\nin the same way that fish are natural mounta"...
0x80ae7f8:      "ineers.  He probably would have\nbeen thrown out of Unseen University anyway--he couldn't remember spells and\nsmoking made hi
m feel ill.\n", ' ' <repeats 16 times>, "-- Terry Pratchett, \"The Light Fantastic\"\n%\n    "...
0x80ae8c0:      ' ' <repeats 13 times>, "___         ______", ' ' <repeats 11 times>, "Frobtech, Inc.\n", ' ' <repeats 16 times>, "/__/\\
___/_____/\\          \n", ' ' <repeats 16 times>, "\\  \\ \\   /         /\\\\\n", ' ' <repeats 17 times>, "\\  \\ \\_/__       /  \\
\"If you'"...
0x80ae988:      "ve got the job,\n", ' ' <repeats 17 times>, "_\\  \\ \\  /\\_____/___ \\         we've got the frob.\"\n", ' ' <repeats 16 tim
es>, "// \\__\\/ /  \\       /\\ \\\n       _______//_______/    \\     / _\\/______\n       /      / \\       \\  "...
0x80aea50:      "  /    / /        /\\\n    __/      /   \\       \\  /    / /       / _\\__\n   / /      /     \\_______\\/    / /        / /
   /\\\n  /_/______/", '_' <repeats 19 times>, "/ /________/ /___/  \\\n  \\ \\      \\     _______"...
0x80aeb18:      "____    \\ \\       \\ \\   \\  /\n   \\_\\      \\  /        /\\     \\ \\        \\ \\___\\/\n      \\      \\/          /
  \\    \\ \\       \\  /\n      \\_____/          /    \\    \\ \\________\\/\n", ' ' <repeats 12 times>, "/________"...
0x80aebe0:      "__/       \\    \\  /\n", ' ' <repeats 12 times>, "\\   _____  \\      /_____\\/\n", ' ' <repeats 13 times>, "\\ /    /\\  \\
  / \\  \\ \\\n", ' ' <repeats 14 times>, "/____/  \\  \\  /   \\  \\ \\\n", ' ' <repeats 14 times>, "\\    \\  /___\\/     \\  \\ \\\n", ' ' <
repeats 15 times>, "\\____\\/   "...
0x80aeca8:      "        \\__\\/\n%\nWin98 error 001: Unexpected condition: booted without crashing.\n%\nWin98 error 002: Insufficient diskspa
ce. You need at least 300 GB free memory.\n%\nWin98 error 003: Illegal ASM instruc"...
0x80aed70:      "tion. If your modem worked properly, the\nFBI would have been called.\n%\nWin NT error 001: Error recording error codes. All f
urther errors not\ndisplayed.\n%\nWin98 error 004: Virus activated from DOS Prom"...
0x80aee38:      "pt - but the virus requires\nWindows. Your system will be rebooted for the Virus to take effect. [ OK ]\n%\nWin98 error 005: M
ouse not found. Click left mouse button on ok to continue.\n%\nWin98 error 006:"...
0x80aef00:      " Keyboard not found. Press F1 to continue.\n%\n(1)     Office employees will daily sweep the floors, dust the\n        furnitu
re, shelves, and showcases.\n(2)     Each day fill lamps, clean chimneys, and "...
0x80aefc8:      "trim wicks.\n        Wash the windows once a week.\n(3)     Each clerk will bring a bucket of water and a scuttle of\n
coal for the day's business.\n(4)     Make your pens carefully.  You may whitt"...
0x80af090:      "le nibs to your\n        individual taste.\n(5)     This office will open at 7 a.m. and close at 8 p.m. except\n        on the
 Sabbath, on which day we will remain closed.  Each\n        employee is expec"...
0x80af158:      "ted to spend the Sabbath by attending\n        church and contributing liberally to the cause of the Lord.\n", ' ' <repeats 16
 times>, "-- \"Office Worker's Guide\", New England Carriage\n", ' ' <repeats 20 times>, "Works, 18"...
---Type <return> to continue, or q <return> to quit---
```

Below are a list of all 13 fortunes that I found.

```
Win NT error 001: Error recording error codes. All further errors not
displayed.

Win98 error 001: Unexpected condition: booted without crashing.

Win98 error 002: Insufficient diskspace. You need at least 300 GB free
memory.

Win98 error 003: Illegal ASM instruction. If your modem worked properly,
the FBI would have been called.
```

Win98 error 004: Virus activated from DOS Prompt - but the virus requires

Windows. Your system will be rebooted for the Virus to take effect. [OK]

Win98 error 005: Mouse not found. Click left mouse button on ok to continue.

Win98 error 006: Keyboard not found. Press F1 to continue.

Rincewind had generally been considered by his tutors to be a natural wizard in the same way that fish are natural mountaineers. He probably would have been thrown out of Unseen University anyway--he couldn't remember spells and smoking made him feel ill.
-- Terry Pratchett, "The Light Fantastic"

A Thaum is the basic unit of magical strength. It has been universally established as the amount of magic needed to create one small white pigeon or three normal sized billiard balls.
-- Terry Pratchett, "The Light Fantastic"

"Do not meddle in the affairs of wizards, for you are crunchy and good with ketchup."

"A wizard cannot do everything; a fact most magicians are reticent to admit, let alone discuss with prospective clients. Still, the fact remains that there are certain objects, and people, that are, for one reason or another, completely immune to any direct magical spell. It is for this group of beings that the magician learns the subtleties of using indirect spells.
It also does no harm, in dealing with these matters, to carry a large club near your person at all times."
-- The Teachings of Ebenezum, Volume VIII

(1) Office employees will daily sweep the floors, dust the furniture, shelves, and showcases.

(2) Each day fill lamps, clean chimneys, and trim wicks. Wash the windows once a week.

(3) Each clerk will bring a bucket of water and a scuttle of coal for the day's business.

(4) Make your pens carefully. You may whittle nibs to your individual taste.

(5) This office will open at 7 a.m. and close at 8 p.m. except on the Sabbath, on which day we will remain closed. Each employee is expected to spend the Sabbath by attending church and contributing liberally to the cause of the Lord.

-- "Office Worker's Guide", New England Carriage Works, 1872

```
                 ___          ______           Frobtech, Inc.
                /__/\     ___/_____/\
                \  \ \   /         /\\
                 \  \ \_/__       /  \         "If you've got the job,
                 _\  \ \  /\_____/___ \         we've got the frob."
                // \__\/ /  \       /\ \
        _______//_______/    \     / _\/______
       /      / \       \    /    / /        /\
    __/      /   \       \  /    / /        / _\__
   / /      /     \_______\/    / /        / /   /\
  /_/______/___________________/ /________/ /___/  \
  \ \      \    ___________    \ \        \ \   \  /
   \_\      \  /          /\    \ \        \ \___\/
      \      \/          /  \    \ \        \  /
       \_____/          /    \    \ \________\/
            /__________/      \    \  /
            \   _____  \      /_____\/
             \ /    /\  \    / \  \ \
              /____/  \  \  /   \  \ \
              \    \  /___\/     \  \ \
               \____\/            \__\/
```